International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 24 Issue 03, MAR, 2024

Role of Machine Learning in Retrieving and Classifying Anomaly from IoT Based Wireless Multimedia Sensor Networks: A survey

[1]**P.Rajyalakshmi**, Assistant Professor, Dept of CSE, TKRCET(A), Hyderabad
[2]**B.S.Swapna Shanthi**, Assistant Professor, Dept of CSE, Sri Indu Institute of Engineering and Technology(A), Hyderabad
[3]**K.MOUNIKA**, Assistant Professor, Dept of CSE, Sri Indu Institute of Engineering and Technology(A), Hyderabad
[4]**Dr. Rajeshwari D,** Assistant Professor, Dept of CSE, Sri Indu Institute of Engineering and Technology(A), Hyderabad

Abstract-*Anomaly detection serves as a critical security feature, pinpointing instances where system behavior diverges from the expected norm, thereby enabling swift identification and resolution of anomalies. The integration of AI and IoT amplifies the efficacy of anomaly detection, bolstering the reliability, effectiveness, and integrity of IoT systems. AI-driven anomaly detection systems exhibit the capability to discern an array of threats within IoT environments, including brute force attacks, buffer overflow, injection attacks, etc.. With the proliferation of Internet-connected devices and the surging demand for IoT devices in various domains, such as home automation, personal wearable's, vehicular applications, and smart infrastructure, anomaly detection assumes paramount importance. This paper constitutes a survey of anomaly detection techniques in sensor networks and IoT realms, elucidating the concept of anomalies and conducting a comprehensive review of pertinent literature sources. The primary objective of this survey is to shed light on the methodologies employed for anomaly detection in IoT and sensor network domains, identifying existing approaches and delineating research gaps within this field. The study undertakes a thorough examination of anomaly detection techniques in IoT infrastructure, leveraging both machine learning and deep learning methodologies. It addresses the inherent challenges associated with intrusion and anomaly detection in IoT systems, underscoring the escalating frequency of cyber-attacks targeting IoT ecosystems. By reviewing recent advancements in machine learning and deep learning-based anomaly detection schemes tailored for IoT networks, the paper succinctly summarizes the prevailing literature. In conclusion, the survey underscores the imperative for further refinement of existing anomaly detection systems, advocating for the utilization of diverse datasets, real-time validation, and scalability enhancements to meet the evolving demands of IoT environments.*

Keywords: *anomaly detection ; Internet of Things; artificial intelligence; machine learning and Multimedia* Sensor Networks

I. Introduction

The IoT can be classified into either three-, four-, five-, or seven-layer architectures [1], while generally, the four-layer architecture is considered the essential component of the IoT [2]. These four layers are the Perception layer, Network layer, Middleware layer, and Application layer [2,3,4,5]. The Perception layer contains physical devices such as sensors and actuators that collect data for processing. The Network layer is the communication gateway for the Perception layer and the IoT system. The Middleware layer is where the collected data from the Perception layer are processed, stored, and managed. Finally, the Application layer contains the end-user applications that hold all of the processed data in meaningful values [4]. Other studies consider more layers to have an integral part in IoT architecture, such as the Security layer [6,7], Management layer [6], Business layer [1], and Environmental layer [8], which can also be considered as the Management layer.

IoT attacks are classified into four types: physical, encryption, network, and software-based attacks [9]. There has been a plethora of attacks in the IoT environment, namely buffer overflow attacks, brute-force attacks, DNS poisoning, injection attacks, replay attacks, DDoS attacks, SQL injection, back-door exploits, and more [10]. Additionally, research has been conducted revealing that the IoT can be used to facilitate violence between intimate partners who share a smart home [11]. Many attacks in the IoT can be prevented by using an anomaly detection mechanism, which can send an alert when any unusual behavior is detected. This can help in preventing attacks when they are attempted or indicating issues with system function that may result in downtime or failure. **Table 1** highlights a summary of the attacks that occur in the IoT according to previous studies.

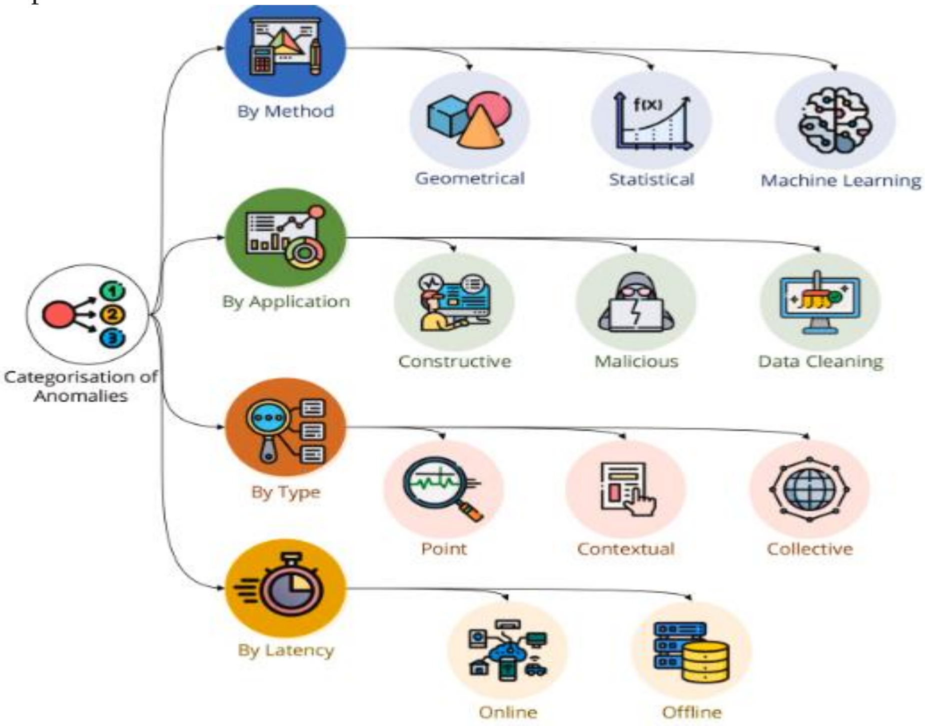

Fig 1: Categories of Anomalies

Anomaly detection is a security mechanism that distinguishes when a system's behavior departs from the normal baseline [12,13]. It can be either host-based (HIDS) or network-based (NIDS) and is integral for IoT systems as it can detect variations in sensor readings, network abnormality, and so on [14,15]. Intrusion detection systems are categorized into three types: signature-based, anomaly-based, and stateful protocol [16,17]. Additionally, IDS methods can be implemented in three ways: supervised, unsupervised, or semi-supervised, which can be implemented through AI, statistical modeling, and so on [18]. To detect anomalies, the system first has to be trained on what behavior is normal in a given system and what the normal traffic pattern appears to be. Departure from this normality will be considered an anomaly [19,20]. Training the system will require a vast amount of complex IoT data with the usual network traffic pattern and considerable time to build a profile based on the IoT data [21]. Moreover, the traditional methods are not useful in detecting newer threats and need more time for updates [**31**], which can be mitigated with the use of artificial intelligence techniques such as machine learning (ML) and deep learning (DL) techniques.

ML is a subfield of AI that comprises algorithms and models that help complete tasks through learning patterns and relationships rather than being explicitly programmed to do so. DL is a subset of ML that uses Artificial Neural Networks, which are more complex and can deal better with large amounts of complex data [**22**]. ML and DL techniques can use sophisticated analytical techniques to use the enormous and complex data of IoT systems cohesively to form a normal baseline for the network traffic of IoT devices [**22**,**2**4]. This will result in improved accuracy, faster response times, cost-effectiveness, real-time detection, and more. As a result, the ML and DL techniques can help detect when a system diverts from the baseline. ML and DL can detect anomalies by learning relationships and patterns from data, which can then be used to distinguish between normal and abnormal behavior. However, the differing factors between ML and DL techniques lie in their architecture and complexity, with DL being more complex as it deals with Neural Networks [25]. DL uses Neural Networks to learn a hierarchical representation of the data, which enables it to learn complex patterns [**2**]. ML and DL techniques combined with the IoT result in efficient anomaly detection that allows abnormalities to be found and fixed quickly. This strengthens the integrity, dependability, and effectiveness of IoT systems. This combination can also be used in any domain of the IoT, such as in healthcare, industrial settings, smart homes, and more [**27**].

To train ML and DL algorithms with IoT data, a dataset needs to be formed, which ideally should comprise real-time data of the IoT system. However, due to the complexity of IoT data, datasets are pre-formed by collecting the different types of traffic in IoT systems along with attack signatures. These datasets are used to train ML and DL algorithms and analyze the effectiveness of their various algorithms. Existing research mentions [**19**] that the datasets formed must simulate real-world settings and must be comprehensive and labeled. For the use of datasets in ML and DL techniques, the importance of feature extraction techniques, data cleaning, and conditioning routines are also emphasized. The accuracy of the dataset to real-world data will result in sound and reliable results from the AI algorithm detection. Commonly used datasets are the IoT-23, DS2OS, and Bot-IoT datasets, and more.

II. Literature Survey

Wilkinson and Leland [9] have proposed a novel algorithm hdoutliers for effectively detecting outliers in high-dimensional data and visualizing big data outliers through efficient ML algorithms. Nevertheless, they visualized big data effectively, but not analysed the proposed algorithm with any benchmark data sets and evaluation metrics. Yu et al. [11] have propounded a Recursive-Principal Component Analysis (R-PCA) technique with a cluster analysis framework for aggregate the redundant data attributes and detect outliers in IoT sensor data. The performance analysis of the proposed technique has been handing noise data is still a challenging issue. Pang et al. [12] have reviewed the anomaly detection or outlier detection through deep learning techniques.

They addressed the various challenges, the taxonomy of outlier detection methods, problem nature and categorization, future research directions, data sources, and metrics. Also, pointed the various pro’s and con’s of each deep learning techniques precisely. Li et al. [13] have proposed a weighted WATCH algorithm too effectively and efficiently the identification of outliers in high-dimensional categorical data. Initially, they identified the feature groupings by the correlation between data objects. Thereafter, assigning some relevant scores to each data attribute of each feature grouping. The proposed algorithm evaluated on both synthetic and real-world datasets to detect outlier's high-dimensional categorical data. Nonetheless, the incorporation of data attributes with local correlations is not addressed properly. Liu et al. [14] have discussed that cleaning and removing noisy sensor data is a challenging issue over the Industrial IoT (IIoT) applications, it improves the accuracy of the data analysis over it. Usually, anomaly or outlier detection methods give more false positives. Moreover, the traditional techniques are not applied to sensor data directly and it gives inaccurate and inefficient results. Finally, the missing value imputation between various data objects also not addressed. Deng et al. [15] have proposed One-Class Support Tucker Machine (OCSTuM) to resolve the curse of dimensionality with the identification of outliers in IoT big sensor data.

They would have also adopted a genetic algorithm for unsupervised learning-based anomaly detection over IoT sensor data. In addition, they retain better accuracy and efficient detection of outliers while compared to state-of-the-art algorithms. Nevertheless, these algorithms are good for big sensor data but they may consume more time to analyze big sensor data. Rahman et al. [16] have presented a novel and efficient Parameter Independent Density-based Clustering (PIDC) algorithm for setting parameters of various ML-based techniques such as Classification, Regression, and Clustering. They also proposed PIDC without an outlier's algorithm for detecting unique neighboring sets in IoT sensor big data with unsupervised learning-based clustering methods.

However, the computational complexity of these algorithms is more while dealing with big dynamic sensor data. Lu et al. [17] have proposed Outlier Detection-based Correlation Analysis (ODCA) algorithm to detect anomalies in IoT time-series data. In addition to that, they also adopted the cross-correlation coefficient method to identify the similarity between various data objects. The proposed ODCA algorithm outperforms in terms of scalability, accessibility, time complexity, effectiveness, and robustness. Ren et al. [18] have built a classifier and proposed a framework for Positive-Unlabelled (PU) data classification of feature data objects. It has been done through two stages. In the first stage, the effective feature selection of data objects that significantly reduces irrelevant features in the dataset. In the second stage, the outlier detection of data objects obtained that the data is highly biased. The integrated approach has been formulated for PU data classification of feature data objects. This framework has demonstrated the synthetic and real-world datasets. Liu et al. [19] have addressed the problem of outlier detection in IoT data with the Single Objective Generative Adversarial Active Learning (SO-GAAL) technique that can potentially generate the outliers based on the max-min approach. They also expanded their technique towards Multiple-Objective Generative Adversarial Active Learning (MO-GAAL) should easily identify cluster types with outliers of data objects. The embedded ensemble techniques are incorporated for future selection among various sensor data objects.

Imran et al. [22] have addressed the problem of detection of unusual patterns from largescale datasets and adopted a one-class support vector machine with bounded loss function for effective identification of outliers in high-dimensional data environments. They would have also experimented with proposed methods over benchmarked datasets and obtained notable results.

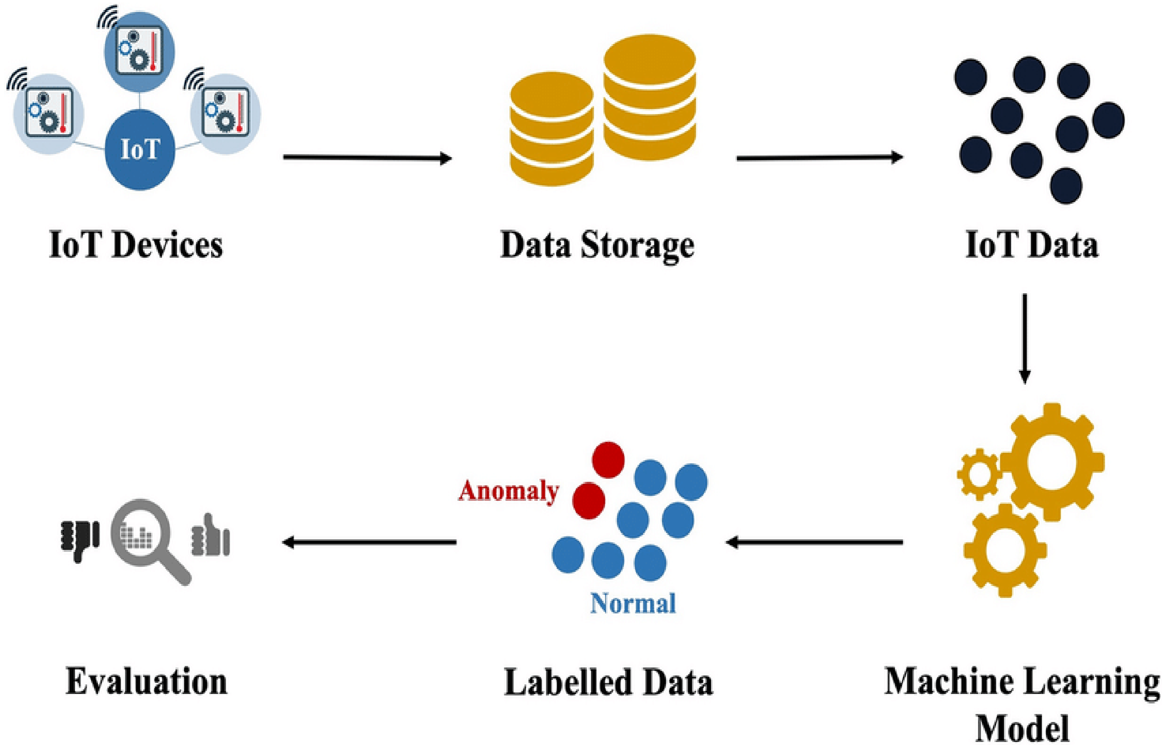

Fig 2:Anomoly detection flow from IoT sensor Data

Machine learning-based (ML-based) anomaly detection is highly researched and is a valuable technique for identifying anomalies in IoT systems [4]. There are four methods of learning in ML, which are supervised learning, unsupervised learning, semi-supervised learning, and reinforcement learning [14]. In supervised learning, the system is trained on labeled datasets and the system explicitly identifies the anomalies. However, unsupervised learning depends on the structure of the data, as it uses unlabeled data, hence the anomaly is detected according to the structure of the data [2]. ML is said to be effective in detecting anomalies and threats in real time [13]. The use of ML in the IoT also provides scalability, real-time decision making, predictive maintenance, resource optimization, automation, and more [14].

Using an ML-based approach to detect and prevent attacks and anomalies in IoT sensors, the study in [8] attempted to address cybersecurity concerns in IoT infrastructure. To show how well-suited basic models like Decision Tree (DT) or Random Forest (RF) models are for anomaly detection, the study evaluated the effectiveness of several ML models in terms of accurately predicting attacks and abnormalities on IoT systems using open-source datasets from Kaggle. The results of the study showed that Random Forest and Artificial Neural Network (ANN) techniques outperform Decision Trees in terms of testing and training accuracy with an accuracy rate of 99.4%, while Support Vector Machine and Logistic Regression methods are less effective. While the paper proposed models that can detect attacks with high accuracy, it also notes that the datasets only contain certain types of attacks and anomalies and hence they may not be scalable in real IoT environments.

To prevent system failure, the research in [19] proposed ways to address the problem of detecting attacks and abnormalities in IoT systems. It suggested a novel approach to a feature-transformation-based classifier for the classification and imputation of missing data values and evaluated its performance on real datasets. The classifiers it examined were Naïve Bayes (NB), Decision Tree (DT), Support Vector Machine (SVM), and Random Forest (RF) models with the DS2OS dataset. The suggested approach replaces missing values in a dataset using state-of-the-art imputation technology, and then it uses a feature transformation strategy to lower the dataset's dimensionality and improve classification performance. The findings demonstrated that the proposed strategy beat baseline approaches in terms of performance metrics including F1 score, accuracy, precision, and recall.

III. Machine learning Models

Machine learning can be broadly categorized into three main types based on the nature of the learning process and the availability of labeled data:

Supervised Learning: In supervised learning, the model is trained on a labeled dataset, where each input example is associated with a corresponding target or output label.

The goal of supervised learning is to learn a mapping from input features to output labels, such that the model can accurately predict the target variable for new, unseen data.

Examples of supervised learning algorithms include linear regression, logistic regression, decision trees, random forests, support vector machines (SVM), and neural networks.

Unsupervised Learning: In unsupervised learning, the model is trained on an unlabeled dataset, where the input examples are not associated with any corresponding output labels.

The goal of unsupervised learning is to extract meaningful patterns, structures, or relationships from the input data without explicit guidance.

Clustering and dimensionality reduction are common tasks in unsupervised learning. Examples of algorithms include K-means clustering, hierarchical clustering, principal component analysis (PCA), and autoencoders.

Reinforcement Learning: Reinforcement learning involves training an agent to interact with an environment in order to maximize cumulative rewards over time.

The agent learns by taking actions in the environment and observing the resulting rewards and state transitions. The goal of reinforcement learning is to learn an optimal policy or strategy that maximizes the expected cumulative reward. Examples of reinforcement learning algorithms include Q-learning, deep Q-networks (DQN), policy gradients, and actor-critic methods.

IV. Wireless Sensor Multimedia Network in IoT

Wireless Multimedia Sensor Networks (WMSNs) play a crucial role in the Internet of Things (IoT) ecosystem by enabling the collection, processing, and transmission of multimedia data from the physical world to the digital domain.

Data Collection: WMSNs are deployed in various environments to collect multimedia data such as images, videos, audio, and other sensory information from the surrounding environment. This data could include information about temperature, humidity, sound levels, visual information, etc.

Real-time Monitoring: WMSNs enable real-time monitoring of physical environments by continuously collecting multimedia data. This allows for the timely detection and response to events or changes in the environment. For example, in a smart city scenario, WMSNs can monitor traffic flow, detect accidents, or monitor environmental pollution levels.

Multimedia Data Processing: WMSNs often have embedded processing capabilities to analyze multimedia data locally before transmitting it to the central server or cloud. This localized processing reduces the amount of data that needs to be transmitted over the network, conserving bandwidth and reducing latency.

Resource-Constrained Environments: Many IoT applications operate in resource-constrained environments where power, bandwidth, and processing capabilities are limited. WMSNs are designed to operate efficiently in such environments by employing energy-efficient communication protocols, lightweight data compression techniques, and optimized routing algorithms.

Integration with IoT Applications: WMSNs serve as a critical component in various IoT applications such as smart surveillance, environmental monitoring, healthcare monitoring, industrial automation, and smart agriculture. They provide the necessary sensory data that feeds into these applications, enabling them to make informed decisions and take appropriate actions.

Enhanced Sensing Capabilities: With the integration of multimedia sensors, WMSNs offer enhanced sensing capabilities compared to traditional wireless sensor networks (WSNs). This allows for more comprehensive monitoring and analysis of the environment, leading to improved situational awareness and decision-making.

Scalability and Flexibility: WMSNs are designed to be scalable and flexible, allowing for the deployment of large-scale sensor networks covering vast geographical areas or complex environments. They can adapt to changing network conditions and environmental dynamics, ensuring reliable operation over time.

V. Performance metrics

Performance evaluation metrics play a crucial role in assessing the effectiveness of outlier detection algorithms.

Precision and Recall: Precision measures the proportion of true outliers among the instances classified as outliers. Recall (also known as sensitivity) measures the proportion of true outliers that are correctly identified by the algorithm.

F1 Score: The F1 score is the harmonic mean of precision and recall. It provides a balance between precision and recall and is particularly useful when the classes are imbalanced.

Receiver Operating Characteristic (ROC) Curve: ROC curves plot the true positive rate (TPR) against the false positive rate (FPR) at various threshold settings.

The Area Under the ROC Curve (AUC-ROC) provides a single scalar value summarizing the performance of the classifier across all thresholds.

Precision-Recall (PR) Curve: PR curves plot precision against recall at various threshold settings.

The Area Under the PR Curve (AUC-PR) quantifies the average precision across all recall levels.

F-measure at a Given Threshold: The F-measure at a specific threshold provides a single performance metric that combines precision and recall at that threshold.

Average Precision (AP): AP calculates the area under the precision-recall curve. It measures the average precision across all recall levels and is particularly useful when there are imbalanced classes.

Specificity: Specificity measures the proportion of true negatives that are correctly identified by the algorithm.

Accuracy: Accuracy measures the overall correctness of the outlier detection algorithm, considering both true positives and true negatives.

Confusion Matrix: A confusion matrix provides a tabular representation of the true positives, true negatives, false positives, and false negatives, enabling a more detailed assessment of the algorithm's performance.

Mean Squared Error (MSE): MSE measures the average squared difference between the predicted and actual outlier scores, providing insight into the algorithm's ability to accurately estimate outlier magnitudes.

VI. Attack-Based Anomaly Detection

The challenges associated with detecting distributed denial-of-service (DDoS) attacks in real-world networks using machine learning (ML) methods are discussed in a recent study [61], focusing on issues such as data loss and misclassification of legitimate traffic. The researchers utilized Packet Capture (PCAP) data sourced from the Information Security Centre of Excellence (ISCX) in Canada to train and assess ML algorithms. Their objective was to develop classifiers capable of detecting DDoS attack scenarios. Seven widely recognized classifiers, namely QDA, SVM, KNN, Naïve Bayes, Decision Tree, and Random Forest, were chosen for this purpose, and attributes defining network traffic patterns were identified. To detect and classify DDoS attacks in a real network environment, the researchers utilized the Data Plane Auxiliary Engine (DPAE) within nmeta2, an SDN-based traffic categorization framework. The DPAE demonstrated superior performance, exhibiting reduced processing time and a higher prediction rate compared to alternative methods.

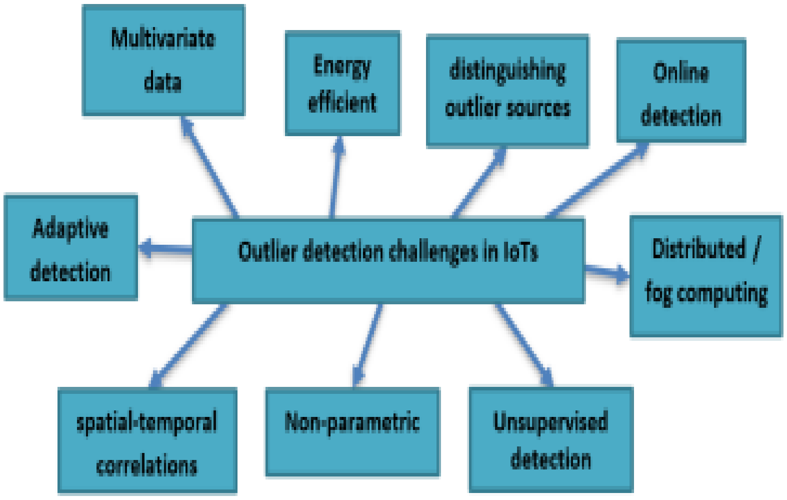
Multivariate data
Energy efficient
distinguishing outlier sources
Online detection
Adaptive detection
Outlier detection challenges in IoTs
Distributed / fog computing
spatial-temporal correlations
Non-parametric
Unsupervised detection

Fig 3:Outlier Detection Challenges

To identify cyberattacks on Industrial IoT (IIoT) networks, the study in [9] proposes a hybrid ML technique. This methodology employs a mixed range of ML techniques to create a hybrid ML (HML) model to discriminate between legitimate and malicious traffic. Ten ML classifiers were combined to make the HML, including KNN, GB, LR, RF, ET AB, LDA, and CART. The efficacy of the technique was assessed using the sophisticated open-source DS2OS dataset. The accuracy rate achieved with the model was 99.8%, with an F1 score of 99%. The model achieved a high rate of accuracy and F1 measure in classifying malware, but it could be computationally heavy when implemented.

VII. Conclusion

This paper explains the challenges associated with detecting intrusions and anomalies within IoT systems, as such occurrences can potentially compromise the integrity of the entire system. The impetus for undertaking this research stems from the escalating frequency of attacks targeting IoT systems. In response, the paper conducts a thorough examination of recent advancements in anomaly detection schemes for IoT networks, particularly those leveraging machine learning (ML) and deep learning (DL) methodologies. A comprehensive overview of pertinent studies from the literature is presented in tabular form. Over the past few years, the issue of outlier detection in IoT data environments has posed significant challenges. While numerous outlier detection techniques have been proposed, the exponential growth in IoT sensor data renders conventional methods ineffective and inefficient. Consequently, there is a growing need for advanced ML-based techniques to effectively identify outliers and anomalies within sensor data. The reviewed literature predominantly focuses on the development of innovative intrusion detection systems tailored for IoT environments. These systems are often subjected to comparative analyses against existing models, using diverse performance and security metrics to gauge their efficacy and accuracy. Many of the surveyed research endeavors lay the groundwork for anomaly detection, providing a foundational framework for further refinement and development. To enhance existing systems, researchers advocate for the utilization of more diverse datasets training AI systems. Additionally, real-time testing in varied environments is deemed crucial to validate the systems' efficacy. Moreover, efforts are underway to enhance the scalability and sophistication of these systems, enabling them to effectively detect anomalies within IoT ecosystems in real-world scenarios.

References

[1] NG, B.A.; Selvakumar, S. Anomaly detection framework for Internet of things traffic using vector convolutional deep learning approach in fog environment. *Future Gener. Comput. Syst.* **2020**, *113*, 255–265.

[2] Dhillon, H.; Haque, A. Towards Network Traffic Monitoring Using Deep Transfer Learning. In Proceedings of the 2020 IEEE 19th International Conference on Trust, Security, and Privacy in Computing and Communications (TrustCom), Guangzhou, China, 29 December 2020–1 January 2021.

[3] Sunder Reddy, K. S. ., Lakshmi, P. R. ., Kumar, D. M. ., Naresh, P. ., Gholap, Y. N. ., & Gupta, K. G. . (2024). A Method for Unsupervised Ensemble Clustering to Examine Student Behavioral Patterns. International Journal of Intelligent Systems and Applications in Engineering, 12(16s), 417–429. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/4854.

[4] Ullah, I.; Mahmoud, Q.H. Design and Development of a Deep Learning-Based Model for Anomaly Detection in IoT Networks. *IEEE Access* **2021**, *9*, 103906–103926

[5] Varalakshmi, S.; Premnath, S.P.; Yogalakshmi, V.; Vijayalakshmi, P.; Kavitha, V.R.; Vimalarani, G. Design of IoT Network using Deep Learning-based Model for Anomaly Detection. In Proceedings of the 5th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), I-SMAC 2021, Palladam, India, 11–13 November 2021; pp. 216–220.

[6] Nagesh, C., Chaganti, K.R. , Chaganti, S. , Khaleelullah, S., Naresh, P. and Hussan, M. 2023. Leveraging Machine Learning based Ensemble Time Series Prediction Model for Rainfall Using SVM, KNN and Advanced ARIMA+ E-GARCH. International Journal on Recent and Innovation Trends in Computing and Communication. 11, 7s (Jul. 2023), 353–358. DOI:https://doi.org/10.17762/ijritcc.v11i7s.7010.

[7] Wani, A.; Revathi, S.; Khaliq, R. SDN-based intrusion detection system for IoT using deep learning classifier (IDSIoT-SDL). *CAAI Trans. Intell. Technol.* **2021**, *6*, 281–290.

[8] Saba, T.; Khan, A.R.; Sadad, T.; Hong, S.P. Securing the IoT System of Smart City against Cyber Threats Using Deep Learning. *Discret. Dyn. Nat. Soc.* **2022**, *2022*, 1241122.

[9] Naresh, P., & Suguna, R. (2019). Association Rule Mining Algorithms on Large and Small Datasets: A Comparative Study. 2019 International Conference on Intelligent Computing and Control Systems (ICCS). DOI:10.1109/iccs45141.2019.9065836.

[10] Ishaque, M.; Johar, M.G.M.; Khatibi, A.; Yamin, M. Hybrid deep learning based intrusion detection system using Modified Chicken Swarm Optimization algorithm. *ARPN J. Eng. Appl. Sci.* **2023**, *18*, 1707–1718.

[11] Ahmad, I.; Al Qahtani, H.S. A comparative analysis of gradient boosting, random forest and deep neural networks in the intrusion detection system. *ARPN J. Eng. Appl. Sci.* **2023**, *18*, 1707–1718.

[12] M. I. Thariq Hussan, D. Saidulu, P. T. Anitha, A. Manikandan and P. Naresh (2022), Object Detection and Recognition in Real Time Using Deep Learning for Visually Impaired People. IJEER 10(2), 80-86. DOI: 10.37391/IJEER.100205.

[13] Pannangi, Naresh & Ramadass, Suguna. (2019). Implementation of Improved Association Rule Mining Algorithms for Fast Mining with Efficient Tree Structures on Large Datasets. International Journal of Engineering and Advanced Technology. 9. 5136-5141. 10.35940/ijeat.B3876.129219.

[14] Hussan, M.I. & Reddy, G. & Anitha, P. & Kanagaraj, A. & Pannangi, Naresh. (2023). DDoS attack detection in IoT environment using optimized Elman recurrent neural networks based on chaotic bacterial colony optimization. Cluster Computing. 1-22. 10.1007/s10586-023-04187-4.

[15] Bhayo, J.; Shah, S.A.; Hameed, S.; Ahmed, A.; Nasir, J.; Draheim, D. Towards a machine learning-based framework for DDOS attack detection in software-defined IoT (SD-IoT) networks. *Eng. Appl. Artif. Intell.* **2023**, *123*, 106432.

[16] V. Krishna, Y. D. Solomon Raju, C. V. Raghavendran, P. Naresh and A. Rajesh, "Identification of Nutritional Deficiencies in Crops Using Machine Learning and Image Processing Techniques," 2022 3rd International Conference on Intelligent Engineering and Management (ICIEM), London, United Kingdom, 2022, pp. 925-929, doi: 10.1109/ICIEM54221.2022.9853072.

[17] Liu, S.; Yao, S.; Huang, Y.; Liu, D.; Shao, H.; Zhao, Y.; Li, J.; Wang, T.; Wang, R.; Yang, C.; et al. Handling Missing Sensors in Topology-Aware IoT Applications with Gated Graph Neural Network. *Proc. ACM Interact. Mobile Wearable Ubiquitous Technol.* **2020**, *4*, 1–31.

[18] Ward, I.R.; Joyner, J.; Lickfold, C.; Guo, Y.; Bennamoun, M. A Practical Tutorial on Graph Neural Networks: What Are the Fundamental Motivations and Mechanics That Drive Graph Neural Networks, What Are the Different Variants, and What Are Their Applications? *ACM Comput. Surv.* **2021**, *54*, 1–35.

[19] Banbury, C.; Zhou, C.; Fedorov, I.; Matas, R.; Thakker, U.; Gope, D.; Janapa Reddi, V.; Mattina, M.; Whatmough, P. MicroNets: Neural Network Architectures for Deploying TinyML Applications on Commodity Microcontrollers. *Proc. Mach. Learn. Syst.* **2021**, *3*, 517–532.

[20] P, N., & R Suguna. (2022). Enhancing the Performance of Association Rule Generation over Dynamic Data using Incremental Tree Structures. International Journal of Next-Generation Computing, 13(3). https://doi.org/10.47164/ijngc.v13i3.806.

[21] Meyer-Berg, A.; Egert, R.; Böck, L.; Mühlhäuser, M. IoT Dataset Generation Framework for Evaluating Anomaly Detection Mechanisms. In Proceedings of the 15th International Conference on Availability, Reliability and Security (ARES'20), Virtual, 25–28 August 2020; Association for Computing Machinery: New York, NY, USA, 2020.

[22] Zhou, J. Research on Time Series Anomaly Detection: Based on Deep Learning Methods. *J. Phys. Conf. Ser.* **2021**, *2132*, 012012.

[23] B. Narsimha, Ch V Raghavendran, Pannangi Rajyalakshmi, G Kasi Reddy, M. Bhargavi and P. Naresh (2022), Cyber Defense in the Age of Artificial Intelligence and Machine Learning for Financial Fraud Detection Application. IJEER 10(2), 87-92. DOI: 10.37391/IJEER.100206.

[24] Aggarwal, S.; Gulati, R.; Bhushan, B. Monitoring of Input and Output Water Quality in Treatment of Urban Waste Water Using IOT and Artificial Neural Network. In Proceedings of the 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT), Kannur, Kerala, India, 5–6 July 2019; Volume 1, pp. 897–901.

[25] Naresh, P., & Suguna, R. (2021). IPOC: An efficient approach for dynamic association rule generation using incremental data with updating supports. Indonesian Journal of Electrical Engineering and Computer Science, 24(2), 1084. https://doi.org/10.11591/ijeecs.v24.i2.pp1084-1090.

[26] Otoum, S.; Guizani, N.; Mouftah, H. Federated Reinforcement Learning-Supported IDS for IoT-steered Healthcare Systems. In Proceedings of the IEEE International Conference on Communications, Montreal, QC, Canada, 14–23 June 2021.

[27] Stach, T.; Kinkel, Y.; Constapel, M.; Burmeister, H.C. Maritime Anomaly Detection for Vessel Traffic Services: A Survey. *J. Mar. Sci. Eng.* **2023**, *11*, 1174.