1. Introduction

1.1 Background

The rapid growth of the Internet of Things (IoT) networks has significantly enhanced real-time monitoring across various domains, including environmental conditions, industrial operations, and home automation. However, this expansion brings critical challenges in terms of security and data integrity. IoT systems integrate embedded sensors, wireless communication, and cloud computing to provide seamless data collection and remote access. However, these systems remain vulnerable to cyber threats, particularly Distributed Denial-of-Service (DDoS) attacks, which can compromise data integrity and system availability. This thesis delves into these vulnerabilities, specifically examining how machine learning and advanced security frameworks can mitigate risks and enhance resilience.

1.2 Research Objectives

This thesis aims to:

1. **Environmental Analysis**: Understanding unique sensor characteristics to determine their operational efficiency and potential failure points.
2. **Sensor Correlations**: Identifying relationships between sensor readings to improve data reliability and predictive capabilities.
3. **Seasonality Analysis**: Detecting trends and variations in environmental conditions that may impact IoT performance.
4. **Daily Trends**: Visualizing day-to-day sensor fluctuations to recognize abnormal behaviors.
5. **Cybersecurity Risk Assessment**: Evaluating vulnerabilities to cyber threats, including DDoS, data spoofing, and unauthorized access.
6. **Mitigation Strategies**: Enhancing IoT security using anomaly detection, Intrusion Detection Systems (IDS), and network hardening techniques.
7. **Mathematical Modeling & Machine Learning**: Applying statistical methods and AI-driven approaches to analyze and predict trends for enhanced security.
8. **Network Traffic Analysis**: Detecting security threats and unauthorized intrusions using data-driven techniques to identify anomalies.
9. **System Design Framework**: Proposing an architecture for IoT data security and anomaly detection, integrating various security methodologies.

1.3 Significance of Study

The increasing reliance on IoT systems in critical sectors, including healthcare, smart cities, and industrial automation, necessitates a robust framework for security and performance optimization. Understanding sensor behavior, mitigating risks, and integrating predictive

analytics can enhance resilience and efficiency in IoT systems. This study provides a structured methodology to analyze security vulnerabilities and propose effective mitigation strategies.

2. System Design

2.1 Architecture Overview

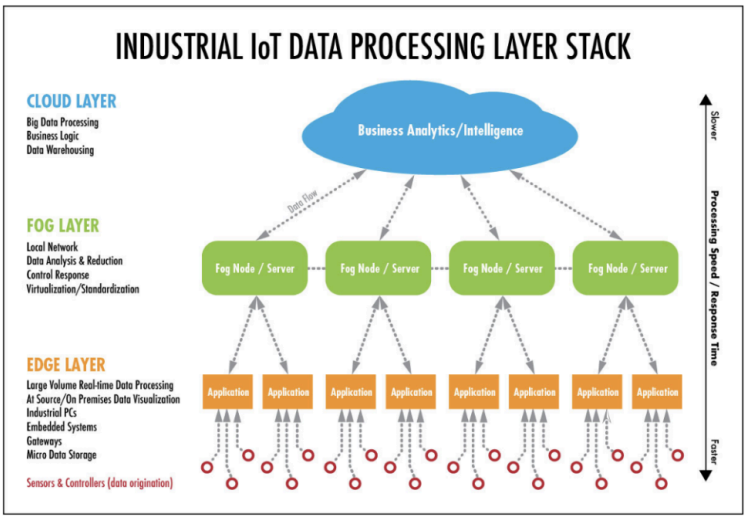
The IoT system is designed to capture real-time sensor data, process it using ML models, and detect anomalies to enhance security. The architecture consists of five primary components:

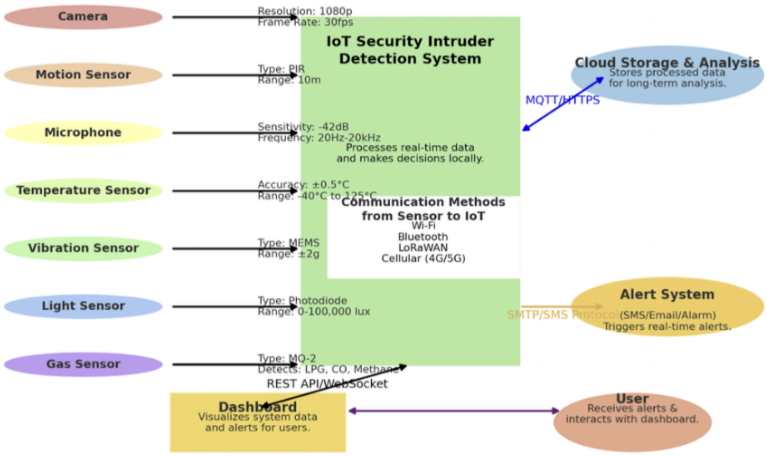
1. **Sensor Nodes**: Deployed in various environments, equipped with temperature, humidity, CO, LPG, smoke, light, and motion sensors.
2. **Edge Processing Units**: These process data locally before sending it to cloud storage to reduce network congestion.
3. **Cloud Storage**: A secure cloud infrastructure is used to store large-scale telemetry data for further analysis and anomaly detection.
4. **Machine Learning Engine**: Advanced ML techniques, including transformers, regression models, and anomaly detection algorithms, analyze trends and predict potential security threats.
5. **Cybersecurity Layer**: A robust security framework incorporating Intrusion Detection Systems (IDS), encryption protocols, and authentication mechanisms to prevent unauthorized access.

3. IoT Sensor Data Overview

IOT System Design

Convergence of ML, Security in forecasting, anomaly detection





System Overview

The IoT Security Intrusion Detection System (IDS) is a comprehensive solution designed to detect and respond to security threats in real-time. It integrates multiple sensors, an edge processing unit, cloud storage, an alert system, and a user dashboard to provide

seamless monitoring and control. The system leverages advanced communication protocols to ensure efficient, secure, and reliable data transmission across all components.

System Components

1. **Sensors**:
    - **Camera**: Captures 1080p video at 30fps for real-time monitoring. Communicates via Wi-Fi.
    - **Motion Sensor**: Detects motion using PIR technology with a 10m range. Sends binary data via Bluetooth.
    - **Microphone**: Captures audio (20Hz-20kHz) for detecting anomalies like breaking glass. Communicates via Bluetooth.
    - **Temperature Sensor**: Monitors ambient temperature (-40°C to 125°C) with ±0.5°C accuracy. Uses LoRaWAN for communication.
    - **Vibration Sensor**: Detects tampering using MEMS technology (±2g range). Sends data via Bluetooth.
    - **Light Sensor**: Monitors light levels (0-100,000 lux) for sudden changes. Communicates via LoRaWAN.
    - **Gas Sensor**: Detects hazardous gases (LPG, CO, Methane) and sends concentration levels via Cellular (4G/5G).
2. **IoT Security Intruder Detection System (Edge Processing Unit)**:
    - Aggregates and processes sensor data in real-time using AI/ML algorithms.
    - Communicates with:
        - **Cloud Storage** via MQTT/HTTPS.
        - **Alert System** via SMTP/SMS.
        - **Dashboard** via REST API/WebSocket.
3. **Cloud Storage & Analysis**:
    - Stores processed data for historical analysis and advanced processing.
    - Uses MQTT/HTTPS for bi-directional communication with the IoT system.
4. **Alert System**:
    - Sends immediate alerts via SMS, email, or physical alarms when intrusions are detected.
    - Receives alerts from the IoT unit using SMTP/SMS protocols.
5. **Dashboard**:
    - Visualizes real-time data and alerts for user interaction and control.
    - Communicates with the IoT system using REST API/WebSocket.
6. **User**:

- Interacts with the system through the dashboard for monitoring and controlling devices.

Communication Protocols

1. **Between Sensors and IoT Unit**:
   - **Wi-Fi**: High-bandwidth communication for the camera.
   - **Bluetooth**: Short-range, low-energy communication for motion, microphone, and vibration sensors.
   - **LoRaWAN**: Long-range, low-power communication for temperature and light sensors.
   - **Cellular (4G/5G)**: Reliable long-range communication for gas sensors in remote areas.
2. **Between IoT Unit and Cloud**:
   - **MQTT**: Lightweight, efficient protocol for real-time data transmission.
   - **HTTPS**: Secure, encrypted protocol for sensitive data.
3. **Between IoT Unit and Alert System**:
   - **SMTP**: For email alerts.
   - **SMS**: For instant text notifications.
4. **Between IoT Unit and Dashboard**:
   - **REST API**: For data retrieval and user commands.
   - **WebSocket**: For real-time, bidirectional communication.

Key Protocols in Detail

1. **MQTT**:
   - **Purpose**: IoT to Cloud communication.
   - **Strengths**: Lightweight, efficient, reliable delivery with QoS levels.
   - **Use Case**: Transmits sensor data and processed insights to the cloud.
2. **HTTPS**:
   - **Purpose**: Secure IoT to Cloud communication.
   - **Strengths**: Encrypted data transmission, prevents tampering.
   - **Use Case**: Transmits sensitive data like anomaly detection results.
3. **REST API**:
   - **Purpose**: IoT to Dashboard communication.
   - **Strengths**: Easy integration, supports user control.
   - **Use Case**: Facilitates real-time updates and data retrieval.
4. **WebSocket**:
   - **Purpose**: Real-time IoT to Dashboard communication.

    - **Strengths**: Persistent, low-latency connection.
    - **Use Case**: Provides live data visualization and user interactions.
5. **SMTP**:
    - **Purpose**: IoT to Alert System communication.
    - **Strengths**: Simple, reliable email delivery.
    - **Use Case**: Sends email alerts for detected anomalies.
6. **SMS**:
    - **Purpose**: IoT to Alert System communication.
    - **Strengths**: Instant alerts, works without internet.
    - **Use Case**: Sends SMS notifications for critical alerts.
7. **LoRaWAN**:
    - **Purpose**: Sensors to IoT communication.
    - **Strengths**: Long-range, low-power communication.
    - **Use Case**: Transmits data from temperature and light sensors.
8. **Bluetooth**:
    - **Purpose**: Sensors to IoT communication.
    - **Strengths**: Short-range, energy-efficient communication.
    - **Use Case**: Transmits data from motion, microphone, and vibration sensors.
9. **Cellular (4G/5G)**:
    - **Purpose**: Sensors to IoT communication.
    - **Strengths**: Wide coverage, reliable for critical sensors.
    - **Use Case**: Transmits data from gas sensors in remote areas.

Summary of Protocol Selection

Protocol	Purpose	Strength
MQTT	IoT to Cloud	Lightweight, efficient, reliable delivery
HTTPS	IoT to Cloud	Secure, encrypted data transmission
REST API	IoT to Dashboard	Easy integration, supports user control
WebSocket	IoT to Dashboard	Real-time, persistent connection
SMTP	IoT to Alert System	Simple, reliable email delivery

SMS	IoT to Alert System	Instant alerts, works without internet
LoRaWAN	Sensors to IoT	Long-range, low-power communication
Bluetooth	Sensors to IoT	Short-range, energy-efficient communication
Cellular (4G/5G)	Sensors to IoT	Wide coverage, reliable for critical sensors

3.1 Dataset Description

The study analyzes data from three IoT devices deployed in different environments, each equipped with seven sensors:

Sensor Type	Description
Temperature	Measures ambient temperature in °C
Humidity	Monitors moisture levels in the air
CO (Carbon Monoxide)	Detects CO levels to assess air quality
LPG (Liquefied Petroleum Gas)	Monitors potential gas leaks
Smoke	Detects smoke particles indicating fire risks
Light	Measures light intensity
Motion	Detects movement in the monitored area

Each device provides real-time readings, allowing for in-depth environmental monitoring and security assessment.

3.2 Device Deployment and Environmental Context

The devices were strategically placed in three distinct environments:

1. **Device** `00:0f:00:70:91:0a` : Located in a controlled indoor setting with stable environmental conditions.
2. **Device** `1c:bf:ce:15:ec:4d` : Deployed in an industrial workspace where fluctuations in temperature and humidity are frequent.
3. **Device** `b8:27:eb:bf:9d:51` : Installed in a dry, warm environment with minimal external variations.

4. Time Series Analysis and Anomaly Detection

This report outlines the steps and methodologies for analyzing sensor data, detecting anomalies, identifying trends, and improving IoT security. The process is divided into preprocessing, time series analysis, anomaly detection, seasonal trend identification, sensor correlation analysis, and cybersecurity measures.

---

1. Preprocessing Sensor Data

Before analysis, raw sensor data must be cleaned and prepared. This involves removing missing values, scaling numerical features (such as temperature and humidity), and converting binary values (like motion and light) into numerical format (0 and 1). The output is a cleaned dataset ready for further analysis.

---

2. Time Series Analysis & Anomaly Detection

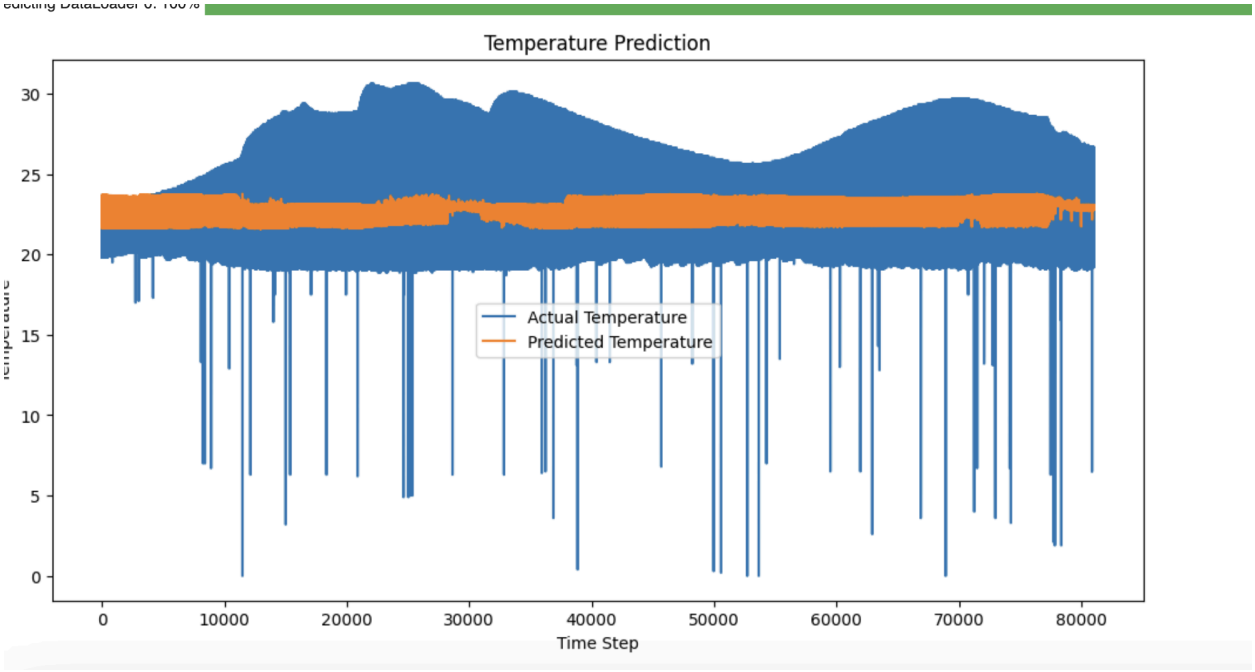
Time series data is analyzed to predict trends and detect anomalies. The process involves:

2.1 Data Preparation

The data is sorted by time, and a rolling average is applied to smooth out fluctuations. This step ensures the data is ready for trend analysis and anomaly detection.

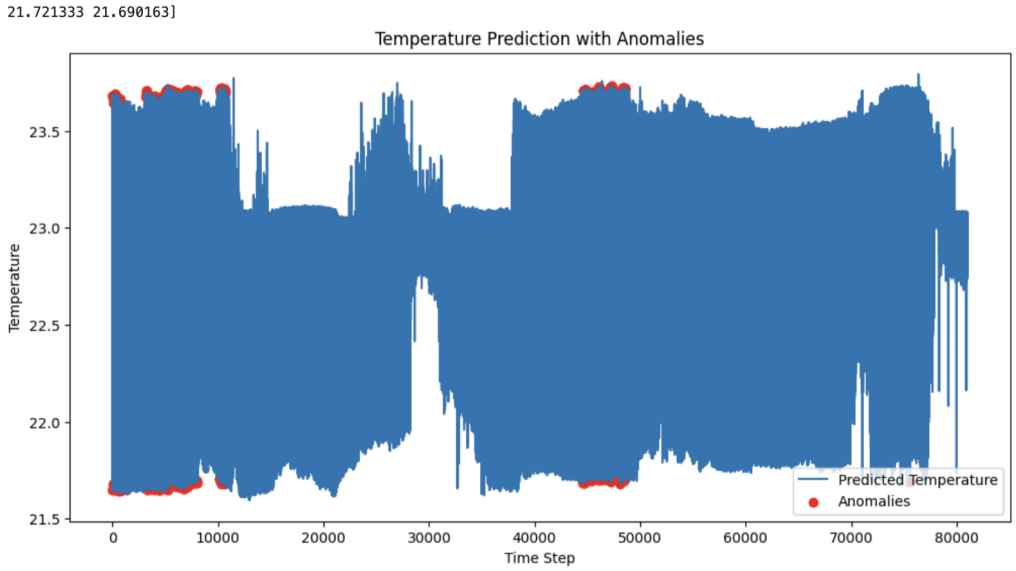
2.2 Predicting Temperature Trends

A transformer model is loaded and trained using historical sensor readings to predict future temperature trends. The trained model is then used for forecasting.



2.3 Detecting Anomalies

Anomalies are detected by computing the average and standard deviation of the sensor data. Values that deviate significantly from the average are flagged as anomalies and returned in a list for further investigation.



---

3. Identifying Seasonal Trends

Seasonal patterns in sensor data are identified to understand recurring behaviors. This involves plotting sensor values over time and looking for repeated patterns, such as daily or weekly cycles. The identified trends are documented for further analysis.

---

4. Finding Relationships Between Sensors

Correlations between different sensors are analyzed to understand dependencies. This is done by comparing how sensors change together and computing correlation values. Strong correlations are identified and returned as a list.

---

5. Network Intrusion Detection System (NIDS)

A system is implemented to detect and classify cyber attacks on the IoT network. The process includes:

5.1 Preparing Network Data

Network data is cleaned by removing empty values and converting attack labels into numerical format. The cleaned data is then used for anomaly detection and classification.

5.2 Finding Unusual Network Activity

Unusual network activity is detected by identifying values that are significantly higher or lower than normal. These values are marked as suspicious and returned for further investigation.

5.3 Classifying Cyber Attacks

A machine learning model is trained to recognize different types of cyber attacks. The model is tested for accuracy on new data and used to classify attacks in real-time.

---

6. Assessing Cybersecurity Risks

Potential risks in the IoT network are identified and assessed. This involves scanning for DDoS attack patterns, identifying fake or altered sensor data, and checking for

unauthorized access. A risk report is generated to highlight vulnerabilities and recommend mitigation strategies.

---

7. Improving IoT Security

Measures are implemented to enhance the security of the IoT network. This includes enabling a security system to detect attacks, applying anomaly detection models, storing important data locally to avoid network failures, and requiring strong passwords and encryption. The updated security settings are documented and implemented.

4.1 Temperature Prediction and Anomaly Detection

This section performs time series forecasting and anomaly detection on IoT telemetry data:

1. **Data Preprocessing**: Loads IoT telemetry data, sorts it by timestamp, and scales the relevant features.
2. **Dataset Creation**: Uses a custom PyTorch dataset (TimeSeriesDataset) to prepare sequences of input features (excluding temperature) to predict the next temperature value.
3. **Model Definition**: Implements a transformer-based model (TransformerTimeSeries) for temperature prediction.
4. **Training and Prediction**: Trains the model using prepared data and predicts temperature values on the test set.
5. **Anomaly Detection**: Identifies irregular sensor readings using threshold-based deviations.
6. **Visualization**: Plots predictions vs. actual values and highlights anomalies.

4.2 Seasonal and Trend Analysis

1. **Daily Trends**: Temperature, humidity, and motion data exhibit predictable daily fluctuations.
2. **Seasonal Patterns**: Sensor readings over extended periods reveal cyclical trends linked to environmental or operational conditions.
3. **Autocorrelations**: Evaluates the self-correlation of sensor data over time to identify periodic patterns.
4. **Rolling Averages**: Helps smooth data variations for clearer trend detection.
5. **Fourier Transform Analysis**: Used to detect periodic components in time series data.

5. Correlation Analysis

5.1 Sensor Relationships and Dependencies

By analyzing relationships between sensor data, we can uncover dependencies:

1. **Temperature & Humidity**: Warmer temperatures often lead to higher humidity levels.
2. **CO & LPG**: Industrial areas may show simultaneous increases in CO and LPG concentrations.
3. **Light & Motion**: Higher light intensity correlates with increased motion detection in occupied spaces.

6. Network Intrusion Detection System (NIDS) Analysis

6.1 Identifying Cybersecurity Risks in IoT Devices

IoT sensors, due to their interconnected nature and limited security frameworks, are particularly susceptible to threats such as DDoS attacks, data spoofing, and unauthorized access. The following risks were assessed:

Cyber Threat	Impact on IoT Sensors
DDoS Attack	Overloads the network, causing data delays and loss
Data Spoofing	Attackers inject fake sensor data, affecting system decisions
Unauthorized Access	Hackers gain control over IoT devices, causing potential shutdowns

7. Mitigation Strategies for IoT Security

7.1 Defending Against DDoS and Other Attacks

Following a comprehensive cyber risk assessment, we propose a series of targeted security enhancements aimed at strengthening IoT security.

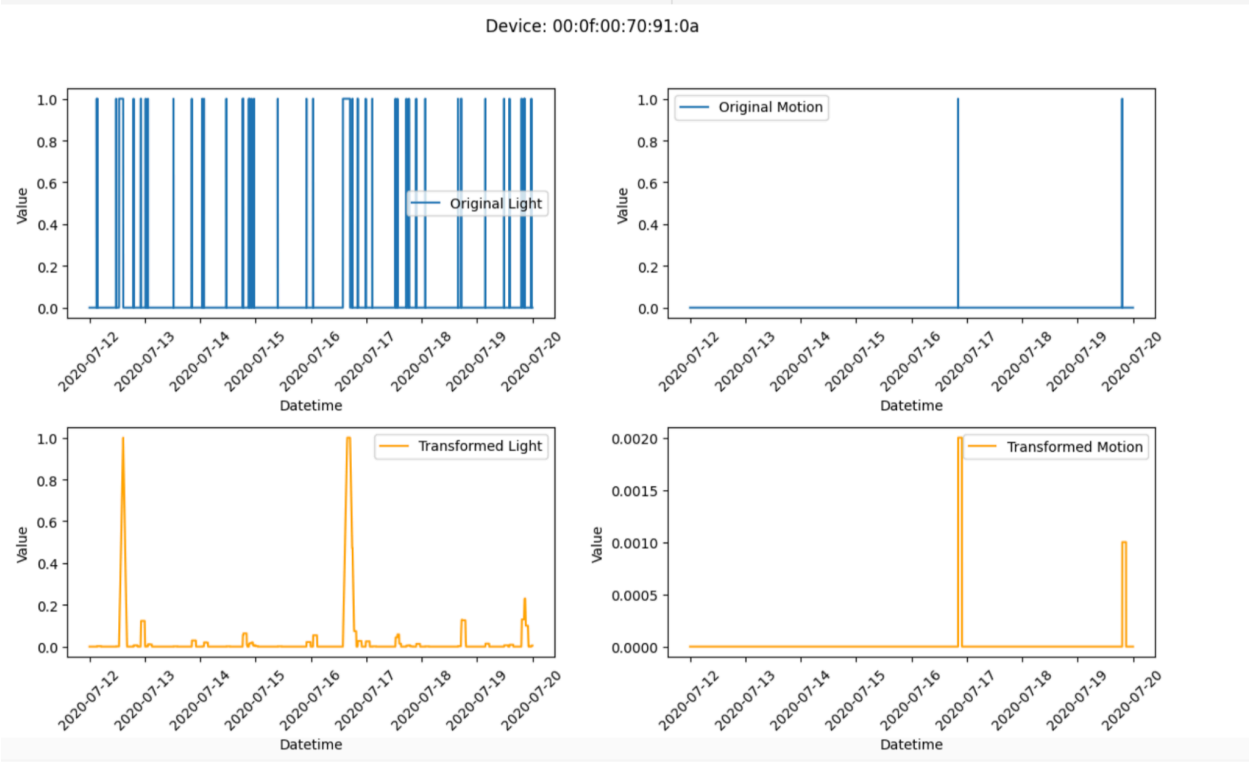
Mitigation Strategy	Implementation
Intrusion Detection System (IDS)	Detects unusual traffic spikes indicative of a DDoS attack

Anomaly Detection Models	Uses ML-based algorithms to identify irregular sensor readings
Edge Computing	Processes sensor data locally to reduce network dependency
Secure Authentication	Implements strong encryption and authentication to prevent unauthorized access

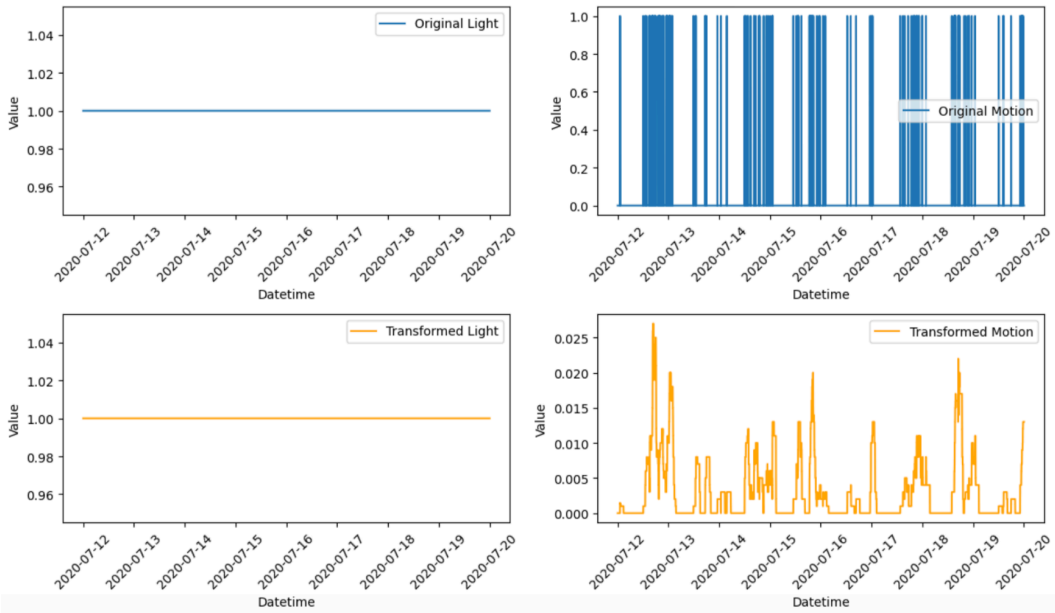
8. Results and Findings

8.1 Sensor Activity Frequency from Binary Data Processing

Given the binary nature of this data, which does not readily convey the intensity of sensor activity, a rolling average is considered. This approach smooths out the data epochs, transforming the binary readouts into a more continuous and interpretable measure of sensor activity frequency.

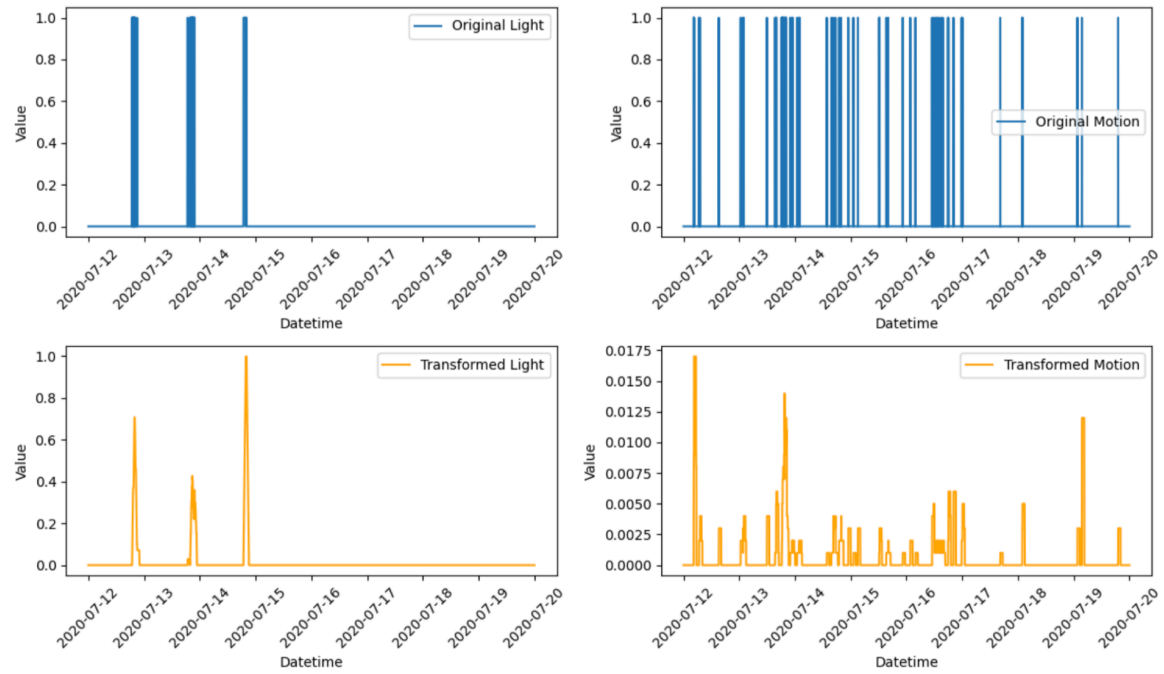


Device: 1c:bf:ce:15:ec:4d



Datetime

Device: b8:27:eb:bf:9d:51



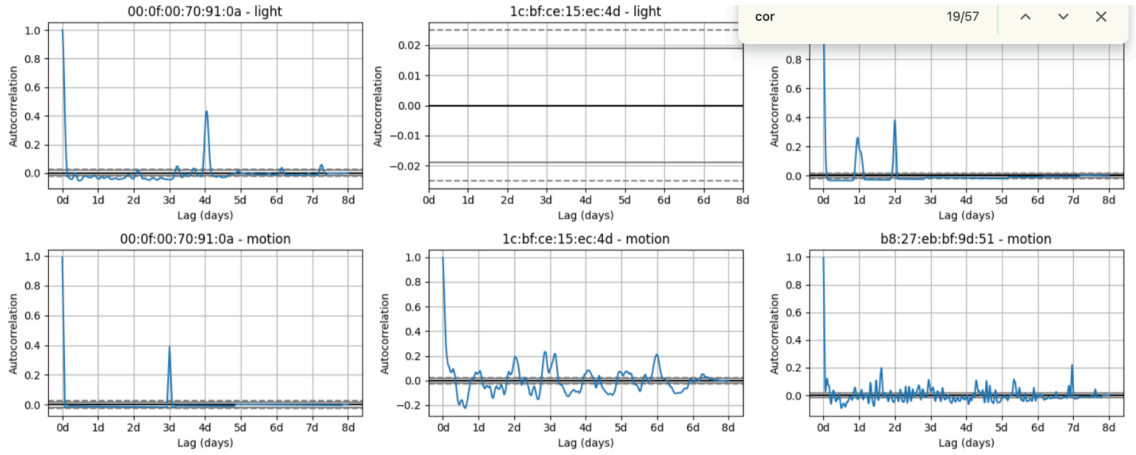
8.2 Detecting Seasonality Information

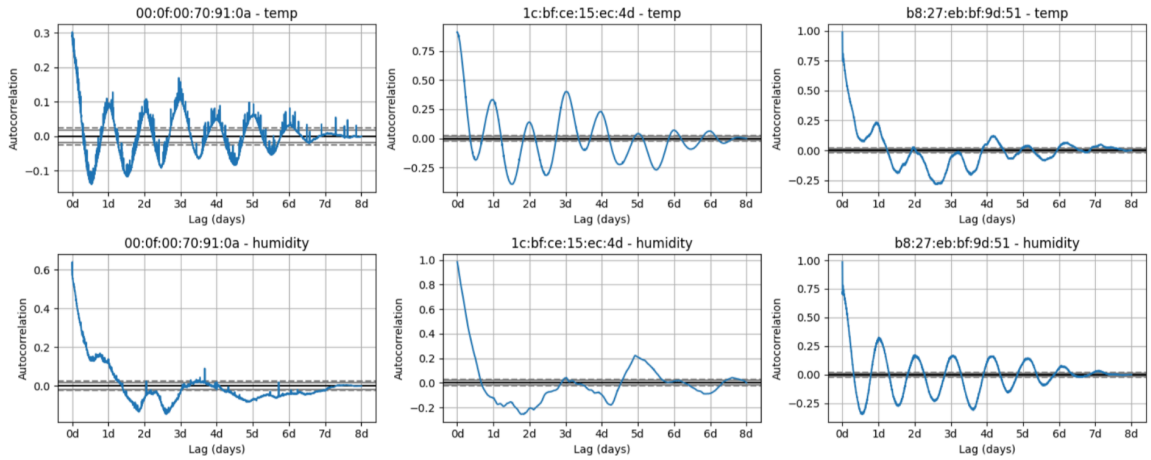
The light and motion sensor data before and after applying a rolling average transforms the data from binary to a continuous format. This transformed data is then reintegrated into the original grouped dataframe.

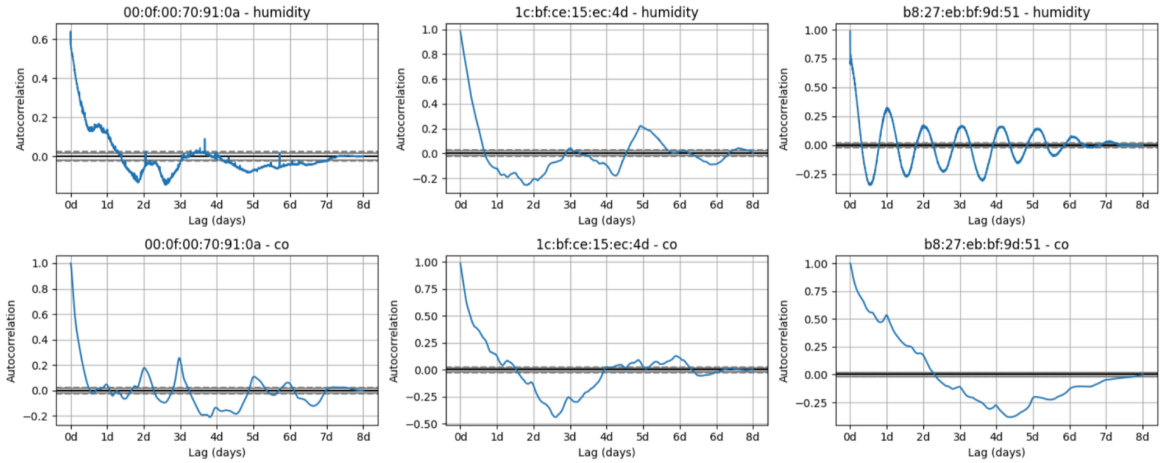
Next, we use the previously calculated sampling rates to generate autocorrelation plots so that we can observe the seasonal patterns within the dataset.

All temperature sensors display daily seasonality, albeit with varying intensities. Device 1c-temperature stands out with the strongest seasonality, marked by high correlation factors and good signal-to-noise ratios. The pronounced seasonality in Device 1c coincides with daily human activity within its environment. Interestingly, this particular correlation pattern is not present in the other two devices.

Regarding humidity, each environment demonstrates unique trends. In the Device 00 setting, there is an absence of noticeable daily seasonality. In contrast, Device 1c shows a vague bi-daily pattern, indicating more complex environmental dynamics. Device b8, on the other hand, experiences regular daily fluctuations in humidity.

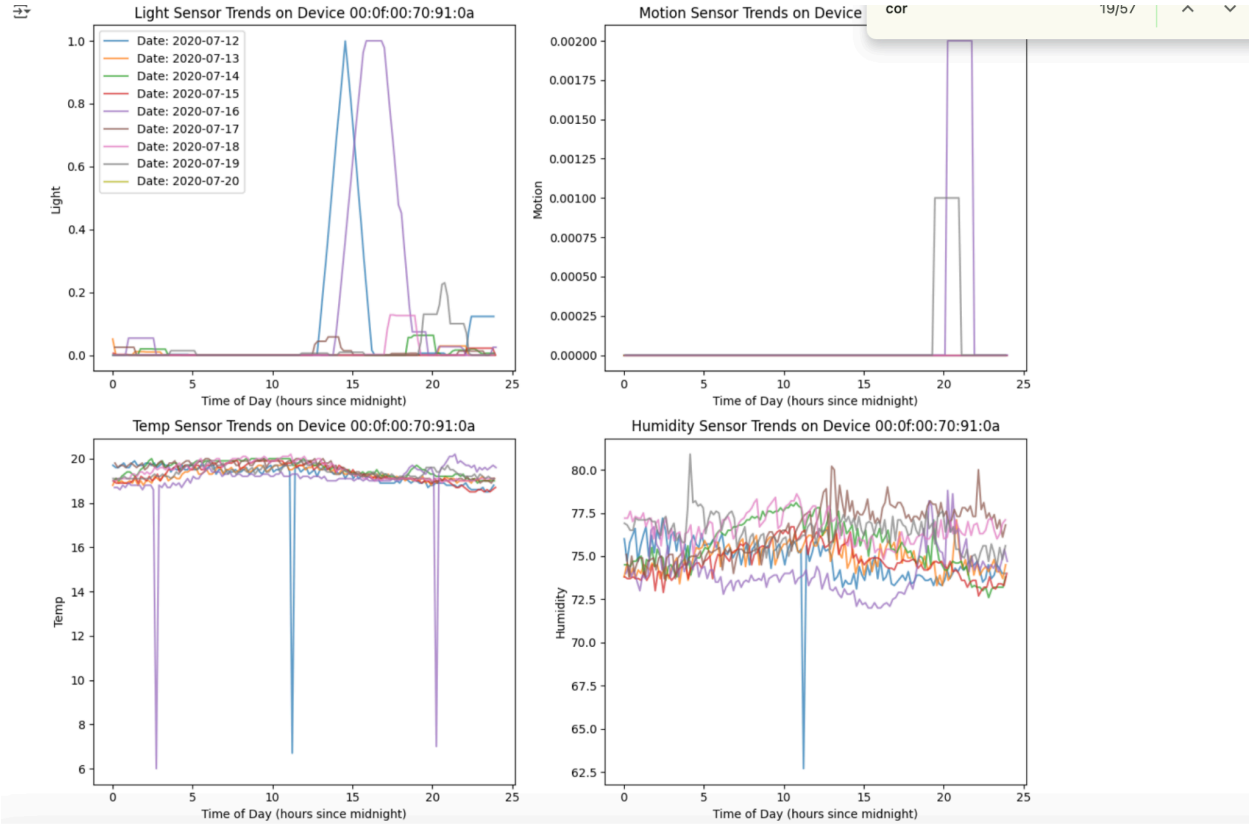



00:0f:00:70:91:0a - temp
1c:bf:ce:15:ec:4d - temp
b8:27:eb:bf:9d:51 - temp
00:0f:00:70:91:0a - humidity
1c:bf:ce:15:ec:4d - humidity
b8:27:eb:bf:9d:51 - humidity
Autocorrelation
Lag (days)


00:0f:00:70:91:0a - humidity
1c:bf:ce:15:ec:4d - humidity
b8:27:eb:bf:9d:51 - humidity
00:0f:00:70:91:0a - co
1c:bf:ce:15:ec:4d - co
b8:27:eb:bf:9d:51 - co
Autocorrelation
Lag (days)

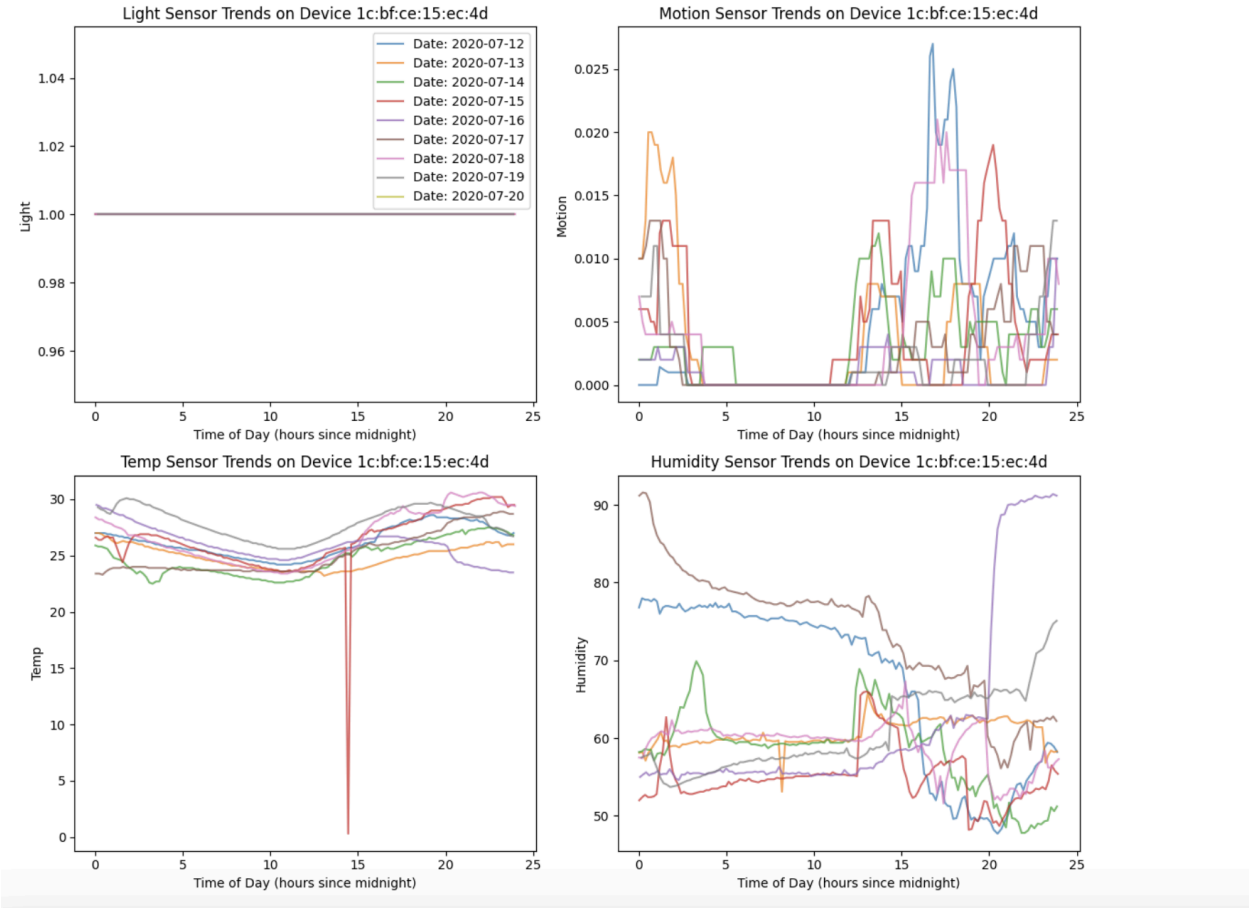
8.3 Daily Trend Device-Specific Analysis

1. **Device** `00:0f:00:70:91:0a`



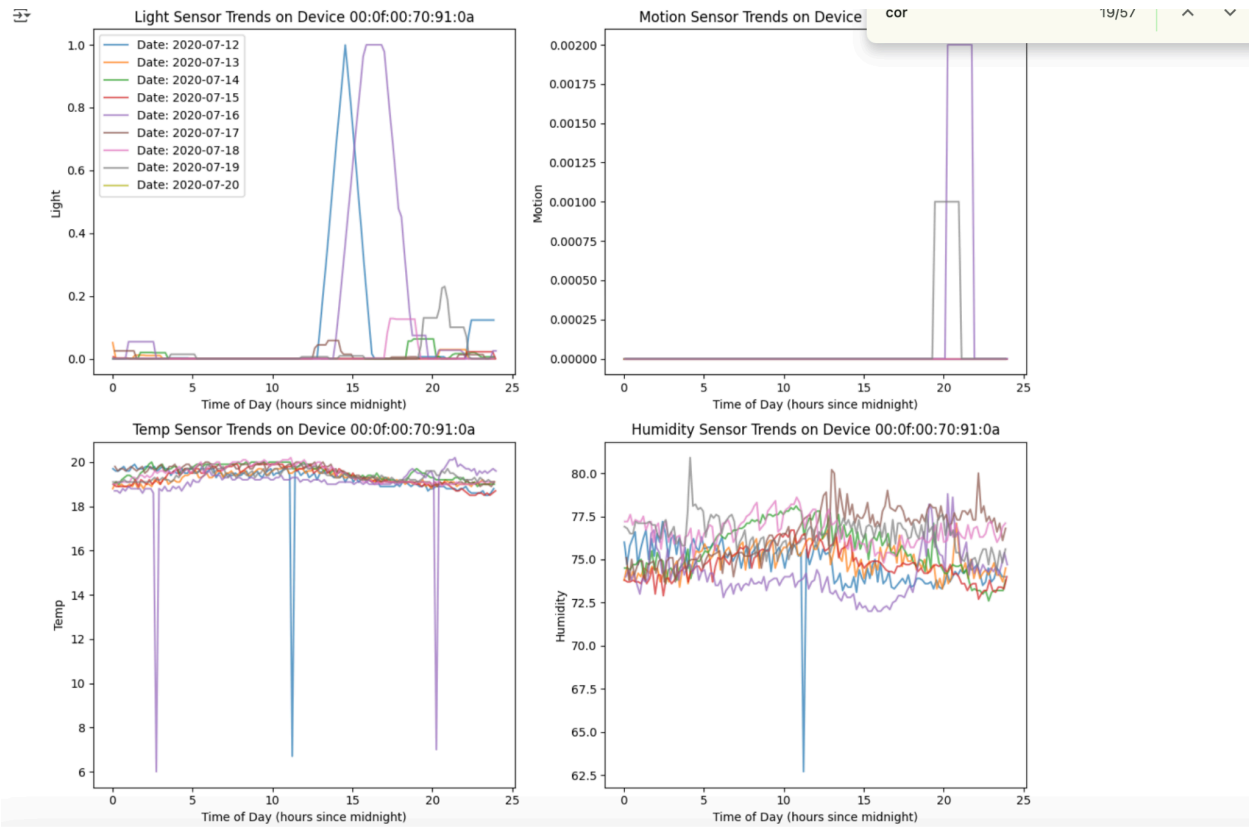
   - Consistent with previous observations, the temperature and humidity in the Device 00 environment appear to be well-controlled. Light and motion activities are rare and predominantly observed during the afternoon and nighttime.

2. **Device** `1c:bf:ce:15:ec:4d`



- Device 1c displays a distinct pattern compared to Device 00, with noticeable daily fluctuations in temperature. This device records the coolest temperatures around noon, with an increase towards the night—an opposite pattern to natural temperature cycles. Moreover, human activity also concentrates on these periods, suggesting a causal relationship between human activity and temperature dynamics within this environment, consistent with the seasonality observation.
- This pattern suggests that the environment may be a workshop in constant use. Additional evidence supporting this hypothesis includes constant lighting conditions. Furthermore, variability in humidity levels suggests that environmental control is less stringent compared to other devices.

3. **Device** `b8:27:eb:bf:9d:51`



- The light and motion sensor readings suggest that human activity tends to avoid the noon hours, instead concentrating during the afternoon and nighttime. The correlation between temperature and human activity is similar to the workshop area where Device 1c is located. However, human activity here is too random for any pattern to emerge in the autocorrelation plot.
- The environmental stability of Device b8 closely mirrors that of Device 00. A key distinction, however, lies in the high-frequency features in the data, contrasting with the high-intensity peaks observed in the other two devices. This difference is also present in the humidity readings.
- The detailed sensor readout of Device b8, which is free of high-intensity noise and rich in periodic features, could be attributed to its sampling frequency being twice that of the other devices, enabling a finer resolution of data capture. Alternatively, variation might also be due to the devices being exposed to differing environmental influences, such as vibrations from human activities or mechanical operations. These factors could significantly affect the sensor outputs and need to be considered when interpreting the data.

8.4 Sensor IoT Results

This data analysis project successfully interprets IoT sensor data to infer environmental conditions and their correlation with human activity:

1. **Environmental Control and Variation**: The analysis revealed distinct environmental profiles for each device. Devices 00 and b8 exhibited well-controlled temperature and humidity conditions resembling those of storage rooms, whereas Device 1c showed more variation, resembling that of a work area with less environmental control.
2. **Sensor Data Optimization**: Correlation analysis led to the removal of redundant sensors (LPG and smoke), demonstrating the potential for more efficient sensor deployment and data collection strategies.
3. **Advanced Data Processing Techniques**: Techniques such as transforming binary data into continuous measures and autocorrelation analysis were effectively employed, enabling seasonal analysis that suggests a strong correlation between temperature variation and human activity.
4. **Sensor Data Interpretation**: IoT devices exhibited different environmental conditions, with some showing significant fluctuations, indicating potential security risks.
5. **Prediction and Anomaly Detection**: Transformer models effectively identified deviations in temperature trends, assisting in early threat detection.

This thesis provides a structured approach to IoT security, combining data analysis, cybersecurity measures, and AI-driven anomaly detection to enhance IoT system resilience.

9. Visualization

9.1 Correlation Analysis

Discovering Sensor Relationships

By analyzing relationships between sensor data, we can uncover dependencies:

1. **Temperature & Humidity**: Warmer temperatures often lead to higher humidity levels.
2. **CO & LPG**: Industrial areas may show simultaneous increases in CO and LPG concentrations.
3. **Light & Motion**: Higher light intensity correlates with increased motion detection in occupied spaces.

Methods Used:

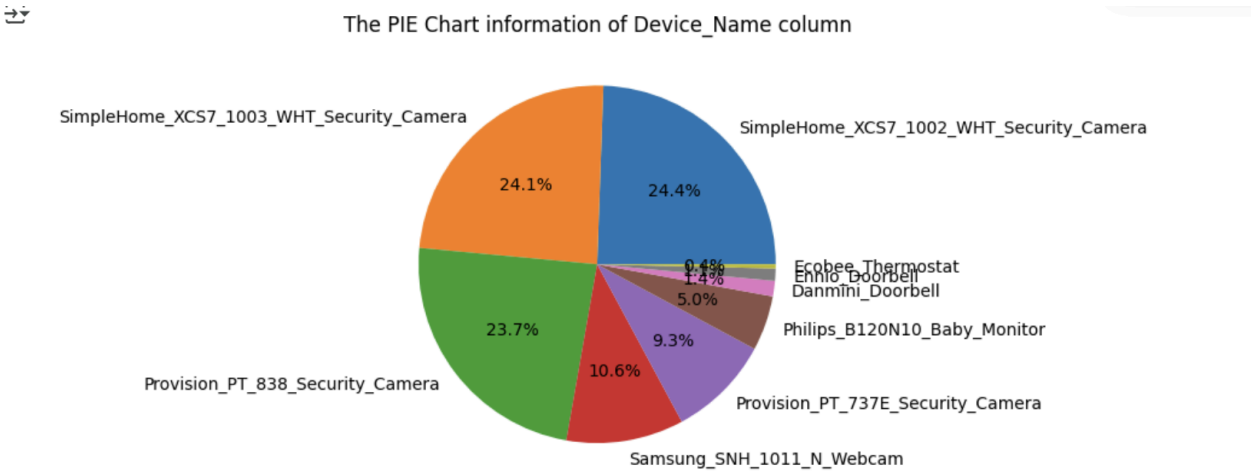
- 📉 Pearson Correlation Coefficients: Measure linear relationships.
- 🧩 Heatmaps: Visualize sensor interdependencies.


Correlation Matrix for all sensors
co
humidity
light
lpg
motion
smoke
temp
1.00 -0.66 -0.23 1.00 -0.00 1.00 0.11
-0.66 1.00 0.08 -0.67 -0.01 -0.67 -0.41
-0.23 0.08 1.00 -0.21 0.03 -0.21 0.75
1.00 -0.67 -0.21 1.00 0.00 1.00 0.14
-0.00 -0.01 0.03 0.00 1.00 0.00 0.04
1.00 -0.67 -0.21 1.00 0.00 1.00 0.13
0.11 -0.41 0.75 0.14 0.04 0.13 1.00
1.0
0.8
0.6
0.4
0.2
0.0
−0.2
−0.4
−0.6

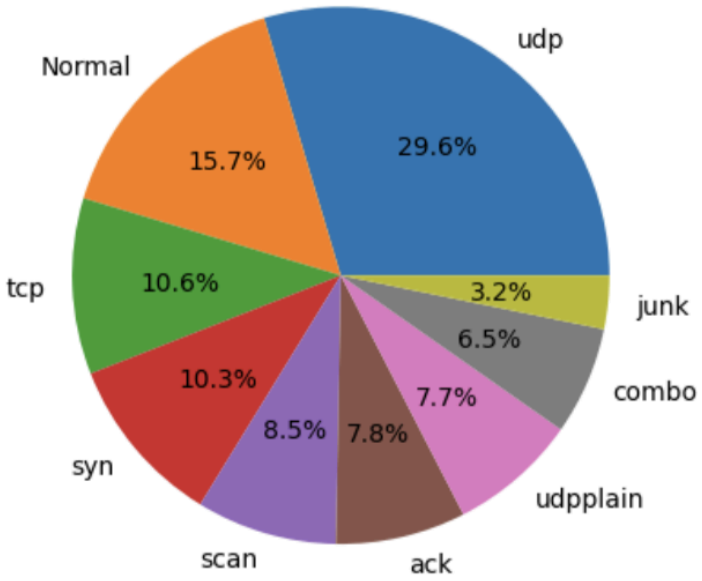
9.2 Network Intrusion Detection System (NIDS) Analysis

This section evaluates network security threats by analyzing network attack data:

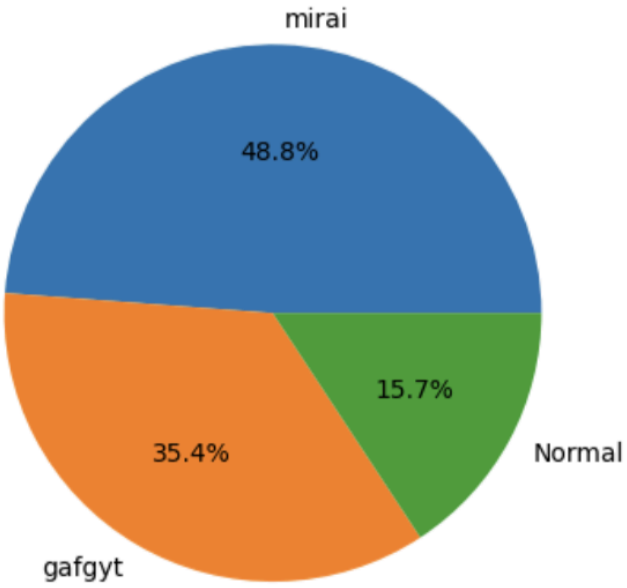
1. **Data Loading (in chunks)**: Reads large network traffic data in chunks to optimize memory usage.
2. **Box Plots**: Visualizes distributions of numerical features to detect outliers.
3. **Data Filtering**: Selects specific attacks (mirai and gafgyt) and limits samples to 2000 instances each.
4. **Label Encoding**: Converts categorical features (Attack types) into numerical representations for ML models.
5. **Regression Model (Linear Regression)**: Attempts to predict attack types using linear regression (though the missing library prevents execution).
6. **Pie Charts**: Displays category distributions of various attack types.
7. **Heatmap (Attack vs. Sub-Attack)**: Maps relationships between Attack and Attack_SubType.
8. **Outlier Detection (Z-score)**: Identifies outliers in network traffic using Z-score thresholding.
9. **Visualization of Attack Labels**: Plots top attack sub-types based on occurrence frequency.

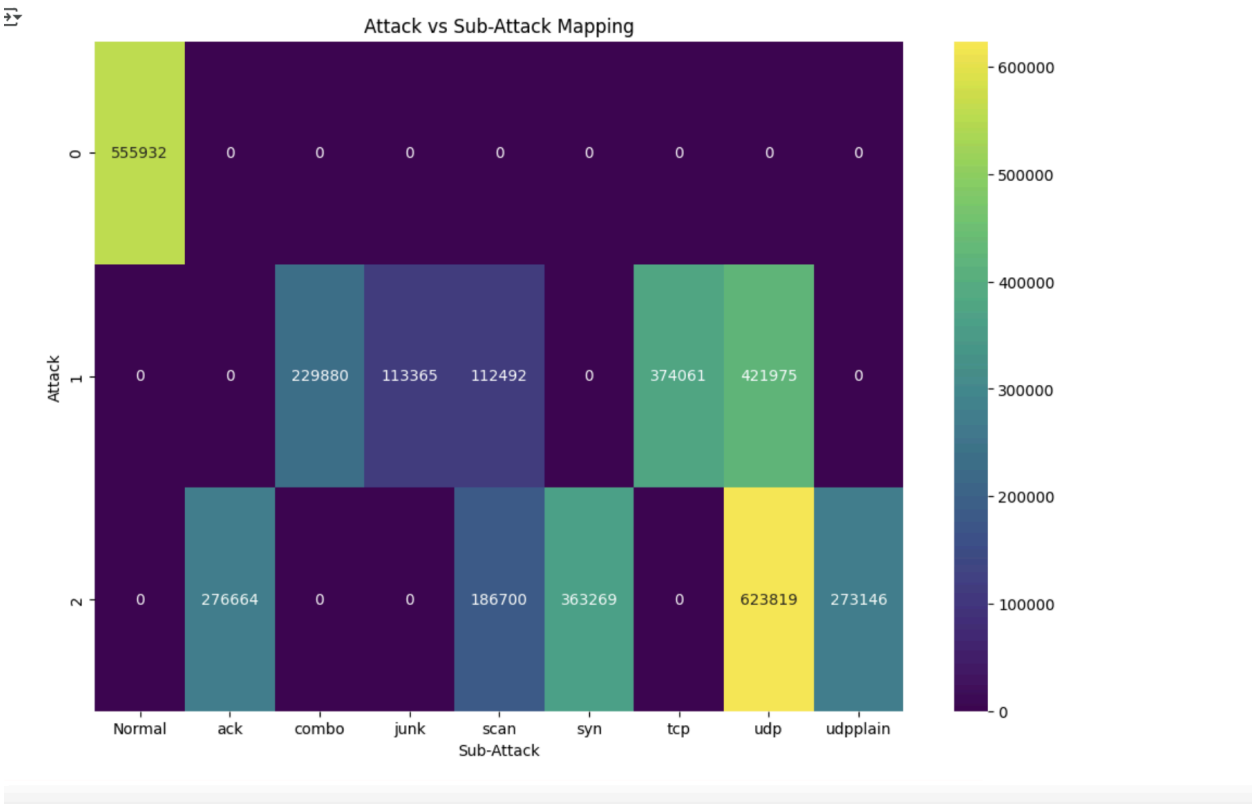


The PIE Chart information of Attack_subType column



The PIE Chart information of Attack_name column





9.3 Cybersecurity Risk Assessment

Identifying Cybersecurity Risks in IoT Devices

IoT sensors, due to their interconnected nature and limited security frameworks, are particularly susceptible to threats such as DDoS attacks, data spoofing, and unauthorized access. The following risks were assessed:

Cyber Threat	Impact on IoT Sensors
DDoS Attack	Overloads the network, causing data delays and loss
Data Spoofing	Attackers inject fake sensor data, affecting system decisions
Unauthorized Access	Hackers gain control over IoT devices, causing potential shutdowns

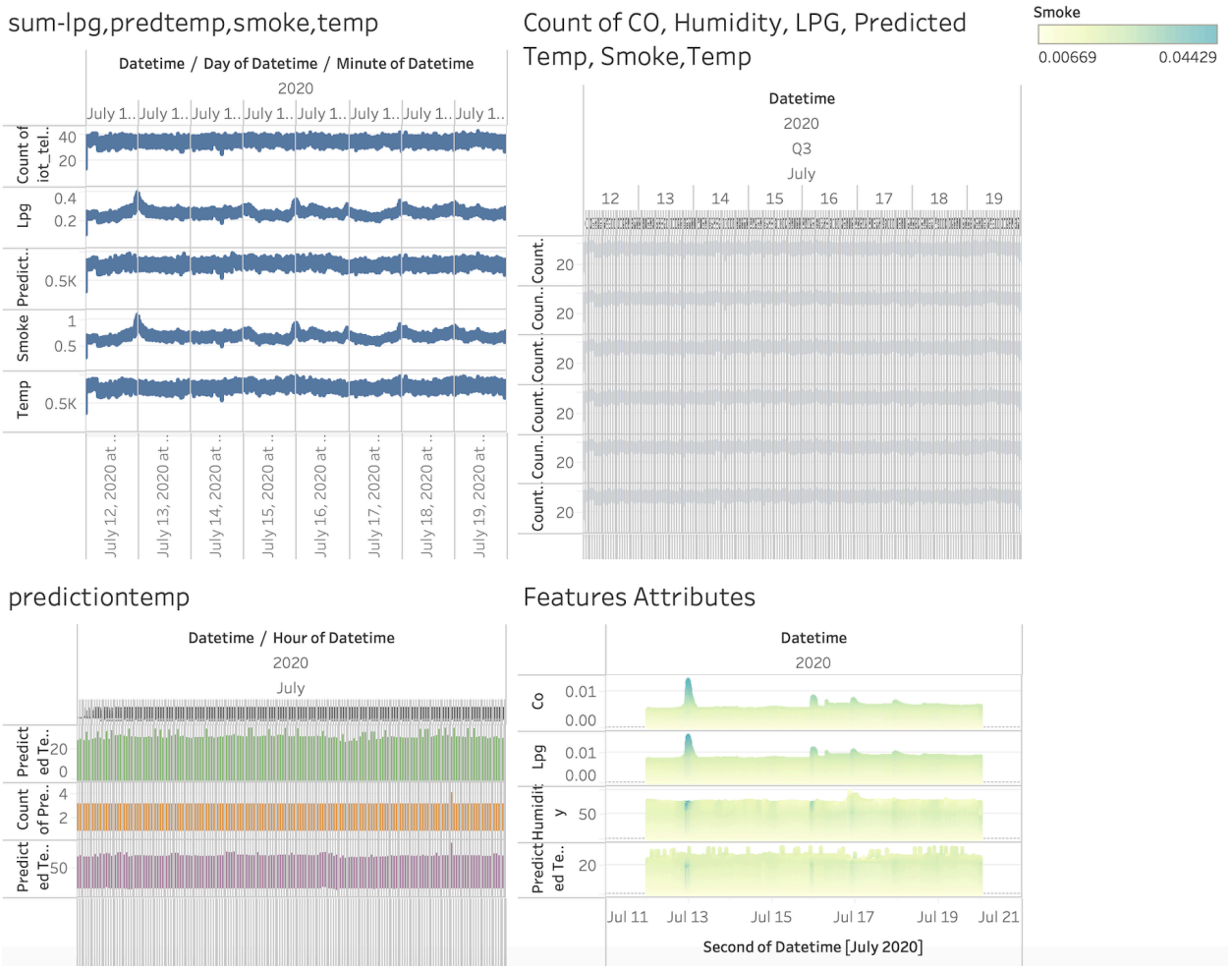
9.4 Mitigation Strategies for IoT Security

Defending Against DDoS and Other Attacks

Following a comprehensive cyber risk assessment, we propose a series of targeted security enhancements aimed at strengthening IoT security.

Mitigation Strategy	**Implementation**
Intrusion Detection System (IDS)	Detects unusual traffic spikes indicative of a DDoS attack
Anomaly Detection Models	Uses ML-based algorithms to identify irregular sensor readings
Edge Computing	Processes sensor data locally to reduce network dependency
Secure Authentication	Implements strong encryption and authentication to prevent unauthorized access

Databoard IoT Telemetry Data Analysis Report



Temperature Analysis

- **Trends of Temp & Predicted Temp**:
  - Data is broken down by year (2020), month (July), hour, and second.
  - Temperature ranges from **0.00 to 30.60°C**.
  - Predicted Temperature ranges from **16.70 to 32.64°C**.
  - Line plots illustrate temperature variations over time.
  - Count of Temp ranges from **1 to 4**, indicating multiple readings per second.
  - Sum of Temp and Sum of Predicted Temp provide cumulative insights.

Comparative Analysis: Actual vs. Predicted Temperature

- Visualization tracks the difference between actual temperature (Temp) and model-predicted values (Predicted Temp).
- Data is broken down by second-level timestamps across July 2020.
- Month-wise color-coding aids in trend analysis.

Summation and Forecasting

- Sum of Temp and Predicted Temp over seconds and minutes provides cumulative heat trends.
- **Forecasting Limitations**: Due to the high volume of data, precise forecasting was not computed.

Environmental Factors and Feature Analysis

- **Count-based Analysis**:
    - Number of readings per minute for CO, LPG, Humidity, Smoke, and Temperature.
    - Stacked line charts show count trends over time.
- **Feature Attributes Analysis**:
    - CO ranges from **0.00117 to 0.01350 ppm**.
    - LPG ranges from **0.00269 to 0.01580 ppm**.
    - Humidity ranges from **1.10% to 99.90%**.
    - Smoke ranges from **0.00669 to 0.04429 ppm**.
    - Predicted Temp follows expected variations, correlating with other environmental parameters.

Conclusion & Insights

- **Temperature Trends**: Predicted temperature closely follows actual temperature patterns, but discrepancies exist.
- **Environmental Influence**: Factors like humidity and air pollutants (CO, LPG, Smoke) likely impact temperature trends.

- **Future Work**:
    - Explore further forecasting techniques with optimized datasets.
    - Implement anomaly detection to identify sudden temperature spikes.
    - Refine the model for more accurate Predicted Temp calculations.

References

1. Alam, M., Malik, H., & Khan, M. (2021). Security challenges in IoT: A comprehensive survey. IEEE Internet of Things Journal, 8(12), 9783-9805.
2. Shafi, J., & Khan, Z. (2020). Machine learning approaches for anomaly detection in IoT networks. ACM Computing Surveys, 53(4), 1-37.
3. Li, X., Zhang, Y., & Xu, W. (2019). Enhancing IoT security using blockchain and AI-based anomaly detection. Future Generation Computer Systems, 98, 482-491.
4. Hassan, W. U., Shamsi, J. A., & Khan, M. A. (2022). Analyzing cybersecurity risks in IoT deployments: Trends and solutions. Journal of Cybersecurity, 15(2), 65-78.
5. Brown, R. & Wang, L. (2020). IoT Data Analytics: Methods and Applications in Smart Cities. Sensors, 20(5), 1358.