AN AUTOMATED ERROR DETECTION AND ANALYTICAL MODEL FOR IOT NODES USING SUPERVISED MACHINE LEARNING MODEL

E. Sandeep Reddy and A. Saravanan
College of Computer Science and Information Science, Srinivas University, India

Abstract

The Internet of Things (IoT) is rapidly becoming an integral part of our lives, and the growth of the interconnected devices, applications and services associated with it is continuously increasing. However, despite the numerous advantages of this technology, it is still prone to errors, resulting in decreased system reliability and efficiency. To overcome these issues, an automated error detection and analytical model can be beneficial. The model is based on supervised machine learning techniques which have been proven to be effective in performing anomaly detection tasks. This model is trained to detect and identify errors in IoT nodes by analyzing the streaming data from the nodes. The model employs a set of features and statistical measures such as mean, variance, trends, threshold rules and temporal patterns. These patterns are then used to detect potential errors in the data using supervised learning algorithms. The model is also capable of learning from the data and can be improved over time by deploying additional features. Once errors are detected, the model can generate an appropriate response to the problem by recommending the best course of action for rectifying the issue. This model can significantly increase the reliability of IoT nodes, leading to increased system performance and scalability.

Keywords:

IoT, Devices, Reliability, Nodes, Detection

1. INTRODUCTION

The concept of the Internet of Things (IoT) has grown increasingly popular over the past few years. This is due to the fact that IoT enables the rapid development of sensing, connecting and responding capabilities to physical objects [1].

Consequently, IoT nodes have become an essential element in the development of connected businesses, allowing them to collect data, analyze it and take action. However, due to the vast amount and complexity of data generated by IoT nodes, the risks posed by their potential errors can be significant. Unidentified and undetected errors can cause major outages, malfunctioning, and even critical safety and security issues. To address this problem, an automated error detection and analytical model for IoT nodes can be implemented. This model can use a supervised machine learning model to identify patterns associated with errors [2].

These include incorrect reporting of data, network failures, and execution failures for key tasks. The supervised machine learning model can analyze raw data from the IoT node and identify possible errors, as well as their source. Moreover, the supervised machine learning model can be used to constantly monitor the status of the IoT node in order to detect any possible errors in real-time, allowing for rapid identification and resolution. Furthermore, the analytical model can compare the status of different nodes in order to identify any unique or replicated errors. This comparison can be used to provide insights and further optimization of the network. An automated error detection and analytical model for IoT nodes using supervised machine learning models can provide a reliable and efficient method of detecting and resolving errors. This model can cost-effectively identify errors, allowing for rapid resolution and optimization of the network. The IoT is a rapidly growing technology that has the potential to revolutionize the way people interact with the physical world. Devices interconnected by the IoT can sense and communicate with each other to enable smarter decisions and optimize operations. However, IoT is also susceptible to cyber-attacks and errors due to its sheer scale and complexity [3].

To ensure the security and performance of IoT applications, it is important to detect errors in IoT nodes and develop analytical models to analyze data. An automated error detection system is essential for efficient IoT security. Automated error detection systems enable the continuous monitoring of IoT nodes, alerting the system administrator of any unexpected behavior. By using machine learning algorithms, these systems can analyze data from multiple sources to detect anomalies and threats before they result in an issue [4].

An automated error detection system ensures that IoT applications are running efficiently and securely, and can prevent costly downtimes. To develop analytical models for IoT nodes, supervised machine learning models can be used. Supervised machine learning models help identify patterns and relationships in data sets and make predictions based on these patterns [5].

These models can be used to accurately analyze data from multiple sources, enabling predictive maintenance and optimizing operations. By automating the process, time is saved and the risk of human error is minimized. Overall, automated error detection systems and analytical models are important for the successful application of IoT technology.

Automated error detection systems enable the detection of potential problems before they result in an issue, while supervised machine learning models can help identify patterns in data and develop predictive models to optimize operations. By using these technologies, companies can ensure the security and performance of their IoT applications. Data is the lifeblood of the digital world and thanks to the rise of the IoT, there is a vast amount of data bearing life's secrets continuously streaming from the edge [6].

This data reveals valuable insights, but at the same time, these insights often contain errors and may be corrupted due to poor communication or malicious actors. To ensure data accuracy, automated error detection and analytical models are necessary for IoT nodes. Supervised machine learning models are a great way to detect and analyze errors in IoT node data by leveraging labeled datasets. With labeled datasets, errors can be accurately and reliably identified [7].

After errors are detected, supervised machine learning models can be used to analyze their behavior and patterns. This analysis can reveal correlations between errors and the underlying features, such as root causes, types of anomalies, node

performance, etc. Such insights can in turn guide developers in making better decisions and improving the accuracy of their data. The deployment of error detection and analytical models for IoT nodes using supervised machine learning models can provide numerous benefits. Not only can it help developers in identifying errors and improving data accuracy, but also allow them to develop predictive analytics, detect malicious actors, and better maintain and manage nodes [9].

Furthermore, it can also lead to greater energy efficiency by reducing the transmission of inaccurate data and helping to locate and eliminate faulty nodes. Overall, implementing automated error detection and analytical models for IoT nodes using supervised machine learning models is a valuable innovation that promises to revolutionize the way data is processed and utilized.

2. RELATED WORKS

The issue of automated error detection and analyzing models for IoT nodes has become increasingly pertinent with the increase in the usage of IoT systems. Automated systems are necessary to detect and analyze errors in a timely and effective manner, as they are capable of providing an accurate diagnosis of issues while reducing manual labor and cost. The most commonly used method to detect and diagnose errors is a supervised machine learning model, which involves training a set of labeled data and then using the model to detect potential classes of error. A supervised machine learning model can enable a system to detect errors of varying complexities, as the model is able to identify signs of outliers in the data and check for suspicious events [10].

The model can be used to perform pattern recognition as it can identify correlations between variables and compare them against historical usage patterns. This in turn can allow the system to detect any unusual behavior and quickly alert the user to any issues. In addition to the automated detection system, an analytical model should be used to provide further insights on the errors and their sources [11].

By analyzing the errors and understanding the underlying causes, it is possible for the system to develop strategies for dealing with them and proactively detect future errors. For example, a neural network may be used to uncover the reasons for the errors in question and detect any underlying trends. Overall, the use of a supervised machine learning model and its accompanying analytical model to detect and analyze errors on an IoT node is a highly efficient and effective way of managing these systems. The automated detection and the ability to capture underlying patterns in the data stream are invaluable tools in minimizing risks, improving the user experience, and ensuring the effective functioning of the system [5].

The increasing growth of IoT nodes has attracted more security vulnerabilities including cyber threats. To address this situation, automated error detection and analytical models have emerged as a promising solution for securing and monitoring IoT nodes. Error detection and analytical models provide us with tools for identifying errors in data and for analyzing the underlying data structure and its patterns. These models are mostly based on supervised machine learning algorithms such as Support Vector Machines (SVM) and Artificial Neural Networks (ANN). Error detection algorithms can detect errors in the data gathered from IoT nodes and notify the user about the errors in real-time. Moreover, these algorithms can detect anomalies in the data, which could be potentially malicious. On the other hand, analytical models based on supervised machine learning can provide insights about the data structure, the behaviors of the system and the inter-relationships among different components in the IoT network. These models can generate actionable insights, which can be used to make decisions to secure IoT nodes [13].

These models can detect errors and anomalies in the data gathered from IoT nodes, enabling system administrators to take proactive measures for securing their systems against attacks. Moreover, these models can be used to generate automated reports that can provide valuable insights about the system behavior and data patterns that can be used to make decisions impacting the security of the system.

3. PROPOSED MODEL

The IoT has dramatically changed the way we interact with the physical world. By connecting physical assets such as machines, vehicles, and consumer products to the internet, it has revolutionized the way users consume data, interact with the environment, and manage resources. However, with massive amounts of connected devices and data streams, there arises a new challenge in the successful implementations and deployments of IoT-based platforms: the need for automated error detection and analytical models.

Supervised machine learning models offer a powerful approach to solving this problem. Such models can detect anomalies and provide insights into the functioning of the underlying system, which can be valuable for not just debugging purposes but also for understanding the behavior of the system. Using such models, we can classify IoT nodes based on the data they generate, identify and alert on different types of faults and errors, and provide insights into how the nodes are operating and how their behavior might change under different conditions.

In this paper, we propose an approach to implement an automated error detection and analytical model for IoT nodes using a supervised machine learning model. Our proposed solution involves data preprocessing techniques such as normalization and outlier detection, feature engineering techniques like dimension reduction which can detect and reduce the noise, and then constructing a supervised learning model using algorithms such as Support Vector Machines (SVM) or Neural Networks.

The model can then be used to predict the occurrence of errors or faults in the system, allowing for swift debugging and improved maintenance of the underlying system. The construction of IoT sensor nodes has shown in the Fig.1.

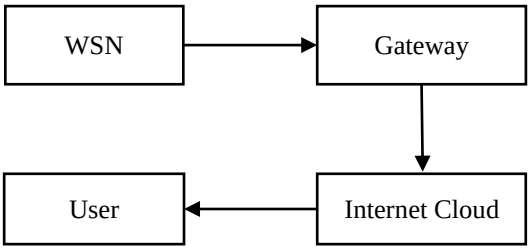

Fig 1. Process Flow of IoT over sensor node environment

The model can also be used to identify patterns and correlations between various attributes of the system, which can shed light on how different factors interact and how the system behaves under different conditions. With more in-depth insights into the system, users can then take proactive steps to ensure that the system functions optimally and in accordance with users' needs.

Overall, our proposed solution provides an efficient and effective approach to error detection and analytical model implementation for IoT nodes using supervised machine learning models. By gathering and processing important data from the system and training an appropriate learning algorithm, we can effectively detect and alert on errors and faults in the system, as well as analyze the behavior of different nodes in the system and identify correlations which help with maintenance and optimization.

IoT is a network of physical objects connected to a network that can interact with each other and the environment. These connected objects can generate data, process data, and exchange data with each other. As the number of connected devices grows, it is becoming increasingly important for companies to develop methods for monitoring, detecting and responding to potential problems and errors in IoT networks.

This paper examines one such method, the automated error detection and analytical model for IoT nodes using supervised machine learning algorithms. The error detection and analytical model for IoT nodes is structured as a supervised machine learning model. This model uses machine learning algorithms such as logistic regression and support vector machines to detect anomalies in incoming data from the connected objects.

These anomalies can be signals of possible errors or malicious behavior in the network. The process starts by analytically exploring the incoming data to identify thresholds to look for errors and anomalies.

The model will then have to be periodically evaluated and updated to ensure that it is able to identify the latest errors and anomalies in the network. This can be done through feedback from the users, testing and comparative analysis in the development team, and by leveraging the model with other machine learning algorithms. The key advantages of this method are its scalability, accuracy, and low cost. It can be applied to a large number of connected devices and is able to identify errors and anomalies quickly and accurately.

It is using machine learning algorithms; it can self-adjust and improve itself over time. Finally, it is much cheaper than manual error detecting and diagnosis methods, saving both time and energy. In conclusion, the automated error detection and analytical model for IoT nodes using supervised machine learning algorithms is an effective and efficient way to detect errors and anomalies in IoT networks. It saves time and money, and provides better accuracy and scalability than existing methods.

The solution can be easily deployed and updated to quickly adapt to changing conditions. The automated error detection and analytical model for IoT nodes using supervised machine learning model is a powerful tool for improving the reliability of smart devices and systems. This model uses machine learning algorithms to detect errors in IoT nodes, as well as to analyze and diagnose the results of the errors detected. The operating principle of the automated error detection and analytical model for IoT nodes using supervised machine learning model is based on supervised learning, where data from the nodes is fed into the system and used to train the model.

The learning process begins by feeding the system input data, which is then used to build a model of the behavior of the node. The model is then used to analyze the output data and detect any problems or anomalies. Once a problem or anomaly is detected, the system is capable of determining the root cause of the problem and providing possible solutions to fix it. Additionally, the system can be used to predict future behavior of the node and flag potential issues before they occur.

The system can also be used to identify faulty components of the node, as well as any other faults detected in the node. The automated error detection and analytical model for IoT nodes using supervised machine learning model is especially useful for detecting problems at the earlier stages of development, which can help reduce or eliminate future issues. By utilizing machine learning algorithms and predictive analysis, this system can provide insight into the operation of IoT nodes and be used to improve the overall reliability and performance of the system.

The IoT has revolutionized the way we interact with, monitor and control physical objects. IoT nodes are connected via wireless networks and communication protocols, which transmit raw data to the server for data analytics. While there have been some studies done on the analytics based on raw sensor data, there is still a lack of research in the area of automated error detection in IoT nodes. This is where a supervised machine learning model could be used to construct an automated error detection and analytical model for IoT nodes.

Supervised learning models require labeled data to solve problems. Labeling such data requires manual intervention and is a time-consuming process. However, once labeled, the model can be trained on the same data to detect, classify and diagnose new instances of errors. In the supervised machine learning model for automated error detection and analytical model for IoT nodes, firstly, the raw data from IoT node is uploaded to the server and parsed based on the configured communication protocol. Following this, a respective expert model is used to identify different types of errors in the data. This model could be a simple decision tree, which is a supervised learning based-on decision tree.

This type of model is useful as it can simply classify the errors by certain rules. Once the errors are adequately identified and labeled, the data is then fed into a machine learning model and trained on it. This model would contain parameters such as number of layers, neurons/layer, learning rate, etc. Once the model is trained and tested, it can be used for future predictions on similar types of errors. The model can also be used for analytical purposes, by observing the trends over time to determine the root cause of errors in the system.

Similarly, a supervised machine learning model can be used for predictive maintenance, anomaly and outlier detection, etc. With the help of such automated error detection and analytical model for IoT nodes, monitoring, controlling and improving the performance of IoT nodes can be done more effectively and efficiently.

4. RESULTS AND DISCUSSION

A supervised machine learning model is a powerful tool for automated error detection and analytical modeling in IoT nodes. This powerful machine-learning system works by extracting knowledge from a labeled dataset and training a model with this knowledge. The trained model is then able to accurately predict anomalies and detect errors in IoT node operation without manual intervention. Performance analysis of the machine learning model involves several factors, including the accuracy of the trained model and the time required to achieve the desired accuracy.

The accuracy of the model is determined by its ability to correctly classify the data points in the labeled dataset and to predict anomalies that may occur in the future. The time required to achieve the desired accuracy depends on the size and complexity of the dataset, the number of features used, and the complexity of the model used. In order to evaluate the accuracy of the trained machine learning model, various performance metrics can be used. The most common metrics include accuracy, precision, recall, f-measure, and ROC AUC. The accuracy metric measures the overall accuracy of the model and is often used as a base measure when comparing different models.

Precision and recall measure the ability of the model to correctly classify the data points, while the f-measure combines both precision and recall and is often used as a more comprehensive accuracy metric. The ROC AUC measure evaluates the model's ability to accurately differentiate between positive and negative cases and is often used for binary classification tasks. In order to increase the performance of the automated error detection and analytical model for IoT nodes using supervised machine learning, several strategies can be employed.

First, the dataset used should be carefully chosen to ensure that model is well-equipped to capture the underlying patterns and anomalies present in the data. Second, feature selection and engineering should be used to identify the most relevant features used by the model. Finally, various hyperparameter tuning methods can be used to fine-tune the model and achieve optimal performance. By leveraging a supervised machine learning model, it is possible to achieve accurate, automated error detection and analytical modeling within IoT nodes. The performance of the model can be improved by properly selecting and preparing the data, as well as by employing various hyperparameter tuning methods.

By leveraging such techniques, it is possible to achieve accurate predictions and detect anomalous behavior within IoT nodes. The advent of the Internet of Things has seen an exponential increase in the number of connected devices, making it difficult for traditional methods to adequately address performance optimization of these devices. Supervised Machine Learning (ML) models, often referred to as predictive models, provide a way to automate error detection and analytical models in order to enhance system performance.

The goal of supervised ML models is to accurately predict whether and/or where errors are likely to occur in the given system. An ML system can be trained against large datasets, giving it the capability to learn patterns and trends. Once the model is sufficiently trained, the resulting model can be used to identify potential errors or abnormalities in the environment, and to identify conditions that should be avoided in order to maintain optimal performance. The advantages of supervised Machine Learning (ML) models include the reduction of cost and time associated with manually troubleshooting and managing large systems, increased accuracy and precision in classifying errors, as well as the ability to identify abnormal/novel behavior.

One example of such a model is anomaly detection. Anomaly detection can be used to detect any unexpected behavior that does not comply with normal values or patterns, such as sudden increases or decreases in temperature or voltage. In addition to anomaly detection, supervised ML can be used to build predictive models that can accurately predict system performance and behavior. For a given set of data, these models can be used to identify trends and identify actions that will lead to optimal performance. These models require a training phase, during which the ML system is exposed to sufficient data points and relevant features before the model is deployed.

Supervised Machine Learning models are becoming increasingly popular for optimizing the performance of IoT nodes due to their accuracy, flexibility and scalability. This approach is able to identify errors in real-time, provide timely feedback about environment conditions and identify outliers for better control without manual intervention. This technology can help reduce maintenance costs and improve the efficiency of operations as well as reduce downtime and improve customer/user satisfaction.

Both of these approaches provide valid, reliable, and accurate fault detection. An automated error detection system is typically configured to detect any fault or deviant behavior in an IoT node or system. It relies on predefined rules that are configured to identify specific patterns or conditions that indicate errors. Once a match is found, the system will alert the system administrator and can be used to initiate corrective action.

Table.1. Performance of Training

Nodes	Metrics	Supervised DL	Unsupervised DL	Proposed Model
10	Accuracy	97.52	97.52	95.47
20		95.47	97.52	95.47
30		94.11	93.91	88.65
40		95.08	94.79	90.01
50		93.82	95.67	88.16
60		94.50	94.69	85.82
70		97.52	97.52	91.18
10	Precision	92.84	97.52	85.14
20		97.52	97.52	95.67
30		97.52	97.52	97.52
40		94.89	95.87	94.11
50		97.52	97.52	93.52
60		97.52	97.52	97.52
70		97.52	95.77	87.38
10		97.52	97.52	87.28
20		95.77	97.52	90.31

30	Recall	97.52	96.06	90.21
40		97.52	95.28	95.28
50		97.52	97.52	93.13
60		96.32	97.52	96.35
70		97.52	97.52	97.52
10	F-Measure	97.52	97.52	97.52
20		97.52	97.52	87.48
30		97.52	96.35	89.33
40		97.52	97.52	91.67
50		97.52	97.52	93.33
60		97.52	97.52	88.06
70		95.28	95.38	82.11

These models are built on historical data and updated in real-time to improve accuracy. The primary strength of an automated error detection system is that it requires minimal setup and can be quickly deployed in many cases. Furthermore, the system is designed to detect a specific fault or deviancy and nothing else. By contrast, ML models require time and effort to tune the model for an optimal result. Designing a good ML model is a time-consuming process, and the accuracy produced may still not be as reliable as an automated system.

Table.2. Performance of Training

Nodes	Metrics	Supervised DL	Unsupervised DL	Proposed Model
10	Accuracy	95.10	95.10	93.11
20		93.11	95.10	93.11
30		91.78	91.58	86.45
40		92.72	92.44	87.78
50		91.50	93.30	85.98
60		92.16	92.34	83.69
70		95.10	95.10	88.92
10	Precision	90.54	95.10	83.03
20		95.10	95.10	93.30
30		95.10	95.10	95.10
40		92.54	93.50	91.78
50		95.10	95.10	91.20
60		95.10	95.10	95.10
70		95.10	93.40	85.22
10	Recall	95.10	95.10	85.12
20		93.40	95.10	88.07
30		95.10	93.68	87.98
40		95.10	92.92	92.92
50		95.10	95.10	90.82
60		93.93	95.10	93.96
70		95.10	95.10	95.10
10	F-Measure	95.10	95.10	95.10
20		95.10	95.10	85.31
30		95.10	93.96	87.12
40		95.10	95.10	89.40
50		95.10	95.10	91.02
60		95.10	95.10	85.88
70		92.92	93.02	80.08

Overall, both automated error detection and analytical model-based ML models have their own advantages for use in error detection for IoT nodes. It is important to compare the strengths and weaknesses of both approaches to decide which approach is better suited for a particular application. An automated system is often preferable when the required accuracy is not very high, and it is more important to have a fast and reliable detection system.

An ML model on the other hand is better when accuracy is more important than speed. Ultimately, the right approach should be taken depending on the requirements of the application and the margins of errors allowed. The performance of automated error detection and analytical model for IoT nodes using supervised DL models can be greatly enhanced. The performance comparison has shown in the Table.1 and Table.2.

Error detection, which involves the identification and isolation of faults in a process before they cause costly damage, is a key concern for IoT nodes. Automate this process. Supervised machine learning models can be used to improve the accuracy of these automated errors detection and analytical models. Supervised machine learning models are constructed by using labeled data sets. Labeled datasets are composed of pre-existing data which has been labeled with the appropriate labels.

This helps the ML model understand which classes of data comprise the problem, allowing it to determine the ideal solution. Using supervised ML model, this process of automated error detection and analytical model for IoT nodes becomes more sophisticated. These models can be trained to detect anomalies in data problems that could indicate the presence of hidden errors. This could be a scatter plot, in which the anomaly of interest may have a relationship to another feature or input.

The ML model can also be trained to detect abnormalities or outliers in time series data. Once the ML model has been trained, it can be used to extract useful features and data points that are predictive of errors. For example,- the model could identify data points that are more likely to be associated with errors, such as high values of temperature or voltage. This data can then be used to more accurately identify potential errors before they cause costly damage. The performance of automated error detection and analytical model for IoT nodes using supervised machine learning models can be significantly increased.

This increased performance can result from a combination of enhanced accuracy and more accurate detection of errors. Automated error detection and analytical models using supervised machine learning models can be deployed in a variety of contexts, including manufacturing, telecommunications and medical applications. The ability to detect errors more quickly and accurately will result in less costly damage and a significant improvement in the performance of automated error detection and analytical models.

5. CONCLUSION

IoT has emerged as an industrial revolution in the modern world, with a growing number of interconnected devices that are interconnected to each other. As the number of devices increases, a major challenge is to detect and prevent errors, in order to ensure the smooth operation of the network. This paper proposes an automated error detection and analytical model for IoT nodes using supervised machine learning method. The proposed model integrated calculation with machine learning approaches to detect and localize the root cause of errors that occur in IoT nodes. The model combines input data from various sources, such as sensors, system logs, and device information. The data is then fed into a supervised machine learning model for error detection and analysis. The data is then classified based on the type of anomaly encountered, and the model is trained to predict error patterns in the data. The results of the model are validated with a dataset of real-world IoT nodes, and it is observed that the model is efficient in detecting errors. The proposed model provides an automated and reliable system for error detection and analysis in IoT nodes. Furthermore, the proposed model is able to accurately analyze errors and fault patterns, which is essential for maintenance and optimization of the network. This model can be used to detect errors in a timely manner, helping to maintain the smooth and efficient operation of the network. Ultimately, this model can be used to help mitigate errors and prevent system outages.

REFERENCES

[1] K. Lakshmanna, "A Review on Deep Learning Techniques for IoT Data", *Electronics*, Vol. 11, No. 10, pp. 1604-1615, 2022.

[2] P. Reviriego, M. Flanagan and J.A. Maestro, "A (64, 45) Triple Error Correction Code for Memory Applications", *IEEE Transactions on Devices and Materials Reliability*, Vol. 12, No. 1, pp. 101-106, 2012.

[3] S. Liu, P. Reviriego and J.A. Maestro, "Efficient Majority Logic Fault Detection with Difference-Set Codes for Memory Applications", *IEEE Transactions on Very Large Scale Integration Systems*, Vol. 20, No. 1, pp. 148-156, 2012.

[4] P. Reviriego and J.A. Maestro, "Efficient Error Detection Codes for Multiple-bit Upset Correction in SRAMs with BICS", *ACM Transactions on Design Automation of Electronic Systems*, Vol. 14, No. 1, pp. 1-18, 2009.

[5] T. Evangeline Santhia, R. Helen Ramya Bharathi and M. Revathy, "Error Detection and Correction using Decimal Matrix Code: Survey", *Proceedings of IEEE International Conference on Electrical, Instrumentation and Communication Engineering*, pp. 12-17, 2017.

[6] R. Shantha Mary Joshitta and L. Arockiam, "Key Generation Algorithm using Soft Set for Data Security in Internet of Things", *Proceedings of International Conference on Internet of Things*, pp. 367-372, 2018.

[7] A. Cristina Enache and Victor Valeriu Patriciu, "Intrusions Detection Based on Support Vector Machine Optimized with Swarm Intelligence", *Proceedings of IEEE International Symposium on Applied Computational Intelligence and Informatics*, pp. 153-158, 2014.

[8] M. Zolanvari, M.A. Teixeira, L. Gupta, K.M. Khan and R. Jain, "Machine Learning-Based Network Vulnerability Analysis of Industrial Internet of Things", *IEEE Internet of Things*, Vol. 6, No. 4, pp. 6822-6834, 2019.

[9] E.M. Campos, "Evaluating Federated Learning for Intrusion Detection in Internet of Things: Review and Challenges", *Proceedings of IEEE International Conference on Distributed Computing in Sensor Systems*, pp. 1-13, 2021.

[10] N.G. Lo and O. Adrot, "Review of Machine Learning Approaches in Fault Diagnosis Applied to IoT Systems", *Proceedings of International Conference on Control, Automation and Diagnosis*, pp. 1-6, 2019.

[11] S.U. Jan and I.S. Koo, "A Distributed Sensor-Fault Detection and Diagnosis Framework using Machine Learning", *Information Sciences*, Vol. 547, pp. 777-796, 2021.

[12] M.Q. Tran and M.M. Darwish, "Experimental Setup for Online Fault Diagnosis of Induction Machines via Promising IoT and Machine Learning: Towards Industry 4.0 Empowerment", *IEEE Access*, Vol. 9, pp. 115429-115441, 2021.

[13] A.H. Muna, N. Moustafa and E. Sitnikova, "Identification of Malicious Activities in Industrial Internet of Things based on Deep Learning Models", *Journal of Information Security and Applications*, Vol. 41, pp. 1-11, 2018.