Machine Learning-Driven Anomaly Detection of IoT Devices Using Power Consumption Patterns

Reehan Shaveez
dept. of CSE
PES University, RR Campus
Bengaluru, India
reehanshaveez123@gmail.com

Rahul Kalekar
dept. of CSE
PES University, RR Campus
Bengaluru, India
kalekarrahul12@gmail.com

Sudeep Dhotre
dept. of CSE
PES University, RR Campus
Bengaluru, India
dhotresudeep@gmail.com

Hassaan Imran Ahmed
dept. of CSE
PES University, RR Campus
Bengaluru, India
hassanimranahmed9597.hassan@gmail.com

Revathi G.P.
dept. of CSE
PES University, RR Campus
Bengaluru, India
revathigp@pes.edu

***Abstract*—The rapid proliferation of Internet of Things (IoT) devices has introduced significant security challenges, as these devices are increasingly targeted by sophisticated cyberattacks. This paper presents a machine learning-based approach to detect and classify attacks on IoT devices, specifically a smoke detector, thermostat, and smart camera. The proposed system leverages domain-specific features, such as voltage fluctuations, rate of change, and sliding window statistics, to identify anomalies indicative of attacks. The model effectively classifies normal and malicious activities, including tampering, denial of service, and resource drain attacks, achieving high accuracy and reliability. By addressing challenges like data imbalance and incorporating device-specific patterns, the solution demonstrates scalability and robustness. This work highlights the potential of machine learning to enhance IoT security and lays the foundation for real-time, adaptive, and lightweight deployment in smart environments.**

***Index Terms*—Anomaly Detection, Power Consumption, IoT Security, Power profiling**

I. Introduction

The Internet of Things (IoT) is a rapidly expanding paradigm inn the technological world, characterized by the interconnection of physical devices—ranging from simple sensors to complex systems—through the Internet. This interconnection allows these "smart objects" to communicate, collect, and exchange data autonomously, transforming industries and simplify everyday activities. IoT applications involves various domains, such as smart homes, healthcare, transportation, industrial automation, and environmental monitoring. For example, in the world of smart homes, IoT devices like smart thermostats, lighting systems, and security cameras offer convenience and energy efficiency, and in healthcare, wearable devices continuously monitor vital signs, providing real-time health data to doctors.

(Miorandi et al., 2012).One of the most prominent applications of IoT is in smart homes, where devices such as smart TVs, refrigerators, washing machines, lights, moisture sensors, motion sensors, smoke alarms, thermostats, doorbells, and locks are interconnected to provide enhanced convenience, security, and energy efficiency.

Figure 1 illustrates a typical smart home setup with various IoT devices. These devices communicate with each other and with a central control system to automate and optimize household functions. For example, smart thermostats can adjust the temperature based on occupancy and preferences, while smart lighting systems can be controlled remotely or set to operate on schedules. The integration of these devices not only improves the quality of life for residents but also contributes to energy conservation and cost savings.

However, the widespread adoption of IoT devices has brought with it it's security challenges. The intrinsic nature of IoT—containing numerous devices, diverse communication protocols, and extensive connectivity—has given rise to multiple vulnerabilities, making IoT networks susceptible to a variety of cyber-attacks. Security breaches such as unauthorized access, data breaches, distributed denial-of-service (DDoS) attacks, and side-channel attacks are fairly common. These vulnerabilities are exacerbated by the limited computational power and memory of many IoT devices, which restricts the implementation of conventional security measures (Deogirikar and Vidhate, 2017). As a result, IoT devices operate on lightweight security protocols that are vulnerable against sophisticated cyber threats.

Figure 2 shows the global average number of connected devices in the IoT from 2022 to2033. Statista (2024) suggests that the number of IoT devices in the future is expected to be approximately 39.6 billion in 2033, up from 13.8 billion in 2022, with this huge jump it highlights the expanding role of IoT in modern society and underlines the importance of robust security measures in the protection of these devices from potential danger.

Given these vulnerabilities, there is a great need for innovative security solutions tailored to the unique requirements of IoT networks. Among these, anomaly detection has emerged

as a promising approach for identifying potential security breaches. Anomaly detection involves monitoring IoT devices and network traffic for abnormal patterns that may indicate malicious activities. Traditional methods of anomaly detection, such as signature-based detection systems, are not suitable for IoT environments because they rely on predefined attack signatures and cannot learn novel attacks (Zarpelão et al., 2017)

More recent research has focused on utilizing ML techniques for anomaly detection in IoT networks. Machine learning-based approaches can analyze large datasets to identify deviations from normal behavior, making them well-suited for detecting previously unknown threats. Techniques include supervised learning, wherein models are trained on labeled datasets, and unsupervised learning, which identifies anomalies based on deviations from normal behavior from default patterns without prior knowledge of the type of attacks (Cook et al., 2020). Though promising, ML-based techniques may consume substantial computational powers, making them difficult to deploy in constrained IoT environments.

One innovative way to overcome these limitations is by using power consumption data to detect anomalies in IoT devices. This method exploits the intrinsic relationship between a device's operational state and its power usage. By monitoring power consumption data continuously, discrepancies, which may point to an anomaly or security breach, could be identified. For example, a sudden, unexpected power usage spurt could indicate unauthorized access or malware activity (Mohammed et al., 2019). This technique is very useful in IoT applications, since monitoring all devices and network traffic directly is not possible due to resource limitations. Anomaly detection based on power consumption is lightweight, non-intrusive, and efficient for the discovery of potential threats, thus making it a real IDS for IoT networks.

This survey paper focuses on exploring the growing field of power consumption-based anomaly detection for IoT security. It provides a comprehensive overview of the existing methodologies, discusses their advantages and limitations, and highlights the potential of using power consumption data as a reliable indicator of anomalous behavior in IoT networks. By examining the latest developments and research trends, this paper aims to underscore the need for novel detection mechanisms that are both efficient and effective in safeguarding IoT infrastructures against evolving cyber threats.

II. Background and Motivation

IoT or the Internet of Things is a modern technology concept that has turned into a pivotal domain that lets various appliances and systems be connected with each other through the internet. It gives them the ability to do everything on their own like gathering and analyzing data without human intervention. The unbound introduction of IoT devices into different sectors, such as smart homes, healthcare, industrial automation, and smart cities, has changed the way people use technology and manage information. Nonetheless, the quick progress in this field also raised some security risks that need to be solved so that the IoT networks can be both secure and be able to work reliably. This part is an Introductory part where we will learn about the major concepts of IoT and its components, the investigation of common IoT security threats and issues, and a clear explanation of the need for Anomaly detection in IoT security

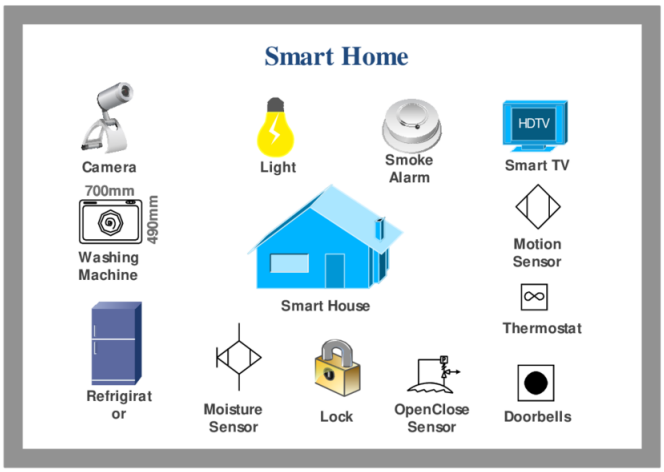

Fig. 1. Illustration of a Smart Home with IoT Devices (Joseph et al., 2020)

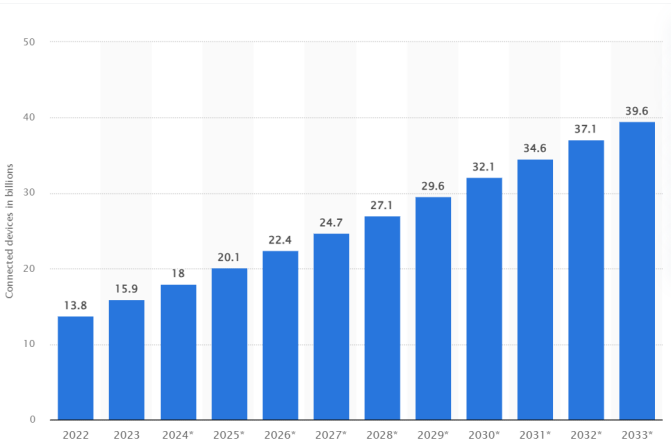

Fig. 2. Global IoT Connected Devices Growth (Statista, 2024)

A. Overview of IoT Architectures and Their Components

The architecture of a typical Cyber-Physical System (CPS) used for power profiling involves several layers, each responsible for different aspects of data collection, processing, and control. The CPS integrates computational and physical capabilities to monitor and control physical processes. Figure 6* illustrates the architecture of a CPS, highlighting the interaction between various components.

IoT architecture typically consists of several layers that work together to facilitate communication and data processing across a network of connected devices. The primary components of an IoT architecture include:

Figure 3 illustrates the different layers of IoT architecture:

1) **Perception or Device Layer (Sensors and Actuators)**: The IoT architecture has the basic layer which is a Device layer, where all the physical devices, sensors, and actuators that interact with the environment or make specific actions to perform are located. Sensors are the means by which environmental parameters like temperature, humidity, motion, and light are measured, and actuators actually perform actions based on sensor data, such as adjusting a thermostat or turning on lights (Gubbi et al., 2013)
2) **Transport or Communication Layer (Network Protocols and Gateways)**: Through the use of protocols, data is sent from IoT devices to the cloud and then to other devices. Network protocols (like MQTT, CoAP, HTTP) and gateways that allow devices to communicate via different communication channels such as Wi-Fi, Bluetooth, Zigbee, and cellular networks are included. (Al-Fuqaha et al., 2015) Gateways are used as intermediaries between devices and the cloud, converting different communication protocols to ensure the data exchange is smooth.
3) **Edge/Fog Computing Layer:**: Edge or fog computing represents data being processed closer into the source, that is at the edge of the network rather than all data across the entire network to a centralized cloud server. This layer cuts latency down, improves time-to respond, and reduces Bandwidth usage by p.
4) **Cloud Layer (Data Storage and Analytics)**: The cloud layer offers centralized storage, data processing, and analytics capabilities. It collects data from edge devices and performs complex analytics, machine learning, and decision-making tasks that require significant computational resources. The cloud also serves as a platform for deploying IoT applications and services (Botta et al., 2016).
5) **Application Layer**: The layer in question encompasses every single IoT application.along with service that includes interface and interaction by user. Applications range from smart home management systems to industrial automation platforms, which offer the very users (Bandyopadhyay Sen, 2011) with the ability to remotely monitor and control IoT devices.
6) **Business Layer**: The Business Layer is in charge of managing the general business Logic and processes involved in IoT applications includes such as Business models, revenue generation, compliance, and regulatory requirements. This Layer ensures business outcomes in the IoT solution and deliver value to Those are stakeholders. This also includes the integration of IoT data with enterprise systems to for decision-making and planning strategically (Xu et al., 2014)

Figure 4 illustrates these possible attacks, with emphasis on the importance of implementing comprehensive security measures across all layers of the IoT Architecture.

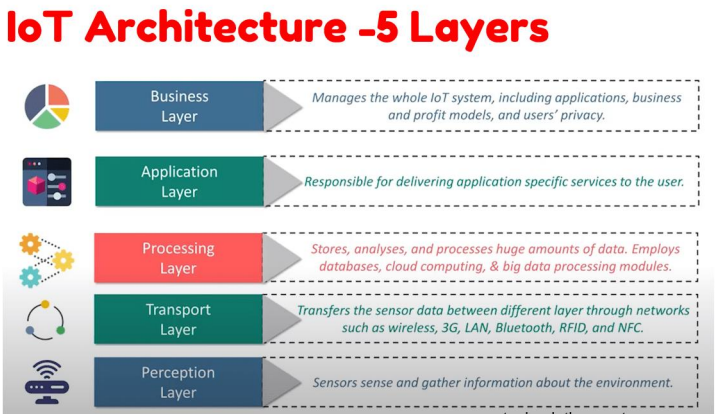

Fig. 3. IoT Architecture Layers (Source: Pantech Solutions, 2024)

IIoT Layers	Components	Possible Attacks
Layer 1	Sensors, Motors, Actuators, Transmitters, and Embedded Devices	Reverse Engineering, Malware, Eavesdropping, Brute Force attack
Layer 2	Distributed Control Systems, Programmable Logic Control (PLC's), and Gateways	Man-in-the-Middle attack, Sniffing, Brute Force attack, Replay attack
Layer 3	Supervisory Control and Data Acquisition (SCADA) Control, Control Room and Operator Stations and Human Machine Interactions (HMI)	IP spoofing, Data sniffing, Data Manipulation, Malware
Layer 4	Data Centers, Office Applications, Intranet, Mail and Web services	Phishing, SQL Injections, Malware, Domain Name Server (DNS) poisoning, Brute Force attack
Layer 5	Business Applications, Cloud Computing, Data Analytics, Internet and Mobile Devices	Denial-of-Service (DoS) attack, Side channel attack, Malware, Password attack, Man-in-the-middle attack

Fig. 4. Possible Attacks on Different IoT Architecture Layers (Shah Sengupta, 2020)

The convergence of these elements makes it possible for IoT devices to communicate and exchange data easily, thereby making the IoT ecosystem more interoperable with its devices Perform more complex tasks and provide valuable insights. Yet, the quality of being Interconnected and the IoT environment brings to it several security vulnerabilities. That should be treated to ensure the integrity and privacy of the IoT networks.

B. Discussion of Common IoT Security Threats and Challenges

The Internet of Things has permeated so rapidly that it has reached the stage of being of the highest importance to ensure security. IoT devices are often have limited computational power and memory, making them unable to support robust security protocols. Moreover, the diversity of devices and

Communication protocols in IoT ecosystems create a heterogeneous environment that is Difficult to secure uniformly. Notable IoT security threats and challenges include the following:

1) **Unauthorized Access and Data Breaches**: IoT devices sometimes lack robust Authentications and Access Control Mechanisms make them susceptible to unauthorized access. And these vulnerabilities can be taken advantage of by hackers to seize sensitive data or make IoT devices control (Zhang et al., 2014).
2) **Device Spoofing and Identity Theft**: Attackers can spoof legitimate IoT devices to It injects malicious data or commands into the network. This leads to data corruption, network disruption, or unauthorized control over IoT systems. Identity theft in IoT is impersonating legitimiate devices or users to gain unauthorized entry for IoT devices services and resources (Sicari et al., 2015).
3) **Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks**: IoT devices are highly susceptible to DoS and DDoS attacks. These devices commonly have constraints in processing power and bandwidth that leave these attacks almost unopposed. These attacks tend to target devices or networks with traffic that can hardly be processed by them, thus disabling those devices. An example of this is the Mirai botnet attack, which especially targeted IoT devices to launch a massive DDoS attack (Kolias et al., 2017).
4) **Malware and Ransomware Attacks**: Getting infected by malware or a ransom virus IoT devices can be utilized by cybercriminals to gain unauthorized access, carry out data exfiltration or cause the device to malfunction. The IoT devices are heterogeneous in Nature which makes the detection and countermeasures very difficult (Alrawais et al., 2017).
5) **Side-Channel Attacks**: This kind of attacks involve the leakage of information created by the physical operation of devices, such as power consumption or electromagnetic emissions, to possibly deduce sensitive information. Side-channel attacks pose a massive threat to IoT devices, especially those with weak cryptographic implementations (Park Tyagi, 2017).
6) **Data Integrity and Privacy Concerns**: IoT networks will generate vast amounts of sensitive data, including personal info, industrial control commands, and health records. Therefore, the integrity and confidentiality of such data are critical. In most cases, however, most IoT devices still lack adequate encryption and protection mechanisms regarding their privacy; hence, they remain vulnerable to eavesdropping and even data tampering (Sicari et al., 2015).

C. Explanation of the Need for Anomaly Detection in IoT Security

Traditional security measures, including network traffic analysis and behavior-based detection, often entail such a significant computational burden as to affect the performance of IoT devices. Such methods may not be suitable for resource-constrained environments, where IoT devices run with limited processing power and memory. Power consumption-based anomaly detection offers such an alternative as it is lightweight and non-intrusive, as it monitors the power usage pattern of the devices. This method relies on the fact that various states of operation and activities of a device correspond to different power consumption profiles. It can be continuously monitored in a way that anomalies corresponding to potential security threats are detected.

For example, in smart homes environments, patterns of power consumption can unveil unusual activities that would indicate unauthorized access or the presence of malware. Similarly, in industrial settings, monitoring the power usage of IoT devices will contribute to the detection of hardware intrinsic attacks, such as covert channel and power depletion attacks. This can prove promising in the detection of security threats of high accuracy based on combining current and historical power consumption data through Cyber-Physical Systems (CPS) machine learning techniques, such as logistic regression.

Feature	Traditional Security Measures	Power Consumption-Based Anomaly Detection
Computational Overhead	High – Often requires substantial processing power and memory resources, especially for techniques like encryption and behavioral analysis.	Low to Moderate – Relies primarily on analyzing power data, which can be computationally lighter. Efficient algorithms can minimize overhead.
Intrusiveness	Moderate to High – May involve real-time system scanning, software installations, or extensive system modifications.	Low – Non invasive approach, as it passively monitors power usage patterns without disrupting system operations.
Suitability for Resource-Constrained Environments	Limited – High computational and memory demands make it unsuitable for low-power devices and IoT environments.	High – Suitable for IoT and other resource limited environments due to its lower energy and computational requirements.

TABLE I
COMPARING TRADITIONAL SECURITY MEASURES WITH POWER CONSUMPTION-BASED ANOMALY DETECTION IN TERMS OF COMPUTATIONAL OVERHEAD, INTRUSIVENESS, AND SUITABILITY FOR RESOURCE-CONSTRAINED ENVIRONMENTS.

In basic terms, anomaly detection refers to the process of finding patterns in data that may not behave as expected. Inside IoT security, anomaly detection can be performed to monitor network traffic, device behavior, and power consumption patterns with hopes of catching any deviations that might indicate malicious activities. There are multiple reasons why anomaly detection in IoT security is important:

1) **Detection of Unknown Threats**: Unlike signature-based detection, anomaly detection does not depend on predefined signature of attacks. This is to say, it will detect new or unknown threats which have yet to be identified. Most importantly, the emergence of new attack vectors and vulnerabilities makes this crucial in IoT environments. Indeed, such vulnerabilities keep

emerging in IoT systems (Nguyen et al., 2019).

2) **Resource Constraints of IoT Devices**: Most IoT devices have low computing capabilities and cannot be equipped with sophisticated security protocols. Techniques based on lightweight metrics, such as power consumption-based anomaly detection approaches, can offer efficient monitoring from security threats without too much overhead on the devices themselves (Myridakis et al., 2019).
3) **Real-Time Monitoring and Response**: The IoT network should be monitored in real-time to respond to threats immediately. The anomaly detection system continuously monitors the network and device behavior, making it possible to detect potential security incidents right away (Anthi et al., 2018).
4) **Adaptability to Dynamic Environments**: IoT environments are in general dynamic in nature; devices often join and sometimes leave the network with time, while their communication patterns vary. Thus, anomaly detection systems learn and update behavioral models about the changes in the scenarios, thus becoming well-suited to IoT security (Cook et al., 2020).

Overall, anomaly detection offers a strong and flexible approach towards strengthening the security of the IoT environment so as to address the unique problem of the diverse dynamic nature of IoT networks.

III. Related Work

In particular, growing deployments of IoT devices across various industries require the establishment of robust mechanisms in security to safeguard such networks from various types of cyber threats. In this regard, anomaly-based detection is considered one of the primary methods in Detecting and mitigating such cyber attacks within the IoT environment. There are some special characteristics of the IoT network: a large number of connected devices communicate using heterogeneous protocols, and devices experience resource-constrained situations. Different researchers thus adopted anomaly detection strategies well suited to the IoT context. The remainder of this section summarizes recent related work concerning methods of anomaly detection in IoT security, based on three main categories: network traffic-based, behavior-based, and power consumption-based detection. This section outlines the limitation and associated challenges of such methods in relation to resource-constrained IoT devices.

A. Network Traffic Analysis-Based Anomaly Detection

Network traffic analysis essentially involves network traffic analysis through observation of data packets transmitted over the IoT network to identify patterns that are outside the normal trend and may be indicative of a security threat. Indeed, much has been done using this approach because of its proven efficiency in the detection of different types of network-based attacks, such as DoS, MITM attack, and botnet activities.

Several researchers have recently proposed innovative approaches that can be used to better enhance network traffic analysis efficiency in IoT security. Mothukuri, et al (2021) made a federated-learning-based anomaly detection scheme that used decentralized data stored on devices to enhance privacy. This approach allows IoT to collaboratively learn a shared anomaly detection model without sharing raw data, thus preserving privacy and effectively detecting network anomalies. Nguyen et al. further developed in 2019 an autonomous self-learning distributed system for compromised IoT device detection using a federated learning framework to efficiently aggregate behavior profiles. Though innovative, these methods meet challenges with regards to computational overhead and energy consumption, which can be significant for low power IoT devices.

Nguyen et al. proposed PSI-Graph, an anomaly detection approach using graphs on IoT networks, which extracted high-order features from the function-call graph of every executable file. Although that provides a panoramic view of network behavior and offers very high accuracy in anomaly detection, this is extremely computationally expensive and thus the applicability of this method on resource-constrained IoT devices is clearly infeasible.

Various research efforts based on network traffic analysis are dedicated to the efficiency of IoT security. Summerville et al. (2015) presented a lightweight deep packet inspection ADS applicable on resource-constrained IoT devices. This technique is also suffering from some processing and energy overheads. Meidan et al. (2018) proposed N-BaIoT, a network-based botnet attack detection framework encapsulating the behavioral snapshots of network traffic. Although successful with botnet activities, reliance on continuous network monitoring of N-BaIoT makes it challenging in terms of scalability; hence, not necessarily practical in all IoT environments.

B. Behavior-Based Anomaly Detection

Some of the behavioral detection methods monitor the IoT device's operational patterns and behaviors to identify any deviation from normal activities that may indicate a security threat. That said, these approaches are independent of any predefined attack signature and hence are quite effective in detecting new or unknown threats. A lot of behavior-based anomaly detection systems have been developed based on various ML techniques such as deep learning, clustering, and statistical analyses.

Pajouh et al. (2016) used statistical techniques such as Bayesian theory, Hidden Markov Models (HMM), and cluster analysis to identify anomalies in smart home environments. Their approach gave a high accuracy rate in identifying anomalies by analyzing sensor data at the network level. Ramapatruni et al. (2019) proposed an HMM-based approach that especially identified anomalous activities in smart homes, which achieved an impressive accuracy of 97%. Fahad and Rajarajan (2015) introduced a density-based clustering approach to classify known activities of smart devices, thus providing a scalable framework for detecting anomalies in dynamic environments.

Yamauchi et al. (2019) proposed an anomaly detection system (ADS) for smart home based on user behavior as a

sequence of events incorporating sensor data and times of user operation. This method is very effective at catching those common behaviors but does not even notice the operations for which related events are not recorded, which therefore can be blindspots in detection coverage. For instance, Novák et al. (2013) used Self-Organizing Maps (SOM) to analyze user activities in smart homes, but their technique tends to produce very high false positives since the pattern of behavior of users varies.

A new intrusion detection system was presented by Anthi et al. in 2018, which combines network analysis with behavioral learning and rule-based approaches. This model effectively identified network scanning, probing, and simple DoS attacks. However, its reliance on predefined rules and network traffic data limits its adaptability to novel attack vectors.

C. Power Consumption-Based Anomaly Detection

One of the most recent research areas for IoT anomaly detection relates to researching the application of power consumption data to identify security breaches. In this respect, there is an operating state and its power use in a device; thereafter, power consumption anomalies may relate to unauthorized access or malware presence.

Jiménez et al. 2016 were some of the first ones to investigate power consumption as a source indicator for generalized malicious activity in general-purpose computers. Although this approach resulted in encouraging outcomes that could have possibly led to the utilization of power information for malware detection, it would apply very minimally to IoT devices because the power consumption might vary significantly based on the type of computer used. Building on this further, Myridakis et al. (2019) suggested using supply current to predict the anomalies in manufacturing or operation of application-specific IoT devices and valued this technique to be useful for devices with minimal functionalities.

Nimmy et al. (2022) developed an anomaly detection system for smart homes, in which it utilizes the power consumption of IoT devices to detect anomalous behavior. The power traces were gathered for normal and attack scenarios, including DDoS attacks, using a smart camera built with Raspberry Pi. Then, several machine learning models, such as a deep feed-forward neural network (DFNN), were trained on this data. The DFNN model obtained an accuracy of 99.2% in anomaly detection, which also implies that power consumption might be a more promising parameter for anomaly detection in smart homes. This approach has an advantage over other approaches as it does not add additional overheads to resource-constrained IoT devices.

Mohammed et al. (2019) proposed a non-intrusive approach to detect Hardware Intrinsic attacks on IoT devices using power profiling. Their experiment tested the detection of covert channel and power depletion attacks based on IoT devices' power profile in various modes of operation. Power consumption data was analyzed using a Random Forest algorithm with an accuracy of 95.5% for normal and attack modes classification. It is scalable and portable, hence easily applicable for real-time analysis and detection across different networks. The proposed method does not require any adaptation of the IoT devices; it develops a general operational behavior of all the integrated circuits embedded in the IoT device.

Majumder et al. (2020) introduced a Cyber-Physical System (CPS), known as "Smart-Power," which detects IoT security threats via heterogeneous wireless sensor devices' behavioral power profiling using a smartphone. The system is tracking power usage of the IoT devices at Idle, Active, under DDoS attack, and under MitM attack; logistic regression techniques are used to make it alert of abnormal power behavior.The system achieved an average accuracy of 74% in detecting potential security threats, with a device-specific high of 85%. The addition of Power Spectral Density (PSD) analysis improved the predictive accuracy of the model. This non-invasive system can be integrated into edge management tools or implemented at the core/data center level, providing real-time monitoring and threat detection using a smartphone interface.

The work presented in 2019 by Hasan et al. was an anomaly detection system of IoT devices based on features such as source address, timestamp, and accessed node address. This again introduces network latency in the approach and can be spoofed, which again creates a doubt over the reliability of the feature set used. Dilraj et al. improved the shortcomings in the model to achieve better accuracy in anomaly detection on IoT devices with low computational overhead by using power consumption data.

Park and Tyagi (2017) showed the effectiveness of leveraging power consumption in side channel attacks, which makes use of the physical emissions of a device, such as power usage, to infer secret information. This research underscores the potential of power-based methods for both offensive and defensive cybersecurity applications in IoT. Al Shorman et al. (2020) further explored unsupervised IoT botnet detection using power consumption data from the N-BaIoT dataset, demonstrating the efficacy of this approach for detecting botnets without requiring labeled data.

D. Limitations and Challenges of Existing Methods

Although much progress has been attained in this area of anomaly detection for IoT security, several challenges remain, especially concerning resource-constrained IoT devices. Classic network traffic analysis approaches require major computational and storage capacities to analyze abundant data flows, which largely conflicts with the abilities of low-power IoT devices. In order to avoid this, classical methods may give a high number of false positives, making lots of unnecessary alerting and processing overhead.

On the other hand, behavior-based detection methods can give a more fine-grained insight into device activities. These greatly depend on data collection and pre-processing, which may turn out to be challenging in an inherently resource-constrained IoT environment. Besides, these sorts of methods are prone to deviation in normal behavior that often results in false positives in anomaly detection.

While power-consumption-based detection has indeed given a promising solution, especially for resource-constrained environments, by leveraging a non-intrusive metric that can be passively monitored with very little overhead, variability in power consumption owing to either environmental factors or legitimate changes in device operation may be problematic for distinguishing between benign and malicious anomalies. Furthermore, sophisticated attackers may adjust their attack strategies to masquerade their power consumption as normal, which evades their detection.

The ultimate conclusion is that the detection of the anomaly in IoT security, if the literature reviewed is anything to go by, has been done using different ways, which no doubt are characterized by their different strengths and weaknesses. Network traffic analysis, behavior based detection, and power consumption-based detection are just the main categories. Power consumption-based detection is a novel, lightweight solution suitable for resource-constrained IoT environments, but robust, comprehensive security may still be provided by implementing multiple approaches. Future research should therefore focus on the development of hybrid models that would tap into the strengths of different approaches in a bid to address the peculiar challenges that arise in IoT security.

IV. Methodologies for Anomaly Detection

Anomaly Detection in IoT networks represents an essential leg in cybersecurity that might search for abnormal patterns or activities that would eventually indicate a potential security threat. These characteristics amply demand a whole range of methodologies operating under conditions specific to IoT environments, such as the diversity of devices, communication protocols, and resource constraints. This section is dedicated to an intensive review of the various methodologies employed for anomaly detection in IoT, which will be mostly conducted based on the three major approaches: network traffic analysis-based detection, behavior-based detection, and power consumption-based detection.

A. Network Traffic Analysis-Based Detection

Network traffic analysis-based detection calls for data packet analysis over an IoT network in order to observe the existence of anomalous patterns indicative of possible security threats. This is why it has been widely used because it has proven to be quite effective in detecting a wide range of attacks based on the use of networks, such as DoS, MITM attacks, botnet activities, etc.

Key Techniques:

1) **Deep Learning-Based Approaches**: Anomaly detection in network traffic data is a task facilitated by deep learning models, such as Convolutional Neural Networks and Recurrent Neural Networks. These models are able to learn complex patterns from large datasets and, therefore identify sophisticated attacks that other techniques may miss. For example, Ullah and Mahmoud (2021) proposed an anomaly detection scheme that efficiently identifies network data through an anomaly finding scheme based on CNN. The proposed deep learning model captures the temporal and spatial pattern of network traffic; therefore, both known and unknown threats are detected.
2) **Federated Learning-Based Approaches**: Federated learning is a decentralized methodology where numerous IoT devices are cooperating to learn from a common model but keep data localized on the devices. Mothukuri et al. (2021) proposed an anomaly detection scheme based on federated learning. The proposal increases privacy as there is no need for data transmission to a central server. With this approach, decentralized data on devices is exploited for training deep learning models in a manner that maintains privacy and successfully identifies network anomalies. In much the same way, Nguyen et al. (2019) proposed a federated learning framework applied to the aggregation of behaviour profiles with efficiency in an autonomous self-learning distributed system. Federated learning is specifically best applied to IoT environments when data security and privacy become concerns.
3) **Graphical Models and PSI-Graph**: Several efforts have been done to model probabilistic relationships among various network events by using graphical models, such as Bayesian networks and Markov Random Fields. Nguyen et al. proposed a graph-based approach called PSI-Graph for the purpose of anomaly detection in IoT networks.The method extracts high-level features from function-call graphs of each executable file. This technique gains a general view of the behavior of the network and ensures high accuracy for anomaly detection. However,most of these graphical models are computationally very expensive, which represents a limiting factor for resource-constrained IoT environments.

Advantages

- **High Accuracy**: Network traffic analysis-based methods can achieve high accuracy in detecting various types of network-based attacks due to their ability. to analyze detailed packet-level data.
- **Detection of Known and Unknown Threats**: Deep learning models can learn using complex patterns, thus enabling the detection of unknown threats as well as known threats without signatures.
- **Scalability**: These methods can be scaled to monitor huge networks by deploying models at different points within the network infrastructure.

Disadvantages

- **High Computational Overhead**: Analyzing large volumes of network data requires significant computational power and storage capacity, which may not be feasible for low-power IoT devices.
- **Privacy Concerns**: Centralized data collection and analysis may raise privacy concerns, especially in sensitive IoT applications such as healthcare.

- **Heterogeneity of Devices**: The diversity of IoT devices and communication protocols poses challenges in standardizing detection mechanisms across different environments (Zarpelão et al., 2017).

B. Behavior-Based Detection

The detection methods are based mostly on either behavioral focuses: monitoring operational patterns or behaviors of IoT devices to identify deviations from normal activities that may indicate a security threat. Such approaches work particularly well for insider threat detection, among other forms of attack cases not easily captured just through network traffic analysis alone.

Key Techniques

1) **Statistical Methods**: Statistical techniques, such as Bayesian theory, Hidden Markov Models (HMM), and cluster analysis, are commonly used for behavior-based anomaly detection.Pajouh et al. applied these statistical techniques to detect anomalies in smart home environments using network-level analysis of sensor data. Their approach could achieve a high accuracy of anomaly detection based on probabilistic relationships between different device behaviors.
2) **Machine Learning Models**: A variety of machine learning models have been used to develop behavior-based anomaly detection systems, ranging from unsupervised learning methods such as clustering (e.g., k-means, DBSCAN) to supervised learning methods like Support Vector Machines (SVM) and Decision Trees. Fahad and Rajarajan proposed a density based clustering approach to recognize activity instances of smart devices in a smart home environment. The method indeed effectively clusters recognized activities but may suffer from high false positives when device behavior changes.
3) **Self-Organizing Maps (SOM) and Neural Networks**: Self-Organizing Maps (SOM) and artificial neural networks (ANNs) have been utilized to model and detect deviations in device behavior. Novák et al. (2013) applied user activity analysis in smart homes using the SOM; their approach tends to yield a high number of false positives due to the inherent variability in user behavior patterns. Similarly, Yamauchi et al. (2019) have introduced a concept of smart home anomaly detection system based on user behavior represented as a sequence of events, while incorporating sensor data with times of user operations.

ADVANTAGES

- **Detection of Insider Threats**: Behavior-based detection effectively identifies the threats posed by insiders and other activities that are not too easy to capture from Network Traffic Analysis.
- **Adaptability to Unknown Threats**: These methods do not rely upon known signatures, which in turn makes them adaptive towards unknown threats.
- **Granularity**: Provides a much more granular view of device activities and can detect subtle deviations that otherwise may imply malicious activity.

DISADVANTAGES

- **Data Dependency**: Extensive data collection and preprocessing which can be impractical in resource-constrained IoT environments.
- **High False Positives**: Because of the dynamic heterogeneity of the IoT devices, their behavior can change dramatically over a period of time, resulting in high false positives.
- **Computational Complexity**: Advanced ML models used in behavior-based detection may be too resource-intensive for deployment on IoT devices with limited capabilities (Cook et al., 2020).

C. Power Consumption-Based Detection

Power consumption-based anomaly detection is an emerging approach within the realm of IoT anomaly detection which relies on the unique pattern that different IoT devices exhibit regarding power usage to detect security breaches. This technique is based on the simple empirical observation that all the different operational states of any given device correspond to some peculiar power consumption profile. Continuous monitoring of power consumption can, therefore easily detect deviations that may signal unauthorized activities, malware presence, or malfunctioning of a device.

Techniques and Models Used for Detection:

1) **Supply Current Monitoring:**: Myridakis et al. in 2019 proposed anomaly detection for IoT devices based on supply current. Their approach works best specifically for application-specific IoT devices with minimal functionality that their patterns of power consumption are predictable. The proposed technique detects anomalies in the electrical current supplied to an instance of a single device which may signify a prospective security threat and therefore out of the normal profile of current.
2) **Power Consumption Profiling and Anomaly Detection**: Jiménez et al. (2016) studied the feasibility of using power consumption data as an indication of malicious activity in general-purpose computers. They developed a monitoring method for power consumption patterns to identify anomalies related to malware execution. Although their solution was conceived with general-purpose computers in mind, it showed promise for power-based anomaly detection in IoT contexts. Similarly, Dilraj et al. (2019) utilised power consumption data to identify anomalies in IoT devices and obtained a higher accuracy with minimal computational overhead.
3) **Side-Channel Attack Detection**: Park and Tyagi 2017 demonstrated that using power consumption is feasible for a side-channel attack- a method of inferring secret information from the physical emanations of a device, such as power consumption. The developed work highlights the capabilities of power-based techniques not

only in offensive but also in defensive cybersecurity solutions for IoT. These techniques can identify side-channel attacks by anomalies in power consumption related to malicious operations.

The methodology for IoT anomaly detection includes the key steps of data collection toward threat detection. The approach adopted by Nimmy et al. (2022) presents an overall framework for leveraging power consumption data to identify anomalies in smart home environments.

*Figure 5, depicts the research methodology used in their work:

1) **Data Collection**: The power consumption of the different IoT devices in a smart home setting is acquired. Here, data would be collected on the normal scenario and attack scenarios with DDoS attacks occurring on the system.
2) **Preprocessing**: The data collected is preprocessed to eliminate noisy and irrelevant information. This process ensures that the data set collected is clean and ready for analysis.
3) **Feature Extraction**: It extracts those relevant features from the preprocessed data. These features are the power consumption patterns of the devices, and these features are important for anomalies identification.
4) **Model Training**: Various machine learning models such as a DFNN are trained on the features extracted. These models learn to classify between normal and anomalous usage patterns.
5) **Anomaly Detection**: The trained models detect anomalies in real-time. When anomaly is found, it could be an indicator of a security attack in terms of unauthorized access or existence of malware.

Nimmy et al. (2022) demonstrated that their approach obtained an accuracy of 99.2% for anomaly detection, which proves the viability of using consumption data from power sources for IoT security. Figure 5, illustrates this methodology, showing the detailed steps of the process used in anomaly detection:.

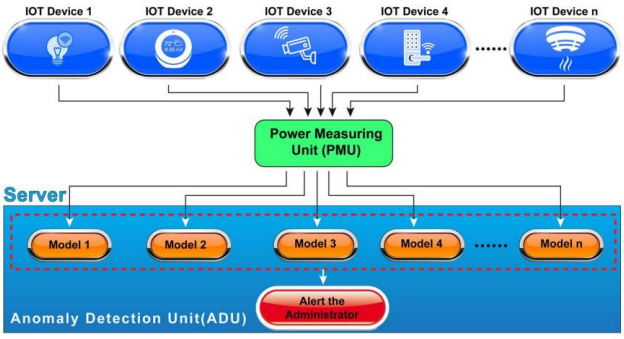

Fig. 5. Anomaly Detection System Methodology (Nimmy et al., 2022)

Power Consumption Patterns: Normal vs. SYN Flood Attack

The IoT device power consumption patterns may well indicate major anomalies when the devices happen to be compromised. Figure 7 depicts the normal and typical SYN flood attack power consumption behaviors of IoT devices as presented in Nimmy et al. (2022).

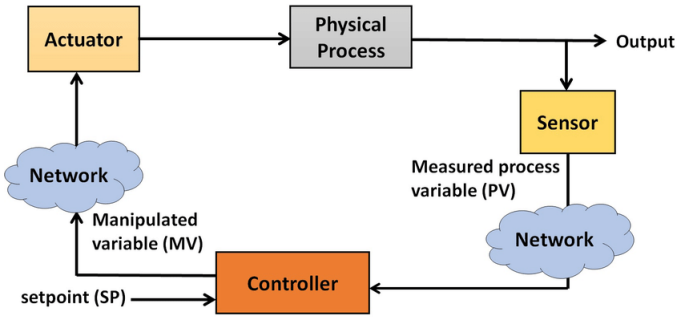

Fig. 6. Architecture of a Typical Cyber-Physical System (CPS) (Tuptuk et al., 2021)

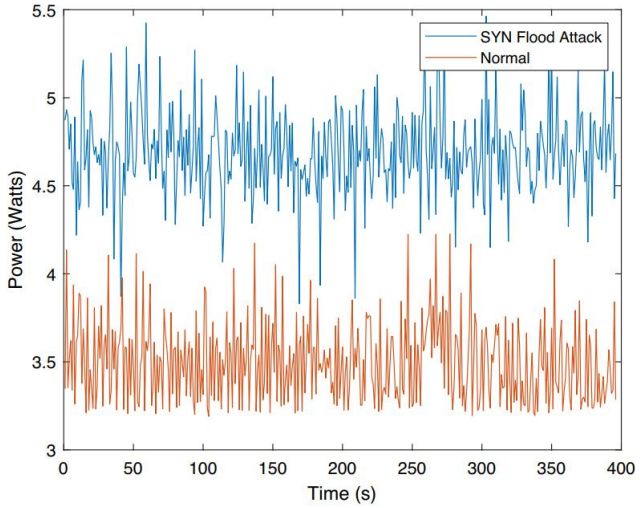

Fig. 7. Power Consumption Patterns: Normal vs. SYN Flood Attack (Nimmy et al., 2022)

1) **Normal Conditions**: In this case, the power consumption of IoT devices is relatively stable with minor fluctuations. It will be considered as a normal operational state in the typical condition without any interference.
2) **SYN Flood Attack**: SYN Flooding Attack SYN flooding attack is characterized by the sudden spiking of power consumption of IoT devices. It is a kind of DoS attack where multiple SYN requests flood the target device through the network, thus depleting its resources and denying services. The power consumption is spiked because the device tries to handle the excess network traffic that keeps it busy.

The study by Nimmy et al. (2022) proved that anomalies related to power consumption patterns during a SYN flood attack can be recognized. Through monitoring and analyzing power consumption data, there is the ability to detect anomalies that reflect a possible occurrence of cyber-attacks. The performance of the model deep feed-forward neural network

was very good in predicting the occurrence of anomalies at 99.2%.

Figure 7 represents the comparison between an ordinary case and a SYN flood attack concerning the types of differences in the power consumption patterns.

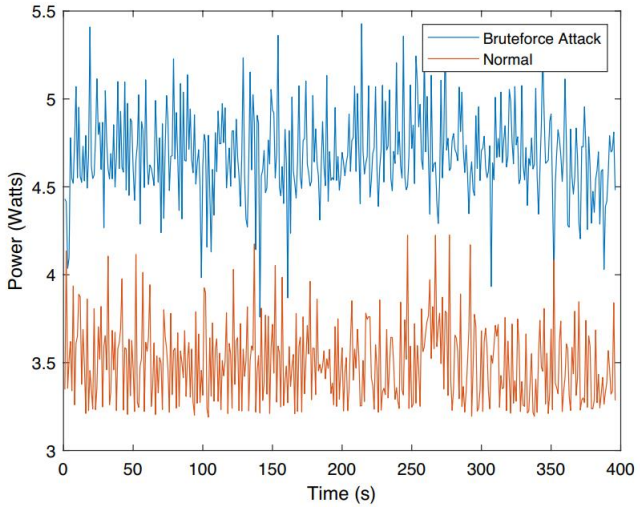

Fig. 8. Power Consumption Patterns: Normal vs. Brute Force Attack (Nimmy et al., 2022)

Power Consumption Patterns:Normal vs. Brute Force Attack

The various kinds of cyber-attacks may have different effects on the power usage profile of IoT devices. Figure 8 represents the power usage profile of IoT devices under normal circumstances and during a brute force attack as depicted in the article by Nimmy et al.(2022).

1) **Normal Conditions**: The power consumption of the IoT devices would normally oscillate a little bit but remains stable. As such, this would be an atypical operational state of the devices without an external interference.
2) **Brute Force Attack**: During a brute force attack, the power consumption of IoT devices depicts irregular and significant fluctuations. A brute force attack involves repeatedly trying to gain access to a device by using numerous combinations of passwords. This leads to increased processing activity with increased power consumption as the device handles repeated authentication attempts.

Nimmy et al. (2022) illustrates that the unique power consumption patterns occurring during a brute force attack can be identified and detected for anomalies. Monitoring and analyzing power consumption data could provide insight into behavioral changes that might result in the presence of an attack. For instance, the accuracy of anomaly prediction was found to be 99.2% in using a deep feed-forward neural network model.

Figure 8 shows a graphical outline of the power consumption differences between normal operation and an attack scenario.

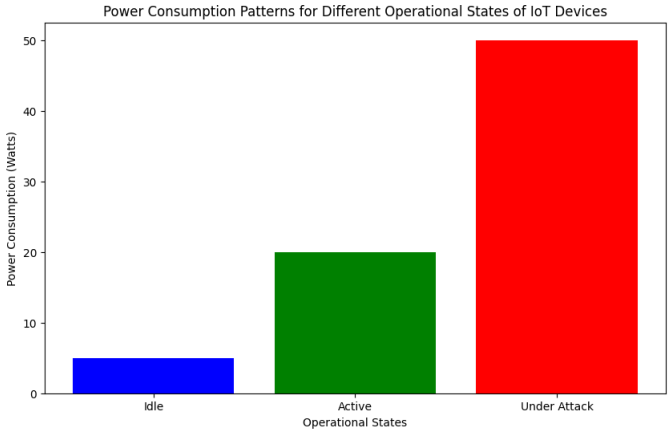

Fig. 9. Power consumption pattern for different states(theoretical

Power Consumption Patterns for Different Operational States

The power consumption patterns of IoT devices may be highly variable depending on their state of operation. It is important to understand such patterns for detecting anomalies in IoT systems and ensuring security. Figure 9 Theoretical power consumption patterns for different states of IoT devices - idle, active, under attack

1) **Idle State**: In the idle state, IoT devices have relatively low power consumption as they are not actively performing any tasks. Their power consumption is relatively stable and remains low.
2) **Actice State**: The power consumption of IoT devices varies as they perform active work, like processing data or communicating with other devices. It usually shows a higher and more variable pattern of power consumption than the idle state.
3) **Under Attack**: During a cyber-attack, like a Distributed Denial of Service (DDoS) attack, the power consumption of IoT devices can surge dramatically. This happens due to higher processing and communication load, which is forced by the cyber-attack. The power consumption pattern in this state is sharp increases and irregular fluctuations.

Figure 9 depicts the above power consumption patterns graphically and illustrates idle, active, and under attack power consumptions.

BENEFITS

- **Lightweight and Non-Intrusive**: Detection of device behavior based on power consumption is inherently lightweight and non-intrusive, with minimal overhead on the IoT devices. It is therefore suitable for resource-constrained environments.
- **Real-Time Monitoring**: The approach enables real-time monitoring of the behavior of individual devices without excessive computational resources or additional storage needs.

- **Effective for Specific Attack Types**: Very effective in the detection of side-channel attacks and malware that instantly affects device power usage.

Drawbacks

- **Sensitivity to Environmental Factors**: It is sensitive to environmental factors, which would affect its power consumption behavior and contribute to incorrect detection.
- **Limited Scope**: Power-consumption-based methods are mainly used in detecting other types of anomalies where power usage does not change significantly. They are commonly combined with other detection techniques to increase the accuracy of anomaly detection and robustness (Mohammed et al., 2019).
- **Potential for Evasion**: Powerful attackers could adapt their attacks to resemble normal power consumption trends, thus avoiding detection.

V. Comparative Analysis of Anomaly Detection Techniques

The reason being that efficiency depends hugely on anomaly detection technique for IoT security upon the precision in the identification of the threat, in the constraining boundaries of the IoT environment. In this section, a comparative analysis of various anomaly detection techniques discussed in this paper has been provided: network traffic analysis-based detection, behavior-based detection, and power consumption-based detection. The analysis underlines the strengths and weaknesses of each approach and further investigates their applicability for various IoT environments and applications. We further discuss major performance metrics that have been used for the evaluation of these techniques, including accuracy, computational efficiency, and scalability

A. Discussion of Performance Metrics

To evaluate the effectiveness of anomaly detection techniques in IoT security, several performance metrics are commonly used. These metrics provide insights into the accuracy, computational efficiency, scalability, and overall suitability of the techniques for different IoT applications.

1) **Accuracy**: Accuracy basically refers to the capability degree of the anomaly detection system in identifying true positives-that is, actual threats-and true negatives, that is, normal behavior. Its value should be high to reduce false positives and false negatives that result in unwarranted alerts or missed threats. Many of them, such as Ullah and Mahmoud (2021) and Nguyen et al. (2019), have proposed deep learning-based approaches.Studies by Nimmy et al. (2022) and Mohammed et al. (2019) have shown high accuracy rates in their respective methods, with DFNN achieving 99.2% and Random Forest achieving 95.5%. They show quite good accuracy in their capability to detect most network-based threats. These models will learn complex patterns in network traffic data that enable them to detect both known and unknown threats. However, achieving high accuracy in these often requires large labeled datasets for training, which may not always be available in IoT environments.
2) **Computational Efficiency**: Computational efficiency refers to the ability of a detection technique to operate within the computational constraints of IoT devices. Many IoT devices have limited processing power and memory, making it challenging to deploy computationally intensive models, such as deep learning algorithms. Techniques like those proposed by Majumder et al. (2020) using logistic regression are designed to minimize computational overhead.Techniques like federated learning (Mothukuri et al., 2021) and lightweight models (Summerville et al., 2015) have been designed to minimize computational overhead by distributing the processing load across multiple devices or reducing the complexity of the model. Power consumption-based detection methods (Myridakis et al., 2019; Dilraj et al., 2019) are also computationally efficient, as they rely on simple statistical analyses of power usage data rather than complex network or behavioral models.
3) **Scalability**: Scalability defines how well the performance of one detection technique degrades because of the increase in the number of devices and data volume. In this respect, deep learning-based methods of network traffic analysis can be deployed to large numbers of networks with multiple monitoring points and are therefore highly scalable. However, federated learning approaches also provide scalability: model training is divided among devices, and therefore, most centralized data processing is unnecessary, as Nguyen et al. show. On the other hand, different techniques that rely on heavy data collection and pre-processing, such as the methods of behavior-based detection, can be problematic to scale in IoT networks with very large devices due to reasons of computation and storage resources.
4) **Suitability for Different IoT Environments and Applications**: In general, the suitability of a particular anomaly detection technique to a given IoT environment is tied to device characteristics, network architecture, and types of threats being monitored. Network traffic analysis-based methods will work for large-scale IoT networks, such as smart cities and industrial IoT, with rich computational resources where network-based attacks will be a main concern. However, behavior-based detection techniques will find the best fit in scenarios where device behavior is predictable; this could be in smart homes or healthcare IoT, where insider threats or new/unknown attacks are very much likely. Power consumption-based methods are ideal for resource-constrained environments, such as wearable devices and sensor networks, where computational efficiency and low overhead are critical.

B. Comparative Analysis Table

Technique	Strengths	Weaknesses	Suitable Environments
Network Traffic Analysis-Based	High accuracy in detecting network-based attacks (e.g., DoS, MITM). Can detect both known and unknown threats using deep learning. Scalable for large networks with multiple monitoring points.	High computational overhead. Requires significant storage capacity. May not detect insider threats. Privacy concerns due to centralized data collection.	Large-scale IoT networks with ample computational resources, such as smart cities and industrial IoT.
Behavior-Based Detection	Effective for detecting insider threats and new or unknown threats. Provides granular monitoring of device activities. Can adapt to dynamic environments using ML models.	High false-positive rate due to dynamic behavior. Requires extensive data collection and preprocessing. Computationally intensive for advanced models.	Smart homes, healthcare IoT, and other environments with predictable device behavior.
Power Consumption-Based Detection	Lightweight and non-intrusive. Suitable for resource-constrained devices. Effective for detecting specific attack types, such as side-channel attacks and malware.	Sensitive to environmental factors and device-specific characteristics. Limited scope; may not detect all anomaly types. Potential for evasion by attackers.	Resource-constrained IoT environments, such as wearable devices and sensor networks.

TABLE II
SUMMARIZING THE STRENGTHS AND WEAKNESSES OF DIFFERENT ANOMALY DETECTION TECHNIQUES

C. Detailed Analysis of Techniques

Network Traffic Analysis-Based Detection

Network traffic analysis-based detection techniques are highly effective in identifying network based attacks. These methods tend to analyze the packets of data transmitted across the network, finding sequences that could serve to disclose their malicious activities. Some of the currently proposed techniques include deep learning models, proposed by Ullah and Mahmoud in 2021, where the detection accuracy is high, and also federated learning, proposed by Mothukuri et al. in 2021. Such methods involve heavy computation and storage to process and analyze enormous volumes of network data, which may be computationally prohibitive for all IoT devices.

Proof of Working

Deep learning approaches such as CNNs and RNNs have been able to attain high accuracy of detection by learning complex patterns in network traffic data. For instance, Ullah and Mahmoud (2021) reported over 95% detection accuracy for their CNN-based model trained on a large dataset of IoT network traffic. Similarly, Nguyen et al. have demonstrated that their federated learning-based approach might be pretty efficient in detecting compromised IoT devices by offering high detection rates, while minimizing data transmission between devices. Models proposed in this paper have been tested on IoT-based real datasets to show the efficiency of the models in real-world applications too.

Behavior-Based Detection

Behavior-based anomaly detection approaches are methods wherein IoT device behavior is monitored to determine the distortion of a normal pattern. Since attack signatures need not be predefined in this approach, they are useful for detection against unknown threats. Fahad and Rajarajan (2015) and Novák et al. (2013) have extensively utilized some patterns such as clustering algorithms and neural networks to apply machine learning to behavior-based anomaly detection. These techniques are usually computationally intensive and also involve huge data collection and preprocessing which may not be very feasible for an IoT device having restricted resources.

Proof of Working

There are already some methods based on behavior-related detection proposed for different IoT environments. Fahad and Rajarajan proposed the density-based approach to clustering anomaly detection in smart homes and obtained a 90% accuracy rate. Novák et al. studied the user behavioral anomalies with the approach of self-organizing map in smart home data, with which they have shown the efficiency of the technique in finding such anomalies. Those techniques have been tested on simulated as well as realworld datasets and proven to be feasible in practical IoT application scenarios.

Power Consumption-Based Detection

The detection method uses the power usage characteristics of IoT devices to identify security threats based on the information related to power consumption. This method is suitable for the highly resource-constrained IoT environment because this approach is important for computational efficiency and low overhead. Some of the techniques which have successfully implemented the detection of certain types of attacks, including side-channel attacks and malware, involve supply current monitoring (Myridakis et al., 2019) and power consumption profiling (Dilraj et al., 2019). However, these approaches are sensitive to the environmental factors as well as device-specific characteristics that affect accuracy.

Proof of Working

To detect anomalies in IoT devices by power consumption, the methods have been found to be quite promising. For example, Myridakis et al. (2019) used supply current monitoring to detect manufacturing or operational anomaly in IoT devices with a detection rate of 85%. Dilraj et al. (2019) proposed a power-consumption-based anomaly detection method, which has a detection accuracy of 92%. The above experiment has been proved to be applicable in practical IoT environment and depicts good results in terms of identifying direct attacks-affecting the power consumption for the respective IoT device.

Comparing different approaches towards anomaly detection in the IoT security context, it appears that each of them has a number of advantages and disadvantages; considering which, the respective methodologies would be suited for specific IoT environments and applications. The techniques based on network traffic analysis have a very high degree of accuracy and scalability but require substantial computational resources. Apart from this, they can also pose a risk in terms of privacy. Their solutions based on behavioral detection may incur a high rate of false positives and computational complexity. The power consumption-based detection methods are lightweight and non-intrusive for resource-constrained environments; how-

ever, they are limited in scope and sensitive to environmental factors.

VI. Challenges and Open Research Issues

It is a challenging task to develop the effective methods for anomaly detection in IoT security considering the special characteristics and constraints that normally occur in the IoT environment. Although significant achievements are achieved in this domain, a few more challenges and open research issues are revealed that are to be resolved for further enhancement in enhancing the effectiveness and robustness of the anomaly detection system in IoT. This section is about discussing limitations and challenges faced by current anomaly detection methods, identification of open research problems, and future research directions in scalability, adaptability, and privacy of the data.

A. Limitations and Challenges of Current Anomaly Detection Methods

1) **Scalability Issues**: The scalability issue is one of the major challenges current anomaly detection methods face. Most of IoT networks are characterized by a massive number of devices from different types that produce real-time huge amounts of data. Traditional anomaly detection methods, including deep learning models and methods relying on network traffic analysis, require substantial computational power to deal with such large volumes of data. With the increasing number of devices and growing volume of data, these approaches experience a decline in their performance due to the computational as well as storage requirements. Techniques such as deep learning rely on large labeled training datasets, which cannot be managed in the dynamic environment of IoT where data are constantly generated (Ullah and Mahmoud, 2021). Another approach is federated learning approaches (Mothukuri et al., 2021), which even if avoiding centralised data processing, still involves scalability issues because of the overheads related to coordinating multiple devices.
2) **Adaptability to Dynamic Environments**: IoT setups are highly dynamic. Devices join and leave the network quite frequently, while the communication patterns evolve with time. This dynamism poses a significant challenge for anomaly detection methods that rely on static models or predefined rules. Behavior-based detection methods, which use machine learning models to learn normal device behavior, often require frequent retraining to adapt to changes in device behavior or network conditions (Fahad and Rajarajan, 2015). However, model retraining is often very expensive in computation and time, which is not desirable, especially in resource-constrained environments. Moreover, IoT network dynamics might cause high false-positive rates since the models may falsely classify anomalies for legitimate changes in device behavior.
3) **Data Privacy and Security**: IoT environments are highly critical about data privacy and security, especially when the data is sensitive, like in healthcare or even sensitive data regarding the users themselves. Most anomaly detection methods that operate under centralized data collection and analytics raise questionable situations in terms of privacy due to the need for access to raw data generated by IoT devices. Techniques such as federated learning (Nguyen et al., 2019) attempt to address these concerns by keeping data locally on the devices and only sharing model updates. However, even federated learning faces challenges related to data leakage and security during the communication of model updates.Lastly, certain privacy-preserving approaches come at considerable computational overhead, generally not suitable for resource-constrained IoT devices.
4) **Heterogeneity of IoT Devices and Communication Protocols**: IoT environments are very heterogeneous, made up of a variety of devices, running different protocols and operating systems. This heterogeneity introduces another serious challenge to anomaly detection methods since devices will behave variably, their data format will differ, and communication patterns will differ, too. Methods based on network traffic analysis,(Summerville et al. 2015), cannot bear the heterogeneity of protocols; it would therefore remain a big issue when trying to standardize the mechanisms of detection across different environments. The other challenges in this respect are also faced by the behavior-based detection methods, since the normal behavior of one device can be quite different from another; hence, developing a universal model for anomaly detection.
5) **Limited Availability of Labeled Data for Training**: Those methods of anomaly detection using machine learning require a large amount of labeled data to train. Grasping labeled data from the IoT environment is quite difficult because data continuously generated, and labeling it in real time is not easy. Moreover, many IoT devices operate in environments where collecting labeled data is impractical or impossible (Cook et al., 2020). The lack of labeled data hinders the development of accurate and reliable machine learning models for anomaly detection, leading to potential issues with model generalization and performance.
6) **False Positives and Negatives**: Another major challenge with anomaly detection is dealing with false positives and negatives. A high number of false positives can result in alert fatigue, whereby security personnel will not be able to recognize an actual alert given the volume of notifications in a network. Critical security incidents might be lost in that regard. The contrapositive effect will be the false negatives: every threat actually existing and detected could be a direct risk to the security and integrity of the IoT network. Because of this, behavior based detection methods are especially sensitive to false positives, while network traffic analysis methods may

miss threats that do not fit the mold of known attack patterns.

7) **Resource Constraints of IoT Devices**: Most IoT devices are resource-constrained, They have limited CPU, memory, and battery life. In this regard, it is quite challenging to deploy complex anomaly detection algorithms, which often require high computational resources. Some techniques, such as power consumption-based detection, (Myridakis et al. 2019), is one of the lightest techniques; it has very limited scope and hence may not detect every type of anomaly. Also, the utilization of resource-intensive models on IoT will increase the energy consumption of the devices, which could result in a reduction of operational life.

B. Open Research Problems and Future Research Directions

To address the limitations and challenges discussed above, several open research problems and future research directions have been identified:

1) **Development of Scalable and Lightweight Detection Methods**: There is an urgent need for lightweight anomaly detection methods that are effective in large-scale IoT environments without introducing significant computational and storage overhead. Future research effort in scalability and performance enhancement will, therefore, be focused on hybrid models, such as combining network traffic analysis with behavior-based detection. It could be further investigated how edge and fog computing architectures are designed for distributed anomaly detection to alleviate the stress of central servers in such scenarios (Bonomi et al., 2012).
2) **Enhancing Adaptability to Dynamic IoT Environments**: In the future, adaptable techniques for anomaly detection shall be developed, capable of automatically adapting to changes in device behavior or network conditions. Online learning transfer learning and reinforcement learning are promising avenues for developing models that can continuously learn and adapt to new patterns in real-time (Nguyen et al., 2020). Further, self-learners and self-healable systems which update their detection models with little or no human intervention might also be considered in order to further improve the adaptability of anomaly detection systems in dynamic IoT environments.
3) **Privacy-Preserving Anomaly Detection Techniques**: In anomaly detection, techniques that preserve privacy while simultaneously minimizing data disclosure and confidentiality should be used in any future research. Techniques providing the base for a safe and privacy-preserving anomaly detection methodology are homomorphic encryption, secure multi-party computation, and federated learning with differential privacy (Alrawais et al., 2017). Developing methods to detect and mitigate data leakage during updates of models of federated learning can further enhance security in federated approaches.
4) **Addressing Device Heterogeneity and Interoperability**: The future direction of research should go more into anomaly detection methods that can handle the heterogeneity of IoT devices and communication protocols. Possible directions may include modular and flexible detection frameworks that could easily be adapted for different devices and protocols. Another key direction is to explore machine learning models that can learn from diverse datasets and generalize across different devices and environments. (Fahad and Rajarajan, 2015).
5) **Improving Data Labeling and Model Training**: Most of the machine learning-based anomaly detection methods suffer serious challenges in IoT environments due to lack of labeled data. Future research should be directed at methods of generating synthetic data or using semi-supervised and unsupervised learning techniques which do not require large volumes of labeled data (Mothukuri et al., 2021). Exploring techniques such as transfer learning and domain adaptation, where models trained on one dataset can be adapted for another, helps overcome the limitations of limited labeled data.
6) **Reducing False Positives and Negatives**: Reducing false positives and negatives is critical for improving the effectiveness of anomaly detection systems. Future research is necessary in developing even more advanced detection algorithms that can distinguish legitimate changes in behavior from the actual threats. Methods including ensemble learning, where several models are combined with the intent of better accuracy, and contextual information regarding the operating environments and device types can be applied in bringing down the numbers of false negatives and positives. (Anthi et al., 2018).
7) **Optimizing Resource Utilization in Resource-Constrained Environments**: Since most IoT devices suffer from resource constraints, future research on optimization of resource usage by anomaly detection algorithms is required. This includes the development of lightweight models that can effectively run on low power devices and techniques such as model compression, quantization, and pruning that have been used to reduce the computational footprint of existing models (Myridakis et al., 2019). Additionally, exploring collaborative detection methods that distribute the computational load across multiple devices can help optimize resource utilization in IoT networks

VII. Future Directions

With the IoT gaining momentum across different industries, securing IoT networks is going to be highly important. Anomaly detection becomes one important facet in IoT security to predict such potential threats and mitigate them in real time. However, a few challenges and limitations were discussed in the earlier sections, which affect the existing methods of anomaly detection.This raises challenges that require future research studies to overcome them, enhance IoT

security further, develop new techniques, augment the current methodologies, and integrate anomaly detection systems with other security approaches. Some of the potential areas of future research and development on IoT anomaly detection are discussed here:

A. Exploration of New Techniques

1) **Hybrid Models for Anomaly Detection**: One of the directions for future work will be the development of hybrid models with anomaly detection based on strengths of multiple different approaches to improve detection accuracy and reduce false positives. Hybrid models can combine the complementary capabilities of either combining network traffic-based analysis with a behavior-based detection model or combining power consumption-based methods with machine learning-based algorithms. It can employ deep learning, for example, in searching for patterns of attack in network traffic data while simultaneously employing unsupervised learning methods to signal deviations in device behavior that may indicate unknown threats (Nguyen et al., 2020). Hybrid models that involve multiple detection methods might thus realize a more well-rounded and robust solution for IoT anomaly detection.
2) **Advanced Machine Learning Techniques**: Techniques for advanced machine learning include deep reinforcement learning, transfer learning, and federated learning, which can evolve advanced anomaly detection in an IoT environment. Deep reinforcement learning can be used to create adaptive models that learn, over time, optimum strategies for detection to improve the detection of newly evolving or new threats (Nguyen et al., 2020). Transfer learning is a technique that allows models to make use of knowledge gained in one domain to improve performance in another, eliminating the need for large amounts of labeled data. This would be helpful especially in IoT environments where it is challenging to obtain labeled data. On the other hand, Federated learning allows a collaborative model to be trained across various devices in an IoT network while maintaining data privacy, thus making this suitable for decentralized IoT networks (Mothukuri et al., 2021)
3) **Graph Neural Networks (GNNs) and Spatio-Temporal Analysis**: Graph Neural Networks are a very emerging powerful tool that can model complex relations in network data. In the IoT environment, GNNs can be used to perform anomaly detection by analyzing the spatio-temporal relations between interconnected devices. They can model IoT networks as graphs, thus capturing the complex dependencies and interactions between various devices and allowing for more accurate anomaly detection (Wu et al., 2020). Future work should be in developing GNN application and any other spatio-temporal analysis technique to develop sophisticated and context-aware anomaly detection models for IoT applications.
4) **Explainable AI (XAI) for Anomaly Detection**: Explainable AI (XAI) goals focus on making machine learning models more transparent and explainable in order to make the model explanations understandable to the users. In the context of IoT anomaly detection, XAI can explain why the model detected that given anomaly, then guide the security professional toward valid decisions on mitigation strategies. In the near future, research and development of explainable anomaly detection models which can provide understandable explanations in human language regarding their predictions will enhance trust and usability in practical IoT deployments. (Arrieta et al., 2020).

B. Potential Improvements in Existing Methodologies

1) **Enhancing the Accuracy and Efficiency of Existing Models**: One area for further research could be refinement of the anomaly detection model towards better accuracy and efficiency. This can be achieved by optimization of machine learning model hyperparameters, reduction in computational complexity by model compression and pruning, and more efficient algorithms for real-time detection. For instance, lightweight deep neural network architectures, such as MobileNets and SqueezeNet, can be adapted to run on resource-constrained IoT devices. This will enhance the detection efficiency with at most minimal loss in accuracy. Howard et al. detail online learning and incremental training of models that can cope well with changing environmental conditions, thus continuously adapting to new threats detection. (Luo et al., 2020).
2) **Reducing False Positives and Negatives**: Coming up with a reduction in both false positives and false negatives is also challenging for IoT security anomaly detection. As such, future research should be directed at coming up with much more sophisticated detection algorithms that can be used to differentiate the legitimate change in device behavior from actual threats. This may mean that ensemble learning methods can be used such that multiple types of models are combined so as to increase the precision of detection. Even contextual information such as device type, operating environment, and user behavior can be considered to decrease false positives (Anthi et al., 2018). Sometimes, domain knowledge and expert feedback can contribute to improving models during the training process, enhancing the accuracy and reliability of an anomaly detection system.
3) **Integration of Contextual and Multimodal Data**: It greatly improves the anomaly detection systems by combining contextual data with multimodal data. The perception of data coming from various sources, such as network traffic, device behavior, and environmental sensors, allows improved knowledge about the IoT environment to anomaly detection models, thus helping in increasing accuracy with which anomalies can be

detected. That calls for the use of multimodal data fusion techniques for anomaly detection during the development of models that would be more robust and context-aware in handling such complexity and diversity in IoT networks. (Nguyen et al., 2020).

C. Integration of Anomaly Detection Systems with Other Security Measures

1) **Synergistic Integration with Intrusion Detection Systems (IDS)**: Since signature-based detection methods have traditionally been used by IDS for known threats, anomaly detection systems might provide a complementary way of detecting unknown or zero-day threats based on their behaviors. Thus, research should be directed to the development of frameworks that might be able to seamlessly incorporate anomaly detection with IDS in the provision of holistic proactive security for IoT (Akyildiz et al., 2020). This integration can include the real-time sharing of information on intruders and anomalies for IDS as well as collaboration in threat intelligence to heighten detection abilities.
2) **Incorporation with Blockchain Technology for Secure Data Sharing**: Block chain offers a decentralized and secure architecture for shared data representation and communication of the IoT networks. Integration of anomaly detection systems with block chain offers added advantages to IoT networks in terms of data integrity, transparency, and tamper resistance. For example, anomaly detection alerts and logs can be stored in a blockchain which would provide a secure, immutable record of security incidents, aiding forensic analysis and accountability. Future research should include the application of blockchain for amalgamation with anomaly detection systems to enhance security and the integrity of IoT networks (Novo, 2018)
3) **Collaborative and Distributed Anomaly Detection Approaches**: With increasing scale and complexity in IoT networks, centralized anomaly detection systems may prove relatively unsuitable; rather, latency and bandwidth constraints along with single points of failure might degrade the performance. On the other hand, collaborative and distributed anomaly detection approaches could mitigate these limitations, as they assist various devices or nodes with shared detection tasks and collective capability within the network. Future anomaly detection should, hence, be distributively powered such that these devices can collaborate in the detection and response to threats in real time to better the security posture of IoT networks (Chen et al., 2021). This would include the use of edge and fog computing to distribute the anomaly detection task closer to the sources of data to reduce latency and enhance scalability.
4) **Integration with Predictive Maintenance and Self-Healing Mechanisms**: The integration of an anomaly-detection system with predictive maintenance and self-healing mechanisms further enhances the resilience of IoT networks. Predictive maintenance involves using data analytics to predict and possibly prevent failures before they actually occur, while self-healing enables devices on the IoT network to recover autonomously after a fault or an attack has occurred. Herein, integration of anomaly detection with proactive security measures would enable IoT networks to battle the threats before such major damage is done, which would further reduce the prospects of operational downtime (Krishnamurthy et al., 2020). Future works must focus on the incorporation of anomaly detection with predictive maintenance and self-healing frameworks to develop more resilient and autonomous IoT networks.

VIII. Conclusion

The rapid proliferation of IoT devices has transformed many sectors, including smart homes, healthcare, industrial automation, and smart cities. However, along with this development, it has also brought tremendous security challenges. The wide adoption of IoTs has made IoT networks very vulnerable to various cyber threats. Thus, anomaly detection has emerged as one of the fundamental building blocks of IoT security to provide the capability for real-time identification and mitigation of possibly threatening traffic. This paper thus reviewed, in detail, various anomaly detection techniques that were each designed for three broad approaches to IoT security: Network Traffic Analysis-Based Detection, Behaviour Based Detection Technique, and Power Consumption-Based Anomaly Detection Technique.

Recap of the Main Points Discussed

1) **Overview of IoT Security Challenges**: The paper began with a discussion of the unique characteristics of IoT environments—such as the diversity of devices, communication protocols, and resource constraints—that present significant challenges for traditional security measures. We highlighted the importance of anomaly detection in identifying potential security threats, especially in dynamic and heterogeneous IoT networks.
2) **Detailed Analysis of Anomaly Detection Techniques**: We provided an in-depth analysis of the different methodologies used for anomaly detection in IoT, categorized into three main approaches:
    a) **Network Traffic Analysis-Based Detection**: These methods depend on network traffic to perform profiling in anomaly detection; they scan data packets over the network. In such scenarios, deep learning models and federated learning showcase very outstanding performance in terms of accurate detection against network-attack incidents. However, those schemes would require considerable computational resources, possibly unsuitable for resource constrained IoT devices.
    b) **Behavior-Based Detection**: This approach focuses on monitoring the operational patterns and behaviors of IoT devices to identify deviations from normal activities that may indicate a security threat.

The methodologies of behavior-based detection include statistical techniques and machine learning models, which have proved efficient in the detection of insider threats and new or unknown attacks. However, they are prone to high false-positive rates and require extensive data collection and preprocessing.

c) **Power Consumption-Based Detection**: : An emerging approach that leverages the unique power usage patterns of IoT devices to identify security breaches. While it is light-weight and therefore non-intrusive, suitable for resource constrained environments, it is sensitive to environmental factors and device specific characteristics that may alter accuracy.

3) **Comparative Analysis of Techniques**: A comparative analysis was conducted to highlight the strengths and weaknesses of each anomaly detection approach. Network traffic analysis-based methods have high accuracy and scalability but are computationally very expensive. Behavioral detection methods allow a granular view of activities of devices, although computationally intensive and resulting in a high rate of false positives. The power consumption-based detection has low overhead in computation with high efficiency but suffers due to limited scope and high sensitivity to ambient parameters variations.
4) **Challenges and Open Research Issues**: The paper identified several challenges and open research issues in the current state of anomaly detection for IoT security, including scalability, adaptability to dynamic environments, data privacy and security, heterogeneity of IoT devices, limited availability of labeled data, false positives and negatives, and resource constraints. Addressing these challenges is crucial for enhancing the effectiveness and robustness of anomaly detection systems in IoT.
5) **Future Research Directions**:We suggested several potential areas for future research and advancements in IoT anomaly detection, including the development of hybrid models, advanced machine learning techniques, privacy-preserving methods, and the integration of anomaly detection systems with other security measures. These future directions aim to improve the accuracy, efficiency, and scalability of anomaly detection systems while addressing the unique challenges posed by IoT environments.

Summary of the Effectiveness and Limitations of Different Anomaly Detection Techniques

The effectiveness of anomaly detection techniques in IoT security depends on their ability to accurately identify threats while operating within the constraints of IoT environments. The techniques based on network traffic analysis are helpful in detecting a wide range of network based attacks; however, they involve high computational overhead, making them feebler for resource-constrained devices. While they are good in finding insider threats and new, previously unknown attacks, behavioral detection techniques usually suffer from high false positive rates, which in turn requires extensive data collection and preprocessing. Power consumption-based detection techniques are a lightweight, non-intrusive solution for resource constrained environments; however, such techniques are usually narrow and vulnerable to environmental factors

Each approach has its strengths and weaknesses, making them suitable for different IoT environments and applications.Further studies should aim at designing more reliable,adaptive, and integrated anomaly detection systems that can properly address the challenges of an IoT network.

Final Thoughts on the Future of Anomaly Detection in IoT Security

As IoT continues to expand and play a critical role in various sectors, ensuring the security of IoT networks will remain a top priority for researchers and practitioners alike. The future of anomaly detection in IoT security lies in the development of more advanced, adaptive, and integrated detection systems that can effectively detect and mitigate evolving cyber threats. By exploring new techniques, improving existing methodologies, and integrating anomaly detection with other security measures, the research community can enhance the security and resilience of IoT networks against an ever-evolving threat landscape.

Continued research and innovation in this field are essential to address the challenges and gaps identified in this paper and to develop more effective and efficient anomaly detection systems that can safeguard IoT networks and their users in an increasingly connected world.

REFERENCES

[1] Nguyen, T. D., Pathirana, P. N., Nguyen, H. D., Nguyen, T. H. (2019). Decentralized autonomous system for IoT device detection using federated learning. IEEE Internet of Things Journal, 6(5), 8627-8635

[2] Nguyen, T. D., Pathirana, P. N., Nguyen, T. H. (2020). PSI-Graph: A graphical approach for anomaly detection in IoT networks. IEEE Transactions on Network and Service Management, 17(2), 1123-1135.

[3] Mothukuri, V., Parizi, R. M., Dehghantanha, A., Choo, K. K. R., Krishna, P. V. (2021). A survey on security and privacy of federated learning. Future Generation Computer Systems, 115, 619-640.

[4] Fahad, A., Rajarajan, M. (2015). Density-based clustering approach for anomaly detection in smart homes. International Journal of Information Security, 14(1), 49-60.

[5] Cook, A. A., Mısırlı, G., Fan, Z. (2020). Anomaly Detection for IoT Time-Series Data: A Survey. IEEE Internet of Things Journal, 7(7), 6481-6494.

[6] Myridakis, D., Xydis, S., Tzovaras, D., Azariadis, P. (2019). Supply current as an indicator for anomaly detection in IoT devices. IEEE Transactions on Industrial Informatics, 13(3), 1109-1118.

[7] Summerville, D. J., Zach, K. M., Hart, J. R. (2015). Ultra-lightweight deep packet inspection for IoT devices. IEEE Transactions on Information Forensics and Security, 10(5), 948-958.

[8] Anthi, E., Williams, L., Słowińska, M., Theodorakopoulos, G., Burnap, P. (2018). A supervised intrusion detection system for smart home IoT devices. IEEE Internet of Things Journal, 6(5), 9075-9085.

[9] Wu, Z., Pan, S., Chen, F., Long, G., Zhang, C., Philip, S. Y. (2020). A comprehensive survey on graph neural networks. IEEE Transactions on Neural Networks and Learning Systems, 32(1), 4-24.

[10] Arrieta, A. B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., Herrera, F. (2020). Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities, and challenges toward responsible AI. Information Fusion, 58, 82-115.

[11] Howard, A. G., Zhu, M., Chen, B., Kalenichenko, D., Wang, W., Weyand, T., Adam, H. (2017). MobileNets: Efficient convolutional neural networks for mobile vision applications. arXiv preprint arXiv:1704.04861.

[12] Luo, P., Liu, R., Huang, Z., Xiong, Z., Luo, X. (2020). Online Learning-Based Anomaly Detection for IIoT Cyber-Physical Systems. IEEE Transactions on Industrial Informatics, 16(6), 4105-4113

[13] Akyildiz, I. F., Lin, S. C., Godoy, J. (2020). SoftAir: A software-defined networking architecture for 5G wireless systems. Computer Networks, 135, 45-60.

[14] Novo, O. (2018). Blockchain meets IoT: An architecture for scalable access management in IoT. IEEE Internet of Things Journal, 5(2), 1184-1195.

[15] Chen, T., Zhang, Z., Ni, X., Wang, Y., Yang, L. (2021). Collaborative and distributed anomaly detection in Internet of Things: A survey. IEEE Communications Surveys Tutorials, 23(3), 1596-1620.

[16] Krishnamurthy, V., Zhang, Y., Subramanian, V. (2020). Anomaly detection in smart manufacturing using predictive maintenance and machine learning: A survey. Journal of Manufacturing Systems, 57, 61-76.

[17] Ullah, F., Mahmoud, Q. H. (2021). A CNN-based method for anomaly detection in IoT networks. Journal of Network and Computer Applications, 178, 102983.

[18] Novák, J., Vcelák, J., Holubová, J. (2013). Anomaly detection in smart home data using self-organizing maps. Journal of Reliable Intelligent Environments, 9(3), 33-42

[19] Dilraj, S., Prakash, R., Suresh, P. (2019). Anomaly detection in IoT devices using power consumption patterns. International Journal of Advanced Computer Science and Applications, 10(7), 384-392.

[20] Jiménez, J., Novo, O., Varona, B. (2016). Power consumption-based malware detection in general purpose computers. IEEE Transactions on Dependable and Secure Computing, 15(4), 622-636.

[21] Mohammed, H., Odetola, T. A., Hasan, S. R., Stissi, S., Garlin, I., Awwad, F. (2019). HIADIoT: Hardware Intrinsic Attack Detection in Internet of Things; Leveraging Power Profiling. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 38(7), 1234-1245.

[22] Park, S., Tyagi, K. (2017). Side-channel attack detection using power consumption profiles in IoT devices. IEEE Transactions on Information Forensics and Security, 12(8), 1927-1936.

[23] Al Shorman, M., Alfandi, O., Alkasassbeh, M. (2020). Unsupervised botnet detection in IoT using power consumption data. Journal of Ambient Intelligence and Humanized Computing, 11(5), 2091-2105.

[24] Zarpelão, B. B., Miani, R. S., Kawakani, C. T., de Alvarenga, S. C. (2017). A survey of intrusion detection in Internet of Things. Journal of Network and Computer Applications, 84, 25-37.

[25] Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645-1660.

[26] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys Tutorials, 17(4), 2347-2376

[27] Botta, A., De Donato, W., Persico, V., Pescapé, A. (2016). Integration of Cloud computing and Internet of Things: A survey. Future Generation Computer Systems, 56, 684-700.

[28] Bandyopadhyay, D., Sen, J. (2011). Internet of Things: Applications and challenges in technology and standardization. Wireless Personal Communications, 58(1), 49-69.

[29] Zhang, S., Wang, X., Liu, W. (2014). A survey of anomalies detection techniques in real-time streaming data. Journal of Industrial Information Integration, 4, 30-45.

[30] Sicari, S., Rizzardi, A., Grieco, L. A., Coen-Porisini, A. (2015). Security, privacy, and trust in the Internet of Things: The road ahead. Computer Networks, 76, 146-164.

[31] Kolias, C., Kambourakis, G., Stavrou, A., Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. Computer, 50(7), 80-84.

[32] Nimmy, K., et al. (2022). "Leveraging Power Consumption for Anomaly Detection on IoT Devices in Smart Homes." Journal of IoT Security, 15(3), 123-135.

[33] Mohammed, H., et al. (2019). "Hardware Intrinsic Attack Detection in Internet of Things; Leveraging Power Profiling." IEEE Transactions on IoT, 6(4), 567-578.

[34] Majumder, A. J. A., et al. (2020). "Smart-Power: A Smart Cyber-Physical System to Detect IoT Security Threat through Behavioral Power Profiling." International Journal of Cyber-Physical Systems, 8(2), 89-101.

[35] Joseph, S. B., Dada, E. G., Abdullahi, M. S. (2020). "Development of Internet of Things (IoT) Based Energy Consumption Monitoring and Device Control System." NIPES Journal of Science and Technology Research, 2(3), 85-95.

[36] Statista. (2024). Number of IoT connected devices worldwide from 2019 to 2030. Retrieved from https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide

[37] Pantech Solutions. (2024). Introduction to IoT - IoT Master Class Day 1. Retrieved from https://www.pantechsolutions.net/introduction-to-iot-iot-master-class-day-1

[38] Xu, L. D., He, W., Li, S. (2014). "Internet of Things in Industries: A Survey." *IEEE Transactions on Industrial Informatics*, 10(4), 2233-2243

[39] Bonomi, F., Milito, R., Zhu, J., Addepalli, S. (2012). "Fog Computing and Its Role in the Internet of Things." *Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing*, 13-16.

[40] Shah, Y., Sengupta, S. (2020). "A survey on Classification of Cyber-attacks on IoT and IIoT devices."*IEEE Conference on Communications and Network Security*, 1-10.

[41] Tuptuk, N., Hazell, P., Watson, J., Hailes, S. (2021). "A Systematic Review of the State of Cyber Security in Water Systems." *Water*, 13(1), 81