Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 3, March : 2024

Anomaly Detection and Classification Using ESP32 and ThingSpeak

[*] Ruchika Rami1[1], Dr.Zakiyabanu Malek2 [1]
[1] Faculty of Computer Application and IT Dept
Gujrat Law Society Ahmedabad, Gujrat India1

[2]Professor Centennial College, Toronto, ON Canada

Abstract. Machine learning (ML) and deep learning (DL) are often used techniques for detecting anomalies (AD). Anomaly detection in Internet-connected devices is crucial due to the significant rise in their numbers, the increasing need for IoT devices in various settings, and the shift towards smart infrastructure and the Industrial IoT (IIoT). This paper provides a comprehensive overview of anomaly detection techniques specifically designed for sensor networks and the Internet of Things (IoT). This paper provides a clear definition of the term "anomaly" and examines many sources that offer similar meanings. The objective of this paper is to detect and classify anomalies of data generated by wireless sensor networks in which we consider different kinds of sensors like DHT11, Moisture sensor, Gas sensor, and LDR these kinds of sensors are used which play an important role in home appliances. Create a WSN node using ESP32 and load data on ThingSpeak. In this study, we discuss the main concerns and difficulties encountered when applying deep anomaly detection approaches to resource-constrained devices in real-world IoT scenarios.

Keywords: ML, DL, IOT, IIOT, Sensors, WSN, ThingSpeak, Anomaly detection.

1 Introduction

The Internet of Things (IoT) allows sensors and smart things to communicate autonomously, without the need for human intervention, requiring immediate processing. Performing data analytics using IoT necessitates the creation of innovative approaches that can operate within the constraints of a restricted computing budget. Anomaly detection, sometimes referred to as outlier detection or event detection, is a form of data analysis that identifies uncommon situations inside a system. Anomaly detection plays a critical role in extracting valuable and actionable information from sparse occurrences of abnormalities in IoT data. This has wide-ranging applications across sectors such as medical, manufacturing, finance, traffic management, and energy. Anomaly detection is utilized in the betting and gambling industry within the Internet of Things (IoT) to identify instances of insider trading. This is achieved by analyzing patterns of trade activity. Conversely, industrial machines employ a detection algorithm to guarantee the safety of production [1].

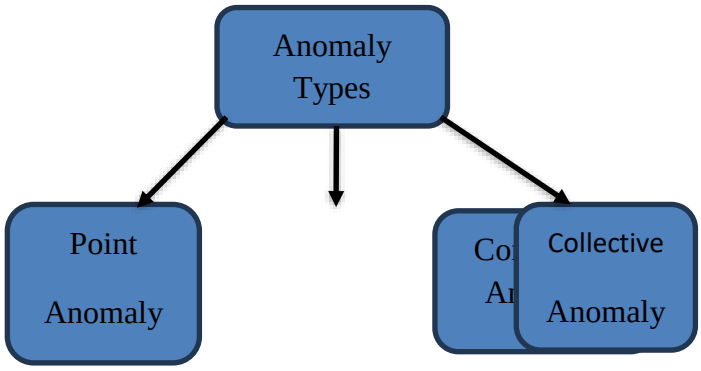

Fig.1. Categorization of Anomalies [1]

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 3, March : 2024

1.1 Anomaly detection

Anomaly identification, sometimes referred to as outlier detection, involves identifying instances within a dataset that significantly vary from the usual pattern. Anomalies hold significant importance in various practical analytical tasks since they pertain to situations that demand particular attention. Detecting suspicious activity can be beneficial for both post-incident investigation and early-warning systems, when abnormalities are identified in current datasets or even in real-time streaming data [6]. An anomaly refers to a specific data point that deviates from the expected behavior within a modeled system. Anomalies typically arise due to external reasons, such as sensor malfunction or deliberate external interference. The primary objective of a detection algorithm is to pinpoint the location of an anomaly and accurately determine its origin. The selection of the most suitable approximation models that accurately represent the predicted data behavior is vital in the binary categorization of an anomaly. Moreover, the intricacies of several scenarios necessitate a unique approach to identifying patterns for every specific use case. Illustrative aberrations are depicted in Figure 1.

1.1.1 Anomaly Type

A point anomaly refers to a single record in a dataset that stands out from the others and is commonly referred to as a point anomaly identification problem [6]. A point anomaly refers to an observation in a data stream that deviates significantly from the other data points. It is alternatively referred to as an "outlier". As an illustration, a satellite sends the data to its base station. The data exhibits a consistent pattern with specific fluctuations in the value [5].
Contextual anomaly detection refers to the task of detecting outliers by considering the context time. This term is used when the time context is important in the detection process [6]. A contextual anomaly refers to a situation where an observation point is considered normal in one setting but aberrant in another. This anomaly necessitates an understanding of the surrounding circumstances and is commonly referred to as a conditional anomaly. Such anomalies are frequently observed in time series data streams [5].
A collective anomaly refers to a situation in which numerous instances come together to generate an anomaly. A collective anomaly refers to a highly intricate situation that can also be considered as a difficulty in detecting anomalies within a specific context [6]. An analysis is conducted on a succession of observations to determine the collective behavior of the data stream. Any departure from the standard pattern can result in a collective abnormality in the overall data patterns throughout successive time intervals. For instance, a solitary instance of observing the heart is inadequate to ascertain its behavior, whereas a combination of signals can indicate if the conduct is normal or aberrant [5].
2. This text discusses the classification of anomalies and the typical methods employed in the field of the Internet of Things (IoT).

$$d = \begin{cases} < t \ , & \text{Normal (under threshold)} \\ > t \ , & \text{Anomaly (above threshold)} \end{cases}$$

These methods utilize either a constant or a changeable threshold 't' on the estimated distance 'd' to classify anomalies, as described below:
Statistical methods, like the minimal volume, aim to represent normal data by utilizing An anomaly is defined as any data that deviates from the expected pattern. Another forecasting method is known as exponential smoothing. This method employs historical data points and a smoothing value to predict future data points. Anomalous data acquired by statistical methodologies are those that significantly diverge from the established model. Traditional geometric and statistical approaches are supported by extensive study and depend on a comprehensive understanding of the true nature of the subject matter. These solutions fail to acknowledge numerous real-world scenarios where data models are highly time-sensitive. Hence, it is imperative to employ data-driven machine learning and deep learning solutions that enable more adaptability for adjustments. The third subcategory is machine learning and deep learning models, which have expanded in publication frequency in recent years. The choice of the model is determined by the characteristics of the provided data [1].
In terms of application, anomalies can be categorized into three routes: constructive, destructive, and data cleaning. Constructive applications are characterized by their productivity and beneficial nature, as they offer value to the world. An example of such an application is the monitoring of the daily behavior of elderly individuals to prevent falls, achieved through the use of image descriptors.
Anomaly: The most commonly found kind is the circumstance-specific type, which is characterized by being specific to a

particular situation, context, and group. A contextual anomaly refers to a certain occurrence that may be seen as abnormal within a specific context. Consequently, the act of comparing several viewpoints regarding a certain data point does not consistently lead to abnormal behavior. A con-textual abnormality is identified when the combination of contextual and behavioral characteristics is taken into account. For instance, when it comes to traffic violations, the irregularities differ based on the geolocation data [1]. In contrast to a singular or contextual anomaly, the collective anomaly type examines the complete dataset.

A) Point Anomalies: These anomalies occur when individual data points are significantly different from the rest of the data. They are typically detected by comparing the properties of individual data points to a threshold or statistical model.
   Example: In a dataset of daily temperature measurements, a single data point shows an unusually high temperature of 40°C during the winter season, while all other temperatures range between 0°C and 20°C. This single data point would be considered a point anomaly.
B) Contextual Anomalies: Contextual anomalies occur when data points are anomalous in a specific context but not necessarily when considered in isolation. These anomalies are detected by considering the relationships and dependencies between data points.
   Example: In a network traffic dataset, a user may typically download large files during working hours as part of their job. However, if the same user starts downloading large files at midnight when they are typically not active, it could be considered a contextual anomaly.
C) Collective Anomalies: Collective anomalies occur when a group or collection of data points is anomalous as a whole, even though individual data points may not be considered anomalous. These anomalies are detected by analyzing patterns and relationships within the data.
   Example: In a dataset of retail transactions, a sudden increase in the number of high-value purchases by multiple customers within a short period may indicate a collective anomaly, such as a special promotion or a data breach.

1.1.2 WSN(Wireless sensor Network)

Detecting the presence of people in a smart building allows for the optimization of services like lighting and temperature management in an energy-efficient manner. This optimization is based on factors such as the number and position of the occupants, as well as the type of event. Within the context of military operations Wireless sensors are mostly utilized for battlefield surveillance and have extensive applications in several industries, such as industrial monitoring and control, consumer applications, and machine health monitoring. The most significant achievement of wireless sensor networks has been their utilization in smart meters. Currently, meter readings are transmitted wirelessly, enabling automatic communication with smart home control systems [8].

1.1.3. Internet of Things (IoT)

The Internet of Things (IoT) refers to the expansion of Internet services to include the connectivity and control of all items. The Internet of Things (IoT) is a burgeoning subject of interest across industry and engineering communities. The Internet has revolutionized human existence by enabling constant contact with anyone, regardless of time or location. The internet enables us to quickly find solutions to many problems and allows us to connect from any location, leading to reduced costs and energy consumption [7].
The Internet of Things (IoT) refers to a situation where objects, sensors, and other devices that are not typically considered computers can connect to a network and exchange, generate, and consume data with minimal human involvement. The rapid advancement of technology has greatly contributed to the expansion of the IoT environment, which has already been established in the Industrial Wireless Sensor Network [7].
The exceptional flexibility and universal applicability of IoT systems make them suitable for various sectors [10].

1.1.4 Home Automation System

Home automation systems have existed for over a decade. The primary idea is to establish a network that interconnects the electrical and electronic devices within a household. This is an emerging technology that has revolutionized people's way

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 3, March : 2024

of life [7].

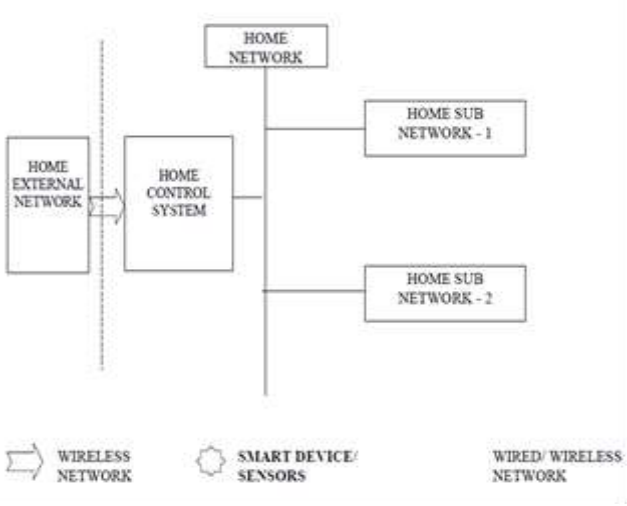

Fig.2. Schematic Structure of Home Automation System [8]

Figure 2 illustrates the fundamental configuration of a home system. Wireless sensor networks (WSNs) equipped with speech recognition technology are tasked with gathering environmental data and transmitting it to WSN coordinators. PLCs serve as a network infrastructure to link all WSN coordinators and transmit the gathered environmental data to the management station, as well as control messages to household appliances. The concept of the smart house embodies the fundamental essence of human nature and the harmonious integration of life [8].
The home automation market is growing in response to the increasing demands of users. Automation and security are the primary concerns in household settings. The emergence of electronic technology is leading to the expansion of the home automation field. The home automation system was developed utilizing a range of technologies including Bluetooth, ZigBee, Internet, and SMS-based communication. These cutting-edge technologies provide a cost-effective home automation system that is easy for users to operate [9].

2 Literature Analysis

Paper 1: IoT anomaly detection methods and applications: A survey [1]
Author: Ayan Chatterjee, Bestoun S. Ahmed
Year:2022
Summary:
Scholarly literature has recently observed a significant lack of methods for identifying abnormalities in the Internet of Things (IoT). The scarcity is especially noticeable when dealing with the difficulties of integrating systems that incorporate a variety of sensors, data and concept shifts, as well as data enhancement in situations where there is a limited supply of accurate reference data. Ultimately, we discuss the present problems and put out innovative perspectives that require further examination. This paper presents a thorough examination of the many techniques and uses of detection in the field of anomaly detection for the Internet of Things (IoT). Furthermore, it covers a comprehensive examination of the classification of algorithms used for detecting anomalies in the Internet of Things (IoT). Following that, a thorough examination is carried out on the current body of literature to discover certain areas of use, where chosen papers are carefully examined based on the predetermined search criteria. The three methods being considered are unsupervised learning, semi-supervised learning, and self-learning.
Drift adjustment: In such cases, it is standard practice for the model to require retraining. Utilizing a proactive strategy is beneficial for an anomaly detection model to efficiently respond to changes in incoming data or shifts in ideas.

Paper 2: A step towards Home Automation using IOT [2]
Author: Harsh Kumar Singh, Saurabh Verma, Shashank Pal, Kavita Pandey

Year: 2019
Summary:
This project aims to create a home automation system using Internet of Things (IoT) technology, specifically with a microcontroller that functions through Wi-Fi networking. With each passing day, technology is rapidly advancing in various domains including mobile technology, robots, and machine learning. Considering this pattern, it is worth contemplating why our residences have not undergone comparable progressions. In modern times, residential homes are increasingly shifting from traditional appliances that require manual operation to smart appliances that are connected with Internet of Things (IoT) capabilities, allowing for remote control and management. Presently, the existing home automation systems employ technology that is limited to the particular device for which it is intended. Our main objective is to enhance the Internet of Things (IoT) functionality of our devices, rather than focusing on implementing it in our homes. For this research, the NodeMCU (ESP8266) microcontroller is used along with relays to provide remote control of electrical switches. The remote-control functionality is enabled by a server built with Node.js. After login, the user can adjust switches through a Web Application.
A log file has been created as a result of modifying the condition of appliances. This technology possesses the capacity to observe and document the user's actions, particularly in regards to the time of appliance manipulation. By leveraging the given log file, it is feasible to apply Machine Learning methodologies to the system. This will allow the system to gather information on the user's interactions with the many appliances in their home. According to the results of the machine learning analysis, the system has the ability to automatically change the operational status of the appliances based on the user's activities.

Paper 3: Anomaly Detection on loT Network Intrusion Using Machine Learning [3]
Author: Zhipeng Liu, Niraj Thapa, Addison Shaver, Kaushik Roy, Xiaohong Yuan, Sajed Khorsandroo
Year:2020
Summary:
Ensuring secure connectivity and maintaining maximum performance is a critical difficulty in the development and deployment of a large number of Internet of Things (IoT) devices. The challenges stem from the inherent power constraints of most Internet of Things (IoT) devices, which therefore limit their processing capabilities. Therefore, the application of encryption and authentication mechanisms poses difficulties in effectively countering hostile cyber-attacks. The Intrusion Detection System (IDS) is a renowned and effective security solution. Anomaly-based network intrusion detection is crucial for safeguarding networks from diverse malicious activity. The objective of this project is to utilize several machine learning techniques to accurately detect anomalies within the IoT Network Intrusion Dataset. The results illustrate promise, as our research attained accuracy rates varying from 99% to 100% while upholding a notable level of efficiency. Overall, while producing the highest metric scores, the Random Forest (RF) technique required the most significant computational resources. The utilization of the support vector machine (SVM) method required a similar level of computational resources, but it resulted in only minimal improvements. Despite the lower computational requirements of the Logistic Regression technique, its accuracy was deemed insufficient. The K-Nearest Neighbors (KNN) and Extreme Gradient Boosting (XGBoost) techniques demonstrated excellent performance in terms of accuracy and numerous other evaluation measures. XGBoost is widely regarded as the optimal technique for real-time detection, surpassing other methods.

Paper 4: A Comprehensive Study of Anomaly Detection Schemes in IoT Networks Using Machine Learning Algorithms [4]
Author: Abebe Diro, Naveen Chilamkurti, Van-Doan Nguyen, and Will Heyne
Year:2021
Summary:
The adoption of the Internet of Things (IoT) has brought about substantial opportunities for innovation in diverse domains, such as industries, households, the environment, and companies. However, the inherent vulnerabilities linked to the Internet of Things (IoT) have caused concerns about its extensive adoption and implementation. The Internet of Things (IoT) ecosystem has distinct security challenges, unlike traditional information technology (I.T.) platforms. These issues stem from constraints in resources, the wide array of devices implicated, and the decentralized structure of these intelligent gadgets. The aforementioned condition renders the adoption of host-based preventive measures, such as anti-malware and anti-virus software, impractical. The aforementioned problems and the intrinsic qualities of Internet of Things (IoT) applications require the development of a monitoring system, specifically one that includes anomaly detection. The monitoring system should expand its capabilities to include monitoring at both the device and network levels, going beyond

the limitations of organizational borders. This indicates that an anomaly detection system has a clear advantage over traditional security measures in efficiently protecting IoT devices. This work aims to thoroughly analyze previous research on the creation of anomaly detection solutions using machine learning methods to protect an Internet of Things (IoT) system. Furthermore, it is important to highlight that anomaly detection systems utilizing Blockchain technology possess the capability to jointly amass knowledge and construct effective machine learning models specifically designed for the detection of anomalies.

Machine learning methods have been employed to create anomaly detection systems in the fields of information technology (I.T.) and Internet of Things (IoT) systems. However, machine learning-based anomaly detection systems have shown better performance in information technology (I.T.) systems compared to the Internet of Things (IoT) environment. The reason for this might be linked to the improved resource capabilities and the strategic location of these systems within the perimeter. Nevertheless, the existing anomaly detection techniques that rely on machine learning are vulnerable to adversarial attacks. The current study has conducted a comprehensive analysis of the utilization of machine learning methods for detecting anomalies in the Internet of Things (IoT) system.

3 Comparision

Sr No.	Title	Publication	Summary
1	IoT anomaly detection methods and applications: A survey	Elsevier, 2022	We strive to condense a vast array of possibilities into a selection of the most consequential challenges now confronting the area.
2	A step towards Home Automation using IOT	IEEE,2019	The Bluetooth system functions within a range of 0 to 15 meters. Furthermore, from the perspective of users, Bluetooth is considered obsolete and likely to have compatibility concerns. ZigBee based systems encounter the same issue of limited range due to their restriction to indoor applications. Typically, these systems are employed for Local Area Networks (LAN).
3	Anomaly Detection on lot Network Intrusion Using Machine Learning	IEEE,2020	We were able to achieve high accuracies while maintaining high efficiencies on the lot Intrusion Network Dataset.
4	A Comprehensive Study of Anomaly Detection Schemes in IoT Networks Using Machine Learning Algorithms	MDPI Abebe Diro, NaveenChilamkurti, Van-Doan Nguyen, WillHeyne	To resolve the issue of trust, one potential solution is to establish a centralized server that manages trust calculation and facilitates the exchange of data.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 3, March : 2024

ESP32

Fig.3. ESP32 Development Board [8]

The ESP32 is a line of cost-effective, energy-efficient microcontrollers that combine Wi-Fi and dual-mode Bluetooth into a single system on a chip. The ESP32 series is equipped with either a dual-core or single-core Ten silica Xtensa LX6 microprocessor, a dual-core Xtensa LX7 microprocessor, or a single-core RISC-V CPU.

The device is equipped with integrated antenna switches, a power amplifier, a low-noise receive amplifier, filters, and power management modules. The ESP32 replaces the ESP8266. The device offers a greater number of GPIOs, two CPU cores, improved Wi-Fi speed, and supports Bluetooth 4.2 and Bluetooth low energy. Additionally, it provides an increased number of GPIOs.

Sensors

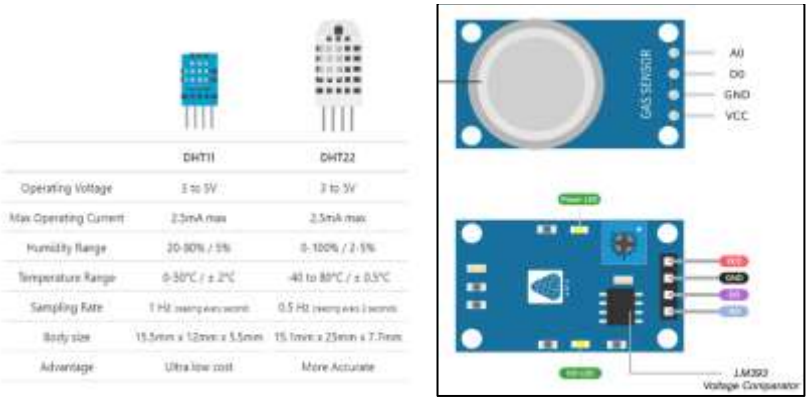

Fig 4: Sensors DHT11 and MQ2

Proposed Model

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 3, March : 2024

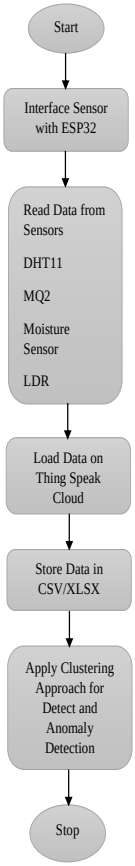

Fig.5. Flow of System

1. This IOT-based anomaly detection system could be installed in industrial and commercial buildings where temperature and humidity, Gas, and sunlight values are Generated form sensors for analysis.
2. This system also gives an alarming beep it user when the temperature or humidity level increases by the set values.
3. This system is less costly, more efficient, and more precise as compared to other systems.
4. Load Data in Thing speak and also analysis the patter and behaviour of data.

ThingSpeak

The utilization of IoT software known as ThingSpeak is employed in this project. ThingSpeak is a freely available Internet of Things (IoT) platform service that enables the collection, processing, visualization, and storage of real-time data streams in the cloud, facilitating the development of IoT applications. It is compatible with IoT technologies such as Arduino, MATLAB, Raspberry-Pi, and NodeMCU. Data from IoT devices can be transmitted to the ThingSpeak cloud for in-depth analysis. The route is the fundamental component of ThingSpeak. Data can be transmitted to this channel, where ThingSpeak will process it, and subsequently retrieved by an application [8].

ThingSpeak is an Internet of Things (IoT) platform that enables users to collect, visualize, analyze, and respond to real-time data. The app is an open source software that was initially launched by I/O Bridge in 2010. It enables the construction of IoT systems without the need for additional computer setup. The information is collected utilizing either the REST API or MQTT. MATLAB analytics is utilized for data processing and visualization. Additionally, users have the choice to incorporate several applications that enable them to display.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 3, March : 2024

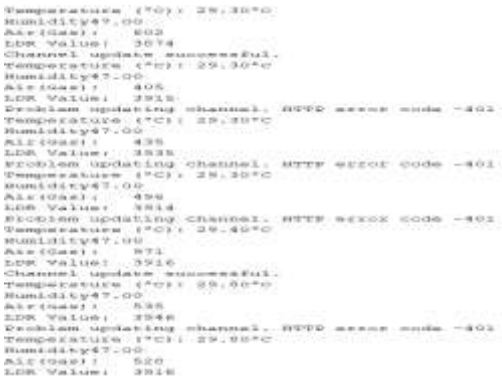

Fig.6: Datadisplay on serial Terminal

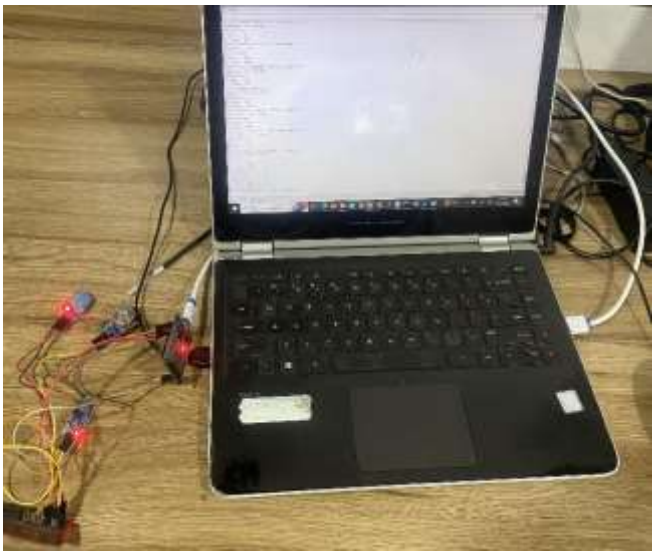

Fig.7. Hardware Connection

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 3, March : 2024

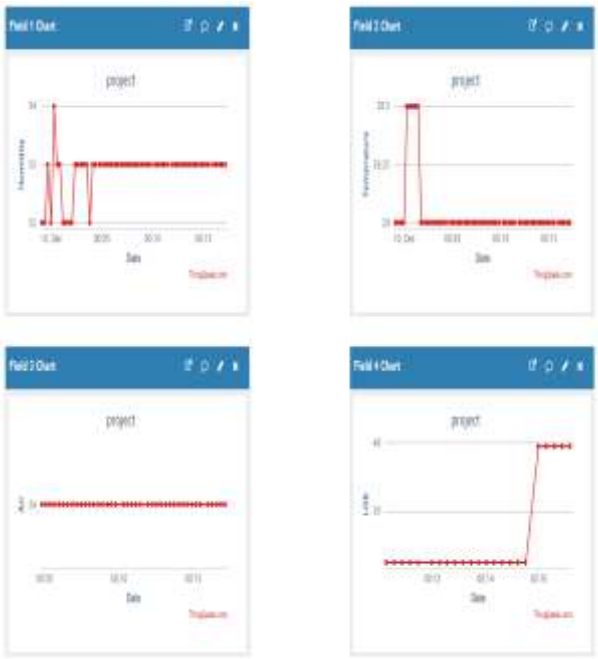

Fig.8. Thinkspeak View

created_at	entry_id	humidity	Temprature	Gas	LDR
2023-12-10T13:39:3	756	53	28	34	
2023-12-10T13:39:4	757	53	28	34	
2023-12-10T13:40:1	758	53	28	34	5
2023-12-10T13:40:3	759	53	28	34	5
2023-12-10T13:40:5	760	53	28	34	5
2023-12-10T13:41:1	761	53	28	34	5
2023-12-10T13:41:2	762	53	28	34	5
2023-12-10T13:41:5	763	53	28	34	5
2023-12-10T13:42:1	764	53	28	34	5
2023-12-10T13:42:3	765	53	28	34	5
2023-12-10T13:42:5	766	53	28	34	5
2023-12-10T13:43:1	767	53	28	34	5
2023-12-10T13:43:2	768	53	28	34	5
2023-12-10T13:43:4	769	53	28	34	5
2023-12-10T13:44:0	770	53	28	34	5
2023-12-10T13:44:2	771	53	28	34	5
2023-12-10T13:44:3	772	53	28	34	5
2023-12-10T13:44:5	773	53	28	34	5
2023-12-10T13:45:1	774	53	28	34	5
2023-12-10T13:45:3	775	53	28	34	5
2023-12-10T13:46:0	776	53	28	34	39
2023-12-10T13:46:1	777	53	28	34	39
2023-12-10T13:46:3	778	53	28	34	39
2023-12-10T13:46:5	779	53	28	34	39
2023-12-10T13:47:1	780	53	28	34	39

Fig.9. Tabular View

Conclusion

The frequency of publication in IoT anomaly detection indicates that the topic is still in its nascent phases. This paper provides a concise overview of the four categories into which anomaly detection methods are grouped. Additionally, it provides a comprehensive compilation of frequently utilized terms and applications, while pinpointing certain application domains that necessitate additional investigation. Instead, there are several methods that are tailored to certain applications. Within this area, our objective is to refine a vast array of potentialities to a selection of the utmost consequential challenges currently confronting the field. Using proposed model, we successfully load data on ThingSpeak cloud and also initialize and detect abnormal activity of sensors using Arduino ide and esp32.

Reference

1. Ayan Chatterjee, Bestoun S. Ahmed, “IoT anomaly detection methods and applications: A survey”, ELSEVIER, 2022.
2. Harsh Kumar Singh, Saurabh Verma, Shashank Pal, Kavita Pandey, “A step towards Home Automation using IOT”, IEEE, 2019.
3. Zhipeng Liu, Niraj Thapa, Addison Shaver, Kaushik Roy, Xiaohong Yuan, Sajad Khorsandroo, “Anomaly Detection on loT Network Intrusion Using Machine Learning”, IEEE, 2020.
4. Abebe Diro, Naveen Chilamkurti, Van-Doan Nguyen, and Will Heyne, “A Comprehensive Study of Anomaly Detection Schemes in IoT Networks Using Machine Learning Algorithms”, MDPI, 2021.
5. Muhammad Fahim, And Alberto Sillitti, “Anomaly Detection, Analysis and Prediction Techniques in IoT Environment: A Systematic Literature Review”, IEEE Access, 2019.
6. Markus Goldstein, “Special Issue on Unsupervised Anomaly Detection”, MDPI, 2023.
7. Radhika C, Menaka M, “Survey on IoT Technologies for Home Automation System”, International Journal of Engineering and Techniques, 2016.
8. M.Agalya, S.Nancy, and R.Selvarasu, “Home Automation System Using Wireless Sensor Networks”, IJETCSE, 2015.
9. Mrs. Bhagyashri R. Wankar, Prof. Vidya Dhamdhere, “Application of WSN to Intelligent Home Automation and Power Monitoring Using Android Smart Phone- A Survey”, IJCSMC, 2015,
10. Kirankumar P. Johare, Vasant G. Wagh, Arvind D. Shaligram, “Smart Home Automation System Using IoT, AI and Communication Protocols”, IJSDR, 2022.
11. Harsh Kumar Singh, Saurabh Verma, Shashank Pal, Kavita Pandey, “A step towards Home Automation using IOT”, IEEE, 2019.
12. Urvi Singh, M. A. Ansari, “Smart Home Automation System Using Internet of Things”, IEEE, 2019.
13. Chwan-Lu Tseng, Che-Shen Cheng, Yu-Hsien Hsu, Bing-Hung Yang, “An IoT-based Home Automation System Using Wi-Fi Wireless Sensor Networks”, IEEE, 2018.
14. Zhipeng Liu, Niraj Thapa, AddisonShaver, Kaushik Roy, XiaohongYuan, Sajad Khorsandroo, “Anomaly Detection on loT Network Intrusion Using Machine Learning”, IEEE, 2020.
15. Ayan Chatterjee, Bestoun S. Ahmed, “IoT anomaly detection methods and applications: A survey”, Elsevier, 2022.
16. S.supriya, R.Charanya, S.J. Madhumitha, “A Review On Home Automation System Using IOT”, ic-ETITE, 2020.
17. Dr. Syeda Gauhar Fatima, Syeda Kausar Fatima, Syed Mohd Ali, Naseer Ahmed Khan, Syed Adil, “Home Automation System with WSN and IoT”, IJARET, 2019.
18. M.Agalya, S.Nancy, and R.Selvarasu, “Home Automation System using Wireless Sensor Networks”, IJETCSE, 2015.
19. Dr. C K Gomathy, MR.Y.Venkata Sai, Mr.Y.Yaswanth Kumar, “The Home Automation using IoT”, IJSREM, 2021.
20. Mrs. S.Subha, “A Survey On Real-Time Anomaly Detection Techniques In IoT Data Streams”, IJCRT, 2021