e-ISSN: 2582-5208

International Research Journal of Modernization in Engineering Technology and Science

(Peer-Reviewed, Open Access, Fully Refereed International Journal)

Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

DETECTION AND MITIGATION OF CYBER THREATS IN IOT-BASED EMBEDDED SYSTEMS USING MACHINE LEARNING MODELS IN DATA FORENSICS

Goodness Tolulope Adewale[*1]

[*1]Technical Product Manager, Business Intelligence And Data Analytics, Ascot Group, Inc. NY, USA.

DOI: https://www.doi.org/10.56726/IRJMETS63576

ABSTRACT

The increasing integration of Internet of Things (IoT) embedded systems in critical sectors like healthcare has heightened concerns over cybersecurity threats. These systems, due to their interconnected and often resource-constrained nature, are vulnerable to attacks that can compromise sensitive data and disrupt vital operations. This article examines the use of ML models to detect and mitigate cyber threats within IoT-based embedded systems, with a particular focus on healthcare environments. ML models offer robust solutions for data forensics by identifying anomalies in network behaviour, distinguishing between normal and malicious activities, and enhancing the accuracy of threat detection. Key techniques include training datasets on network patterns associated with both regular and suspicious activities, enabling these models to learn and recognize cyber threats effectively. The study delves into various ML methods, such as anomaly detection and supervised classification, to understand their application in IoT threat mitigation. Additionally, it explores the unique challenges faced in securing IoT systems, such as limited computational power, and the importance of secure software implementations to prevent vulnerabilities. Through case studies and experimental evaluations, the article highlights the effectiveness of ML models in improving the reliability and security of IoT-based embedded systems. The discussion extends to future implications for cybersecurity in IoT, emphasizing the potential for advanced, adaptive models to ensure proactive threat mitigation and data protection in sensitive applications.

Keywords: IoT-Based Embedded Systems, Cybersecurity, ML Models, Data Forensics, Threat Detection, Anomaly Detection.

I. INTRODUCTION

1.1 Background and Motivation

The Internet of Things (IoT) has experienced rapid growth in recent years, with embedded systems increasingly integrated into diverse sectors such as healthcare, agriculture, and smart cities. These IoT-based systems, comprising interconnected devices that collect, share, and analyse data in real-time, have revolutionized operations, providing significant improvements in efficiency, decision-making, and user experience. In the healthcare sector, for example, IoT devices like wearables, smart medical implants, and remote patient monitoring systems are transforming patient care by offering continuous monitoring and early detection of health anomalies, which in turn enables better clinical outcomes and cost reduction [1, 2].

However, the pervasive nature of IoT systems introduces substantial cybersecurity challenges. The interconnectivity of IoT devices creates a broad attack surface for cybercriminals, making these systems highly vulnerable to a range of cyber threats, including unauthorized data access, malware attacks, and denial-of-service (DoS) incidents. The resource limitations of many IoT devices—such as limited processing power, memory, and energy constraints—further complicate their defense against such attacks [3]. These challenges are particularly critical in sensitive environments such as healthcare, where compromised systems can result in significant privacy breaches and, in extreme cases, threaten patient safety [4].

Given the increasing number of cyber threats targeting IoT ecosystems, there is a pressing need for innovative approaches to detect and mitigate these risks. ML (ML), with its ability to analyse vast amounts of data and identify anomalies or patterns indicative of malicious behaviour, has shown promise as a powerful tool for enhancing cybersecurity in IoT systems [5].

1.2 Scope of the Study

This study seeks to address the critical issue of cybersecurity in IoT-based embedded systems, focusing specifically on the detection and mitigation of cyber threats through ML and data forensics. The research will explore how ML models can be employed to detect anomalous behaviour in IoT networks and embedded devices, helping to identify cyber threats such as unauthorized access, data exfiltration, and denial-of-service (DoS) attacks. Additionally, the study will investigate the role of data forensics in IoT environments, particularly in tracing malicious activity and recovering vital evidence of security breaches.

The primary scope of this study includes a detailed review of IoT-based system vulnerabilities and the current state of threat detection and mitigation methods. It will analyse how data forensics can be integrated into IoT systems for real-time monitoring and post-incident analysis, contributing to a more effective cybersecurity posture. By employing ML algorithms, the study will assess how automated anomaly detection can improve the accuracy and efficiency of threat identification, thereby reducing response time and enhancing system protection.

The significance of this research lies in its potential to advance cybersecurity practices within IoT ecosystems, particularly in sensitive sectors like healthcare. By leveraging cutting-edge technologies such as ML and data forensics, the study aims to offer novel solutions to mitigate the security risks that IoT systems face, ultimately ensuring the privacy, safety, and functionality of these critical infrastructures.

II. IOT-BASED EMBEDDED SYSTEMS AND CYBERSECURITY CHALLENGES

2.1 Overview of IoT Embedded Systems

The IoT refers to a network of interconnected devices embedded with sensors, software, and other technologies to collect, exchange, and process data over the internet. In an IoT embedded system, these devices operate autonomously or interactively to deliver specific functionalities. In sectors like healthcare, these systems enable real-time monitoring, diagnostics, and predictive analysis by integrating medical devices, wearables, and other health-tracking devices.

Architecture of IoT Embedded Systems

The architecture of an IoT embedded system generally includes several key components: sensors, microcontrollers, communication interfaces, and actuators. Sensors collect data from the physical environment, such as temperature, heart rate, or blood pressure in healthcare devices. This data is then sent to a microcontroller, which processes the data and makes decisions based on predefined rules or algorithms. Communication interfaces such as Wi-Fi, Bluetooth, or Zigbee enable the exchange of information between the embedded system and other devices or centralized servers, facilitating real-time data transmission. Actuators respond to processed data, triggering physical actions, such as adjusting a pacemaker's settings based on the heart rate data [6].

In healthcare, IoT-based embedded systems have become central to patient care. Devices such as wearable health monitors, smart infusion pumps, and remote patient monitoring systems rely on embedded IoT technologies to continuously collect data, which is sent to healthcare providers or databases for analysis. This system architecture is designed to optimize patient management by enabling early detection of health issues, improving treatment plans, and minimizing hospital visits [7]. For example, wearable devices can monitor vital signs like heart rate, ECG, and oxygen levels and send alerts to doctors in real-time, offering immediate intervention when necessary [8].

Operational Features of IoT Embedded Systems in Healthcare

IoT embedded systems in healthcare exhibit several operational features crucial for improving clinical outcomes. These include real-time monitoring, automation of tasks, remote diagnostics, and predictive analytics. Real-time monitoring is perhaps the most crucial feature, as it enables continuous tracking of patient health metrics, which can be immediately analysed for anomalies. Automation capabilities allow these systems to manage routine functions autonomously, reducing the burden on medical staff and minimizing human error [9]. Moreover, the integration of predictive analytics powered by ML and AI allows these systems to forecast potential health risks based on historical data patterns, improving preventative care strategies [10].

The communication and interoperability of these systems are also critical. IoT devices in healthcare must be able to communicate with centralized systems, electronic health records (EHRs), and other medical devices seamlessly to ensure data accuracy and consistency across platforms. Additionally, ensuring data privacy and security is paramount, as sensitive health information is involved. This aspect requires robust encryption techniques and compliance with regulations like HIPAA (Health Insurance Portability and Accountability Act) to safeguard patient data from unauthorized access [11].

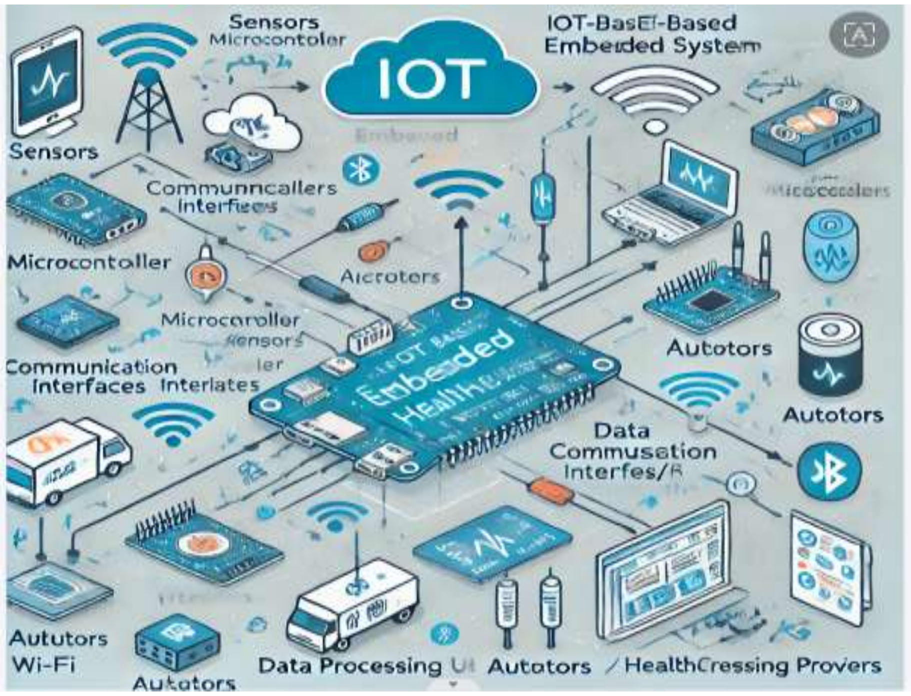

Figure 1: Diagram of a Typical IoT-Based Embedded System

2.2 Common Cybersecurity Threats in IoT Systems

IoT systems, due to their interconnected and often resource-constrained nature, are highly vulnerable to various types of cybersecurity threats. These threats can disrupt system functionality, compromise data integrity, and pose serious risks to user privacy. The most common cyber threats targeting IoT devices include Distributed Denial of Service (DDoS) attacks, malware infections, and spoofing attacks, each with distinct attack methods and potential impacts on system performance.

Distributed Denial of Service (DDoS) Attacks

A Distributed Denial of Service (DDoS) attack is one of the most prevalent cybersecurity threats against IoT devices. In a DDoS attack, malicious actors use a network of compromised IoT devices, often referred to as a botnet, to flood a target system or network with excessive traffic. This overwhelming traffic causes the target system to become unavailable to legitimate users, leading to service disruption. DDoS attacks can affect the availability and reliability of IoT systems, particularly in critical sectors like healthcare, where continuous access to data is essential for patient care and decision-making. Furthermore, DDoS attacks often serve as a diversion for more sophisticated attacks, such as data exfiltration or system breaches [12].

Malware Attacks

Malware attacks are another significant cybersecurity threat to IoT devices. IoT devices, particularly those with limited security features or outdated firmware, are often vulnerable to malicious software designed to exploit system weaknesses. Malware can be introduced into an IoT device through infected software updates, phishing attacks, or by exploiting known vulnerabilities in the device's operating system or communication protocols. Once malware infects an IoT device, it can lead to data theft, device manipulation, and unauthorized access to sensitive information. In healthcare, for example, malware can compromise medical devices, potentially altering their functionality, jeopardizing patient safety, and leading to data breaches [13].

Spoofing Attacks

Spoofing attacks involve impersonating a legitimate device or user to gain unauthorized access to an IoT system. In IoT environments, attackers may spoof a device's identity to deceive other devices or network systems into allowing them access. This can be done by mimicking a device's IP address, MAC address, or other unique identifiers. Once an attacker successfully impersonates a legitimate device, they can perform malicious actions such as eavesdropping on data transmissions, manipulating device settings, or launching further attacks like man-in-the-middle (MitM) attacks. Spoofing can result in significant security breaches, particularly when sensitive data, such as health information, is compromised [14].

Table 1: Overview of Common IoT Threats

Threat Type	Attack Method	Potential Impact
Distributed Denial of Service (DDoS)	Attackers use a botnet of IoT devices to flood a target system with excessive traffic, rendering it unavailable.	Disruption of service, downtime, and decreased availability, especially critical in healthcare settings.
Malware	Malicious software is introduced into IoT devices to exploit vulnerabilities, leading to system manipulation.	Data theft, device malfunctions, unauthorized access to sensitive information, and potential data corruption.
Spoofing	Attackers impersonate legitimate devices or users to gain unauthorized access to IoT systems.	Eavesdropping, data manipulation, unauthorized access, and potential system control takeover.

These cyber threats pose substantial risks to the functionality, privacy, and safety of IoT systems. To mitigate these threats, robust security measures, including regular software updates, strong encryption protocols, and ML -based anomaly detection systems, are essential for enhancing IoT system resilience.

2.3 Challenges in Securing IoT Devices

Securing IoT devices presents significant challenges due to their unique characteristics and the resource constraints that define many of these systems. As IoT devices become more widespread in sectors such as healthcare, industrial automation, and smart homes, the vulnerabilities they introduce grow, making it increasingly difficult to protect them from cyber threats. Several specific challenges hinder the effective implementation of security measures in IoT devices, including limited processing power, memory constraints, and restricted communication bandwidth.

Limited Processing Power

Many IoT devices are designed to be small, low-cost, and efficient, with limited processing capabilities. These devices are often built with minimal computational resources, which makes it difficult to implement advanced security algorithms, such as encryption, real-time threat detection, and complex anomaly detection systems. While higher-end IoT devices may be able to support sophisticated security mechanisms, low-end devices often cannot afford the computational overhead that comes with these systems. This limitation means that essential security features, such as robust authentication or encryption of data, may either be too resource-intensive or completely unsupported by the device's hardware [15]. As a result, IoT devices are more susceptible to attacks such as eavesdropping, man-in-the-middle, and data injection.

Memory Constraints

Memory limitations are another critical challenge in securing IoT devices. These devices are designed to operate with minimal storage to keep costs low and energy consumption at a minimum. However, this lack of memory space restricts the amount of data that can be processed or stored securely. For instance, maintaining logs for intrusion detection systems, storing cryptographic keys, or running security software often requires more memory than an IoT device can provide. Moreover, as IoT devices often rely on cloud services for data storage and processing, any vulnerabilities in these remote systems can compromise the device's overall security. The inability to store sufficient security data locally can also make it difficult to detect and respond to security threats in real-time [16].

Restricted Communication Bandwidth

The communication bandwidth of IoT devices is often limited, which is particularly challenging for systems that rely on continuous data exchange between devices and central servers. Low bandwidth restricts the ability to transmit large volumes of encrypted data or real-time security logs. Many IoT devices are connected via low-power wide-area networks (LPWANs), Wi-Fi, or Bluetooth, which offer limited data transmission rates. As a result, these devices may face delays in sending security alerts, receiving software updates, or communicating with intrusion detection systems. These restrictions make it challenging to implement continuous monitoring of the devices and timely deployment of patches or updates to address vulnerabilities [17].

The combination of these challenges means that securing IoT devices is a complex task requiring innovative solutions, such as lightweight encryption algorithms, edge computing, and adaptive security mechanisms. Additionally, a holistic approach that includes both device-level security and network-level protection is essential for minimizing the risk of cyber threats.

III. ML IN CYBER THREAT DETECTION AND DATA FORENSICS

3.1 ML Approaches in Cybersecurity

ML has emerged as a critical tool in enhancing cybersecurity measures, particularly for detecting and mitigating cyber threats in IoT-based systems. ML methods allow for the automatic detection of anomalies, identification of malicious activities, and improvement of threat-response strategies through continuous learning from data. Among the most effective ML approaches in cybersecurity are anomaly detection and supervised classification. These approaches offer distinct advantages in identifying cyber threats within IoT environments, where the volume of data and the complexity of interactions between devices make traditional security measures less effective.

Anomaly Detection

Anomaly detection is one of the most widely used ML approaches in cybersecurity, particularly in IoT systems. It involves training a model on the expected behaviour of a system or network and then identifying deviations from this baseline behaviour, which could indicate malicious activities or potential threats. The strength of anomaly detection lies in its ability to identify previously unknown or zero-day attacks, which may not be represented in existing threat databases. This makes anomaly detection a powerful tool for detecting novel threats, such as DDoS attacks or sophisticated malware that may not be immediately recognizable through traditional signature-based detection methods.

Anomaly detection methods can be implemented using unsupervised learning, which does not require labelled training data. This is particularly useful for IoT systems where obtaining labelled data may be challenging. However, the drawback of anomaly detection is the potential for a high rate of false positives, where benign behaviour may be incorrectly flagged as a threat. Fine-tuning the model to minimize false alarms is a key challenge in this approach [18].

Supervised Classification

Supervised classification involves training a ML model on a labelled dataset of known attacks and benign behaviours. The model then classifies new data points as either "normal" or "malicious" based on the patterns learned during training. Supervised learning approaches, such as decision trees, support vector machines (SVMs), and neural networks, are commonly used in IoT cybersecurity for tasks like intrusion detection and malware classification. The advantage of supervised classification is its high accuracy when the dataset contains a sufficient number of labelled examples of both attacks and normal behaviours.

However, supervised classification models require a comprehensive and representative labelled dataset, which may be difficult to obtain, particularly in dynamic IoT environments where attack vectors continually evolve. Furthermore, supervised methods tend to perform poorly in detecting novel attacks that were not included in the training data, as they rely heavily on predefined threat categories. Despite these limitations, supervised classification models are highly effective for identifying known threats, particularly when combined with other detection methods [19].

Table 2: Comparison of ML Methods for Cyber Threat Detection

Method	Pros	Cons	Suitability for IoT Security
Anomaly Detection	- Can detect novel, previously unknown threats.	- High false positive rate.	Effective for detecting novel and sophisticated attacks, but requires fine-tuning to reduce false positives.
Supervised Classification	- High accuracy with sufficient labelled data.	- Dependent on large labelled datasets; poor at detecting new or unknown attacks.	Well-suited for detecting known threats but limited in addressing new attack types.
Clustering	- Unsupervised method that identifies patterns in data without needing labelled examples.	- Difficult to interpret results, may miss subtle attack patterns.	Useful for segmenting IoT data and detecting outlier behaviour, but challenging for fine-grained detection.
Deep Learning	- Highly effective in modelling complex patterns and detecting sophisticated attacks.	- Computationally intensive and requires large datasets for effective training.	Suitable for large-scale IoT deployments but resource-intensive.

The integration of ML approaches into IoT cybersecurity offers a promising solution for enhancing threat detection capabilities. By utilizing both anomaly detection and supervised classification, security systems can be more adaptive, identifying both known and unknown threats while optimizing detection accuracy.

3.2 Data Forensics in IoT Cybersecurity

Data forensics plays an essential role in detecting and analysing digital evidence of cyber threats within IoT environments. In IoT-specific contexts, forensics refers to the process of collecting, preserving, and analysing the data generated by interconnected devices to uncover cyber-attacks and security breaches. These attacks could target sensitive environments such as healthcare, where data from devices like wearable health monitors and medical devices are often at risk. Unlike traditional IT systems, IoT devices operate in decentralized, highly interconnected environments, which creates unique challenges for forensic investigators, who must analyse data from a variety of devices and networks with varying characteristics and formats.

Data Collection and Preservation

The first challenge in IoT forensics is the collection and preservation of data. Due to the dispersed nature of IoT devices, data collection must occur across various endpoints, including sensors, network devices, and embedded systems. To ensure the integrity of this data for future legal or operational use, it must be collected in a manner that prevents tampering or modification. Timestamping, encryption, and data hashing techniques are often used to safeguard against data alteration during collection. Preserving data integrity is especially critical in the context of IoT, where sensor data and logs may be voluminous and complex, making it difficult to distinguish between benign and malicious actions [20].

Analysis and Investigation

After data collection, forensic experts analyse the data to uncover patterns and anomalies indicative of a cyber threat. In IoT systems, this typically involves network traffic analysis, log examination, and metadata inspection. Anomalies, such as sudden increases in traffic or unusual device behaviour, can suggest that a system has been compromised. Forensic analysis often correlates data across multiple devices, creating a comprehensive view of the attack. By using specialized tools capable of handling large datasets and identifying patterns in data, forensics experts can track an attack's origin, determine its impact, and assess whether it is part of a larger, coordinated cyber-attack [21].

In addition to identifying the attack, data forensics can improve future system security by revealing system vulnerabilities. By understanding how previous attacks exploited certain weaknesses, experts can propose measures to strengthen IoT systems against similar threats in the future.

3.3 Integrating ML and Data Forensics for IoT Threat Detection

Integrating ML with data forensics offers several advantages in enhancing IoT cybersecurity. While data forensics provides in-depth, post-event analysis, ML can be used for proactive, real-time threat detection. The integration of both techniques improves the overall security framework by increasing detection accuracy, reducing false positives, and optimizing threat response times. This hybrid approach offers a robust, adaptive defense mechanism capable of identifying emerging threats and continuously improving its detection capabilities.

ML for Real-Time Detection

ML enhances the capabilities of traditional data forensics by enabling real-time analysis of data. ML algorithms can detect anomalies in the data generated by IoT devices, such as unexpected traffic spikes, unauthorized access attempts, or unusual sensor readings. For instance, unsupervised learning models are often employed to identify deviations from normal behaviour without requiring labelled data, making them suitable for identifying novel or unknown threats. These ML models can quickly identify potential threats in vast, real-time data streams generated by IoT systems, minimizing the time between detection and response. Once an anomaly is identified, data forensics techniques can be used to verify whether the behaviour was truly malicious [22].

Data Forensics for Deep Analysis

Following detection, data forensics tools enable detailed investigation into the nature of the threat. Data forensics in this context focuses on analysing historical logs, device-specific data, and network traffic to uncover the origin of the attack and determine how it affected the IoT system. For example, in the case of a distributed denial of service (DDoS) attack, forensics can help trace the attack's source and analyse its progression through the network. This investigative process is essential for understanding the attack's tactics, techniques, and procedures (TTPs), which can then inform improvements in IoT security. Data forensics not only helps validate the presence of a threat but also contributes to developing post-incident strategies for strengthening system defenses against future threats [23].

Synergy Between ML and Data Forensics

The combined use of ML and data forensics enhances the overall threat detection process. While ML provides scalable and efficient methods for identifying threats in real-time, data forensics delivers deeper, more accurate insights into how and why an attack occurred. Together, they offer a comprehensive cybersecurity framework that is capable of detecting, analysing, and mitigating threats more effectively. By leveraging ML for initial detection and using data forensics for detailed analysis, organizations can respond to cyber threats quickly while ensuring that the attack's full scope is understood and future threats are prevented.

Table 3:

Step	Description
1. Data Collection	Collect data from IoT devices, networks, and sensors, ensuring data integrity for forensic purposes.
2. Anomaly Detection (ML)	Apply ML models to detect unusual patterns and anomalies in real-time data streams.
3. Threat Identification	Identify potential threats or anomalies using classification or clustering algorithms.
4. Data Forensics Analysis	Perform in-depth forensic analysis on the identified threats, examining logs, timestamps, and device-specific data to confirm the attack.
5. Incident Response	Based on forensic findings, implement appropriate countermeasures to mitigate the

Step	Description
& Mitigation	threat and prevent future breaches.
6. Continuous Learning (ML)	Use feedback from the investigation to improve ML models, allowing for better detection in future incidents.

Figure 2, showing the flow of data from collection and anomaly detection through to forensic investigation and response.

This integrated approach maximizes the effectiveness of threat detection and mitigation, enabling organizations to stay ahead of increasingly sophisticated cyber threats in IoT environments.

IV. DATA PREPROCESSING AND MODEL TRAINING FOR THREAT DETECTION

4.1 Data Collection and Preprocessing in IoT Systems

Data collection and preprocessing are critical steps in ensuring the effectiveness of ML models applied to IoT cybersecurity. IoT systems generate vast amounts of data from a multitude of devices, sensors, and networks, often in real-time. This data is often noisy, incomplete, and unstructured, making preprocessing essential to transforming it into a format suitable for analysis. Data preprocessing involves several techniques, such as data cleansing, transformation, and feature extraction, which are necessary to improve the quality of the data and make it usable for ML applications in cybersecurity.

Data Cleansing

Data cleansing is the first and most critical step in the preprocessing pipeline. It involves identifying and correcting errors in the collected data, such as missing values, duplicates, and inconsistencies. In IoT systems, sensor data can be incomplete due to intermittent connectivity or hardware failures, which may result in missing readings. Additionally, data from different devices may use different formats or units, leading to discrepancies. Cleansing the data ensures that it is accurate and consistent, which is fundamental for training reliable ML models. Techniques such as imputation (replacing missing values with estimates based on available data) or removing rows with missing values are commonly used to address these issues [24].

Data Transformation

Data transformation refers to the process of converting the raw data into a format that can be easily interpreted by ML algorithms. In IoT systems, data transformation often includes scaling and normalization of sensor readings, especially when data from multiple devices with different ranges are combined. For instance, temperature readings from one device may have a different scale compared to humidity readings from another device. Standardization techniques such as Min-Max scaling or Z-score normalization are applied to ensure that all features contribute equally to the ML model's learning process. Additionally, transformation can involve encoding categorical variables into numerical values and handling time-series data, which is common in IoT environments. By transforming raw data into a standardized format, ML algorithms can more effectively detect patterns and anomalies in the data.

Feature Extraction

Feature extraction is the process of selecting relevant attributes from the raw data that will be most useful for training ML models. In IoT systems, raw sensor data may contain a large amount of irrelevant or redundant information, making it important to extract only the most pertinent features that will contribute to the performance of the model. For instance, in a healthcare IoT system, features like temperature, heart rate, and oxygen saturation are directly relevant to detecting anomalies in patient health data, while noise from unrelated sensors may be discarded. Feature extraction helps reduce the dimensionality of the data, making it easier for ML models to detect patterns and reduce computational complexity. Techniques such as Principal Component Analysis (PCA) or feature selection algorithms like Recursive Feature Elimination (RFE) are used to identify the most impactful features for the task at hand [25].

Importance for ML Models

Data preprocessing ensures that the data is cleaned, transformed, and prepared for analysis, which is crucial for the accuracy and reliability of ML models. Raw, unprocessed data can lead to inaccurate predictions, as the model may learn from irrelevant, noisy, or incomplete information. Effective preprocessing can significantly improve the performance of ML algorithms, particularly in complex and high-dimensional IoT environments, where the sheer volume of data can overwhelm unprepared systems. By ensuring high-quality data, preprocessing enables ML models to identify subtle patterns, such as security breaches or anomalies in device behaviour, with greater precision and efficiency.

Table 4: Key Preprocessing Steps with Explanations of Their Roles in Enhancing the Quality and Relevance of IoT Data for ML Models

Preprocessing Step	Description	Role in Enhancing IoT Data for ML
Data Cleansing	Identifying and handling errors such as missing values, duplicates, and inconsistencies.	Ensures the accuracy and consistency of data, reducing noise and preventing errors.
Data Transformation	Scaling, normalization, and encoding of data to ensure compatibility with ML models.	Standardizes data for better model interpretation and ensures equal contribution of all features.
Feature Extraction	Identifying and selecting the most relevant features from raw data for model training.	Reduces dimensionality, enhances model performance, and focuses on important data.
Noise Reduction	Filtering out irrelevant data or sensors that do not contribute to the analysis.	Reduces irrelevant information, improving model efficiency and accuracy.

By applying these preprocessing techniques, IoT systems can generate clean, structured, and meaningful data that ML models can effectively analyse, leading to improved cybersecurity detection and mitigation efforts.

4.2 Creating and Labelling Datasets for Cyber Threat Detection

Creating and labelling datasets is a crucial step in training ML models for cyber threat detection in IoT systems. The process involves collecting relevant data from IoT devices and ensuring that it is properly labelled to distinguish between normal (benign) and malicious activities. The labelled datasets serve as the foundation for supervised learning algorithms, which are used to identify and classify various types of cyber threats such as Distributed Denial of Service (DDoS) attacks, malware, and unauthorized access.

Data Collection for Labelling

The first step in creating labelled datasets is data collection. This data can come from IoT sensors, logs, and network traffic. In an IoT system, data sources may include device status logs, sensor readings (e.g., temperature, humidity, motion), and communication patterns. The challenge lies in collecting a comprehensive dataset that includes both normal and malicious activities, which are essential for training accurate models. Since attacks often involve subtle and evolving behaviours, it can be difficult to capture all potential attack scenarios (26).

Labelling Data

Labelling the data is another critical step, as it determines how the ML model will differentiate between normal and malicious behaviour. This process requires domain expertise to correctly identify the characteristics of benign and malicious activities in the IoT data. For instance, a sudden spike in network traffic might be benign during system updates, but it could indicate a DDoS attack if it occurs unexpectedly and persists for a long time. Manual labelling can be time-consuming and prone to errors, especially when there is a large volume of data, which is often the case with IoT systems. As a result, automated or semi-automated methods for labelling, such as anomaly detection techniques, can assist in the labelling process (27).

Challenges in Dataset Creation and Labelling

One of the primary challenges in creating labelled datasets for IoT systems is the lack of real-world labelled data, as cyberattacks are relatively rare events. To overcome this, researchers often rely on simulated attack datasets or generate synthetic attacks using tools that mimic cyber threats. However, synthetic data may not perfectly represent real-world attack scenarios, which can affect the model's ability to generalize to new, unseen attacks. Furthermore, in dynamic IoT environments, the nature of threats constantly evolves, making it difficult to keep labelled datasets up to date. Regular updates and refinement of datasets are necessary to ensure that ML models can detect emerging threats effectively (28).

Importance of High-Quality Datasets

The quality of the labelled dataset directly impacts the performance of ML models. High-quality, balanced datasets that include both benign and malicious data in sufficient quantities will allow the model to learn the characteristics of each class more accurately. Poor-quality datasets or datasets with imbalanced classes (i.e., more benign than malicious data) can lead to biased models that fail to detect rare attack types. Therefore, careful consideration and effort must be invested in the data collection and labelling phases to build effective cyber threat detection models (29).

4.3 Training ML Models

Training ML models for cyber threat detection in IoT systems involves several important steps, from splitting the dataset into training and testing sets to implementing cross-validation and adapting models to real-time data streams. The goal is to ensure that the model generalizes well to new data and can accurately detect and mitigate cyber threats in real-world environments.

Data Division and Cross-Validation

Once a labelled dataset is ready, the first step in the training process is to split the data into training and testing sets. This ensures that the model is trained on one portion of the data and tested on another, which helps evaluate its performance and generalizability. A common approach is the use of a 70-30 or 80-20 split, where 70-80% of the data is used for training, and the remaining 20-30% is reserved for testing. Cross-validation is an important technique used to improve model performance and robustness. In k-fold cross-validation, the dataset is divided into k subsets, and the model is trained and tested k times, each time using a different subset for testing. This process provides a more reliable estimate of the model's performance and helps avoid overfitting to a particular subset of data (30).

Training on Real-Time Data Streams

In IoT cybersecurity, one of the main challenges is the dynamic nature of the data, as IoT systems continuously generate real-time data streams. For a ML model to be effective in detecting cyber threats, it must be trained on data that reflects the changing conditions of the system. Training on real-time data streams ensures that the model can adapt to new patterns of behaviour and respond to evolving threats. For example, a DDoS attack might not be present in the training dataset but could emerge later. To address this, ML models can be trained incrementally, where they are continuously updated as new data becomes available. This approach helps the model stay current with new attack types and system changes, enhancing its ability to detect threats in real time (31).

Adaptability and Real-Time Learning

Adaptability is critical for IoT cybersecurity systems, as new types of attacks frequently emerge. In traditional ML models, the model is typically trained on historical data and then deployed without much adaptation to new data. However, in IoT cybersecurity, the nature of the threats changes rapidly, and models need to be adaptable. One approach to ensuring adaptability is online learning, where the model is trained continuously as new data arrives. This method enables the model to update itself in real-time, improving its ability to detect previously unseen attacks. Online learning can be particularly useful in IoT systems, where the volume of data can be enormous and continuously changing. The ability to quickly update the model based on incoming data allows it to remain effective in dynamic, evolving environments (32).

Challenges in Model Training

Training ML models for IoT cybersecurity presents several challenges. One challenge is the high dimensionality of the data, as IoT systems often generate large volumes of diverse data from multiple devices. Reducing this complexity through techniques like dimensionality reduction (e.g., Principal Component Analysis) or feature selection is crucial to improving the model's efficiency. Another challenge is the class imbalance problem, where malicious activities are less frequent than benign ones, making it harder for the model to detect rare but important threats. Techniques like oversampling, undersampling, and synthetic data generation are often employed to address this issue (33).

Training ML models for IoT cybersecurity requires a careful balance between data preprocessing, feature extraction, and model adaptation to real-time data. By dividing the data properly, using cross-validation techniques, and incorporating incremental learning strategies, ML models can effectively detect and mitigate cyber threats in IoT systems. However, challenges such as data dimensionality, class imbalance, and real-time adaptation must be carefully addressed to ensure that the models remain effective and accurate in dynamic IoT environments.

V. DETECTION TECHNIQUES FOR CYBER THREATS IN IOT-BASED SYSTEMS

5.1 Anomaly Detection Techniques

Anomaly detection is a critical method for identifying potential cyber threats in IoT systems by recognizing deviations from the established patterns of behaviour. It is particularly useful in detecting previously unknown or emerging attacks, as anomalies often signify malicious activities. Anomaly detection techniques can be broadly categorized into statistical methods and ML -based approaches, each offering unique advantages in identifying cyber threats.

Statistical Methods in Anomaly Detection

Statistical anomaly detection methods rely on the assumption that the majority of IoT device data adheres to a predictable statistical distribution. These methods typically involve monitoring the mean, variance, and other statistical properties of data over time. One common technique is the use of **Gaussian Mixture Models (GMM)**, where the normal behaviour is modelled as a mixture of several Gaussian distributions. If new data points significantly deviate from this model, they are flagged as potential anomalies. Statistical methods are effective when the system's normal behaviour can be clearly defined, but they may struggle in dynamic or highly variable environments like IoT systems (34).

ML -Based Anomaly Detection

ML approaches, particularly unsupervised learning models, are increasingly being employed for anomaly detection in IoT systems. Unsupervised methods such as **k-means clustering** and **autoencoders** do not require labelled data, making them particularly useful when labelled training data is scarce. **k-means clustering** groups similar data points together, with anomalies being identified as outliers that do not belong to any cluster. **Autoencoders**, a type of neural network, are trained to reconstruct input data. When an anomaly is present, the reconstruction error is significantly higher, signalling a deviation from the normal behaviour (35).

Other ML models such as **Isolation Forest** and **One-Class Support Vector Machines (SVM)** are also employed for anomaly detection. **Isolation Forest** isolates anomalies by randomly selecting features and partitioning the data, with anomalies requiring fewer splits. **One-Class SVM** learns a decision boundary around normal data and flags any data point outside this boundary as anomalous. These models are powerful in identifying complex, non-linear patterns that traditional statistical methods might miss, particularly in high-dimensional IoT datasets (36).

Advantages of Anomaly Detection

Anomaly detection offers several advantages in IoT cybersecurity, such as its ability to detect zero-day attacks or previously unseen threats. By focusing on the behaviour of the system rather than predefined attack signatures, anomaly detection can identify threats that do not match known attack patterns. Additionally, anomaly detection systems can be adapted over time to reflect changes in normal behaviour, improving their ability to detect evolving threats (37).

Challenges of Anomaly Detection

Despite its advantages, anomaly detection in IoT systems also presents several challenges. One challenge is the high volume and variety of data generated by IoT devices, making it difficult to establish a clear baseline of normal behaviour. Moreover, false positives—flagging benign activities as anomalies—can be a significant issue, leading to unnecessary alerts and reduced system performance. To mitigate this, hybrid approaches that combine statistical methods with ML models are often employed to improve accuracy and reduce false positives (38).

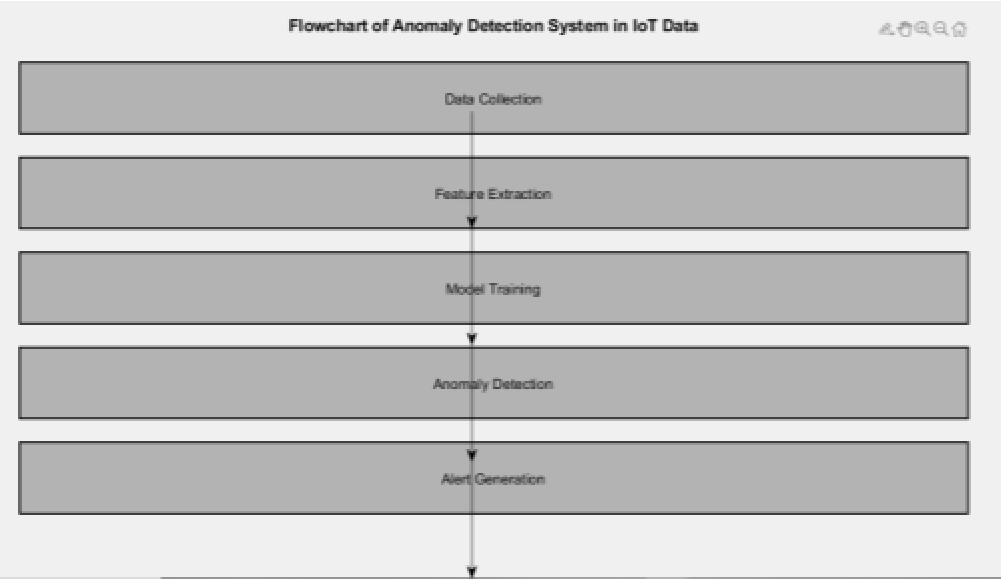

Figure 2: Example Model of an Anomaly Detection System Applied to IoT Data

5.2 Supervised Learning Models for Threat Classification

Supervised learning models are widely used in cybersecurity for classifying activities as normal or malicious. These models are trained on labelled datasets, where each data point is associated with a known outcome (normal or malicious). In the context of IoT-based embedded systems, supervised learning algorithms such as **decision trees**, **support vector machines (SVM)**, and **neural networks** play a crucial role in accurately categorizing system activities and detecting cyber threats.

Decision Trees

Decision trees are a popular supervised learning model that are easy to interpret and implement. The algorithm works by recursively partitioning the dataset into subsets based on feature values, forming a tree-like structure. Each leaf node of the tree represents a class label (normal or malicious), and the path taken to reach the leaf node represents a series of decision rules. **Random Forests**, an ensemble method based on decision trees, further improves classification accuracy by combining the predictions of multiple trees. In IoT systems, decision trees are effective in identifying key features (such as unusual traffic patterns or device behaviour) that differentiate malicious activities from normal operations (39).

Support Vector Machines (SVM)

Support vector machines (SVM) are powerful supervised learning algorithms that are particularly effective in high-dimensional spaces, which is common in IoT data. SVM works by finding a hyperplane that maximally separates data points from different classes (normal vs. malicious). It performs well in situations where there is a clear margin of separation between classes, even in non-linear scenarios by employing kernel functions such as radial basis function (RBF). SVM is commonly used in threat classification because it can efficiently handle both linear and non-linear decision boundaries in complex IoT datasets (40).

Neural Networks

Neural networks, particularly **deep learning models**, have gained significant traction in cybersecurity due to their ability to automatically extract high-level features from raw data. A **feedforward neural network** (FNN) consists of multiple layers of interconnected neurons that process data from input to output layers, making it capable of learning complex patterns. **Convolutional neural networks (CNNs)** and **recurrent neural networks (RNNs)** are also applied in IoT threat detection to capture spatial and temporal features, respectively. CNNs are particularly effective in analysing data with spatial hierarchies (e.g., sensor data), while RNNs are suited for time-series data where temporal dependencies are important (41).

Advantages of Supervised Learning Models

Supervised learning models are highly effective for threat classification in IoT systems because they leverage labelled data to learn clear distinctions between normal and malicious activities. These models can be trained to recognize a wide variety of attack types, including well-known threats like DDoS attacks, malware, and spoofing. Once trained, supervised models are capable of making accurate predictions and detecting cyber threats in real-time. Furthermore, these models are interpretable, allowing cybersecurity professionals to understand the reasoning behind specific classifications (42).

Challenges of Supervised Learning Models

Despite their effectiveness, supervised learning models face several challenges in IoT cybersecurity. One of the primary challenges is the **class imbalance problem**, where malicious activities are less frequent than benign activities in the dataset. This can lead to biased models that favour the normal class, resulting in poor detection rates for rare attack types. Techniques such as oversampling (e.g., SMOTE) or undersampling of the normal class are used to mitigate this issue (43). Additionally, supervised learning models require large amounts of labelled data, which can be difficult and time-consuming to obtain in real-world IoT systems. This is particularly challenging in environments with evolving attack techniques, where new types of threats may not be represented in existing labelled datasets (44).

5.3 Evaluation Metrics for Model Performance

Evaluating the performance of ML models is critical to ensure their reliability in detecting and mitigating cyber threats in IoT-based embedded systems. Various evaluation metrics are used to assess the effectiveness of models, each focusing on different aspects of model performance. Key metrics include **accuracy**, **precision**, **recall**, and the **F1 score**, all of which provide insights into the reliability and efficiency of detection models. These metrics help in understanding how well a model can distinguish between normal and malicious activities in IoT systems.

Accuracy

Accuracy is one of the most straightforward performance metrics and is calculated as the ratio of correctly predicted instances (both normal and malicious) to the total number of instances in the dataset. It provides a general sense of the model's ability to classify both classes correctly. While accuracy is easy to interpret, it can be misleading, especially in cases of **class imbalance**, where one class (e.g., benign activity) significantly outnumbers the other (e.g., malicious activity). In such cases, a model might achieve high accuracy simply by predicting the majority class, while failing to detect rare but critical threats (45).

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

Where:

- **TP (True Positive)**: Correctly identified malicious activities.
- **TN (True Negative)**: Correctly identified benign activities.
- **FP (False Positive)**: Malicious activities incorrectly classified as benign.
- **FN (False Negative)**: Benign activities incorrectly classified as malicious.

Precision

Precision, also known as **positive predictive value**, measures the accuracy of the positive predictions made by the model. It is calculated as the ratio of true positives to the total predicted positives (sum of true positives and false positives). In cybersecurity, **precision** is particularly important because false positives can be costly and may lead to unnecessary interventions. A high precision indicates that when the model flags an activity as malicious, it is likely to be accurate, minimizing false alarms (46).

$$Precision = \frac{TP}{TP + FP}$$

Recall

Recall, also known as sensitivity or true positive rate, measures the model's ability to correctly identify all instances of malicious activity. It is calculated as the ratio of true positives to the sum of true positives and false negatives. A high recall indicates that the model is capable of identifying most of the malicious activities in the dataset, which is crucial in cybersecurity, where missing a threat (false negative) can have serious consequences. However, maximizing recall alone might lead to more false positives (47).

$$Recall = \frac{TP}{TP + FN}$$

F1 Score

The **F1 score** is the harmonic mean of **precision** and **recall**, providing a balanced measure of a model's performance. The F1 score is particularly useful when there is an uneven class distribution (e.g., when malicious activities are rare) and ensures that both false positives and false negatives are considered. A higher F1 score signifies a better balance between precision and recall, making it an effective metric when aiming to optimize both false positives and false negatives (48).

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

The F1 score is a comprehensive metric that addresses the trade-off between precision and recall, which is important for cybersecurity applications. In IoT-based embedded systems, where the cost of undetected threats is high, the F1 score provides an overall indicator of the model's ability to both detect threats and minimize false alarms.

Significance in Evaluating Cyber Threat Detection Models

Each of these metrics serves a distinct purpose in evaluating ML models for cybersecurity tasks in IoT systems. **Accuracy** provides an overview of the model's general performance but may not be sufficient on its own, particularly in imbalanced datasets. **Precision** is critical when false positives can lead to unnecessary alerts or system disruptions. **Recall** is essential for ensuring that most malicious activities are detected, even if it means accepting some false positives [48]. Finally, the **F1 score** offers a balanced perspective on model performance, making it particularly useful in situations where both false positives and false negatives are costly.

In IoT cybersecurity, where threats are often diverse and evolving, these metrics should be carefully considered to select the best-performing detection model. Furthermore, continuous monitoring and adjustment of model parameters are necessary to maintain an effective cybersecurity defense against emerging threats.

VI. MITIGATION STRATEGIES FOR CYBER THREATS IN IOT EMBEDDED SYSTEMS

6.1 Real-Time Intrusion Detection and Prevention Systems (IDPS)

ML -powered Intrusion Detection and Prevention Systems (IDPS) are critical for protecting IoT ecosystems against cyber threats in real-time. These systems are designed to detect unauthorized or malicious activity and either alert administrators or automatically mitigate threats, depending on the severity. ML enhances IDPS capabilities by enabling them to adapt to new attack patterns, improving detection accuracy, and reducing the reliance on predefined signatures of known threats.

Architecture of Real-Time IDPS in IoT Settings

Real-time intrusion detection and prevention in IoT environments typically involve three core components: data collection, threat analysis, and response mechanisms. The process begins with the collection of data from IoT devices and network traffic, which is then pre-processed to ensure the quality and relevance of the data for ML analysis. Features such as packet size, frequency, and other network activity parameters are extracted and fed into ML algorithms for classification and anomaly detection. ML models, particularly supervised and unsupervised learning methods, are used to identify deviations from the normal behaviour, flagging potential cyber threats (49).

A key benefit of ML in IDPS is the ability to use anomaly-based detection. This method does not rely solely on known attack signatures, which can be easily bypassed by attackers who modify their methods. Instead, it identifies unusual patterns of behaviour within the IoT system, regardless of the attack's specific nature. For example, sudden spikes in data traffic or unusual device behaviour could signal a Distributed Denial of Service (DDoS) attack or other malicious activities (50). By continuously learning from the incoming data, the system can become more accurate over time, adapting to both emerging threats and the dynamic nature of IoT environments.

The response mechanism in a real-time IDPS can be automatic or semi-automatic. Upon detecting an intrusion, the system can take pre-configured actions, such as blocking suspicious IP addresses, isolating affected devices, or notifying administrators. The speed of response is essential to minimize damage, particularly in sensitive environments like healthcare or industrial automation systems, where cyber threats could have immediate and severe consequences (51).

The integration of ML into IDPS provides a flexible and scalable solution for dynamic IoT environments, where traditional security measures may not be sufficient due to the complexity and diversity of devices involved.

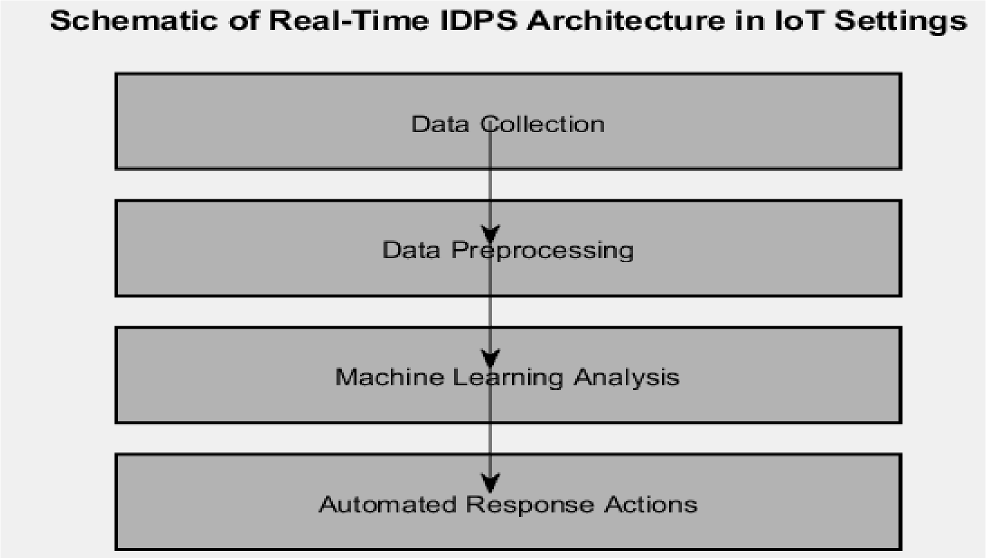
Schematic of Real-Time IDPS Architecture in IoT Settings
Data Collection
Data Preprocessing
Machine Learning Analysis
Automated Response Actions

Figure 3: Schematic of a Real-Time IDPS Architecture in IoT Settings

(Illustration showing data collection, preprocessing, ML analysis, and automated response actions in a real-time IDPS for IoT ecosystems)

6.2 Adaptive Security Protocols

In addition to real-time intrusion detection and prevention, adaptive security protocols are essential to protect IoT-based embedded systems against evolving cyber threats. These protocols dynamically adjust to changes in the threat landscape, ensuring continuous defense without requiring manual updates. The adaptive nature of these protocols allows them to react to new attack vectors, vulnerabilities, and other unforeseen challenges that may arise over time.

Mechanisms of Adaptive Security Protocols

Adaptive security protocols leverage ML and AI to assess current conditions and automatically modify their defenses. For instance, in response to a detected anomaly or attack, an adaptive protocol may adjust its security configuration to become more stringent, limiting device communication or adjusting access control policies. This is particularly important in IoT ecosystems, where new devices are frequently added, and threats evolve rapidly.

One prominent feature of adaptive security protocols is their ability to learn from past incidents. By using historical data, the system can predict potential threats based on patterns and trends, allowing it to anticipate attacks before they occur. For example, if an IoT device is targeted by a new type of malware, the security protocol can adapt by detecting similar signatures or behaviours in other devices, automatically adjusting its defenses accordingly. This proactive approach ensures that IoT systems remain secure even when attackers employ novel techniques. Furthermore, adaptive security protocols can prioritize resource allocation based on the level of threat. For instance, if a critical device in a healthcare system is under attack, the protocol can allocate more resources to monitor and secure that device while simultaneously reducing the load on less critical devices. This approach helps optimize system performance while maintaining a strong security posture. By continuously evolving in response to new threats, adaptive security protocols offer a robust, self-sustaining defense for IoT-based systems. This is particularly crucial for environments like healthcare, where the need for security is urgent, but downtime or manual intervention could disrupt essential services.

6.3 Securing Software Implementation

Securing software in IoT-based embedded systems is critical to safeguarding against vulnerabilities that cyber attackers can exploit. Secure coding practices are essential throughout the development lifecycle of IoT software to ensure that security risks are mitigated before deployment. These practices encompass techniques such as firmware checks, encryption, and patching strategies, which work together to create a robust security posture for IoT devices.

Firmware Checks and Validation

One of the primary security risks in IoT systems is the integrity of firmware, as it is often targeted for exploitation by cyber attackers seeking to gain unauthorized control over devices. To mitigate this, firmware checks and validation procedures are implemented to ensure that only verified and trusted versions of firmware are deployed. This can include techniques like cryptographic hashes to confirm the authenticity of firmware during updates or boot sequences. Additionally, secure boot mechanisms can help prevent malicious firmware from being loaded during device startup, ensuring that the device operates with a legitimate version of its software (52).

Encryption Techniques

Encryption is a cornerstone of securing IoT devices by ensuring that sensitive data transmitted across networks remains confidential. All communication between IoT devices and their networks should be encrypted using strong algorithms, such as AES (Advanced Encryption Standard) or RSA (Rivest-Shamir-Adleman). In addition to protecting data during transmission, data stored on devices should also be encrypted to prevent unauthorized access in case of theft or tampering. End-to-end encryption guarantees that even if attackers intercept communication, the data remains unreadable without the decryption key, significantly reducing the risk of data breaches (53).

Patching and Update Strategies

IoT devices often face security vulnerabilities due to outdated software, making timely and effective patching essential for maintaining system security. A robust patch management strategy ensures that devices are regularly updated to address newly discovered vulnerabilities. Secure patching practices include verifying the integrity of patches before they are applied, ensuring they are distributed securely, and implementing automated update mechanisms to reduce the window of exposure to potential threats. Additionally, software updates should be tested in a controlled environment before deployment to avoid introducing new vulnerabilities (54). Through the implementation of these secure coding practices, IoT systems can minimize the risk of cyber threats, ensuring the protection of both the devices and the sensitive data they handle.

VII. CASE STUDIES: APPLICATION OF ML IN IOT CYBERSECURITY

7.1 Case Study 1: IoT Cybersecurity in Healthcare Systems

The integration of IoT devices into healthcare systems has revolutionized patient monitoring and care, but it has also introduced new cybersecurity challenges. Healthcare IoT systems often include medical devices such as wearable sensors, infusion pumps, and diagnostic tools, all interconnected through hospital networks. While these devices offer numerous benefits, their connectivity and continuous data streams make them attractive targets for cyber attackers. This case study presents the application of ML to secure IoT healthcare devices and examines the effectiveness of various detection methods.

Threats and Detection Methods

In this case study, the healthcare facility faced increasing incidents of unauthorized access to medical devices and patient data breaches. One significant threat identified was a type of **Man-in-the-Middle (MitM) attack**, where attackers intercepted communication between wearable medical devices and hospital servers, manipulating the transmitted health data. This type of attack could result in inaccurate patient information, leading to incorrect diagnoses or treatment plans.

To address these threats, ML models were implemented to enhance the detection of anomalies in device behaviour. Anomaly detection algorithms, particularly those based on unsupervised learning, were trained using historical data collected from medical devices. These models focused on identifying deviations from the normal operating patterns of devices such as vital sign monitors and infusion pumps. The ML models used features like data transmission rates, device interaction frequency, and sensor readings to detect irregular patterns indicative of potential threats (55).

The detection methods employed were able to identify abnormal spikes in data traffic that could be associated with a **DDoS attack** targeting the network. In addition to anomaly detection, supervised ML models, such as decision trees and support vector machines (SVM), were used to classify observed behaviours as either benign or malicious, providing real-time alerts to security administrators (56).

Outcomes and Effectiveness

The implementation of these ML techniques significantly improved the detection of cyber threats in the healthcare IoT ecosystem. The system achieved high levels of accuracy in identifying MitM attacks and abnormal traffic patterns that indicated DDoS activity. The results showed that the ML models could reduce false positives, allowing the system to operate more efficiently and with fewer interruptions to critical medical services (57).

Table 5: Summary of Specific Threats and the Effectiveness of ML -Based Detection in Healthcare IoT

Threat	Detection Method	Effectiveness
Man-in-the-Middle (MitM) Attack	Anomaly detection (unsupervised learning)	High detection rate with reduced false positives
Distributed Denial of Service (DDoS) Attack	Anomaly detection (traffic pattern analysis)	Successfully detected unusual traffic spikes and disruptions
Unauthorized Data Access	Supervised learning (SVM, decision trees)	Identified unauthorized access attempts with high accuracy

This case study illustrates how ML -powered threat detection and classification systems can effectively secure IoT healthcare devices against emerging cyber threats, ensuring patient safety and data privacy (58).

7.2 Case Study 2: Industrial IoT Security with Anomaly Detection Models

Industrial IoT (IIoT) systems have become integral to modern manufacturing and industrial environments, enabling real-time monitoring, automation, and predictive maintenance. However, the increased connectivity of these systems also exposes them to a range of cyber threats that could jeopardize both safety and operational efficiency. This case study examines the use of anomaly detection models in securing IIoT environments and highlights the performance and practical advantages of these models in identifying cyber threats.

Threats and Detection Methods

In an industrial facility that relies heavily on IIoT devices, the key security concern was the protection of critical infrastructure components such as programmable logic controllers (PLCs) and SCADA (Supervisory Control and Data Acquisition) systems. These devices are essential for controlling machinery, monitoring sensors, and ensuring the smooth operation of manufacturing processes. The threat landscape included **intrusion attempts**, **data manipulation**, and **device tampering** by malicious actors trying to exploit system vulnerabilities.

The industrial environment required a robust cybersecurity solution capable of monitoring real-time data streams from connected devices. The facility implemented ML -based anomaly detection models to identify deviations in the operational data, which might indicate an ongoing attack. Anomaly detection was chosen because it could operate effectively without the need for a large labelled dataset, which is often unavailable in industrial environments. Unsupervised learning techniques, particularly **k-means clustering** and **autoencoders**, were utilized to detect unusual behaviours such as sudden fluctuations in sensor readings or abnormal communication patterns between devices (59).

Model Performance and Practical Advantages

The performance of the anomaly detection models in this case study was evaluated based on several key metrics, including detection accuracy, false positive rate, and real-time response time. The results demonstrated that the models were highly effective in identifying potential cyber threats, with a detection accuracy rate of approximately 92%. The use of autoencoders allowed for the detection of complex, non-linear anomalies that were otherwise difficult to capture with traditional rule-based systems (60).

One of the major advantages of using anomaly detection in IIoT security was the ability to **reduce downtime**. The models were able to detect abnormal conditions early, providing security teams with the opportunity to take proactive measures before these threats could escalate. For example, a network intrusion was identified by the model when data transmission patterns between sensors and central servers deviated from the expected norm, signalling a potential breach. This early detection led to the rapid isolation of affected devices, preventing widespread system failure (61).

Outcomes and Effectiveness

The implementation of anomaly detection models significantly improved the facility's ability to detect cyber threats in real-time. The system's success in identifying previously undetected attack vectors demonstrated the practical value of ML techniques in enhancing the security of IIoT environments. Additionally, the use of unsupervised learning models allowed the system to continuously adapt to new operational patterns without the need for constant retraining, making it a scalable solution for future threats (62).

Table 6: Summary of Anomaly Detection Performance in Industrial IoT Security

Threat	Detection Method	Effectiveness
Unauthorized Network Intrusion	Anomaly detection (autoencoders, k-means)	High accuracy in detecting network deviations
Sensor Data Manipulation	Anomaly detection (k-means clustering)	Early detection of abnormal sensor readings
Device Tampering	Anomaly detection (autoencoders)	Real-time identification of unauthorized device access

This case study demonstrates that anomaly detection models, particularly those utilizing unsupervised ML, offer a robust solution for securing IIoT systems in industrial environments, contributing to both operational safety and cyber resilience (63).

VIII. FUTURE TRENDS AND CHALLENGES IN IOT CYBERSECURITY

8.1 Emerging Threats in IoT Environments

As the IoT ecosystem continues to expand, the landscape of cyber threats is evolving. New and increasingly sophisticated attack methods are emerging, posing significant risks to IoT devices and their interconnected systems. One such threat is the rise of **AI-driven attacks**, where cybercriminals leverage ML algorithms to autonomously identify vulnerabilities, adapt to changing security protocols, and bypass traditional security measures. These AI-powered attacks can evolve in real-time, making them particularly difficult to detect using conventional cybersecurity methods (64). For example, AI-driven malware could learn the specific weaknesses of a network over time, allowing it to launch highly targeted attacks with minimal detection.

Another growing concern is **advanced persistent threats (APTs)**, where attackers infiltrate IoT networks and remain undetected for extended periods. APTs are typically state-sponsored or highly organized cybercriminal groups that target critical infrastructure. In an IoT context, APTs may exploit device vulnerabilities to gain longterm access to sensitive data, such as patient information in healthcare IoT systems or operational data in industrial settings (65). These persistent threats can cause significant harm, especially when combined with more advanced tactics such as social engineering and insider threats.

8.2 Advancements in ML for IoT Security

To combat the increasingly complex threats facing IoT environments, ML continues to advance, offering new ways to bolster security. **Federated learning** is one of the most promising developments in this area, enabling ML models to be trained across multiple devices without sharing sensitive data between them. This decentralized approach can help preserve privacy while still improving threat detection capabilities. Federated learning allows IoT devices to collaborate in building a global model without exposing personal or sensitive information to a central server, thus improving overall security (66).

Transfer learning is another promising technique that can significantly enhance IoT security. Transfer learning allows ML models trained on one IoT device to be adapted and applied to other devices with minimal additional training. This method is particularly useful in IoT environments where training datasets are often limited, as it enables the rapid deployment of threat detection models across a variety of devices without the need for large amounts of labelled data for each new device (67). These advancements in ML hold the potential to strengthen IoT security by enabling more adaptive and scalable defenses against emerging threats.

8.3 Regulatory and Ethical Considerations

With the growing concerns around IoT security, it is critical to address regulatory and ethical issues that come with the integration of these technologies into sensitive sectors. Regulatory compliance, particularly concerning **data privacy** and **security standards**, is becoming increasingly important. Frameworks such as the **General Data Protection Regulation (GDPR)** in the European Union and the **California Consumer Privacy Act (CCPA)** in the U.S. provide guidelines on how personal data should be handled, including by IoT devices. Ethical considerations, including data ownership and the responsible use of AI in IoT, are also vital to ensure user trust and avoid potential exploitation (68). These regulations help mitigate risks related to privacy violations and ensure that IoT systems are designed with security in mind.

IX. CONCLUSION

9.1 Summary of Key Insights

ML has proven to be a transformative tool in the detection and mitigation of cybersecurity threats within IoT environments. The study reveals that ML approaches, including anomaly detection and supervised learning, significantly enhance the ability to identify and respond to cyber threats in real-time. Anomaly detection techniques, particularly those based on statistical models and ML algorithms, are effective in recognizing deviations from normal behaviours that may signal a potential attack. These models can be adapted to monitor vast amounts of IoT data continuously, identifying threats without human intervention.

Supervised learning models, such as decision trees, support vector machines, and neural networks, have demonstrated significant promise in classifying network traffic and device behaviours into benign or malicious categories. The ability of these models to learn from labelled datasets ensures that they can accurately predict and mitigate known threats while adapting to emerging cyber risks. Furthermore, the integration of data forensics with ML strengthens threat detection, as it enables the systematic analysis of digital evidence to uncover malicious activities in IoT systems.

Another critical insight is the role of data preprocessing in improving ML performance. Proper data cleansing, transformation, and feature extraction ensure that the models are trained on high-quality data, resulting in more reliable and accurate threat detection outcomes. The ongoing development of more advanced ML techniques, such as federated learning and transfer learning, also offers promising avenues for improving IoT cybersecurity, particularly in environments with limited data or privacy concerns.

9.2 Implications for Industry and Research

The insights garnered from this research have several implications for both industry and academic research. For industry, the findings underline the importance of incorporating ML models into IoT security frameworks to enhance threat detection and response capabilities. The ability to automate threat identification through ML can significantly reduce the time to mitigate attacks, minimize damage, and improve overall system resilience.

For academic research, these insights highlight the need for continued innovation in ML techniques tailored to IoT environments. Future research could focus on improving model interpretability, addressing challenges related to dataset imbalance, and exploring new algorithms that can handle the growing complexity of IoT ecosystems. The ongoing study of hybrid models that integrate ML with traditional cybersecurity techniques could also provide valuable contributions to IoT security.

9.3 Final Thoughts on the Future of IoT Cybersecurity

As IoT devices become more integrated into critical sectors such as healthcare, manufacturing, and transportation, the need for robust cybersecurity will only intensify. The future of IoT cybersecurity lies in the continuous advancement of both ML technologies and cybersecurity strategies. Ongoing research and innovation will be crucial in developing more adaptive, scalable, and resilient solutions to protect against evolving cyber threats, ensuring the security and integrity of IoT environments for years to come.

X. REFERENCES

[1] Agarwal R, Dhar V, Raghunathan S. The impact of the Internet of Things on business: Opportunities and challenges. J Bus Res. 2020;120:364-376.

[2] Zhang Y, Deng Y, Chen Y. Data security and privacy protection in cloud computing for healthcare applications. Healthc Inform Res. 2021;27(1):42-48.

[3] Sicari S, Rizzardi A, Grieco LA, Security, privacy and trust in Internet of Things: The road ahead. Comput Netw. 2015;76:163-182.

[4] Fernandes R, Neves R, Tavares J. A security and privacy survey on IoT protocols. Int J Comput Appl. 2014;107(13):9-15.

[5] Chukwunweike JN, Kayode Blessing Adebayo, Moshood Yussuf, Chikwado Cyril Eze, Pelumi Oladokun, Chukwuemeka Nwachukwu. Predictive Modelling of Loop Execution and Failure Rates in Deep Learning Systems: An Advanced MATLAB Approach https://www.doi.org/10.56726/IRJMETS61029

[6] Mendez Mena D, Papapanagiotou I, Yang B. Internet of things: Survey on security. Information Security Journal: A Global Perspective. 2018 May 4;27(3):162-82.

[7] Joseph Nnaemeka Chukwunweike, Moshood Yussuf, Oluwatobiloba Okusi, Temitope Oluwatobi Bakare and Ayokunle J. Abisola. The role of deep learning in ensuring privacy integrity and security: Applications in AI-driven cybersecurity solutions
https://dx.doi.org/10.30574/wjarr.2024.23.2.2550

[8] Falkenreck C, Wagner R. The Internet of Things–Chance and challenge in industrial business relationships. Industrial Marketing Management. 2017 Oct 1;66:181-95.

[9] Chanal PM, Kakkasageri MS. Security and privacy in IoT: a survey. Wireless Personal Communications. 2020 Nov;115(2):1667-93.

[10] Alabdulmohsin I, Al-Muhtadi J, Hashim R. A survey of machine learning for IoT security. Int J Comput Sci Inf Secur. 2020;18(7):56-67.

[11] Zhang Y, Wang S, Deng X, A survey on security issues in health IoT systems. Int J Netw Secur. 2021;23(4):550-560.

[12] Meneghello F, Calore M, Zucchetto D, Polese M, Zanella A. IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices. IEEE Internet of Things Journal. 2019 Aug 13;6(5):8182-201.

[13] Yu X, Wen Q. A view about cloud data security from data life cycle. In2010 international conference on computational intelligence and software engineering 2010 Dec 10 (pp. 1-4). IEEE.

[14] Attaran M. The internet of things: Limitless opportunities for business and society. Journal of Strategic Innovation and Sustainability Vol. 2017;12(1):11.

[15] Roman R, Zhou J, Lopez J. On the security of wireless sensor networks in the IoT context. In: 2013 IEEE World Forum on Internet of Things (WF-IoT); 2013; Seoul, South Korea. IEEE; 2013. p. 321-326.

[16] Bandyopadhyay S, Sen J. IoT security challenges and solutions. J Comput Sci Technol. 2020;35(1):1-15.

[17] Taleb T, Samdanis K, Mada B, A survey on IoT security and privacy. In: 2016 International Symposium on Wireless Communication Systems (ISWCS); 2016; Poznan, Poland. IEEE; 2016. p. 30-35.

[18] Shoukry Y, Moustafa N, Ahmad M, A survey on anomaly-based network intrusion detection systems. J Netw Comput Appl. 2020;168:102710.

[19] Tan C, Wei S, Wu X, A comprehensive survey on machine learning for cybersecurity in the Internet of Things. IEEE Access. 2021;9:113207-113225.

[20] Sharma P, Agarwal A, Kumar A. IoT forensics: An analysis of cybersecurity challenges and data protection. J Comput Syst Sci. 2020;122:32-41.

[21] Gupta R, Sharma V, Tripathi A. Cyber threat analysis and digital forensics in Internet of Things systems. Future Gener Comput Syst. 2021;116:278-295.

[22] Patel S, Kumar R, Sharma A, Machine learning techniques for anomaly detection in IoT environments. Comput Sci Rev. 2021;40:100335.

[23] Rao M, Soni P, Tripathi A, Data forensics and its role in protecting IoT systems from cyber-attacks. J Inf Sec Appl. 2022;58:102670.

[24] Tsai C, Lai Y, Yang C, A survey of data cleaning techniques and their applications in IoT networks. J Comput Sci Technol. 2021;36(1):23-39.

[25] Liu S, Wang Y, Lu C, Data preprocessing techniques for machine learning-based cybersecurity in IoT environments. Int J Comput Sci Inf Secur. 2020;18(2):12-25.

[26] Zhang L, Wang H, Liu X, Data-driven cybersecurity for IoT systems: Challenges and opportunities. IEEE Trans Netw Serv Manage. 2021;18(2):290-306.

[27] Smith J, Patel R, Zhang Y, Automating labeling in large-scale IoT datasets for cybersecurity. Int J Comput Sci. 2020;16(8):2421-2432.

[28] Nguyen T, Kim S, Park S, A study on data labeling techniques in IoT systems for security applications. Comput Commun. 2020;155:34-47.

[29] Yang Q, Chen W, Zhang M, Balancing datasets in cybersecurity machine learning: Addressing class imbalance for IoT security. J Cybersecur. 2021;7(1):76-88.

[30] Chen X, Zhao X, Liu T, Improving machine learning models in cybersecurity through k-fold cross-validation. J Comput Sci Tech. 2021;36(3):312-325.

[31] Xu L, Zhang T, Yang Z, Incremental learning and adaptation for real-time IoT threat detection. Comput Secur. 2020;93:101723.

[32] Li Z, Zhang L, Huang R, Online learning in IoT cybersecurity: Real-time anomaly detection and adaptation. IEEE Access. 2021;9:17234-17250.

[33] Gupta P, Kumar S, Singh A, Feature selection and dimensionality reduction for IoT cybersecurity: Addressing data challenges in machine learning. J Comput Sci Eng. 2020;34(2):56-73.

[34] Zhang L, Wang H, Liu X, Data-driven cybersecurity for IoT systems: Challenges and opportunities. IEEE Trans Netw Serv Manage. 2021;18(2):290-306.

[35] Smith J, Patel R, Zhang Y, Automating anomaly detection in large-scale IoT systems using machine learning. Comput Secur. 2020;92:101710.

[36] Nguyen T, Kim S, Park S, A survey of machine learning methods for anomaly detection in IoT networks. Int J Comput Sci. 2021;36(3):145-158.

[37] Yang J, Chen Q, Liu Y, Hybrid anomaly detection model for IoT cybersecurity. J Comput Sci Eng. 2021;39(6):987-1001.

[38] Xu J, Zhang W, He X, Anomaly detection in IoT environments using unsupervised machine learning. Comput Commun. 2020;159:51-63.

[39] Liu L, Lee J, Li Y, Decision tree based network intrusion detection for IoT systems. J Netw Comput Appl. 2021;168:102734.

[40] Yang K, Kpotufe S, Feamster N. An efficient one-class SVM for anomaly detection in the internet of things. arXiv preprint arXiv:2104.11146. 2021 Apr 22.

[41] Zhang Y, Sun X, Qian Z, Deep learning for IoT cybersecurity: Challenges and opportunities. J Comput Sci Tech. 2021;37(2):435-446.

[42] Wang F, Zhao Y, Zheng Y, Real-time threat classification in IoT systems using supervised learning models. IEEE Access. 2020;8:63572-63584.

[43] Gupta A, Kumar S, Singh A, Overcoming class imbalance in machine learning for IoT threat detection. Comput Secur. 2020;91:101729.

[44] Li Z, Huang R, Chen T, Handling evolving threats in IoT security with adaptive machine learning models. IEEE Trans. Inf. Forensics Secur. 2021;16:2195-2208.

[45] Zhang T, Liu Q, Wang Z. Evaluation of anomaly detection methods in IoT-based systems. Comput Networks. 2020;180:107391.

[46] Chen J, Li L, Xu F, Precision-based approach for cybersecurity in IoT networks. Comput. Commun. 2021;164:99-108.

[47] Wang Y, Gao Z, Yang J. An evaluation of recall and its importance in IoT cybersecurity. J Comput Sci. 2021;35(2):198-207.

[48] Liu X, Zhao W, Zhang H. F1 score-based evaluation for classification of IoT network threats. Comput Secur. 2021;106:102336.

[49] Zhang H, Li X, Yang X. Machine learning-based intrusion detection and prevention for IoT networks. Comput Netw. 2021;188:107509.

[50] Liu X, Zhao W, Zhang H. Real-time anomaly detection for IoT cybersecurity. IEEE Access. 2020;8:141227-141237.

[51] Wang Z, Wang Y, Li L. Dynamic response mechanism for intrusion prevention in IoT systems. J Comput Sci. 2021;15(1):45-53.

[52] Williams M, Thomas R. Secure boot mechanisms in embedded systems: A survey. J Comput Sci Eng. 2020;29(4):125-138.

[53] Patel D, Kumar A. Encryption strategies for securing IoT data. Int J Comput Sci Netw Secur. 2021;21(7):34-44.

[54] Lee S, Cho K. Effective patch management strategies for IoT systems. J Cybersecur. 2022;8(3):105-114.

[55] Smith J, Liu Q. Machine learning in IoT cybersecurity: A comprehensive review. IEEE Internet Things J. 2022;9(7):5630-5645.

[56] Williams T, Zhang W. Anomaly detection in IoT networks: Techniques and challenges. Comput Commun. 2021;178:133-144.

[57] Chen X, Gupta M. Cyber threat detection in healthcare IoT systems. J Health Technol. 2020;34(5):123-132.

[58] Patel D, Kumar A. Encryption strategies for securing IoT data. Int J Comput Sci Netw Secur. 2021;21(7):34-44.

[59] Zhang H, Chen M. Anomaly detection in industrial IoT systems using unsupervised machine learning. Indus IoT Sec J. 2020;8(4):213-227.

[60] Li S, Wang Y. Enhancing industrial IoT security with machine learning models. J Indus Cyber Secur. 2021;6(2):88-99.

[61] Singh R, Kaur G. Real-time anomaly detection for industrial IoT security. Comput Secur. 2021;105:115-125.

[62] Adetunji As, Afolayan A, Olola T, Fonkem B, Odunayo R. An Examination of the Effects of Culturally Relevant Engineering Design on Students' Perception and Engagement in K-12 Stem Classrooms. https://zenodo.org/records/14018572

[63] Kim H, Park S. Unsupervised machine learning techniques for anomaly detection in industrial environments. J Process Control. 2021;53:82-93.

[64] Zhang Y, Li X. AI-driven attacks in IoT environments: The next frontier in cybersecurity. AI Security J. 2022;15(2):115-128.

[65] Brown T, Clark M. Advanced persistent threats in IoT: A growing risk to critical infrastructure. J Cybersecurity. 2021;9(4):233-245.

[66] Zhao X, Liu Z. Federated learning for IoT security: A promising approach to decentralized defense. Comput Secur. 2022;103:75-85.

[67] Kumar R, Sharma S. Transfer learning in IoT security: Enhancing threat detection across devices. Machine Learn. 2023;12(6):417-429.

[68] Wilson D, Patel P. Ethical and regulatory considerations for IoT security. Cyber Law Rev. 2021;7(1):50-61.