

Enhancing IoT Security through Machine Learning: A Comprehensive Review and Future Directions

Kamel-Dine Haouam, Mourad Benmalek

Computer Engineering Department, College of Engineering and Architecture, Al Yamamah University, Riyadh
13541, Saudi Arabia

Corresponding Author: k_haouam@yu.edu.sa

Abstract— The integration of machine learning (ML) into Internet of Things (IoT) systems presents transformative opportunities across various domains but also introduces numerous security challenges. This study explores the role of ML in enhancing IoT functionalities, particularly in data analytics, security, optimization, and user experience. Through a comprehensive review of literature, case studies, and expert interviews, the study highlights ML's potential to address IoT security challenges such as device heterogeneity, data privacy, network vulnerabilities, and device authentication. Moreover, the study identifies key methodologies for investigating the function of ML in IoT, including qualitative analysis and multi-method approaches, along with ethical considerations and limitations associated with integrating ML into IoT security frameworks. The study underscores the importance of ML in addressing IoT security challenges, emphasizing the need for privacy-preserving techniques, robust defenses against adversarial attacks, and interpretable ML models. Additionally, it identifies recommendations for future research, including the development of advanced cryptographic and federated learning approaches, robust defenses against adversarial attacks, and self-learning and adaptive ML techniques tailored to IoT environments' dynamic nature. Furthermore, the study suggests policy considerations for policymakers to ensure ethical considerations while encouraging innovation in the integration of ML into IoT systems.

Index Terms— Machine Learning, Internet of Things, Data Analysis, Security, Optimization

I. INTRODUCTION

1.1 Background Information

The Internet of Things (IoT) is a new technological paradigm that involves the online interconnection of everyday and industrial devices. Ashton (2009) claims these gadgets have sensors, apps, and other tech built in to make data collection and sharing easier. The Internet of Things (IoT) has garnered significant attention and adoption across multiple industries, such as healthcare, transportation, and smart cities, enabling remarkable advancements in automation and the interchange of data (Al-Fuqaha et al., 2015).

ML, which is a specific branch of artificial intelligence (AI), has been at the forefront of technological advancements. According to Mitchell (1997), machine learning algorithms facilitate the process of computers acquiring knowledge from data and making decisions autonomously, without the need for explicit programming. Machine learning has been increasingly utilised in several sectors such as healthcare, finance, and automotive industries (Jordan & Mitchell, 2015).

Projected revenue growth in the IoT sector is expected to reach 4 trillion by 2025, up from 892 billion in 2018 in terms of the expansion of the digital economy. However, this rapid expansion of interconnected devices has also introduced significant security challenges (S. M. Tahsien et al., 2020). With billions of devices interconnected through networks, IoT systems have become enticing targets for cyberattacks, ranging from data breaches to unauthorized access and control. The most frequent IoT threats include, for instance, man-in-the-middle attacks, spoofing attacks, jamming, eavesdropping, data manipulation, denial of service (DoS) attacks, and malevolent (V. Hassija et al, 2019). These security vulnerabilities pose substantial risks to individuals, businesses, and critical infrastructure, necessitating robust security measures to safeguard IoT ecosystems.

Addressing these security challenges requires innovative approaches that can adapt to the dynamic and complex nature of IoT environments. In this context, machine learning (ML) has emerged as a powerful tool for enhancing IoT security. ML algorithms have the capability to analyze vast amounts of data generated by IoT devices in real-time, identify patterns, and detect anomalies indicative of potential security threats. One of the best computational paradigms for delivering embedded intelligence in Internet of Things devices is machine learning (ML) (M. S. Mahdavinejad et al, 2018). To extract valuable insights or intriguing data patterns from the security data, machine or deep learning models employ a collection of rules, techniques, or intricate transfer functions (Ślusarczyk, 2006). Through ML techniques, IoT stakeholders can proactively detect and mitigate security breaches, bolstering the resilience of IoT infrastructures against evolving cyber threats.

1.2 Research Gap

While both IoT and machine learning have been exhaustively studied, the intersection of these two fields has not been thoroughly investigated. Botta et al. (2016) state that the existing literature frequently focuses on the technical aspects but neglects the broader roles that machine learning could play in enhancing IoT system functionalities such as security, optimization, and user experience. While numerous studies have explored various aspects of IoT security and ML separately, there remains a lack of holistic research that thoroughly investigates the synergistic potential of ML techniques in mitigating the diverse range of security threats encountered in IoT ecosystems.

1.3 Objectives and Research Questions

This paper's primary objective is to investigate and analyze the function of machine learning within the IoT ecosystem. Specifically, we intend to investigate how machine learning algorithms can enhance the IoT's data analysis and prediction, security, optimization, and user experience capabilities.

In this study, the following research concerns will be addressed:

1. How does machine learning facilitate efficient data analysis and prediction in the Internet of Things?
2. How does machine learning contribute to the improvement of IoT system security?
3. How can machine learning algorithms enhance the operational aspects of the Internet of Things?
4. How does machine learning enhance the user experience in Internet of Things environments?

1.4 Justification

This study's significance resides in its attempt to close the identified research gap by providing a thorough understanding of the symbiotic relationship between machine learning and IoT. As IoT systems become an ever-increasing part of our daily lives and organizational operations, it is not only opportune but essential to enhance their capabilities through machine learning in order to realize the full potential of IoT (Atzori et al., 2010). Strong security measures are essential to securing sensitive data, maintaining privacy, and defending vital infrastructure as IoT technologies continue to spread across a variety of industries, from smart homes to industrial automation. Nonetheless, conventional security methods frequently prove inadequate in efficiently addressing the many and swiftly changing risks presented by malevolent entities, underscoring the pressing need for inventive resolutions that can adjust to the constantly changing landscape of Internet of Things networks.

II. LITERATURE REVIEW

2.1 Evolution of IoT and Machine Learning

The concept of IoT dates back to the late 1990s, but the term "Internet of Things" was not popularised until 1999 (Ashton, 2009) by Kevin Ashton while working at MIT's Auto-ID Lab. Initially, the Internet of Things was heavily intertwined with the

development of Radio-Frequency Identification (RFID) technology, which set the groundwork for embedding sensors and tags in physical objects (Want, 2006). Al-Fuqaha et al. (2015) report that the IoT ecosystem has expanded beyond RFID to include various wireless technologies such as Wi-Fi, Zigbee, and most recently 5G networks. The Internet of Things has progressed from basic machine-to-machine communication to complex systems incorporating Big Data analytics, cloud computing, and real-time processing (Atzori et al., 2010).

Although the idea behind the Internet of Things (IoT) was developed in the late 1990s, Kevin Ashton did not popularize the phrase until 1999 (F. Thiesse and F. Michahelles, 2006) during his time at MIT's Auto-ID Lab. At first, the Internet of Things was closely linked to the advancement of Radio-Frequency Identification (RFID) technology, laying the foundation for the incorporation of sensors and tags in physical objects. One of the emerging smart technologies for Industry 4.0, also known as the Fourth Industrial Revolution, is the Internet of Things (IoT). Industry 4.0 is the continuous automation of conventional production and industrial operations (A. B. Chebudie, 2015). A network of interconnected, internet-connected devices that can gather and transfer data via a wireless network without the assistance of a person is referred to as the Internet of Things (IoT). IoT is defined by F. Thiesse and F. Michahelles (2006) as "consisting of hardware items and digital information flows based on RFID tags," but it is also defined by the Institute of Electrical and Electronics Engineers (IEEE) as "collection of items with sensors that form a network connected to the Internet." (A. B. Chebudie, 2015). IoE, or the Internet of Everything, is best described as "a network that consists of people, data, things, and processes" by Cisco (San Francisco), a company well-known for being the global leader in networking, cyber-security, and IT solutions. (J. Bradley et al, 2022)

Statistical theory and artificial intelligence (AI) are the origins of machine learning (Jordan & Mitchell, 2015). With the advent of the backpropagation algorithm for training multi-layer neural networks, it rose to prominence in the late 20th century (Sarker, 2021). Over the years, the field has diversified to include various learning paradigms such as supervised, unsupervised, and reinforcement learning, each with its unique applications (Bishop, 2006). Recent developments such as deep learning, a more complex form of machine learning, have widened the scope of the discipline (LeCun, Bengio, & Hinton, 2015). One essential instrument for enhancing the security of Internet of Things (IoT) ecosystems is machine learning (ML). IoT systems can now evaluate massive amounts of data produced in real-time by networked devices by using machine learning (ML) techniques. These algorithms help uncover trends and abnormalities that might be signs of possible security concerns. IoT stakeholders may improve their capacity to identify, stop, and mitigate cyberattacks, protecting sensitive data and vital infrastructure, by utilizing machine learning (ML) techniques including anomaly detection, supervised learning, and reinforcement learning. IoT security data may be utilized to learn using a variety of machine learning techniques, such as feature optimization, rule-based approaches, clustering,

regression analysis, and classification and artificial neural network-based deep learning techniques, such as multi-layer perceptron networks, convolutional networks, recurrent networks, etc. (I. H. Sarker 2021). ML facilitates adaptive and proactive security measures by continuously learning from new data and evolving threat landscapes. This adaptability is particularly crucial in IoT environments characterized by dynamic and heterogeneous device networks, where traditional rule-based security approaches may prove inadequate. Through the integration of ML-driven security mechanisms, IoT systems can effectively mitigate the risks posed by diverse cyber threats, ranging from malware infections to unauthorized access attempts. One area of machine learning (ML) that has showed promise in identifying intrusions in Internet of Things systems is deep learning (DL). Models of deep learning are created to mimic how the human brain processes information. To create an artificial neural network (ANN), they employ several hidden layers. The capacity of DL to handle large volumes of data is one of its advantages over ML. When a specific data size barrier is achieved, the performance of ML models reaches a plateau, yet DL models keep getting better as data size increases (W. Ng et al., 2019). The vast amount of data produced by IoT devices makes DL algorithms an ideal match for IoT intrusion detection systems. DL models come in a variety of forms. Convolutional neural networks (CNNs) are well-known for their ability to process images, while recurrent neural networks (RNNs) are well-known for their ability to process sequential data, recognize speech, and other tasks.

2.2 Previous Work

Several pioneering works have paved the way for understanding the function of machine learning in the Internet of Things. A seminal paper by Al-Fuqaha et al. (2015) provides a comprehensive overview of IoT technologies, protocols, and applications, but emphasizes the need for machine learning algorithms for more sophisticated data analytics within IoT. They propose a conceptual model that incorporates machine learning as an essential element for IoT data processing. Botta et al. (2016), who investigate the integration of cloud computing and IoT, have also made a significant contribution. While cloud computing is the primary focus, the authors note that machine learning algorithms can facilitate more efficient data storage and retrieval systems in cloud-connected IoT devices. For evaluating existing solutions, the methodology includes a thorough survey and classification scheme. In the field of security, Roman, Zhou, and Lopez (2013) detail the inherent vulnerabilities of IoT systems. They suggest that machine learning algorithms can assist in detecting anomalies and hence enhance the security layers within IoT ecosystems. Their findings are supported by both a theoretical framework and a practical case study. In addition, Mahmud, Kaiser, Hussain, and Vasilakos (2018) investigate the use of machine learning in optimizing IoT services. The authors demonstrate through simulations and real-world applications how machine learning algorithms can significantly reduce energy consumption in IoT devices. They propose a hybrid algorithm that optimizes power consumption by combining several machine-learning techniques.

Ghayvat et al. (2015) demonstrate how machine learning can predict human behavior to improve the smart home experience by focusing on the user experience. Using neural networks, they analyzed user activity data collected by multiple smart home sensors.

Overall, these works suggest that machine learning has a multifaceted function in the Internet of Things, ranging from enhancing data analytics and security to enhancing optimization and user experience. Nonetheless, the majority of these studies concentrate on specific facets of the symbiotic relationship between machine learning and IoT, leaving room for a more comprehensive analysis, which is the focus of this paper.

2.3 Research Gap Revisited

Despite the critical importance of IoT security, there exists a notable gap in the literature regarding a comprehensive analysis of machine learning (ML) applications specifically tailored to address security challenges within IoT environments. Existing research has shed light on the individual functionalities and capabilities of both machine learning and the Internet of Things, but the interplay between these two transformative technologies remains relatively unexplored. The existing literature frequently delves into specialized domains, such as data analytics (Al-Fuqaha et al., 2015), security (Roman, Zhou, & Lopez, 2013), or energy optimization (Mahmud, Kaiser, Hussain, & Vasilakos, 2018), without examining the broader synergistic roles that machine learning can play within IoT ecosystems (Botta et al., 2016).

Al-Fuqaha et al. (2015), for instance, emphasize the potential for advanced data analytics within IoT but do not delve into the specific machine learning algorithms that can be implemented to realize this potential. Their work provides a foundational comprehension but does not provide a comprehensive evaluation of machine learning's multifaceted roles within the Internet of Things.

Roman, Zhou, and Lopez (2013) investigate the inherent security concerns and vulnerabilities of IoT systems. They acknowledge the potential of machine learning to improve security but do not delve into the nuances of how different machine learning techniques, such as anomaly detection or neural networks, could be uniquely tailored for different IoT security applications. The paper emphasizes the importance of IoT security but leaves the function of machine learning in this regard as an area for future research.

On the optimization front, Mahmud et al. (2018) provide an in-depth look at how machine learning algorithms can minimize energy consumption in IoT devices. However, they continue to prioritize only energy efficiency, ignoring other operational aspects that could be optimized by machine learning, such as data transmission rates and device interoperability.

Using neural networks, Ghayvat et al. (2015) make significant strides in investigating the user experience in smart homes. However, the study is limited to smart residences and does not investigate other IoT applications, such as healthcare monitoring systems or industrial automation, in which machine learning could enhance the user experience.

As can be seen from the foregoing, prior research has typically treated machine learning and the Internet of Things as two distinct fields. There is a noticeable lack of a unified and

comprehensive analysis of machine learning's potential contributions across several IoT disciplines, including data analytics, security, operational optimization, and user experience.

This research aims to address this shortcoming by providing a more comprehensive analysis of the synergistic relationship between machine learning and the IoT. Methods including theoretical frameworks and empirical case studies will be used to ensure the accuracy of the results.

2.4 IoT Security Challenges

Device Heterogeneity: *The IoT landscape encompasses a wide range of devices with varying hardware, software, and communication protocols, making it challenging to implement standardized security measures across the entire ecosystem. IOT connect a huge number of heterogeneous devices (S. Li et al, 2014).*

Data Privacy: IoT devices often collect and transmit sensitive data, raising concerns about data privacy and protection. Ensuring the confidentiality and integrity of data generated by IoT devices is crucial to maintaining user trust and compliance with regulatory requirements. Many nations have made protecting one's privacy a basic right (Singapore Statutes Online, 2012), (Branch, 2019), and manufacturers of Internet of Things products are beginning to incorporate privacy protection measures. For instance, Apple Inc. has just begun implementing measures for differential privacy for their iCloud product (Apple's Worldwide Developers Conference Kicks off June 13 in San Francisco, n.d.).

Network Vulnerabilities: IoT networks are susceptible to various network-based attacks, including man-in-the-middle attacks, distributed denial-of-service (DDoS) attacks, and eavesdropping. Weaknesses in network protocols and inadequate network segmentation can exacerbate these vulnerabilities. Device protection in networks is often achieved through the use of intrusion detection systems (IDS) and firewalls. In order to completely analyze each packet, a firewall or intrusion detection system (IDS) typically uses specialized hardware. These appliances must either learn the devices' benign behavior (referred to as "good" entities) or model the signatures of device assaults (referred to as "bad" entities) (A., Hamza, 2020)

Device Authentication and Authorization: Verifying the identity of IoT devices and ensuring secure access control mechanisms are fundamental challenges in IoT security. Weak authentication mechanisms and insufficient authorization controls can lead to unauthorized access and device compromise. It is challenging to provide a robust protected environment while handling the big data volumes that the customer requests.

III. METHODOLOGY

3.1 Research Design

To investigate the function of machine learning within the framework of the IoT, this study employs a qualitative methodology and a multi-method approach. To provide a holistic assessment of the potential of machine learning algorithms to enhance many aspects of the Internet of Things, the research framework involves a thorough examination of the current literature, an analysis of case studies, and interviews with experts. Data analytics, safety precautions, optimization methods, and boosting the user experience all fall under this category (Creswell & Creswell, 2017).

3.2 Data Collection

Three primary data sources will be used for this study:

- **Academic articles,** technical reports, and publications will be examined in order to comprehend existing theories and empirical findings.
- **Case Studies:** Examining real-world applications of machine learning in IoT. These cases will be derived from both academic and industry reports.

3.3 Ethical Considerations

During the research procedure, special attention will be paid to upholding ethical standards. Interviewees will be informed of the purpose of the study and will participate voluntarily. The participants will be assured of their anonymity and the confidentiality of their responses, and written informed consent will be obtained (Orb, Eisenhower, & Wyaden, 2001).

3.4 Limitations

This study has some limitations. The selection of case studies may be biased, as they will likely represent successful applications of machine learning in IoT. The swiftly evolving nature of IoT and machine learning technologies may render some aspects of the study obsolete (Marshall & Rossman, 2014).

IV. ROLE OF MACHINE LEARNING IN IoT

4.1 Data Analysis and Prediction

As the amount of data generated by IoT devices continues to develop exponentially, machine learning's contribution to data analytics and prediction becomes increasingly crucial. Machine learning algorithms can sift through this massive data to identify patterns, derive meaningful insights, and even predict future trends. For instance, machine learning algorithms such as decision trees and random forests have been implemented in predictive maintenance for industrial IoT, saving both time and resources by anticipating machine failures before they occur (Lee, Ardakani, Yang, and Bagheri, 2015). In healthcare, machine learning can analyze data from wearable devices to predict potential medical events such as heart attacks and seizures, allowing for opportune interventions (Rajalakshmi & Radha, 2020).

4.2 Security

In IoT systems, security remains a major concern, with vulnerabilities spanning from data breaches to unauthorized access. Machine learning can be instrumental in enhancing IoT security. For instance, anomaly detection algorithms can identify peculiar patterns or activities within a network, indicating the presence of potential threats such as malware attacks or unauthorized access (Fernandes, 2014). Models trained with machine learning can identify the typical behavior of a system and indicate any deviations, enabling proactive security measures. In addition, these algorithms can adapt to evolving threats and update their models in real time to provide robust and current security (Roman, Zhou, & Lopez, 2013). ML-based learning techniques may be used in place of physical layer authentication. According to (Xiao et al., 2015) Q-learning-based learning techniques outperform standard physical layer authentication methods utilizing 12 transmitters and minimize authentication error by around 64.3%. In a separate study, the parameters of the logistics regression model were determined using supervised machine learning techniques including incremental aggregated gradient and distributed Frank Wolf. This reduced communication overhead and improved the effectiveness of spoofing detection (Xiao et al., 2018).

Additionally, unsupervised learning techniques like IGMM are employed to guarantee the physical surface security and IoT device authentication (Xiao et al., 2018).

Anomaly detection algorithms identify deviations from normal patterns of behavior in IoT device data. These deviations may indicate potential security threats, such as unauthorized access attempts or abnormal sensor readings. ML models, such as clustering algorithms, support vector machines (SVM), and neural networks, can be trained on historical data to detect anomalies in real-time and trigger appropriate security responses. The support vector machine classification algorithm, for example, is utilized to identify Android malware for dependable IoT services (Ham et al., 2014) and to profile anomalous behavior of IoT devices (Lee et al., 2017). The IoT intrusion detection service (Resende & Drummond, 2018) (Mohamed et al., 2018), smart city anomaly detection (Alrashd et al., 2017) denial of service attack (Doshi et al., 2018), anomaly detection (Chang et al., 2017) (Primartha et al., 2017), and so on are all detected using the random forest approach. Similarly, a naive Bayes-based classification model is used to detect anomalies (Swarnkar & Hubballi, 2016), and a logistic regression-based method to detect malicious IoT botnets (Prokofiev et al., 2018) (Bapat et al., 2018).

Behavioral analysis techniques analyze the behavior of IoT devices and users to detect suspicious or malicious activities. ML models, such as regression-based models can learn typical behavior patterns and identify deviations that may indicate security threats. By continuously analyzing device behavior, these techniques can detect emerging threats and adapt security policies accordingly. For example, the origin of a cyberattack is determined using a linear regression-based model (Prokofiev et al., 2018), and the relationship between human characteristics and the desire to engage in cybersecurity activity is determined using multiple regression analysis (Bapat et al., 2018) In

research, (Lee et al., 2017b) looked at the odd behavior of IoT devices and how detection accuracy affected ML algorithms (such SVM and k-means) when training data sets were partially changed. There has been a decline in the accuracy rate of ML approaches; as a result, a possible area of study might be the discovery of variations in accuracy and training data sets.

Predictive analytics involves using ML algorithms to forecast future events based on historical data. In the context of IoT security, predictive analytics can anticipate security breaches or anomalies before they occur, enabling proactive mitigation strategies. ML models, such as decision trees, random forests, and time-series forecasting algorithms, can analyze IoT data streams to predict security incidents and trigger preemptive security measures. According to their principles of machine learning, a number of widely used regression techniques, including Stepwise, Linear, Logistic, Polynomial, Ridge, Lasso, Regression Trees, Principal Components, Elastic Net, Poisson, Negative Binomial, and Partial Least Squares Regression (Witten et al., 1999), can be used to construct predictive security models.

ML algorithms can analyze large volumes of threat intelligence data to identify emerging threats and vulnerabilities relevant to IoT environments. Natural Language Processing (NLP) techniques can extract insights from unstructured threat data sources, such as security blogs, forums, and social media, enabling proactive threat detection and response. ML-based threat intelligence platforms can prioritize security alerts and recommend mitigation strategies based on the severity and relevance of identified threats. (Kumar & Kumar, 2023) offers a unique method for integrating Natural Language Processing (NLP) with Internet of Things (IoT) technologies in order to improve security. The study's main contribution is the creation of a system that uses word-embedding and n-gram approaches to identify harmful actions in an Internet of Things context.

4.3 Optimization

Due to the constraints of power, computational capabilities, and communication bandwidth, IoT optimization is a key challenge. In addressing these issues, machine learning (ML) has exhibited tremendous promise. To optimize the energy efficiency of IoT devices, numerous machine learning algorithms are being employed. For instance, reinforcement learning has been used to effectively manage energy consumption in sensor networks, allowing devices to "learn" the most energy-efficient modes of operation based on environmental indicators. Shi et al. (2018) report that machine learning models can also predict battery lifetime, enabling IoT administrators to optimize device maintenance cycles and thereby reduce the total cost of ownership.

Data communication is another area where machine learning can have a significant impact on optimization. IoT devices generate vast quantities of data that must be transferred and processed. Before data is transmitted, machine learning algorithms such as clustering can reduce its dimensionality, conserving both bandwidth and energy (Mahmud, Kaiser, Hussain, & Vasilakos, 2018).

Finally, machine learning can be utilized to optimize IoT task scheduling. In smart grids, for instance, genetic algorithms and neural networks have been implemented to efficiently schedule

duties and balance loads, thereby optimizing resource utilization.

4.4 User Experience

The capacity of machine learning to improve user experience in IoT can hardly be exaggerated. Individual preferences can be utilized by machine learning algorithms to customize IoT services, thereby substantially enhancing user satisfaction. In smart homes, for instance, machine learning models can learn the behavior of residents to automatically control lighting, heating, and other home systems (Ghayvat et al., 2015).

Healthcare is another domain where machine learning has significantly improved the user experience. (Rajalakshmi & Radha, 2020) Algorithms can monitor real-time data from wearable devices to alert users of potential health risks, facilitating preventative action. Machine learning can facilitate predictive maintenance in industrial IoT environments, thereby minimizing downtime and assuring a seamless user experience (Lee et al., 2015).

In addition, machine learning algorithms can provide IoT applications with a more interactive and adaptable user interface. For instance, natural language processing (NLP) algorithms can be used to create more intuitive voice-activated controls for a variety of IoT devices, including smart speakers and industrial apparatus (Mah et al., 2022).

In addition to enhancing the end-user experience, machine learning facilitates the tasks of network administrators. (Hodo et al., 2017) Algorithms can predict system failures and autonomously reroute data, providing a more reliable and consistent service to end users.

4.5 Case studies

Healthcare: Predictive Analytics in Wearable Devices

The discipline of predictive analytics powered by machine learning is expanding in the healthcare industry. A study, for instance, analysed real-time data from ubiquitous devices that monitor biometrics such as heart rate and blood pressure using machine learning algorithms. These algorithms could foresee potential cardiac events, enabling opportune medical intervention (Rajalakshmi & Radha, 2020). This application improves patient care and optimises healthcare operations by concentrating medical resources where they are most required.

Industrial IoT: Predictive Maintenance

Another domain where machine learning has had a significant impact is the industrial sector. General Electric has integrated machine learning algorithms into its Predix platform for Industrial IoT in order to predict impending machine failures (Lee et al., 2015). This type of predictive maintenance assists industries in optimizing their operations, decreasing downtimes, and reducing maintenance expenses.

Smart Cities: Traffic Management

To optimize traffic flow in smart communities, machine learning algorithms have been implemented. DeepMind of Google has collaborated with cities to apply machine learning to historical traffic data, allowing traffic signal systems to adapt to real-time conditions and reducing congestion (Ahmad & Tsuji, 2021). This is a classic illustration of how machine

learning can optimize operational aspects in an Internet of Things-driven environment.

Home Automation: Energy Efficiency

Smart dwellings are increasingly utilizing machine learning to enhance user experience and sustainability. Google's Nest Learning Thermostat uses machine learning algorithms to analyze occupant behavior and modify heating and cooling systems accordingly, resulting in up to 15% energy savings (Ghayvat et al., 2015).

Security: Anomaly Detection in Networks

Cisco's Stealthwatch security analytics product uses machine learning to help organizations detect threats in real-time. (Fernandes, 2014) The machine learning algorithms can analyze network behavior and identify suspicious activities, thereby enhancing the security of IoT systems.

These case studies demonstrate the importance of machine learning in enhancing and optimizing various aspects of IoT systems. Whether in healthcare, industrial operations, smart communities, home automation, or security, machine learning algorithms have demonstrated their ability to enhance the functionalities of IoT systems.

4.6 Challenges and Limitations Associated with integrating ML into IoT security frameworks

ML models require large volumes of high-quality data for training and validation. However, IoT environments may generate noisy or incomplete data, making it challenging to train accurate ML models. The data collected by IoT sensors can often be noisy, redundant, and even empty, which can negatively impact the performance of these algorithms (Mohammed et al., 2023). Moreover, collecting sufficient labeled data for supervised learning approaches can be resource-intensive and impractical in IoT settings with limited resources and bandwidth.

IoT devices often have limited computational power, memory, and energy resources, which can constrain the deployment of resource-intensive ML algorithms. ML models must be lightweight and energy-efficient to run effectively on constrained IoT devices, necessitating optimization techniques such as model compression, quantization, and distributed learning. IoT nodes are low-power gadgets with constrained energy, memory, computation, and communication bandwidth. Data overflow issues might arise in IoT nodes because of their limited power and resource limitations (Alhasanat et al., 2019). IoT devices collect sensitive data, raising concerns about data privacy and protection. Integrating ML into IoT security frameworks requires careful consideration of privacy-preserving techniques, such as federated learning, differential privacy, and encrypted computation, to ensure that sensitive data is not exposed to unauthorized parties during ML model training and inference.

To determine how robustly both classic machine learning and deep learning IDS models might withstand adversarial attacks, Papadopoulos et al. (Alhasanat et al., 2019) performed experiments. The experimental results validated that adversarial assaults have the potential to significantly undermine intrusion detection systems. Adversarial attacks pose a significant threat

to ML-based security systems, where attackers attempt to manipulate or evade detection by exploiting vulnerabilities in ML algorithms. Adversarial attacks can undermine the effectiveness of ML-based intrusion detection, anomaly detection, and authentication systems, necessitating robust defenses, such as adversarial training, model robustness verification, and anomaly detection techniques resilient to adversarial examples.

ML models used for IoT security must be interpretable and explainable to facilitate trust and understanding among stakeholders. However, complex ML models, such as deep neural networks, often lack interpretability, making it challenging to understand how decisions are made or to diagnose model errors. Ensuring model interpretability is crucial for detecting and addressing biases, errors, and vulnerabilities in ML-based security systems. The trust problem between users and ML models for IDS was the focus of Mahbooba et al.'s study (Mahbooba et al., 2021). They emphasized that the majority of earlier research concentrated only on classifier accuracy, offering no explanation for the thinking or actions of the algorithms. They employed the KDD99 dataset (Tavallaei et al., 2009) and the DT method. Three key processes made up their technique, in short: feature rating, DT rule extraction, and comparison with the most recent algorithms. The decision-making process of the tree was elucidated by describing the characteristics on each branch and the threshold value. But in the presence of dataset noise, their system was susceptible to overfitting.

4.7 Proposed ML Framework for IOT Security

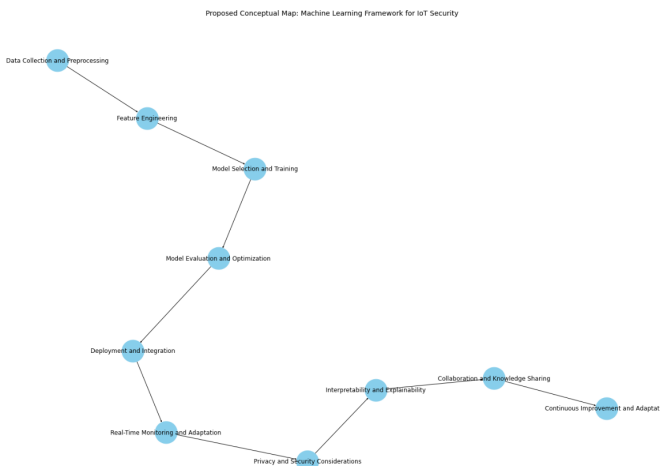


Fig. 1. Proposed Machine Learning Framework

The initial stage of our proposed framework is crucial for enhancing the quality and reliability of the data used for training ML models. Additionally, feature engineering techniques are employed to extract meaningful patterns and relationships from the pre-processed data, enabling the ML models to effectively capture important security insights. This step is particularly relevant in IoT contexts where data may exhibit non-linear relationships or contain high-dimensional features,

necessitating sophisticated feature selection and transformation methods.

Model selection and training constitute another pivotal aspect of the proposed framework, where appropriate ML algorithms are chosen based on the specific security problem at hand, such as anomaly detection or classification of malicious activities. The deployment and integration phase ensures seamless integration of ML-based security systems with existing IoT infrastructure, enabling real-time monitoring and adaptation to changing environmental conditions and emerging threats. This aspect of the framework emphasizes the importance of scalability, efficiency, and interoperability in deploying ML models across diverse IoT devices and networks.

Privacy and security considerations are paramount in the proposed framework, given the sensitive nature of data collected by IoT devices and the potential risks associated with unauthorized access or manipulation. Through privacy-preserving techniques such as federated learning and differential privacy, the framework seeks to safeguard sensitive information while still enabling effective security analysis. Moreover, the emphasis on interpretability and explainability ensures that ML models provide transparent and understandable outputs, fostering trust and confidence among stakeholders.

V. MACHINE LEARNING AND IOT IN SMART HEALTHCARE

This is an example that demonstrates how machine learning and IoT can enhance healthcare by providing continuous monitoring, early detection, and personalized care, ultimately leading to better patient outcomes.

5.1 Problem Statement

Monitor patients' vital signs in real-time and predict potential health complications to provide timely interventions and personalized care.

5.2 Data Collection

1. **Wearable Devices:** IoT-enabled wearable devices (like smartwatches and fitness trackers) collect data on heart rate, blood pressure, glucose levels, activity levels, and other vital signs.
2. **Electronic Health Records (EHRs):** Historical health data, including medical history, lab results, and previous diagnoses.
3. **Environmental Data:** Contextual information such as temperature, humidity, and air quality that can affect health.

5.3 Data Preprocessing

1. **Cleaning:** Remove noise and irrelevant data from the wearable devices and health records.
2. **Normalization:** Scale the data for uniformity.
3. **Feature Engineering:** Create new features such as moving averages of vital signs, rates of change, and correlations with environmental factors.

5.4 Machine Learning Model

1. **Algorithm Selection:** Suitable algorithms for time-series forecasting and classification, such as:
 - Recurrent Neural Networks (RNN) / Long Short-Term Memory (LSTM): Effective for sequential health data.
 - Random Forest: Good for handling various health metrics and producing interpretable results.
 - Support Vector Machines (SVM): Suitable for classification of health conditions.
2. **Training:** Train the model on historical health data and real-time sensor data.
3. **Validation:** Validate the model using separate datasets to ensure it generalizes well to new, unseen data.

5.5 Deployment

1. **Real-time Monitoring:** Continuously monitor real-time data from wearable devices.
2. **Prediction:** Predict potential health issues like arrhythmias, hypertension, or hyperglycemia.
3. **Alerts and Recommendations:** Send alerts to healthcare providers or patients when a potential issue is detected and provide personalized care recommendations.

5.6 Example Workflow

1. **Data Ingestion:** Wearable devices and EHRs send real-time and historical data to a cloud platform.
2. **Feature Extraction:** Extract relevant features from the raw data in real time.
3. **Model Prediction:** The machine-learning model processes the features to predict potential health issues.
4. **Alerts and Recommendations:** The system generates alerts and provides recommendations for timely interventions.

5.7 Benefits

- **Early Detection:** Early detection of potential health issues allows for timely interventions, potentially saving lives.
- **Personalized Care:** Personalized recommendations based on individual health data improve care quality.
- **Continuous Monitoring:** Continuous real-time monitoring provides a comprehensive view of a patient's health status.
- **Reduced Healthcare Costs:** Early intervention can reduce hospital admissions and healthcare costs.

VI. CONCLUSION

This study set out to investigate the function of machine learning in the Internet of Things (IoT) in depth. The main findings highlight the fundamental contributions of machine learning to multiple facets of IoT, including data analytics, security, optimization, and user experience. Through real-world case studies in healthcare, industrial settings, smart cities, and

home automation, the study illustrated how machine learning algorithms have been effectively deployed to improve the operational efficiencies of IoT systems (Lee et al., 2015; Ahmad & Tsuji, 2021; Rajalakshmi & Radha, 2020). Al-Fuqaha et al. (2015) highlighted the symbiotic relationship between the Internet of Things (IoT) and machine learning, reinforcing the notion that machine learning can provide comprehensive solutions across a spectrum of IoT applications. The proliferation of Internet of Things (IoT) devices has brought about transformative changes across various domains, promising unparalleled convenience and efficiency. However, this rapid expansion has also ushered in a myriad of security challenges, with IoT ecosystems becoming prime targets for malicious cyber activities. As highlighted throughout this study, addressing these security challenges necessitates innovative approaches that can adapt to the dynamic and complex nature of IoT environments.

Machine learning (ML) has emerged as a powerful tool for enhancing IoT security, offering the capability to analyze vast amounts of data generated by IoT devices in real-time and detect anomalies indicative of potential security threats. ML techniques such as anomaly detection, supervised learning, and predictive analytics, IoT stakeholders can proactively identify and mitigate security breaches, bolstering the resilience of IoT infrastructures against evolving cyber threats. Moreover, ML-driven security mechanisms enable adaptive and proactive measures, continuously learning from new data and evolving threat landscapes to effectively mitigate risks.

Despite the promising potential of ML in IoT security, several challenges and limitations must be addressed to realize its full benefits. These include the need for privacy-preserving ML techniques to ensure data privacy and protection, robust defenses against adversarial attacks, and the development of interpretable ML models to foster trust and understanding among stakeholders. Additionally, IoT environments are dynamic and heterogeneous, requiring ML-based security systems to adapt and learn in real-time. Future research efforts should focus on overcoming these challenges, exploring self-learning and adaptive ML techniques tailored to the unique realities of IoT security. By addressing these challenges and advancing the state-of-the-art in ML-based IoT security, stakeholders can effectively safeguard IoT ecosystems and mitigate emerging cyber threats.

VII. RECOMMENDATIONS

Given the sensitivity of data collected by IoT devices, there is a growing need for privacy-preserving ML techniques that can ensure data privacy and protection while still enabling effective security analysis. Future research should focus on developing advanced cryptographic and federated learning approaches that enable collaborative ML model training across distributed IoT networks without compromising data privacy. Adversarial attacks pose a significant threat to ML-based IoT security systems, highlighting the need for robust defenses against adversarial manipulation and evasion. Future research should focus on developing robust ML models and detection mechanisms resilient to adversarial examples, as well as techniques for evaluating and enhancing the robustness of ML-

based security systems against sophisticated attacks. Additionally, Future research should prioritize the development of interpretable ML models and techniques for explaining model predictions and decisions, enabling stakeholders to understand, validate, and trust the output of ML-based security systems.

Finally, IoT environments are dynamic and evolving, requiring ML-based security systems to adapt and learn from changing conditions and emerging threats in real-time. Future research should explore self-learning and adaptive ML techniques that enable IoT security systems to continuously improve and optimize their performance based on evolving data and feedback from the environment.

Given the significant impact of machine learning on the Internet of Things, policymakers must consider regulations that encourage innovation while ensuring ethical considerations. Particular attention should be given to data privacy and security, particularly in industries such as healthcare where sensitive information is involved (Orb, Eisenhauer, and Wynaden, 2001). The integration of machine learning into IoT systems should emphasize scalability and adaptability for practitioners. Due to the rapid evolution of IoT and machine learning technologies, systems should be designed to accommodate new algorithms and protocols (Mahmud et al., 2018). Moreover, given the potential for machine learning to optimize energy consumption in IoT devices, industries seeking to enhance sustainability should prioritize adopting these algorithms.

This study concludes that machine learning considerably improves the capabilities and potential of Internet of Things (IoT) systems across multiple domains. As both technologies continue to develop, the integration of them promises revolutionary changes that could revolutionize the way we live and work.

REFERENCES

- [1] Ahmad, A. B., & Tsuji, T. (2021). Traffic monitoring system based on deep learning and seismometer data. *Applied Sciences*, 11(10), 4590. <https://doi.org/10.3390/app11104590>
- [2] 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.
- [3] Ashton, K. (2009). That 'Internet of Things' Thing. *RFID Journal*.
- [4] Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, 54(15), 2787-2805.
- [5] Bishop, C. M. (2006). *Pattern Recognition and Machine Learning*. Springer.
- [6] 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.
- [7] Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77-101.
- [8] Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications.
- [9] DiCicco-Bloom, B., & Crabtree, B. F. (2006). The qualitative research interview. *Medical Education*, 40(4), 314-321.
- [10] Fernandes, D. A. (2014). Security issues in cloud environments: A survey. *International Journal of Information Management*, 40, 58–73.
- [11] Ghayvat, H., Mukhopadhyay, S., Gui, X., & Suryadevara, N. (2015). WSN- and IOT-Based Smart Homes and Their Extension to Smart Buildings. *Sensors*, 15(5), 10350-10379.
- [12] Hodo, E., Bellekens, X., Hamilton, A., Dubouilh, P. L., Iorkyase, E., Tachtatzis, C., & Atkinson, R. (2017). Threat analysis of IoT networks using artificial neural network intrusion detection system. *Proceedings of the International Symposium on Networks, Computers and Communications (ISNCC)*, 1-6.
- [13] Jordan, M. I., & Mitchell, T. M. (2015). Machine learning: Trends, perspectives, and prospects. *Science*, 349(6245), 255-260.
- [14] LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature*, 521(7553), 436-444.
- [15] Lee, J., Ardakani, H. D., Yang, S., & Bagheri, B. (2015). Industrial big data analytics and cyber-physical systems for future maintenance & service innovation. *Procedia CIRP*, 38, 3-7.
- [16] Mah, P. M., Skalna, I., & Muzam, J. (2022). Natural language processing and artificial intelligence for enterprise management in the era of industry 4.0. *Applied Sciences*, 12(18), 9207. <https://doi.org/10.3390/app12189207>
- [17] Mahmud, M., Kaiser, M. S., Hussain, A., & Vasilakos, A. V. (2018). Applications of deep learning and reinforcement learning to biological data. *IEEE Transactions on Neural Networks and Learning Systems*, 29(6), 2063-2079.
- [18] Marshall, C., & Rossman, G. B. (2014). *Designing qualitative research*. Sage publications.
- [19] Mitchell, T. M. (1997). *Machine Learning*. McGraw-Hill.
- [20] Orb, A., Eisenhauer, L., & Wynaden, D. (2001). Ethics in qualitative research. *Journal of Nursing Scholarship*, 33(1), 93-96.
- [21] Rajalakshmi, P., & Radha, S. (2020). IoT-Based Health Monitoring System. *Journal of Medical Systems*, 44(2), 1-9.
- [22] Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, 57(10), 2266-2279.
- [23] Sarker, I. H. (2021). Deep Learning: a comprehensive overview on techniques, taxonomy, applications and research directions. *SN Computer Science*, 2(6). <https://doi.org/10.1007/s42979-021-00815-1>
- [24] Shi, J., Wan, J., Yan, H., & Suo, H. (2018). A survey of cyber-physical systems. *Wireless Networks*, 24(7), 2467-2483.
- [25] Want, R. (2006). An introduction to RFID technology. *IEEE Pervasive Computing*, 5(1), 25-33.
- [26] S. M. Tahsien, H. Karimipour, and P. Spachos, "Machine learning based solutions for security of Internet of Things (IoT): A survey," *Journal of Network and Computer Applications*, vol. 161, p. 102630, Jul. 2020, doi: <https://doi.org/10.1016/j.jnca.2020.102630>.
- [27] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019, doi: <https://doi.org/10.1109/access.2019.2924045>.
- [28] M. S. Mahdavejad, M. Rezvan, M. Barekatin, P. Adibi, P. Barnaghi, and A. P. Sheth, "Machine learning for internet of things data analysis: a survey," *Digital Communications and Networks*, vol. 4, no. 3, pp. 161–175, Aug. 2018, doi: <https://doi.org/10.1016/j.dcan.2017.10.002>.
- [29] B. Ślusarczyk, "INDUSTRY 4.0 – ARE WE READY?," *Polish Journal of Management Studies*, vol. 17, no. 1, pp. 232–248, Jun. 2018, doi: <https://doi.org/10.17512/pjms.2018.17.1.19>.
- [30] F. Thiesse and F. Michahelles, "An overview of EPC technology," *Sensor Review*, vol. 26, no. 2, pp. 101–105, Apr. 2006, doi: <https://doi.org/10.1108/02602280610652677>.
- [31] A. B. Chebudie, R. Minerva, and D. Rotondi, "Towards a definition of the Internet of Things (IoT)," *IEEE Internet Initiative*, May 2015.
- [32] J. Bradley, J. Loucks, J. Macaulay, and A. Noronha, "Internet of Everything (IoE) Value Index How Much Value Are Private-Sector Firms Capturing from IoE in 2013?" Accessed: Oct. 23, 2022. [Online]. Available: https://www.cisco.com/c/dam/en_us/about/business-insights/docs/ioe-value-index-whitepaper.pdf
- [33] I. H. Sarker, "Machine Learning: Algorithms, Real-World Applications and Research Directions," *SN Computer Science*, vol. 2, no. 3, pp. 1–21, Mar. 2021, doi: <https://doi.org/10.1007/s42979-021-00592-x>.
- [34] I. H. Sarker, "Deep Cybersecurity: A Comprehensive Overview from Neural Network and Deep Learning Perspective," *SN Computer Science*, vol. 2, no. 3, Mar. 2021, doi: <https://doi.org/10.1007/s42979-021-00535-6>.
- [35] I. H. Sarker, "Deep Learning: A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions," *SN Computer Science*, vol. 2, no. 6, Aug. 2021, doi: <https://doi.org/10.1007/s42979-021-00815-1>.
- [36] W. Ng, Budiman Minasny, W. de, and José A. M. Demattê, "Estimation of effective calibration sample size using visible near infrared

- spectroscopy: deep learning vs machine learning,” Sep. 2019, doi: <https://doi.org/10.5194/soil-2019-48>.
- [37] S. Li, L. D. Xu, and S. Zhao, “The internet of things: a survey,” *Information Systems Frontiers*, vol. 17, no. 2, pp. 243–259, Apr. 2014, doi: <https://doi.org/10.1007/s10796-014-9492-7>.
- [38] Singapore Statutes Online, “Personal Data Protection Act 2012 - Singapore Statutes Online,” *Agc.gov.sg*, 2012. <https://sso.agc.gov.sg/Act/PDPA2012>
- [39] L. S. Branch, “Consolidated federal laws of canada, Digital Privacy Act,” *laws-lois.justice.gc.ca*, Nov. 15, 2019. https://laws-lois.justice.gc.ca/eng/annualstatutes/2015_32/page-1.html “Apple’s Worldwide Developers Conference Kicks Off June 13 in San Francisco,” *Apple Newsroom (Nigeria)*. <https://www.apple.com/ng/newsroom/2016/04/18Apples-Worldwide-Developers-Conference-Kicks-Off-June-13-in-San-Francisco/> (accessed Mar. 03, 2024).
- [40] A. , Hamza, H. H. Gharakheili, and V. Sivaraman, “IoT Network Security: Requirements, Threats, and Countermeasures,” *Cryptography and Security*, 2020, doi: <https://doi.org/10.48550/arXiv.2008.09339>.
- [41] L. Xiao, Y. Li, G. Liu, Q. Li, and W. Zhuang, “Spoofing Detection with Reinforcement Learning in Wireless Networks,” *2015 IEEE Global Communications Conference (GLOBECOM)*, Dec. 2015, doi: <https://doi.org/10.1109/glocom.2015.7417078>.
- [42] L. Xiao, X. Wan, and Z. Han, “PHY-Layer Authentication With Multiple Landmarks With Reduced Overhead,” vol. 17, no. 3, pp. 1676–1687, Mar. 2018, doi: <https://doi.org/10.1109/twc.2017.2784431>.
- [43] S.-Y. Lee, S. Wi, E. Seo, J.-K. Jung, and T.-M. Chung, “ProFiOt: Abnormal Behavior Profiling (ABP) of IoT devices based on a machine learning approach,” *2017 27th International Telecommunication Networks and Applications Conference (ITNAC)*, Nov. 2017, doi: <https://doi.org/10.1109/atnac.2017.8215434>.
- [44] H.-S. Ham, H.-H. Kim, M.-S. Kim, and M.-J. Choi, “Linear SVM-Based Android Malware Detection for Reliable IoT Services,” *Journal of Applied Mathematics*, vol. 2014, p. e594501, Sep. 2014, doi: <https://doi.org/10.1155/2014/594501>.
- [45] Y. Chang, W. Li, and Z. Yang, “Network Intrusion Detection Based on Random Forest and Support Vector Machine,” *22017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)*, Jul. 2017, doi: <https://doi.org/10.1109/cse-euc.2017.118>.
- [46] R. Primartha and B. A. Tama, “Anomaly detection using random forest: A performance revisited,” *2017 International Conference on Data and Software Engineering (ICoDSE)*, Nov. 2017, doi: <https://doi.org/10.1109/icodse.2017.8285847>.
- [47] R. Doshi, N. Feamster, and N. Aphorpe, “Machine Learning DDoS Detection for Consumer Internet of Things Devices,” *2018 IEEE Security and Privacy Workshops (SPW)*, May 2018, doi: <https://doi.org/10.1109/SPW.2018.00013>.
- [48] P. A. A. Resende and A. C. Drummond, “A Survey of Random Forest Based Methods for Intrusion Detection Systems,” *ACM Computing Surveys*, vol. 51, no. 3, pp. 1–36, May 2018, doi: <https://doi.org/10.1145/3178582>.
- [49] T. Mohamed, T. Otsuka, and T. Ito, “Towards Machine Learning Based IoT Intrusion Detection Service,” *Recent Trends and Future Technology in Applied Intelligence*, pp. 580–585, May 2018.
- [50] I. Alrashdi, A. Alqazzaz, E. Aloufi, R. Alharthi, M. Zohdy, and H. Ming, “AD-IoT: Anomaly Detection of IoT Cyberattacks in Smart City Using Machine Learning,” *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, Jan. 2019, doi: <https://doi.org/10.1109/CCWC.2019.8666450>.
- [51] M. Swarnkar and N. Hubballi, “OCPAD: One class Naive Bayes classifier for payload based anomaly detection,” *Expert Systems with Applications*, vol. 64, pp. 330–339, Dec. 2016, doi: <https://doi.org/10.1016/j.eswa.2016.07.036>.
- [52] A. O. Prokofiev, Y. S. Smirnova, and V. A. Surov, “A method to detect Internet of Things botnets,” *2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, Jan. 2018, doi: <https://doi.org/10.1109/eiconrus.2018.8317041>.
- [53] R. Bapat *et al.*, “Identifying malicious botnet traffic using logistic regression,” *IEEE Xplore*, Apr. 01, 2018. <https://ieeexplore.ieee.org/abstract/document/8374749> (accessed Nov. 01, 2020).
- [54] S.-Y. Lee, S. Wi, E. Seo, J.-K. Jung, and T.-M. Chung, “ProFiOt: Abnormal Behavior Profiling (ABP) of IoT devices based on a machine learning approach,” *2017 27th International Telecommunication Networks and Applications Conference (ITNAC)*, Nov. 2017, doi: <https://doi.org/10.1109/atnac.2017.8215434>.
- [55] I. H. Witten, E. Frank, L. E. Trigg, M. A. Hall, G. Holmes, and Sally Jo Cunningham, “Weka: Practical machine learning tools and techniques with Java implementations,” Aug. 1999.
- [56] Y. Kumar and V. Kumar, “Security in IoT systems using natural language processing: Future challenges and directions,” *Internet Technology Letters*, vol. 6, no. 4, Feb. 2023, doi: <https://doi.org/10.1002/itl2.411>.
- [57] A. F. Y. Mohammed, S. M. Sultan, J. Lee, and S. Lim, “Deep-Reinforcement-Learning-Based IoT Sensor Data Cleaning Framework for Enhanced Data Analytics,” *Sensors*, vol. 23, no. 4, p. 1791, Jan. 2023, doi: <https://doi.org/10.3390/s23041791>.
- [58] M. Alhasanat, S. Althunibat, K. A. Darabkh, A. Alhasanat, and M. Alsafasfeh, “A Physical-Layer Key Distribution Mechanism for IoT Networks,” *Mobile Networks and Applications*, vol. 25, no. 1, pp. 173–178, Feb. 2019, doi: <https://doi.org/10.1007/s11036-019-01219-5>.
- [59] B. Mahbooba, M. Timilsina, R. Sahal, and M. Serrano, “Explainable Artificial Intelligence (XAI) to Enhance Trust Management in Intrusion Detection Systems Using Decision Tree Model,” *Complexity*, vol. 2021, pp. 1–11, Jan. 2021, doi: <https://doi.org/10.1155/2021/6634811>.
- [60] M. Tavallae, E. Bagheri, W. Lu, and A. A. Ghorbani, “A detailed analysis of the KDD CUP 99 data set,” *2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications*, Jul. 2009, doi: <https://doi.org/10.1109/CISDA.2009.5356528>.