ISSN 2664-4150 (Print) & ISSN 2664-794X (Online)
South Asian Research Journal of Engineering and Technology
Abbreviated Key Title: South Asian Res J Eng Tech

| Volume-4 | Issue-6 | Nov-Dec- 2022 | **DOI: 10.36346/sarjet.2022.v04i06.001**

Review Article

A Review on Outliers in IoT

Y. Harshavardhan Reddy[1*], M. Hari Srinivas[1], Adnan Ali[1], A. Zaheer Sha[1]
[1]G. Pullaiah College of Engineering and Technology, Kurnool, India

***Corresponding Author:** Y. Harshavardhan Reddy
G. Pullaiah College of Engineering and Technology, Kurnool, India

Article History
Received: 16.09.2022
Accepted: 31.10.2022
Published: 10.11.2022

Abstract: In recent decades, the Internet of Things (IoT) has grown rapidly, attracting the attention of scientists and businesspeople. In extreme conditions, autonomously scattered sensor nodes pose a high risk of failure and intrusion into the IoT, skewing sensor values. Abnormal data, anomalies, or outliers are sensor values that depart from norms. When abnormalities are factored into data analytics, the ultimate judgment is affected. Using data-driven algorithms for IoT outlier detection is a cutting-edge tactic in Machine Learning (ML). However, evaluating the effectiveness of implemented ML techniques for outlier detection in IoT, which have the minimal processing power and power sources to ensure data quality, raises several difficulties that have just recently begun to be addressed in the academic literature. This paper analyses the cutting-edge architecture, type, degree, technique, and detection mode of AI and statistical outlier detection strategies in IoTs. Also, each of the ways to find outliers is talked about in detail, along with ways to make them better.

Keywords: Outlier, Internet of Things (IoT).

1. INTRODUCTION

IoT sensor nodes are spread throughout a "sensor field" [1]. Every IoT node has access to radio channels and processing modules [2]. IoT nodes acquire data and transfer it to a central sink node for processing [3]. Installing an IoT device in any field requires three features. First, an IoT sensor node collects environmental data. Second, it must store preparation techniques and data. All sensor nodes must also connect to sink nodes. Every IoT node has a sensor, a CPU, a transmitter, and a battery. First, the ADC converts analog signals to digital ones. Second, a microprocessor or microcontroller and a small memory unit provide the sensor node's intelligence. Third, a short-range transceiver handles network data transmission and reception. The power unit powers the other units.

Most IoT devices are utilized in severe settings where establishing a dependable network is challenging. IoTs began in the military but have now moved to environmental, architectural, catastrophe, farming, targeting, and manufacturing uses [4]. Recent trials aim to optimize IoT effectiveness and value in smart cities [5]. Smart decision making requires error-free sensor data [6]. Internal and external variables affect IoT data monitoring and collection. Internal factors include sensor node properties. These features include resource restrictions, memory needs, cost, battery life, communication capacity, and unreliable, noisy, incorrect, and missing data from sensor nodes. External considerations include a IoT's number of sensor nodes and susceptibility to denial-of-service, reply, and black-hole attacks [3]. Due to these and other internal and external causes, sensor node data in IoTs [7] is thought to be unreliable and aberrant. An outlier or anomaly is a sensor node measurement that doesn't fit previous values. Detecting anomalies in field-placed IoT sensor nodes gives relevant data [8]. Real-time health, environmental, fraud, intrusion, fire, pipe leaking, and target tracking applications rely on IoT outlier detection methods. Identifying outliers requires particular guidelines if the data's attributes are unknown. Predefined classifier-based machine learning techniques [9, 10] can discover outliers in datasets with regular and atypical data. Outliers that could cause a natural disaster should be watched closely [11].

Outlier detection helps us comprehend what's happening. Data must inspire new ideas. ML-based data-driven algorithms work well with pre-processed data, but real-time is difficult. DL [12] models using windowing approaches

have gained appeal as a way to mitigate ML's flaws [13]. Most data-driven algorithms [14] treat outliers as mistakes and don't pay attention to events, which can cause them to miss game-changing hidden information [4].

Fig. 1 depicts IoT outlier detection. Outlier detection in IoTs can be done using three broad methodologies. First, there's misuse/signature-based detection, which compares new attacks to previously created ones. The primary advantage of this technology is its ability to detect past attacks reliably and effectively with lower false promise rates. Nevertheless, it does not deal with conventional attacks such as DoS and reply attacks. Second, protocol state analysis checks known sensor node profiles for outliers. Both solutions need substantial processing and memory that IoTs don't have [15]. In modern academia, a data-driven strategy is highly respected. This research analyses statistical, AI, distance, cluster, and classification-based algorithms for finding IoT outliers. Using the best available metrics, all data-driven outlier identification strategies are compared.

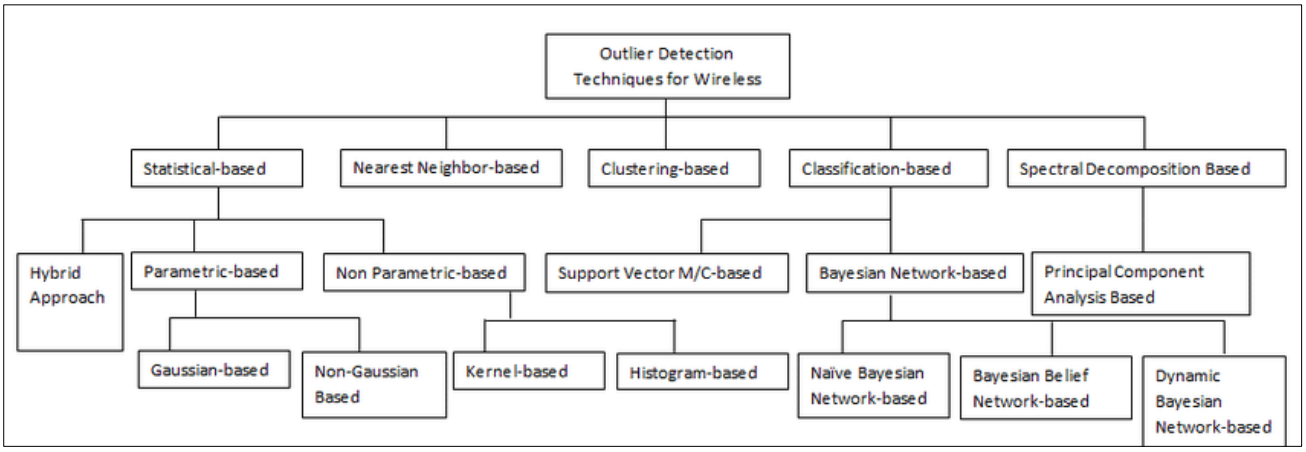

Fig. 1: Outlier Detection Techniques in IoT

2. CONTEXT AND PRECEDING MATTERS

2.1 Concept

IoTs have received interest in the industrial and scientific communities because of their potential to observe and access a specific location, giving researchers more information [3]. Outlier detection is crucial as data analytics advances. Outlier detection is a major research topic due to its importance in modern appliances [16]. All allude to this issue, in which outlier detection in IoT [17] becomes a divided effort against the rising scale of real-world sensed data. In the literature, an outlier has been defined as follows:

"A piece of evidence that doesn't seem to fit in with the rest of the facts"

According to the literature on outliers, "outliers" are sites that lie in the lower local density compared to the density of their local neighbourhood[18].

According to a 2001 paper by [19]"outliers" are "points that do not belong to clusters of the data set or that clusters that are much smaller than other clusters" [14].

A spatial-temporal outlier is a site whose nonspatial attribute values differ significantly from other geographically and temporally referenced locations.

Despite its features, a single data point cannot be termed an outlier [20]. In this scenario, system failures and natural disasters must be handled with care. We can't envision what an outlier looks like, but we can recognize deviations from the typical. An outlier is an interesting and unnecessary difference from the estimate. This strategy for discovering outliers is unique. We're looking for any odd connections to find out what's happening and where to focus. The anomaly detector should be updated as new samples are obtained.

2.2 Categories of Outliers

Outlier detection strategies are designed to find unusual data [21]. With this overview, we may identify outliers as global or local based on their position in relation to the remaining datasets. It's easy to discover and eliminate global outliers, which differ substantially from conventional outliers and encompass all available data points [22]. First-order internal outliers categorize a sensor node's full dataset as an outlier compared to its neighbors. Third-order or category 2 external outliers are a sensor subtree. When you look for this, you get high-order, external outliers. Local outliers indicate data items that are anomalous relative to their immediate neighbors, a phenomenon known as first-order outliers.

Category 1 data points, often known as absolute outliers, vary greatly from the regular distribution of high or low values. Category 2 outliers, also known as clustered absolute outliers, routinely yield extreme values. Category 3 outliers, also known as random outliers, are observations that arise unexpectedly and outside the initial data threshold [23]. Local outlier detection approaches decrease the stress on the network by eliminating the need to contact the sink node (base station). It is harder to find and get rid of local outliers than global ones.

2.3 Several Methods for Identifying Outliers

Sensor nodes are usually installed in difficult environments where conventional network development is unfeasible. Due to situational fluctuations and limited resources, sensor nodes are prone to outliers. Outlier detection in IoT [24] helps ensure data quality and trustworthiness. Figure 2 shows the abnormal data origins.

i. **Noise or Error:** Outliers can be caused by noise or error, which signals incorrect data from malfunctioning nodes [25]. Incorrect information encourages us to infer unreasonable deviations from the norm in other data. Environmental, roughness, and difficulty differences cause most background noise and deployment problems. IoT [26] s have communication, software, battery, hardware, topological, and base station failures [16]. Faulty sensors, processors, GPS receivers, power supplies, and memory caused hardware failures. Sensor software bugs cause software failures. Transceiver problems cause communication failures. Identifying malfunctioning sensor nodes in IoT [27] is difficult due to resource limitations, deployment shifts, environmental variables, and similarities between normal and problematic nodes. This means the cause of noise or error must be located and eliminated (or remedied, if possible) before affecting data quality [28]. Developing an outlier detection technique will be more accurate if researchers exclude this class of IoT outliers. When a sensor node has too many errors to rectify, researchers must tread carefully when determining which ones to eliminate [29].

ii. **Event:** Unanticipated deployment changes might also cause outliers [30]. Chemical leaks, wildfires, floods, volcanic eruptions, earthquakes, and extreme weather are all likely [31]. In the larger scheme of things, rare events influence the historical pattern of sensory input. The loss of high-importance hidden data about the upcoming event owing to event outliers.

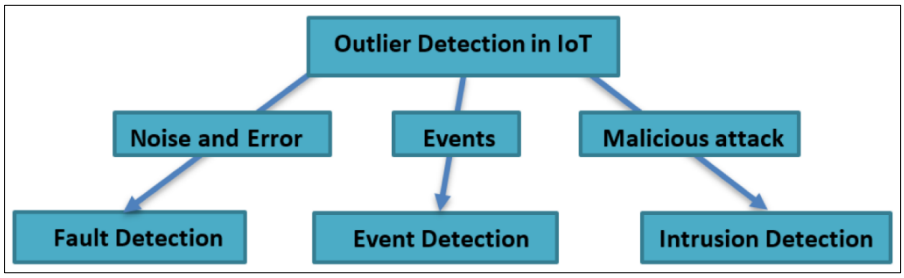

Fig. 2: Sources of outlier in IoT

iii. **Malicious Attack:** Malware affects message meaning malicious attacks create outliers by capturing control of sensor nodes and inserting bogus data to bring them down. Outliers can be passive or active. Passive attacks acquire information without actively affecting network traffic. Examples include spoofed, reply, sinkhole, and selective forward attacks. Active attacks, such as man-in-the-middle or DOS, steal information by interfering with system operation [32].

2.4 Outlier Aspects

Data collected by IoT [33] s can be viewed in a variety of ways, including as static data, stream data, and real-time data.

In almost all outlier identification systems, this is an essential component to have. When applied to real-time sensor data, the same approaches produce significantly different outcomes. Sensors in various appliances collect real-time data, making outlier detection difficult. Real-time connectivity to the sensor node is required for some IoT appliances [34], such as medical or security monitoring. Traditional IoT [35]s assess pressure, humidity, etc. [36]. IoTs are built to receive multivariate data, which is collected by individual sensor nodes. Outliers are statistical data points with unusual properties relative to similar datasets. A univariate outlier is a single data point that stands out due to an irregularity in one statistical metric [37]. Compare your age and height. Univariate outlier analyses disregard correlations between components, but multivariate ones do. Continuous and categorical variables are univariate. Means, medians, modes, variances, standard deviations, ranges, percentages, box plots, dot plots, line charts, and uniforms are univariate continuous variables. Figures, frequencies, odds, bar charts, and graphs are categorical univariate variables. Outliers across multiple variables have similar characteristics. A trademarked outlier has few characteristics with unusual norms relative to the rest of the sample [38]. Multivariate analysis includes multiple regression, logistic regression, ANOVA, life table, and factor analysis. IoTs can discover univariate outliers by comparing a single feature to the others.

Multivariate outlier detection is difficult and time-consuming since it requires collective properties. Linking numerous data parameters improves outlier detection accuracy.

2.5. Attribute Correlation

IoTs acquire vital information from the current world, where entities may have unclear or ambiguous links based on their attributes [39]. Attribute correlation measures their dependability. Due to time-varying sensor data, IoTs rely on attribute correlation. It enhances outlier detection over approaches that ignore such linkages. Real-time environmental monitoring uses sensor data to link place and time. Outlier detection methods use temporal and spatial correlations to evaluate if an observation is an actual event [40] or noise. Second, sensor evaluations of estimated nodes in the past and nearby. The findings of past study are essential to understanding a temporal relationship, which is defined by a measurement at a specific instant in time. A sensor node that is moving through a vast spatial range and collecting data at a specific time instant assesses the node-to-node spatial correlation. When sensor observations are combined with information about time, it is easy to tell the difference between error and an outlier.

2.5 Architectural Framework of Outlier Detection Techniques

Depending on the use case, the Internet of Things [8, 41] can consist of anywhere from dozens to hundreds of sensors. IoT outlier identification involves centralized, distributed [42], or local architectures. Data was sent from a sensor node to a base station or cluster head, which was then used to perform an outlier exposure. In a distributed design, the sensor node coordinates with nearby nodes to construct a global reference model. It alerts the cluster leader or neighbouring nodes if it finds questionable behavior. Each sensor node in a local structure identifies anomalies separately, without sharing data. Sensor nodes waste more power on communication than computation, according to studies. A centralized system uses more energy because sensor data must be sent to a central point for analysis. Decentralized outlier detection saves power. Local data is compiled and supplied to the CH to construct a global reference model. This cuts expenses and boosts efficiency.

3. Performance Strategies for Outlier Detection

For IoTs, the fundamental criterion for evaluating outlier detection strategies is whether the method reliably recovers actionable observations with minimum resource usage [43]. Most outlier identification strategies use cross validation to approximate prediction errors. Its major measurements (RMSE) are mean prediction error (MPE) and root mean square error (RMSE). The concept of an outlier is context-specific, not number-specific. Similarly, numerous quantitative measurements can be generated by experimenting with different input settings and datasets to test outlier identification performance. Various researchers employ the aforementioned method in their own domains. Existing strategies may outperform similar procedures due to changing factors and experimental setups.

The following metrics are introduced as a series of unique conditions for refining outlier and event identification algorithms:

i. **Detection Rate:** Outlier detection accuracy is measured by the detection rate (DR). The average detection rate is really close to 1. It's possible for an algorithm to be good at seeing both events and outliers, and given the correct conditions, the detection rate can reflect these two rates in a way that's distinct from one another. Obviously, IoT used in potentially harmful settings need to be maintained during everyday operations. Therefore, it is preferable for the method to keep high rates of event and outlier detection. The inability to distinguish between different sources of outliers, as seen by high outlier and subsequent poor event identification rates, suggests the approach is not robust.

ii. **False Positive Rate:** A false positive rate (FPR) is the fraction of normal data identified as an outlier. The FPR should be the opposite of the DR and be close to zero. Outlier and event detection must have a high detection rate without incorrectly identifying typical data as an outlier or event. False positives are divided into "event false positive" and "outlier false positive" types.

iii. **Receiver Operating Specifications:** Receiver operating characteristics will reveal the relationship between detection efficiency and false-positive occurrences (ROC). The ROC curve's coverage area should ideally be close to 1. Plots of ROC curves illustrate how the detection accuracy varies in relation to the false positive rate.

iv. **Metric for Event Attribution:** When analysing data from a single class for event-related issues, it is necessary to take into account both the detection rate and the false-positive rate. When dealing with multi-class data, precise measurements are needed to identify the most relevant inter-class miss classifications for event detection. Identifying an anomaly or incident in real-time IoT depends on its nature and relevant criteria. In multi-class data, set DR to 100% and FPR as low as possible for exact event detection.

v. **Computational Complexity:** IoT sensors gather data 24/7. This data set is so large that identifying outliers is difficult. Outlier identification methods are measured by their duration and spatial complexity. Due to limited memory on sensor nodes, it was possible to figure out how much space was needed to record outlier exposure options.

vi. **User Specific Parameter:** Dynamic changes in the environment where sensor nodes are deployed make it challenging to specify user-specific parameters in IoT circumstances. It also affects how well and efficiently outlier detection systems work. There is a positive/negative association between the detection rate of outlier detection algorithms and the number of user-specific parameters in the algorithm. Several studies support this notion.

4. Limitations with IoT Outlier Detection

The complexity of outlier identification design is augmented by sensor data and the sensor network environment. Many outlier detection algorithms are proposed for earlier systems, but IoT resource limits make them inappropriate. Existing methods minimize energy use while maximizing detection and lowering false positives. Developing outlier identification algorithms for IoT has its challenges.

i. **Communication Cost:** The cost of transmitting data from a sensor node is several times higher than the cost of calculating the same quantity of data. Historically, most outlier identification systems send all sensor data to a central location for preprocessing. Some have a good detection rate, but transmission costs rise. Distributed outlier detection is well-suited to sensor nodes with restricted resources due to minimal communication. Long delays in propagation, signal attenuation, long pathways, rapidly changing time-varying channels, noise, and diffusion limit communication. High transmission costs hinder outlier detection approaches in IoT. Reduce IoT communication costs to boost the system's lifespan and reduce network traffic.

ii. **Dynamic Network Topology:** It is common for sensor networks to fail due to the fact that they are deployed in unknowable surroundings for a finite amount of time. In order to carry out their duties, certain sensor nodes may move, and each of these nodes may have a unique set of processing and sensing capabilities. Communication breakdowns and node movement change the network's topology[44]. Pre-deployed networks may gain or lose cutting-edge nodes based on appliance needs. Individual node failures can also modify the network's topology. These shifts affect the outlier detection standard reference model. IoT uses several sensor nodes (infrared and thermal) to complete jobs (such as measuring temperature, pressure, etc.). Variation increases outlier identification algorithm complexity.

iii. **Resource Constraints:** Sensor nodes are low-resource microelectronic devices. low power, weak broadcasting capability, minimal storage, and limited processing [45]. Most IoT outlier detection approaches require a lot of data storage, analytical memory, computational complexity, and radio transmission capacity. When constructing sensor networks, low-quality sensors are sometimes utilized for cost-savings. Outlier detection techniques for IoT must manage memory for storage and processing in a way that uses as little energy as possible.

iv. **Distributed Streaming Data:** Alterations to data streams are another difficulty posed by the IoT. The implementation of the gold-standard benchmark outlier method in a decentralized paradigm requires the use of streaming data.. However, it is possible that this information is not a priori. Disseminated data is only available for a short time, which is improper moving forward because dynamic streaming may render distribution obsolete. Most outlier identification approaches presume offline data meets requirements for processing dispersed stream data [46]; this may not be true for online streaming sensor data [47]. Therefore, researchers need to figure out how to analyze data from remote internet streams and implement outlier identification in IoT.

v. **High Dimensional Data:** In a IoT, each data point may have several attributes. Network expansion can add dimension to integrated data. These dimensions lower the computational load of outlier identification approaches but raise sensor node resource needs. Growing data dimensionality hurts outlier identification efficiency.

5. Important Research Objectives in IoT outlier

a. Both clustering and classification identify outliers using Euclidean or Mahala Nobis distance. High-dimensional and mixed-type structures do poorly with either metric. In this case, it is also a good idea to make a ranked list of outliers and a list of major deviations.

b. Choosing a distance for distance-based outlier detection techniques for real-time devices is tricky. In distance-based systems, it's hard to determine the optimal number of neighbors. A modified Mahala Nobis distance metric could help find close neighbors.

c. Due to the large amount of data, outlier detection in streaming data is tough. IoT lack memory for storing sensor data streams. To solve these issues, a new low-memory online approach is needed.

d. Anomalies in categorical sensor data can be easily discovered using ranking-based algorithms; employing cluster confident determinations increases anomaly identification results.

e. In spite of the fact that subspace-based outlier identification approaches promise excellent performance and generalizability, there are still a great number of challenges involved in selecting the most appropriate subspaces and classifiers. The use of soft computing, game theories, and adaptive learning methods are some of the potential solutions to these problems.

f. While clustering systems are good at finding outliers, they need to be improved so they can offer appropriate grading schemes like degree of divergence and originality score.

g. Using Rough-sets to Find Outliers Outlier scores are improved via rough-sets-based grouping. Even so, we can improve our rough-set settings.
h. Network anomalies are the focus of graph-based outlier identification algorithms. New subgraphs and random walks need more focus. Graph invariants in IoT drive temporal outlier detection. Using attributes to create networks helps understand their dynamic actions.
i. It is challenging to train with high-dimensional datasets when using learning approaches that are based on AI since these techniques require the learning rate, mini-batch size, momentum, and weight regularization cost to be initialized properly for optimal convergence.
j. The computational and memory limitations of classification, AI, and clustering-based approaches are often neglected. Using streaming data to find outliers and events in real time without having to solve optimization problems at each time point needs more paper.
k. Persistence Theory The theory and concept of consistency are key to building a network that can detect anomalies. Researchers require fresh approaches if they seek a workable solution.
l. If an unidentified attack is spotted via outlier detection, the profile database must be rearranged. Dynamic profile changes impair system performance and compete with other tasks.
m. Standard datasets: There are only a small number of standard datasets that contain sufficient details about assaults, incidents, and noise. There is still a problem with the fact that there aren't enough public datasets that are all the same and can be used to figure out how equivalent networks are set up.
n. Due to the fact that the data are noisy, extra vigilance is required while generating a dataset profile. This is because routine changes could lead to problems if they are incorrectly recognized as outliers. The vast majority of public and private databases contain errors and are vulnerable to modification. There are many different techniques to process data, some of which include filters, wrappers, and autoencoders. Each of these processes helps get rid of unnecessary or distracting aspects of the data that has been acquired.
o. Outlier detectors now require manually configured thresholds to identify promising outliers. When this statistic exceeds a predetermined threshold, an alert will sound after a predetermined time. Better methodologies are needed to establish the optimal system alert threshold. The correct threshold setting may increase the number of outliers. If everyday noise is mistaken for unusual things, the system needs to be returned to cut down on false positives.
p. A large number of false positives will result from using a low threshold value, which wastes time and money. Furthermore, it diverts attention, slows down progress, and may have catastrophic effects on individuals who need to react. So, we need to choose a threshold that controls the true alarms well within a certain amount of time.
q. In the context of high-dimensional sensor data, the unsupervised feature selection method that is based on correlation measurements is an approach that works exceptionally well for identifying outliers. Changes to the feature weight, ensemble filter, and wrapper approaches are three areas where researchers might concentrate their efforts in order to create an effective method for locating outliers.
r. Resilience: Outliers and anomalies are always changing, either as a result of established detection methods being sidestepped or as a result of fresh data instances becoming familiar enough to established detection techniques to trick them. Therefore, the approaches that have been proposed for discovering outliers in the not too distant future will need to be updated frequently in order to stay up with these beneficial improvements.
s. Unlabelled data outlier detection is ambiguous due to the link to common cluster data. Rough set clustering approaches that use soft computation can handle improbable or unlabelled data.
t. Parametric methods based on statistics have trouble choosing the best model for data distribution; distance-based methods were developed as a solution. However, if there are more local densities, these methods will not produce optimal outcomes. Here, scientists might zero in on modified forms of LoF with a specific focus.
u. Problems with event detection arise because it is not obvious how to take advantage of existing outlier detection methods to spot irregularities in an event feed. In light of the fact that events have symbolic rather than numerical significance, If you, I, or anybody else thinks that measuring the number of events that happen in successive fixed-length time intervals is an easy way to discover outliers in event streams, then use that metric to inform your selection of an appropriate outlier model for event detection.
v. The model's reliance on the outlier score makes it difficult to detect even subtle shifts in system performance. And because it's impractical to look for anomalies unless the event rate is high, waiting for enormous score counts makes it difficult to spot them. In some systems, the frequency of events is so high that we can see both high numbers and brief intervals. It makes sense to use counts as estimates in modelling since they can be easily processed with a wide variety of ML techniques.

6. CONCLUSION

Outlier detection is significant in many academic domains. This research focuses on IoT outlier detection. Most IoT studies focus on increasing bandwidth, reducing computing complexity, and reducing energy use. This paper evaluates IoT outlier identification systems by their methodological frameworks. In addition, we evaluated various AI-

based data-driven methodologies by contrasting them on the basis of sensor information, architectural, method, data correlation, detection accuracy, false-positive rate, and accuracy. Outliers can vary in kind, dimension, and size, so researchers must consider the testing dataset when picking outlier identification approach. We've covered the most important IoT outlier identification needs. We also identified unsolved research questions for the future.

REFERENCES

1. Reddy, Y. H., Ali, A., Kumar, P. V., Srinivas, M. H., Netra, K., Achari, V. J., & Varaprasad, R. (2022). A Comprehensive Survey of Internet of Things Applications, Threats, and Security Issues. *South Asian Res J Eng Tech*, *4*(4), 63-77.
2. Amer, M., Goldstein, M., & Abdennadher, S. (2013, August). Enhancing one-class support vector machines for unsupervised anomaly detection. In *Proceedings of the ACM SIGKDD workshop on outlier detection and description* (pp. 8-15).
3. Chander, B. (2018). Kumaravelan, One class SVMs outlier detection for wireless sensor networks in harsh environments: Analysis. *International Journal of Recent Technology and Engineering*, *7*(4), 294-301.
4. Kurniabudi, K., Purnama, B., Sharipuddin, S., Darmawijoyo, D., Stiawan, D., Samsuryadi, S., ... & Budiarto, R. (2019). Network anomaly detection research: a survey. *Indonesian Journal of Electrical Engineering and Informatics (IJEEI)*, *7*(1), 37-50.
5. Srinivas, T. A. S., Babu, B. R., Tsige, M. S., Rajagopal, R., Devi, S., & Chowdhury, S. (2022, July). Effective implementation of the Prototype of a digital stethoscope using a Smartphone. In *2022 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES)* (pp. 1-8). IEEE.
6. Perrig, A., Stankovic, J., & Wagner, D. (2004). Security in wireless sensor networks. *Communications of the ACM*, *47*(6), 53-57.
7. Sankar, S., Somula, R., Kumar, R. L., Srinivasan, P., & Jayanthi, M. A. (2021). Trust-aware routing framework for internet of things. *International Journal of Knowledge and Systems Science (IJKSS)*, *12*(1), 48-59.
8. Srinivas, T. A. S., & Manivannan, S. S. (2020). Prevention of hello flood attack in IoT using combination of deep learning with improved rider optimization algorithm. *Computer Communications*, *163*, 162-175.
9. Sarabu, A., & Santra, A. K. (2020). Distinct two-stream convolutional networks for human action recognition in videos using segment-based temporal modeling. *Data*, *5*(4), 104.
10. Sarabu, A., & Santra, A. K. (2021). Human action recognition in videos using convolution long short-term memory network with spatio-temporal networks. *Emerging Science Journal*, *5*(1), 25-33.
11. Ni, Y. Q., Xia, Y., Liao, W. Y., & Ko, J. M. (2009). Technology innovation in developing the structural health monitoring system for Guangzhou New TV Tower. *Structural Control and Health Monitoring: The Official Journal of the International Association for Structural Control and Monitoring and of the European Association for the Control of Structures*, *16*(1), 73-98.
12. Srinivas, T., Aditya Sai, G., & Mahalaxmi, R. (2022). A Comprehensive Survey of Techniques, Applications, and Challenges in Deep Learning: A Revolution in Machine Learning. *International Journal of Mechanical Engineering*, *7*(5), 286-296.
13. Đurišić, M. P., Tafa, Z., Dimić, G., & Milutinović, V. (2012, June). A survey of military applications of wireless sensor networks. In *2012 Mediterranean conference on embedded computing (MECO)* (pp. 196-199). IEEE.
14. Cheng, T., & Li, Z. (2006). A multiscale approach for spatio-temporal outlier detection. *Transactions in GIS*, *10*(2), 253-263.
15. Sankar, S., Ramasubbareddy, S., Luhach, A. K., & Chatterjee, P. (2022). NCCLA: new caledonian crow learning algorithm based cluster head selection for Internet of Things in smart cities. *Journal of Ambient Intelligence and Humanized Computing*, 1-11.
16. Chirayil, A., Maharjan, R., & Wu, C. S. (2019, July). Survey on anomaly detection in wireless sensor networks (WSNs). In *2019 20th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)* (pp. 150-157). IEEE.
17. Shukla, A. K., Pippal, S., Singh, D., & Reddy, S. R. (2021). An evolutionary-based technique to characterise an anomaly in internet of things networks. *International Journal of Internet Technology and Secured Transactions*, *11*(5-6), 452-469.
18. Breunig, M. M., Kriegel, H. P., Ng, R. T., & Sander, J. (2000, May). LOF: identifying density-based local outliers. In *Proceedings of the 2000 ACM SIGMOD international conference on Management of data* (pp. 93-104).
19. Jiang, M., Luo, J., Jiang, D., Xiong, J., Song, H., & Shen, J. (2016). A cuckoo search-support vector machine model for predicting dynamic measurement errors of sensors. *IEEE Access*, *4*, 5030-5037.
20. Aggarwal, C. C., & Yu, P. S. (2005). An effective and efficient algorithm for high-dimensional outlier detection. *The VLDB journal*, *14*(2), 211-221.
21. Gupta, S. K., & Sinha, P. (2014). Overview of wireless sensor network: a survey. *Telos*, *3*(15µW), 38mW.
22. Hodge, V., & Austin, J. (2004). A survey of outlier detection methodologies. *Artificial intelligence review*, *22*(2), 85-126.
23. Hawkins, D. M. (1980). *Identification of outliers* (Vol. 11). London: Chapman and Hall.

24. Sankar, S., Ramasubbareddy, S., Chen, F., & Gandomi, A. H. (2020, December). Energy-efficient cluster-based routing protocol in internet of things using swarm intelligence. In *2020 IEEE Symposium Series on Computational Intelligence (SSCI)* (pp. 219-224). IEEE.
25. Chen, J., Kher, S., & Somani, A. (2006, September). Distributed fault detection of wireless sensor networks. In *Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks* (pp. 65-72).
26. T Srinivas, A. S., Govinda, K., Ramasubbareddy, S., & Swetha, E. (2019). Sentimental Analysis of Demonetization Over Twitter Data Using Machine Learning. *Journal of Computational and Theoretical Nanoscience*, *16*(5-6), 2055-2058.
27. Samanta, S., Singhar, S. S., Gandomi, A. H., Ramasubbareddy, S., & Sankar, S. (2020, September). A WiVi based IoT framework for detection of human trafficking victims kept in hideouts. In *International Conference on Internet of Things* (pp. 96-107). Springer, Cham.
28. Zidi, S., Moulahi, T., & Alaya, B. (2017). Fault detection in wireless sensor networks through SVM classifier. *IEEE Sensors Journal*, *18*(1), 340-347.
29. Titouna, C., Naït-Abdesselam, F., & Khokhar, A. (2019). DODS: A distributed outlier detection scheme for wireless sensor networks. *Computer Networks*, *161*, 93-101.
30. Ayadi, A., Ghorbel, O., Obeid, A. M., & Abid, M. (2017). Outlier detection approaches for wireless sensor networks: A survey. *Computer Networks*, *129*, 319-333.
31. Dhanya, C. T., & Kumar, D. N. (2009). Data mining for evolving fuzzy association rules for predicting monsoon rainfall of India. *Journal of intelligent systems*, *18*(3), 193-210.
32. Nskh, P., Varma, M. N., & Naik, R. R. (2016, May). Principle component analysis based intrusion detection system using support vector machine. In *2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)* (pp. 1344-1350). IEEE.
33. Mohanta, B. K., Samal, K., Jena, D., Ramasubbareddy, S., & Karuppiah, M. (2022). Blockchain-based consensus algorithm for solving security issues in distributed internet of things. *International Journal of Electronic Business*, *17*(3), 283-304.
34. Sennan, S., Ramasubbareddy, S., Nayyar, A., Nam, Y., & Abouhawwash, M. (2021). LOA-RPL: novel energy-efficient routing protocol for the internet of things using lion optimization algorithm to maximize network lifetime.
35. Sankar, S., Somula, R., Parvathala, B., Kolli, S., & Pulipati, S. (2022). SOA-EACR: Seagull optimization algorithm based energy aware cluster routing protocol for wireless sensor networks in the livestock industry. *Sustainable Computing: Informatics and Systems*, *33*, 100645.
36. Gil, P., Martins, H., & Januário, F. (2019). Outliers detection methods in wireless sensor networks. *Artificial Intelligence Review*, *52*(4), 2411-2436.
37. Sharma, A. B., Golubchik, L., & Govindan, R. (2010). Sensor faults: Detection methods and prevalence in real-world datasets. *ACM Transactions on Sensor Networks (TOSN)*, *6*(3), 1-39.
38. Chander, B., & Kumaravelan, G. (2022). Outlier detection strategies for WSNs: A survey. *Journal of King Saud University-Computer and Information Sciences*, *34*(8), 5684-5707.
39. Chander, B., & Kumaravelan, G. (2022). Outlier detection strategies for WSNs: A survey. *Journal of King Saud University-Computer and Information Sciences*, *34*(8), 5684-5707.
40. Varaprasad, R., Ramasubbareddy, S., & Govinda, K. (2022). Event Recommendation System Using Machine Learning Techniques. In *Innovations in Computer Science and Engineering* (pp. 627-634). Springer, Singapore.
41. Srinivas, T. A. S., & Manivannan, S. S. (2020). Prevention of hello flood attack in IoT using combination of deep learning with improved rider optimization algorithm. *Computer Communications*, *163*, 162-175.
42. Srinivas, T. A. S., Ramasubbareddy, S., Sharma, A., & Kannayaram, G. (2020). Optimal Energy Distribution in Smart Grid. In *FICTA, 2*, 383–391.
43. Rajasegarar, S., Leckie, C., Palaniswami, M., & Bezdek, J. C. (2006, October). Distributed anomaly detection in wireless sensor networks. In *2006 10th IEEE Singapore international conference on communication systems* (pp. 1-5). IEEE.
44. Mahalaxmi, G., Tirupal, T., Srinivas, T., & Raziya, D. (2022). Categorization of Leaf Ailments Using Deep Learning Techniques: A Review. *IUP Journal of Telecommunications*, *14*(1).
45. Aditya Sai Srinivas, T., Somula, R., & Govinda, K. (2020). Privacy and security in Aadhaar. In *Smart Intelligent Computing and Applications* (pp. 405-410). Springer, Singapore.
46. Mahalaxmi, G., Tirupal, T., & Srinivas, T. (2022). Advanced Image Processing Algorithms for Categorizing and Evaluating Plant Diseases: A Study. *IUP Journal of Telecommunications*, *14*(1).
47. Kim, S., Choi, Y., & Lee, M. (2015). Deep learning with support vector data description. *Neurocomputing*, *165*, 111-117.