International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(REVIEW ARTICLE)

AI-enabled intrusion detection systems in IoT networks: Advancing defense mechanisms for resource-constrained devices

Sridevi Kakolu [1, 2, *], Muhammad Ashraf Faheem [3, 4] and Muhammad Aslam [3, 5]

[1] *Boardwalk Pipelines, Houston, Texas, USA.*
[2] *Jawaharlal Nehru Technological University, Hyderabad, India.*
[3] *Speridian Technologies, Lahore, Pakistan.*
[4] *Lahore Leads University, Lahore, Pakistan.*
[5] *University of Punjab, Lahore, Pakistan*

International Journal of Science and Research Archive, 2023, 09(01), 752–769

Publication history: Received on 08 March 2023; revised on 23 June 2023; accepted on 26 June 2023

Article DOI: https://doi.org/10.30574/ijsra.2023.9.1.0316

Abstract

With the rapid expansion of Internet of Things (IoT) networks comes an urgent need for advanced security mechanisms to combat ever more sophisticated cyber threats. Although intrusion detection systems (IDS) are vital, more is needed to detect IoT intrusion in resource-limited IoT devices with constrained processing capabilities and memory. In this paper, we discuss how Artificial Intelligence (AI) can be embedded into IDS frameworks to improve the security of IoT networks. Using available resources, machine learning, and deep learning techniques in AI-enabled IDS can enhance detection and mitigate intrusions. The existing methodologies are reviewed comprehensively, implementation challenges are assessed, and potential future research directions are discussed in this study. The conclusions show that AI-based IDS can significantly enable a more secure and resilient IoT ecosystem, provide innovative defense strategies, and open up opportunities for next-generation network security solutions.

Keywords: IoT; Intrusion Detection Systems; AI; Machine Learning; Deep Learning; Resource-Constrained Devices; Cybersecurity; Network Security; Threat Mitigation

1. Introduction

1.1. Background on IoT Networks

With the Internet of Things or IoT, we have a new class of technology where a massive, networked collection of physical devices can connect and communicate. It is an ecosystem of everyday objects, vehicles, buildings, and other things rigged with sensors, software, and network connectivity that are now interlinked. The IoT enables data collection and exchange, allowing devices and central systems to interact with each other more efficiently and smarter.

There are diverse and transformative IoT applications across all segments of the industry. In smart homes, devices such as thermostats, lighting, and security cameras offer improved control automation and provide convenience and safety. In healthcare, wearables and smart medical devices allow real-time data to be shared between patients and providers to help patients and enable remote monitoring.

Predictive maintenance and real-time machinery monitoring on manufacturing sites have leveraged the Industrial internet to achieve more operational efficiency. IoT is used in smart cities for traffic management and energy-efficient buildings to encourage sustainable living and better urban infrastructure. IoT devices generally monitor soil and crop

* Corresponding author: Sridevi Kakolu

health so that farmers can improve their practices while saving resources, including water, soil, and energy in agriculture. Lastly, the automotive segment utilizes IoT in connected vehicles to provide better navigation, predictive maintenance, and more safety options, improving the driving experience.

1.2. Challenges of Securing IoT Networks

Securing IoT networks is a great challenge. Major issues are resource constraints. Many IoT devices have limited processing power and energy, making implementing traditional security measures, such as encryption, hard. That makes them vulnerable to attack. Security is further complicated by scalability as IoT devices grow in volume and since the Internet of Things consists of many devices, each with different security needs. Devices are all other hardware, software, and communication protocols; therefore, establishing universal security standards is stalled by their diversity.

Figureure 1 IoT security challenges

In addition, IoT devices being distributed in nature puts them at risk of both physical tampering and cyberattacks such as DDoS attacks. Large volumes of data lead to privacy concerns related to intentional or unintentional unauthorized data access and data personal information integrity concerns. In security, a lack of standardization means a lack of consistency in protection, and lifecycle management is tricky, with many devices unlikely to get frequent updates, meaning they are being confronted with new threats. A comprehensive set of standards, coupled with lightweight security protocols and robust authentication mechanisms, are needed to enable the incorporation of these security functions into the corresponding IoT network without compromising the capabilities and innovation that IoT is designed to deliver.

1.3. Importance of Intrusion Detection Systems (IDS)

Intrusion Detection Systems (IDS), such as network and host-based, are key security tools enabling Intrusion intrusion detection (ID), which captures for detecting unauthorized access, intrusion, and anomalies. Analyzing these interactions through IDS is important to protecting sensitive data, maintaining network integrity, and identifying possible security breaches in real-time. The main functions of IDS are to detect threats – suspicious activity such as suspicious patterns of downloads, malware infections, and unauthorized access attempts, and to respond to incidents in real-time by sending real-time alerts and detailed logs that facilitate immediate action against threats. Logging network activities logged by IDS also helps organizations achieve compliance with data protection regulations during audits.

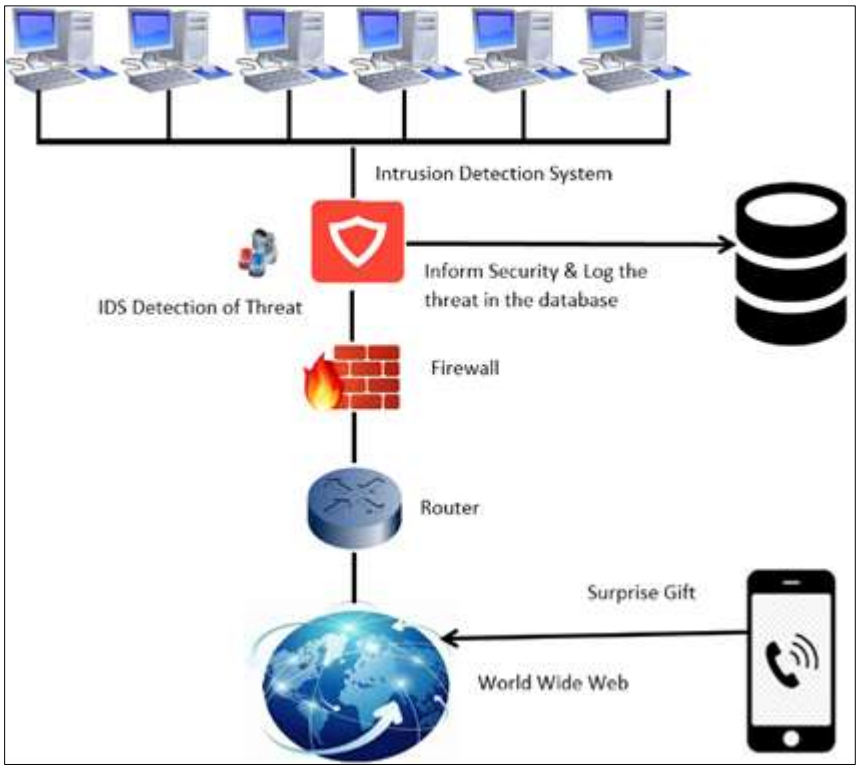

Figure 2 Intrusion Detection System in General

They also provide improved network visibility, allowing visibility into traffic patterns and user behavior — all of which can be used to improve security policies and overall the security posture of your business.

2. Comparing traditional IDS to AI-enabled IDS

2.1. Traditional IDS

Signature-based and anomaly-based detection have been the traditional approaches for Intrusion detection systems (IDS). On the other hand, signature-based detection uses the known patterns of malicious activity, which will detect when known threats are present but won't pick up new or evolving threats. The anomaly-based approach spots deviations from normal behavior; however, it may produce high false positive rates, hence explaining every single time why only the security teams suffer from alert fatigue. They also flag suspicious activities, but it [rule-based systems] takes a lot of effort to update rules constantly. However, these traditional systems suffer from high false positive rates, frequent updates, and high computational demands (particularly in the resource-constrained IoT environment).

2.2. AI-Enabled IDS

Using sophisticated algorithms and machine learning models, an AI-enabled IDS is a significant advancement in intrusion detection. Deep learning techniques, which can analyze large datasets and detect sophisticated patterns, enable these systems to adapt to new attack types better than traditional IDS. By performing the behavioral analysis to observe normal network traffic, they can more precisely detect anomalies and get fewer false positives. Unlike conventional IDS, which are typically triggered externally by changes in the conFigureuration file or are manually updated, AI-enabled IDS is more efficient and can be applied in diverse situations, e.g., in resource-constrained environments where, without any manual intervention in between, the IDS learns and adapts as the system evolves.

Yet, like any other technology, AI-enabled IDS has challenges like the need for specialized expertise to develop and maintain AI models and its dependence on large datasets for training in order to work effectively. Lastly, many AI models are considered a 'black box,' meaning the steps necessary to identify threats in the system are not transparent, making them difficult for the security teams to comprehend.

To sum up, though traditional IDS have formed the foundation of network security, AI-aided IDS greatly improved threat detection and responsiveness, making them indispensable for modern cybersecurity strategies.

2.3. Objective of the Research

In this Research, we craft a balanced approach to provide advanced security solutions to resource-constrained IoT devices, which are notorious for the shortage of computational power to support traditional security measures. It concerns lightweight security protocols that are efficient, scalable, and AI-driven intrusion detection systems built using adaptive learning algorithms to tackle emerging threats.

3. Literature review

3.1. Types of Traditional IDS

Intrusion detection systems (IDS) are important in maintaining the security of IoT networks with a huge number of different kinds of devices and applications. There are three primary types of traditional IDS:

1. Signature-Based IDS: It depends on a predefined database of known threat signatures to identify malicious ones. It effectively identifies known threats, resulting in a relatively low rate of false positives, which is good for security operations. However, its effectiveness fades away in the presence of new or unknown attacks ('zero-day vulnerabilities'). Another major limitation of the system is the need for regular database updates, which must be constantly managed and monitored so that the IDS system is aware of current threats. However, relying on up-to-date signatures can be challenging in such dynamic IoT environments where threat signatures can quickly change.

2. Anomaly-based IDS: This creates a baseline of normal network behavior and watches for deviations from that baseline. Detection of unknown threats is permitted with this approach, enabling the identification of variations of known attacks. However, perhaps the biggest issue is anomaly-based systems. They generate very high false positive rates. Benign deviations from expected behavior can be mistaken for malicious activity and can instead cause alert fatigue on security teams. Moreover, anomaly-based detection necessitates exhaustive training data to precisely pinpoint what 'normal' behavior is, which can be a painful experience to get in environments that typically constrain IoT deployments regarding resources.

3. Hybrid IDS: This encompasses signature-based and anomaly-based detection methods. This integration exploits each approach's strengths to increase overall detection rates with fewer associated false positives. Hybrid systems provide a fuller security solution; however, they have become more complex and need more computational resources than purely software systems. In IoT environments, though, where devices typically have limited processing power and memory, this additional demand can be difficult to manage. Therefore, hybrid IDS can boost the security of IoT applications, but this is only sometimes viable for all IoT applications.

3.2. Limitations of Traditional IDS

Although traditional IDS are key to network security, they have severe limitations that render them ineffective for providing IoT security. First, resource constraints confront one of the biggest challenges; IoT devices are small devices with limited power and processing capabilities, such as a CPU and memory, which restricts the feasibility of supporting IDS. These limits can cause the security measures taken inadequate, and they will fail to protect from sophisticated cyber threats.

Traditional IDS implementation in IoT networks has further scalability issues. As [systems continue to grow] in the number of connected devices, and that number continues to grow exponentially, traditional IDS may need to scale better to effectively and efficiently manage and monitor the ever-increasing wealth of devices that come to characterize a modern IoT environment.

Another challenge is the heterogeneity of IoT devices as well. Devices now come in great numbers and use various communication protocols and standards, making the development of universal IDS solutions that could provide the monitoring and security of multiple devices more difficult. The diversity complicates IDS deployment and management because each device may need special security measures.

Another critical limitation is latency. The limited resources on many IoT devices can hinder traditional IDS's real-time detection capabilities. As a result of this restriction, potential threats are identified later, perhaps letting vulnerabilities be exploited before security measures can be put in place.

3.3. Case Studies and Previous Research

Various case studies and research initiatives illustrate traditional IDS's challenges in the IoT environment. In one case study, I concentrated on smart home security, specifically how well signature-based IDS would work in a smart home. The results showed that while the IDS could detect known attacks, new malware aimed at IoT devices caused major issues for the IDS. It also underscores an extremely important limitation of signature-based systems in these rapidly changing threat landscapes.

Important insights were also obtained from Research on anomaly detection techniques in IoT networks. These studies revealed that anomaly detection could detect such patterns indicating probable threats. However, the drawback was the high rate of false positives. This highlighted the need for a more sophisticated model to more accurately characterize normal behavior without having an alarm count go through the roof.

Another research study has explored the feasibility of deploying a hybrid IDS in industrial IoT. Results from this study showed that the hybrid approach of shoaling mode detection achieved greater detection than that of classical methods. However, it also asserted that such measures needed optimization, which would ensure good utilization of the resources; in an environment where resources are limited, deployment of robust security measures appears to get complicated.

3.4. AI Techniques in IDS

3.4.1. Machine Learning Approaches

This thesis shows that Artificial Intelligence (AI) techniques, such as machine learning, provide the means to enhance Intrusion Detection Systems (IDS) for IoT networks. Supervised learning is one machine learning approach that trains models on the labeled dataset. They train in this manner to differentiate normal from malicious activities. Supervised learning can employ a rich dataset of labeled network behaviors, including common examples like decision trees, support vector machines, and random forests.

In comparison, Unsupervised learning methods do not use the labeled data and concentrate on finding unique patterns and anomalies in the given set. In this context, clustering algorithms like k-means and hierarchical clustering are used. Because labeled data is usually scarce in the IoT environment, unsupervised learning is of particular value in many IoT applications in detecting unknown threats.

Semi-supervised learning is another innovative approach to this problem, and it combines training with a small amount of labeled data with a large amount of unlabeled data during training. Semi-supervised SVM and co-training approaches illustrate this approach; it provides a good trade-off between the need for labeled data and the availability of labeled data in Settings that lack labeled data, such as IoT scenarios. This hybrid approach permits effective training even when the labeled training datasets are not comprehensive.

3.4.2. Deep Learning Approaches

Intrusion detection is also afforded powerful additional tools from the world of machine learning, in particular, deep learning. Artificial Neural Networks (ANN) are machine learning algorithms designed to imitate how the human brain works and can learn to recognize more complex patterns from data. Different types of neural networks can be used depending on requirements during the analysis, including feedforward neural networks and recurrent neural networks (RNN) for analyzing sequential data and time series prediction in network traffic.

CNNs are mainly used for image operations, especially image recognition, so they were adapted for IDS, where they identify the spatial patterns in the network data. This adaptability shows that the ability of CNNs to recognize complex patterns states would serve as a warning for security breaches.

A deep learning architecture that remains equally important is the Long Short Term Memory (LSTM) network, an RNN with a special capacity that performs well in retaining long-term dependencies. Therefore, LSTMs are great for working with data sequences such as network traffic over time and are very useful for finding anomalies or patterns that may indicate possible threats.

3.5. Benefits of current AI in IDS for IoT networks.

Introducing AI techniques in an IDS presents many advantages, mostly for IoT networks with limited resources. One of the biggest advantages of AI models is that they allow for much better detection. They can learn and adjust to new and

ever-changing threats, enhancing detection rates of previously unknown attacks. In addition, due to reduced false positive rates, threat identification is more accurate and dependable in AI models than in traditional IDS.

Another advantage of using AI in IDS is scalability and efficiency. Even AI algorithms can be optimized to run on resource-strapped IoT devices, i.e., efficiently using the available processing power and memory. Furthermore, machine learning and deep learning capabilities for real-time processing are important to respond (in real-time) to traffic analysis and quickly mitigate possible threats.

AI techniques allow for the automation of threat response, bringing this threat defense more into the proactive realm. AI-enabled IDS can learn by learning or updating themselves based on new data without manual intervention. This proactive method allows the systems to predict how a threat would behave and pre-emptive security measures to be taken even before an incident.

Lastly, AI gives you complete network visibility of device behavior to perform advanced pattern recognition and behavioral analysis. The use of AI techniques for continuous monitoring and analysis of device behavior provides the means to detect subtle deviations of behavior that could indicate security breaches, improving the security posture of IoT networks.

4. Challenges in IoT Security

4.1. Resource Constraints

The Internet of Things (IoT) is an expanding ecosystem of connected devices communicating and transferring data. Yet, these devices are often constrained by their resources, making it difficult to implement them effectively, such as intrusion detection systems powered by AI. It is fundamental to understand these constraints to develop effective and efficient solutions regarding the constraints of IoT devices.

4.2. Limited Processing Power and Memory

The real challenge of developing the firmware of the IoT device is that it needs more processing power and memory. Owing to the inherent nature of these devices to be compact, cost-effective, and energy-efficient, their computational capabilities have intrinsic limitations. Low-power processors or microcontrollers are used by many IoT devices, which are unable to handle intensive practices. This makes it difficult for algorithms too complex to be deployed on these devices.

Not only do we have processing limitations, but memory constraints complicate it further. Generally, an IoT device has very limited memory for storing data and running the application. Since it is hard to manage larger datasets or use complex AI models that are resource-intensive. To deal with these challenges, developers work on creating lightweight algorithms that will run on the device's limited memory. Compression techniques are often applied to AI models to enable better operation, including reduction of computational load and memory use (such as model compression, pruning quantization, etc.).

4.3. Energy Efficiency Concerns

Energy efficiency is a second critical factor for IoT devices, many of which are battery or energy-harvesting-powered. It presents a challenging balancing act to maintain energy efficiency by integrating robust security controls. This increased power consumption can be prohibitive, given that complex algorithms can be run on such devices and the devices themselves rely on a limited energy source. Large amounts of energy usage have another nasty effect, requiring more frequent replacements or battery recharging, which reduces both the deployability and longevity of IoT systems.

Different methods have been introduced to address energy problems. Duty cycling, a technique in which devices move between active and sleep modes to avoid energy waste, is one such approach. On the other hand, edge computing has been seen as a reasonable fix, performing offloading processing tasks to local gateways with higher computational resources than current Internet of Things devices. This leaves the burden of hosting complex AI honestly up to cloud machines instead of individual IoT devices, yet the devices can still benefit from AI.

Focusing on lightweight algorithms and using edge computing, developers can utilize AI to create intrusion detection systems that cater to IoT devices' limited resources. By leveraging this approach, the security is improved without impacting the device performance or energy efficiency, and therefore, to construct a more secure and sustainable IoT ecosystem.

4.4. Diverse and Dynamic Environment

The Internet of Things or IoT refers to an ecosystem of connected devices that speak, collaborate, and perform several tasks. However, diversity and dynamism are fundamental in IoT networks and introduce unique challenges in implementing effective security measures. It is essential to understand these complexities to create security solutions that are at once robust and adaptable to the myriad complexities of an ever-changing technology and threat landscape.

4.5. Variety of Devices and Communication Protocols

IoT networks are distinguished by the wide range of devices they use. These all fall into the category of basic sensors to check environmental conditions and smart appliances that can perform complicated tasks. Every device has its computational capability, operating system, and functionality. These varying devices are also diverse, making it difficult to create universal solutions to security problems, as what works for one device style only works for another.

In addition, IoT devices communicate using many different protocols like MQTT, CoAP, Zigbee Bluetooth, etc. These protocols all operate on various characteristics and have different properties for security assurance. For example, some are designed to minimize power consumption for battery-operated sensors, while others optimize for high throughput on data. The multiplicity of communication standards requires security solutions that efficiently operate over the various protocols. One outcome of this leads to modular and protocol-agnostic security frameworks that allow different and scalable security to be instantiated with custom security tailored to a particular device type and how they communicate.

4.6. Evolving Threat Landscape

IoT networks have a changing security landscape, and new vulnerabilities and attack vectors appear as technology advances. In the last couple of years, however, cyber attackers have been improving, using advanced methods to attack the apparent weaker link in IoT systems. However, with threats constantly evolving, this presents a real challenge with security measures in that more than traditional methods may be required to deal with new approaches to attacks.

The possible attack scenarios on IoT networks are a Denial of Service (DoS) attack, data breach attack, man-in-the-middle attack, and many others. Each one of these attack types can have dire consequences, from compromising sensitive data to disrupting critical services. Intrusion detection systems (IDS) must exhibit high adaptability as these threats change rapidly, including the capability to learn and evolve to cope with new threats.

AI-powered IDS rely upon machine learning and deep learning techniques to Figureht the constantly changing landscape of threats. They can analyze historical data and patterns and anomalies, informing them of new threats as they are started. Adaptiveness and learning over time are key to retaining high security in an ever-changing world of attack strategies.

4.7. Importance of Adaptability and Resilience

The diverse and dynamic nature of the IoT network environment makes the need for adaptive and resilient security solutions much sought after. The design of security measures requires consideration of current threats and anticipation of likely future vulnerabilities. To do this, you need to approach security proactively, including regular monitoring and real-time analysis to anticipate threats.

User tailoring security solutions to support all those devices and communication protocols can be accomplished by emphasizing adaptability. In addition, resilience to gun attacks is essential to operate in the face of attack. A resilient security framework can survive and rebound from incidents and reduce its impact to a large extent on the core network, thus continuing to run.

Overall, the diverse and dynamic IoT network's characteristics pose formidable challenges to deploying security strategies. To build more secure IoT environments, we can create robust and adaptable security solutions that can handle various devices and communication protocols and be on our toes when faced with an ever-changing threat landscape. As these interconnected systems become an ever more critical part of our lives, the ability to proactively protect sensitive data and ensure reliability is very important.

5. AI-enabled ids approaches

5.1. Machine learning models in Intrusion Detection Systems for IoT networks.

This work focuses on machine learning models as a key enhancement of intrusion detection systems (IDS) in the Internet of Things (IoT) networks. Since IoT systems are becoming increasingly complex and interconnected as the scale of use expands, these models are dynamic and adaptive solutions to identify security threats. Through large amounts of data, machine learning can identify anomalies and patterns that signify potential intrusions to enhance the overall security standing of IoT environments.

Supervised and unsupervised learning is an acute distinction in the application of machine learning for intrusion detection. Supervised learning refers to using labeled datasets to train models in which every input is linked with a predicted output. In particular, this approach is highly efficient for classification problems like identifying normal vs malicious network traffic. Another advantage is that many supervised learning models can be fine-tuned to detect known threats accurately using extensive labeled data. However, it's a big limitation that relies heavily on the comprehensive data with the labels, which is very difficult to make available in an IoT setup. Furthermore, supervised models can need to catch up in stopping previously unseen or new threats, which are lackluster in keeping up with rapid development in the threat landscape.

However, unsupervised learning uses unlabeled data so that models can pick up patterns and anomalies without knowing what a threat is. Because this method does not rely on predefined labels, this method is particularly advantageous for detecting novel threats or zero-day attacks. Using unsupervised learning can expose abnormal patterns differing from normal behaviors and be a useful technique in a constantly evolving attack space. While this means that the false positive rate is high, this partly stems from the fact that we cannot label guidance; thus, it is more difficult to distinguish between false positives and actual threats.

Practitioners often use hybrid models incorporating both supervised and unsupervised learning to maximize the effectiveness of intrusion detection systems. By employing this integrative approach, we can capitalize on the strengths of each methodology and combine them in a manner that provides the complementary view that is unavailable when using a single method to understand network behavior at a more nuanced level. Through this, these models can respond to the intricacies of IoT environments and adequately deal with the dynamic nature of cyber threats.

5.2. Data preprocessing and feature selection

Finally, feature selection and data preprocessing are other critical aspects of developing effective machine-learning models for intrusion detection. Feature selection is the effective committee that finds the most relevant attributes in a dataset that increase the accuracy of the predictions. Reducing dimensionality and having good performance is possible by focusing on a model's key features. Common techniques in this process include filter, wrapper, and embedded methods. For example, filter methods determine feature relevance utilizing statistical measures, while wrapper methods iteratively try out subsets of features relying on model performance.

Just as important is data preprocessing, without which raw data is not ready for analysis and cannot be effectively understood by machine learning models. Normalization or standardization, filling in gaps or removing them, and encoding categorical data into numerical forms (to make the data compatible with most machine learning algorithms) are all important steps in the data preprocessing process. Preprocessing is needed to improve model accuracy and minimize the chance of overfitting so that the model generalizes well to new data.

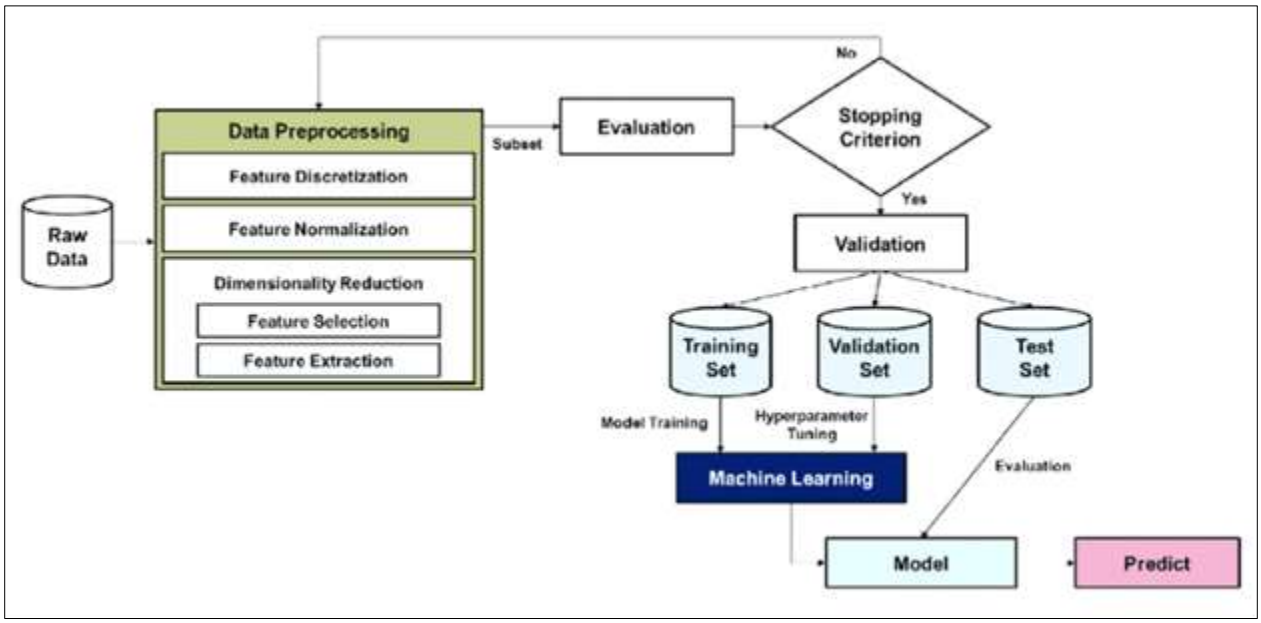

Figure 3 Data preprocessing in the machine learning process

Finally, securing networks containing IoT systems, whether network to one another or servers, is imperative, requiring integrating machine-learned models into AI-driven intrusion detection systems. Using expert knowledge, these systems use supervised and unsupervised learning strategies combined with powerful feature selection and data preprocessing methods to improve their accuracy and efficiency in threat detection. The expansion of the cyber threats landscape calls for the essentiality of machine learning adaptability in securing and maintaining IoT environment integrity.

5.3. Deep Learning Models in Intrusion Detection System for IoT Network Using

The advancement of intrusion detection systems (IDS) is due to deep learning models for IoT networks. These models use neural networks to look at and see through complex data patterns, thus making the threat detection systems more accurate and flexible. In parallel, as IoT networks become more complicated and larger, deep learning is valuable because it can handle many different kinds of data and increase cybersecurity.

On the other hand, the heart of deep learning is neural networks—that is, computational structures inspired by how the human brain is structured. Neural networks, called networks of neurons, are multiple layers of interconnected nodes (or neurons) that take input data and generate outputs. Raw data comes into the network starting from the input layer as the first part. Then, it is transformed through one or more hidden layers that perform complex computations and feature transformations. The output layer takes in the processed information and produces the final output, which provides predictions or classifications. Changing the depth and width of these layers changes the learning capacity and performance of the model.

There are many architectural forms of deep learning models for each data type. For example, convolutional neural networks (CNNs) were originally designed for image or spatial data but have been successfully applied to network traffic analysis for feature extraction. On the other hand, Recurrent Neural Networks (RNNs) are perfect for working with sequential data and, thus, for time series analysis in network traffic. Long Short-Term Memory Networks (LSTMs) are an advanced variant of RNNs, specifically designed to capture long-range dependencies in the data, which is of the essence for understanding patterns in time in the dynamic environment of the IoT.

It is important to note the advantages of deep learning models before traditional intrusion detection methods. Automatic feature extraction is one of the biggest benefits; deep learning models can learn features from raw data independently without manually inputting many items. It enhances the accuracy and, at the same time, eliminates most of the manual intervention that has characterized traditional feature selection algorithms. Additionally, deep learning excels at detecting overlapping and complex patterns and correlations between elements within large informational sets that are not usually looked for by conventional methods. Detection and protection against sophisticated and evolving cyber threats that do not follow known patterns rely on this capability. Besides, deep learning models have tremendous scalability and adaptability. As IoT networks become larger, the amount of data created becomes enormous, and deep learning models will also scale to analyze this massive amount of data efficiently. They are

inherently adaptive and capable of improving their effectiveness in detecting novel attacks over time by learning from new data. Due to this, the accuracy rates of intrusion detection of these models are higher than traditional methods.

From the above results, we summarized that deep learning models used in IoT networks can improve intrusion detection capabilities. These models use advanced neural network architectures to deliver robust security solutions that can keep up with today's cyber threats' fast-changing and complex nature. The cybersecurity landscape's future depends on applying deep learning to IDS to protect the IoT backfield and the integrity of interconnected systems.

5.4. Hybrid Intrusion Detection Models

In the context of the Internet of Things (IoT), hybrid models constitute a powerful way to augment the performance of intrusion detection systems (IDS). These models integrate machine learning and deep learning techniques to exploit the power of both approaches to deliver strong and adaptive threat detection for security threats that may be complex.

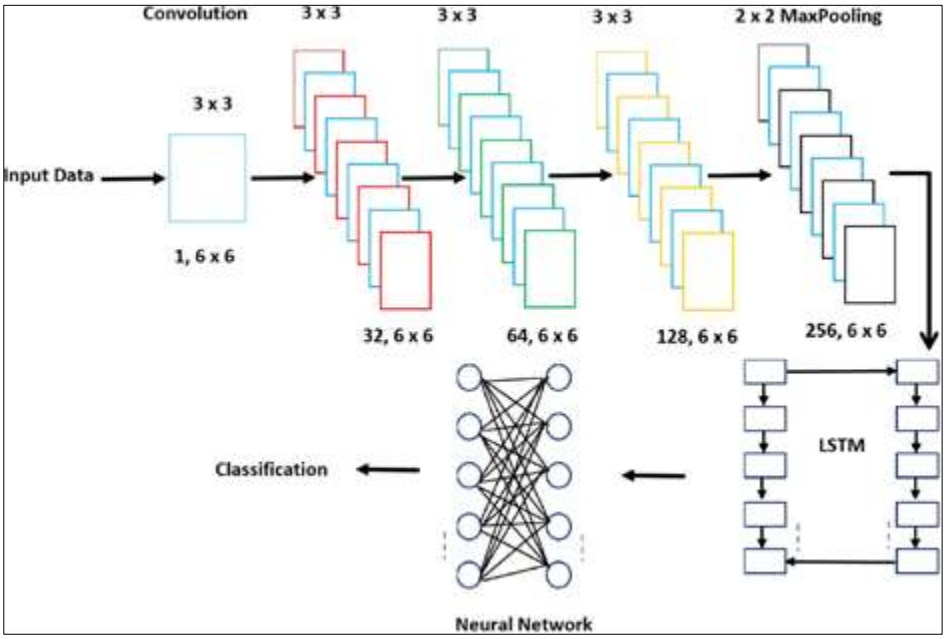

Figure 4 Hybrid Model Architecture using CNN and LSTM

The more complicated and diversified IoT networks become, the more vital it is for features to be detected effectively and the more necessary it is to have an extra tool, like a hybrid model, to support cybersecurity strategy.

5.5. Diving into Deep Learning and Machine Learning

Intrusion detection has been improved by hybrid models based on repeated machine learning algorithms and architectures previously used in deep learning. Initial data preprocessing and feature selection can be accomplished using machine learning techniques, including decision trees, support vector machines (SVM), and ensemble methods. Thus, these methods are good at finding key attributes of datasets that are relevant to classification tasks. On the other hand, deep learning models (e.g., neural networks) are good at learning complex patterns and relationships from huge amounts of data. Hybrid models integrate control theory and data analysis advantages and can perform a complete network behavior analysis.

Hybrid models employ the layered approach, where machine learning is used in the early stage work, e.g., feature extraction, anomaly detection, and deep understanding for the deeper work. This structure enables greater accuracy because the first machine learning step can remove unwanted data and concentrate on a feature. In contrast, the second step, deep learning, can analyze features in greater detail. The benefits of this integration are manifold: In comparison, hybrid models achieve higher detection rates and greater versatility to handle different kinds of data. At the same time, reducing false positives, leading to a higher degree of reliability of the intrusion detection system.

5.6. Examples and Case Studies

We show hybrid models to be effective in several practical IoT applications. A hybrid system combining K-means clustering for initial anomaly detection in detecting unusual network traffic patterns that are finally analyzed through a deep learning-based autoencoder. This improves the detection of abnormal activities while minimizing false alarms.

In industrial IoT security, a hybrid model could run random forests over network data to show preliminary classification and then proceed with a convolutional neural network (CNN) to detect more complex cyber attack patterns. The result is increased accuracy in identifying advanced persistent threats (APTs) in critical infrastructure, enhancing protection for sensitive systems.

One case study using a hybrid IDS, combining a support vector machine for feature reduction and a recurrent neural network (RNN) for temporal network traffic analysis, stood out. We adapted the hybrid model to the changing nature of threats and achieved high accuracy in detecting known and unknown attacks.

The hybrid models can help IoT networks strike a balance between computational efficiency and detection accuracy, addressing the problem of modern cyber threats with comprehensive security. These same models will be needed to improve the resilience of IoT systems, enabling detection and response to new and existing threats as cybersecurity continues to change. Machine learning and deep learning techniques are integrated. Besides increasing intrusion detection accuracy, they help create a self-evolving (called) adaptive security environment that can constantly adapt to new (in this case, sophisticated) cyber attackers.

6. Implementation strategies

Implementing intrusion detection systems (IDS) in Internet of Things (IoT) networks is difficult and involves strategic planning to achieve the best possible performance in a resource-constrained situation. Two primary deployment strategies are often considered: edge computing and based cloud solutions. Each approach has pros and cons, and an organization needs to consider its specific needs and environment when deciding on a strategy.

6.1. Deployment Scenarios

Edge Computing is where data processing is done closer to the source, like on IoT devices or local gateways instead of among centralized servers. One of the benefits of this approach is. Secondly, it greatly reduces latency, facilitating rapid detection and response to potential threats, which is important in security.

6.2. Alternative Response

It greatly reduces latency, so you can detect and respond to threats much more quickly, which is important in security. Furthermore, edge computing limits privacy by 'keeping sensitive data near the point of where it will be used,' securing it from eventual exposure by avoiding transmission. In addition, it optimizes bandwidth since it sends less data to a central server, saving network resources.

Now, edge computing sits uneasily with these very policies, however. The computational power and storage found in many IoT devices limit the complexity and sophistication of the deployed intrusion detection models. In addition, managing and maintaining a distributed network of edge devices can bring its share of complexities, e.g., updates and security patches, but this is another story.

However, cloud-based solutions concentrate on processing and analyzing data in the cloud servers. This model scales allows you to manage large amounts of data and quickly scale resources as needed. Traditional intrusion detection systems (IDSs) are deployed in a hub and spoke model, often requiring IDS agents to be deployed where sensors (such as desktop monitors, firewalls, routers, etc.) are located, originally to minimize the network bandwidth consumed by detected network packets and flows. Moreover, since central management is involved in updating and maintaining the IDS, the updating procedure becomes simpler, and it can also be manually rolled out from a single place.

Cloud-based solutions come with their own set of disadvantages. However, transmitting data to and from the cloud adds latency that might not be acceptable for real-time threat detection. Also, sending sensitive information might be tied to privacy concerns, as sending sensitive information to the cloud might lead to security risks. Furthermore, continuous data transmission often results in high bandwidth consumption, which could strain network resources and is particularly relevant in cases where many IoT devices are densely packed together.

6.3. Trade-offs Between Performance and Resource Usage

Many factors balance performance vs. resource usage. Comparisons are made based on performance considerations in each approach. The low latency processing capabilities of edge computing make it more suitable for real-time detection and, as such, more opt for critical applications requiring immediate response. However, for analyzing complex data that demands a lot of computing power, cloud solutions present themselves as an advantage that enables deeper insight and more complicated threat detection methods.

From the resource usage point of view, edge computing is highly efficient regarding bandwidth. It can provide real-time processing on-site but is limited by the hardware specifications of each device. While cloud solutions offer plenty of processing resources and capabilities, they come with much more bandwidth demands, and data transmission can be delayed.

With edge and cloud solutions for IoT, organizations will need to Figureure out if the requirements of their specific IoT network call for more edge or more cloud proportions. Considering this, they need to analyze the types of devices they use, the nature of the data fed for processing, and the importance of real-time detection of the applications. However, in many cases, the best solution might be a hybrid one combining edge and cloud computing. By taking this approach, organizations can utilize the strong points of each deployment model and use them in unison to achieve maximum performance at minimal resource utilization. Through judicious application of (both) of these approaches, it is possible to develop an intrusion detection system in IoT environments capable of adapting to the needs of the various applications it must support.

6.4. Optimization Techniques

The requirement for optimizing AI models for intrusion detection systems (IDS) in Internet of Things (IoT) networks stems from the need to improve efficiency and performance in IoT networks, particularly since many IoT devices are limited in resources. However, as these networks continue to grow and change, it is increasingly important for security measures to be put in place not to overwhelm the systems they are meant to protect. However, this balance can be achieved through several important optimization strategies that decrease model complexity and increase computational efficiency.

6.4.1. Reducing Model Complexity

Reducing model complexity is one of the main ways for optimization. It means lighter AI models, meaning the least resources and maintaining the same performance.

Model Pruning: Model Pruning is a technique that removes redundant or less significant neurons and connections in a neural network. In addition to shrinking the model's size, this process lowers the computational load, permitting its utilization on resource-constrained devices with no loss of accuracy.

Quantization: Another effective tactic here is Quantization, in which we reduce the number of bits needed to represent the weights and activities of the model. Quantization simplifies the numerical representation and allows smaller models to require less memory and computational power consumption, making them more attractive for low-resource setups.

Knowledge Distillation: Knowledge Distillation is a method to train a smaller, simpler network (called a student network) to mimic the behavior of a larger, complex network (called a teacher network). It is demonstrated that such a student model can achieve accuracy comparable to the teacher at the cost of being more efficient to run, making this a practical choice for IoT applications.

Feature Selection: Feature Selection is important because not all the features are relevant; instead, using only the most pertinent features reduces the model's complexity drastically. This helps speed up the training and inference times and helps to make a model more interpretable, which makes the system understand and trust the system decisions easily.

6.4.2. Efficient Computation Techniques

Other than complexity reduction, techniques for efficient computing are equally important in optimizing AI models in IDS.

Batch processing: Processing multiple data instances in parallel rather than on one by one basis. If the approach works, it will make the system more responsive and reduce the processing time since it will greatly improve computational efficiency.

Parallel and Distributed Computing: Parallel and Distributed Computing uses multiple processors or systems to solve a problem. It can also speed up model training and inference, especially in the case of large datasets, thus improving the whole system's performance.

Hardware Acceleration: Hardware Acceleration is just making use of specialized hardware (Graphics Processing Units (GPUs), Tensor Processing Units (TPUs)) that is equipped to do the matrix operations required for neural networks much more quickly than CPUs. This can be a huge performance booster for training and inference.

Edge Computing: Edge Computing is a method of processing data near its source, avoiding sending enormous amounts of data to centralized servers. Moreover, this approach saves bandwidth, minimizes latency, and responds faster to potential threats.

6.5. Adaptive Algorithms

These Algorithms change complexity according to the amount of Resources available or the specialization of a particular task. For instance, if computational means are limited, simpler models can ensure that the IDS remains functional and effective under whatever condition. This work aids the development of AI models for intrusion detection in IoT networks, enabling them to strike an efficient balance between their performance and resource usage by applying the optimization techniques discussed. This guarantees that sensible system security measures are set up without overwhelming the gadgets, finally bringing about additionally steady and proficient IoT frameworks. However, as the complexity of the environments in which we insert our systems grows, these optimizations should also be required to keep effective intrusion detection capabilities in the increasingly hostile cyber threat landscape.

7. Case studies

To illustrate the practical application of AI in intrusion detection, we will explore three distinct case studies from various sectors: a financial institution, a healthcare provider, and an e-commerce platform. The unique challenges encountered by each organization are revealed within each case study and how AI-infused intrusion detection systems resolved them.

7.1. Case Study 1: Large Financial Institution

7.1.1. Background

Increasingly, a multinational bank with over 50 million customers in 40 countries was becoming more vulnerable to cybersecurity threats. The sheer number and sophistication of attacks and the bank's reliance on traditional intrusion detection methods needed improvement. It lacked the foundation to detect false positives and failed to notice actual threats.

7.1.2. Challenges

The bank faced harsh challenges, such as over 10 million daily transactions, government-enforced rules, and highly developed attacks, particularly from state backers. On top of that, enemy agents needed real-time threat detection and response to protect customer data and retain customer trust.

7.1.3. AI Solution Implemented

Addressing these challenges, the bank implemented a multi-layered AI intrusion detection system using supervised and unsupervised learning methods. An autoencoder neural network was trained to detect normal transaction patterns and flag any real-time deviations via an anomaly detection mechanism. However, these anomalies were categorized into threat types through a Random Forest classifier at greater granularity. In addition, Long Short Term Memory (LSTM) networks were used to analyze the sequence of users' actions to help catch potential account takeover attempts. An ensemble approach, which used the output of several input models to generate improved accuracy, also enhanced the final decision-making process.

7.1.4. Implementation Process

From the implementation, qualitative data was collected from transaction logs, user authentication events, and network traffic to complete the overview. Preprocessing was then done meticulously to pristine via cleaning, normalization, and feature engineering so that the data was ready for AI models to ingest in revealing inputs. Historical data were fed into the models, including known attack patterns and normal user behavior, and it was trained. The transition needed to be

fully integrated with the existing Security Information and Event Management (SIEM) system and the security operations center (SOC). It was designed to learn and adapt itself—or, in other words, continuously learn based on feedback from security analysts so that the system remained effective over time.

7.1.5. Results

The results from this AI-driven approach were enormous. The bank achieved exceptional results with an 85% false positive reduction and a 92% increase in detection of newly introduced unknown threats. Moreover, there was a 60% response time increase in incidents, allowing the bank to detect and stop an APT attack never detected by conventional security methods.

7.1.6. Key Metrics

The effectiveness of the AI solution was reflected in key metrics: When the classifier begins with a random reduction, the false positive rate drops from 15% to 2.3%, and the true positive rate increases from 78% to 94%. In addition, the Mean Time to Detect (MTTD) was decreased from six hours to 15 minutes, and the Mean Time to Respond (MTTR) improved from four hours to 45 minutes.

7.1.7. Lessons Learned

This case underscored several important lessons: Acquiring high-quality, diverse training data to improve model performance was necessary, explainable AI models were needed to satisfy regulatory requirements, and combining multiple AI techniques resulted in a more robust detection system. Other companies seeking to boost their cybersecurity using AI may find these insights useful.

7.2. Case Study 2: Healthcare Provider

7.2.1. Background

The target is a large healthcare provider network, consisting of 20 hospitals and over 100 clinics, that was under assault by an increasingly hostile attack landscape of ransomware attacks and attempts to steal data on patients. Due to the pressing requirement to increase intrusion detection, it was imperative to maintain the HIPAA regulations, as there was a need to comply with respectable privacy and security in the patient's records.

7.2.2. Challenges

There were several significant challenges that the healthcare provider had. Its IT infrastructure was spread out and quite varied, and the implementation of a unified approach to security took a lot of work. Because patient data was sensitive, any breach could have significantly impacted patient privacy and organizational trust. Furthermore, the provider needed to operate the system at high availability to support continuous patient care while working under a constrained cybersecurity budget and with limited expertise in advanced security technologies.

7.2.3. AI Solution Implemented

In response to these challenges, the healthcare provider developed an AI intrusion detection system adapted to its needs. Using a combined convolutional neural network and Long Short-Term Memory (LSTM) models, this system leveraged network behavior analysis to analyze network traffic patterns and detect anomalies associated with potential threats. An ensemble of Random Forest and gradient-boosting classifiers were used to improve the detection of unusual user behavior for insider threats and compromised accounts. In addition, a deep learning model based on CNNs was implemented to analyze file behaviors and then utilized to recognize file behaviors, which can be considered potential malware, including zero-day threats undetectable by conventional detection methods.

7.2.4. Implementation Process

The implementation process started with data collection from various sources, including network logs, endpoint telemetry, and access control mechanisms. Data anonymization and encryption techniques were used to comply with HIPAA regulations and create privacy-preserving techniques while training and operating AI models. Federated learning was also used to train models on different hospitals' data without centralizing sensitive patient data, reducing privacy risk. The AI system was integrated into existing security tools and workflows to increase overall optimization and provide several training sessions on integrated actresses for the IT and security staff.

7.2.5. Results

The initiative's results were significant and encouraging. As a result, the healthcare provider reduced its undetected security incidents by 70% and decreased the time to detect initial security alerts by an amazing 95%. During the system's first six months of deployment, it successfully blocked two ransomware attacks, proving itself in practice. In addition, compliance with HIPAA security requirements was enhanced, prioritizing the protection of patient data.

7.2.6. Key Metrics

Key performance indicators reflected the success of the AI implementation: These results show that detection accuracy increased from 82% to 96% while the false alarm rate decreased dramatically from 20% to 3%. Alerts were triaged in 5 minutes—down from an average of 45 minutes and 90% fewer instances of data exfiltration.

7.2.7. Lessons Learned

We highlighted several key healthcare lessons from this case. We started by indicating the need for privacy-preserving AI techniques to ensure patient data remains protected while allowing access to advanced analytics. Adapting constantly to the ever-changing threat landscape is essential, and this can only happen by continuously updating the AI models. Lastly, the execution highlighted the utility of AI to serve as a means to add limited human resources to alleviate the need for more specialization in cybersecurity teams that are grappling with an increasingly dynamic volume of threats.

7.3. Case Study 3: E-commerce Platform

7.3.1. Background

As an e-commerce platform with over 50 million active users, the attack landscape against our site became increasingly challenging, marked by multiple sophisticated cyber attacks simultaneously. It consisted of account takeovers, payment fraud, and Distributed Denial of Service (DDoS) attacks. The company realized that it urgently needed to improve its intrusion detection capability to safeguard its infrastructure and customer trust.

7.3.2. Challenges

E-commerce platforms faced several formidable challenges. The velocity and sheer volume of user transactions made it easier for suspicion of activity to go unnoticed. At the same time, the platform was based on a microservices architecture, which complicated its security measures even more. The security buckeye grew more complex with frequent code deployments and infrastructure changes. In addition, the various attack vectors present against the platform itself and its users called for a solid and flexible security solution.

7.3.3. AI Solution Implemented

The e-commerce platform developed a full-fledged AI-powered full-fledged AI-powered intrusion detection system to handle these issues. Based on independently developed autoencoders and Isolation Forest anomaly detection in a real-time system, this system monitored user behavior and transaction patterns for abnormalities. A combination of Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) was applied for traffic analysis on network traffic, and API calls were altogether analyzed to detect possible DDoS attacks and API abuse. Finally, a Graph Neural Network (GNN) was presented, which explores relationships among users, transactions, and IP addresses to detect complex fraud patterns and help the intelligent system Figureht fraud. Besides, a dynamic security policy adapting mechanism based on reinforcement learning was also proposed to adaptively change the security policies according to the ever-changing threat landscape.

7.3.4. Implementation Process

The implementation process should start with a strong data pipeline and process lots of data in real time. Domain-specific features were invented to express nuances in user behavior, transaction characteristics, and network patterns, which were instrumental in learning through feature engineering. We iterated AI models through A/B testing methodologies to get better and better. Thus, the chosen system's architecture was distributed and cloud-based, efficiently and effectively serving the users with large amounts of incoming requests. A system for continuous monitoring and automated alerting of model performance drift over time was established.

7.3.5. Results

The results of this AI project were excellent. The platform has succeeded with 99.9% reduced successful account takeover attempts and 80% reduced fraudulent transactions. Furthermore, downtime due to DDoS attacks was cut in half by 95%, massively improving the platform's reliability—additionally, the implementation improved user experience, smoother transactions, and higher customer satisfaction.

7.3.6. Key Metrics

Key performance metrics demonstrated the effectiveness of the AI system: Fraud detection accuracy improved from 90% to near-perfect 98%, and the account takeover detection rate increased from 75% to 99.5%. The system also performed efficiently, helping to decrease the time to mitigate DDoS attacks from 15 minutes to 30 seconds. Moreover, the fraud detection false positive rate dropped from 5% to 0.5%.

7.3.7. Lessons Learned

Several important lessons for e-commerce environments were demonstrated with this case study. Secondly, it brought forth the need for real-time processing capabilities because detecting and responding to cyber threats in a reasonable time is of utmost importance in eradicating them. It highlighted that graph-based AI models are an effective tool for uncovering complex, interconnected fraud patterns. It was also recognized that the current AI models need the ability to explain themselves, assist in fraud investigations, and increase user trust through transparency.

These case studies demonstrate the disruptive power of AI for data mining in intrusion detection across industry sectors.

8. Future directions

8.1. Emerging Technologies

8.1.1. Federated Learning and Reinforcement Learning.

Federated learning is touted as a promising approach to improving IoT network security. It permits several devices to collaboratively find a typical mannequin while preserving the native information, which might be essential for privateness and effectiveness in a skewed atmosphere. This approach minimizes the risk of a data breach, and confidential information never leaves the local device. However, reinforcement learning provides important potential for dynamic adaptation to constantly changing threats. Continuous interaction with the environment can allow IoT systems to learn optimal defense strategies over time, improving the system's resilience to evolving cyber threats.

8.1.2. Enhancing Security Through Blockchain

The promise blockchain technology can bring to enforce enhanced IoT security lies in the decentralized and tamper-proof ledger it supplies. This serves as a means to ensure data integrity and transparency so that information is incredibly hard to change without detection. On the other hand, when using blockchain, IoT devices can safely log transactions and communications between devices to allow for reliable communications. Also, this technology can assist with secure identity management and access control to reduce the chances of unauthorized authentication in IoT networks.

8.2. Research Gaps

8.2.1. Areas Requiring Further Investigation

However, the potential for AI-enabled IDS to exploit the Internet of Things remains underutilized, as many areas still need to be fully explored. Another primary focus is the creation of lightweight AI algorithms that will function on what are typically computationally sparse embedded devices. Markedly, there is a demand for more complete datasets that can accurately map the diversity present in IoT environments to support model training and evaluations. Additionally, research is needed to improve the interpretability of AI models to aid understanding and trust in AI-driven decision-making.

8.2.2. Long-term Challenges and Opportunities

In the long term, integrating AIAI-enabledDS into IoT networks will require the management of high device heterogeneity and interoperability of IoT devices with different systems. The opportunities for achieving more robust

and adaptive security frameworks will be opened by addressing these challenges. Additionally, continuous improvement in AI and computing technologies allows for the possibility of more efficient and scalable security solutions. Overcoming these challenges is critical for the industry to bring security and reliability improvements to IoT networks, making them more broad in their adoption and ability for innovation.

9. Conclusion

9.1. Summary of Key Findings

Intrusion Detection Systems (IDS) equipped with AI represent a big step towards securing IoT networks. Traditional methods don't change, but such methods can adapt to evolving cyber threats and enhance threat detection accuracy. Nevertheless, the application of such systems still needs to be improved by challenges, one of them being its deployment on resource-constrained devices. When implementing the techniques, careful consideration must be given to limited processing power, memory, and energy efficiency.

9.2. Implications for the Future

This is where IoT security is going to change with the power of the AI-enabled IDSs. If they offer more robust, adaptive defenses, they can greatly reduce vulnerabilities in an IoT network and build more trust in IoT technologies and adoption. The focus for researchers is to develop lightweight and efficient AI models that are geared to work in IoT environments. It should be required from practitioners to integrate these systems into IoT infrastructure with assured interoperability and scalability. It will also help us address security challenges and prepare for future threats.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Dam, S. (2023, November 06). Significance of AI in Intrusion Detection Systems. AZoAi. Retrieved November 01, 2024, from https://www.azoai.com/article/Significance-of-AI-in-Intrusion-Detection-Systems.aspx

[2] Ahmad Z, Shahid Khan A, Wai Shiang C, Abdullah J, Ahmad F (2021) Network intrusion detection system: a systematic study of machine learning and deep learning approaches. Trans Emerg Telecommun Technol 32:e4150

[3] Heidari A, Navimipour NJ, Unal M (2023) A secure intrusion detection platform using blockchain and radial basis function neural networks for internet of drones. IEEE Internet Things J. 10:8445–54

[4] Chkirbene Z, Erbad A, Hamila R, Mohamed A, Guizani M, Hamdi M (2020) Tidcs: A dynamic intrusion detection and classification system based feature selection. IEEE Access 8:95864–95877

[5] Junwon K, Jiho S, Ki-Woong P, Jung TS (2022) "Improving Method of Anomaly Detection Performance for Industrial IoT Environment". Computers, Materials & Continua. 72(3):5377–94. https://doi.org/10.32604/cmc.2022.026619.

[6] Katyal, Kamaldeep & Dutta, Maitreyee & Granjal, Jorge. (2020). Towards a Secure Internet of Things: A Comprehensive Study of Second Line Defense Mechanisms. IEEE Access. 8. 1-1. 10.1109/ACCESS.2020.3005643.

[7] Alturfi, Sabah & Kadhim, Dena & Mohammed, Mohammed & Aziz, Israa & Aljshamee, Mustafa. (2021). A Combination Techniques of Intrusion Prevention and Detection for Cloud Computing. Journal of Physics: Conference Series. 1804. 012121. 10.1088/1742-6596/1804/1/012121.

[8] Halbouni A, Gunawan TS, Habaebi MH, Halbouni M, Kartiwi M, Ahmad R (2022) Cnn-lstm: hybrid deep neural network for network intrusion detection system. IEEE Access 10:99837–99849

[9] Molina-Coronado B, Mori U, Mendiburu A, Miguel-Alonso J (2020) Survey of network intrusion detection methods from the perspective of the knowledge discovery in databases process. IEEE Trans Netw Serv Manag 17(4):2451–2479

[10] Heidari A, Jafari Navimipour N, Unal M, Zhang G (2023) Machine learning applications in internet-of-drones: Systematic review, recent deployments, and open issues. ACM Comput Surv 55(12):1–45

[11] Bukhari SMS, Zafar MH, Abou Houran M, Moosavi SKR, Mansoor M, Muaaz M, Sanfilippo F (2024) Secure and privacy-preserving intrusion detection in wireless sensor networks: Federated learning with scnn-bi-lstm for enhanced reliability. Ad Hoc Netw 155(103):407

[12] Hanafi AV, Ghaffari A, Rezaei H, Valipour A, Arasteh B (2024) Intrusion detection in internet of things using improved binary golden jackal optimization algorithm and lstm. Clust Comput 27(3):2673–2690

[13] Belouch M, hadaj SE (2017) Comparison of ensemble learning methods applied to network intrusion detection. ACM, pp 1–4

[14] Wu P (2020) Deep learning for network intrusion detection: Attack recognition with computational intelligence. PhD thesis, UNSW Sydney

[15] Quinlan JR (2014) C4. 5: programs for machine learning. Elsevier

[16] Cristianini N, Shawe-Taylor J (2000) An introduction to support vector machines and other kernel-based learning methods. Cambridge University Press

[17] Vashishtha LK, Singh AP, Chatterjee K (2023) Hidm: A hybrid intrusion detection model for cloud based systems. Wirel Pers Commun 128:2637–2666

[18] Hnamte V, Nhung-Nguyen H, Hussain J, Hwa-Kim Y (2023) A novel two-stage deep learning model for network intrusion detection: Lstm-ae. IEEE Access

[19] Talukder MA, Hasan KF, Islam MM, Uddin MA, Akhter A, Yousuf MA, Alharbi F, Moni MA (2023) A dependable hybrid machine learning model for network intrusion detection. J Inf Secur Appl 72:103405

[20] Kumar, J.S.; Patel, D.R. A survey on internet of things: Security and privacy issues. Int. J. Comput. Appl. 2014,90, 100312.

[21] Yadav, T.; Rao, A.M. Technical aspects of cyber kill chain. In Proceedings of the International Symposium on Security inComputing and Communication, Kochi, India, 10–13 August 2015; pp. 438–452.

[22] Wang, W.; Xia, F.; Nie, H.; Chen, Z.; Gong, Z.; Kong, X.; Wei, W. Vehicle Trajectory Clustering Based on Dynamic RepresentationLearning of Internet of Vehicles. IEEE Trans. Intell. Transp. Syst. 2020.

[23] Wang, W.; Chen, J.; Wang, J.; Chen, J.; Gong, Z. Geography-aware inductive matrix completion for personalized Point-of-Interestrecommendation in smart cities. IEEE Internet Things J. 2019,7, 4361–4370.

[24] Wang, W.; Chen, J.; Wang, J.; Chen, J.; Liu, J.; Gong, Z. Trust-Enhanced Collaborative Filtering for Personalized Point of InterestsRecommendation. IEEE Trans. Ind. Inf. 2020,16, 6124–6132.

[25] Chahid, Y.; Benabdellah, M.; Azizi, A. Internet of things security. In Proceedings of the 2017 International Conference on WirelessTechnologies, Embedded and Intelligent Systems (WITS), Fez, Morocco, 19–20 April 2017; pp. 1–6.

[26] Patil, S., Varadarajan, V., Mazhar, S. M., Sahibzada, A., Ahmed, N., Sinha, O., Kumar, S., Shaw, K., Kotecha, K. (2021). Explainable Artificial Intelligence for Intrusion Detection System. Electronics, 11(19), 3079. https://doi.org/10.3390/electronics11193079

[27] Park, C., Lee, J., Kim, Y., Park, J. –G., Kim, H., Hong, D. (2023). An Enhanced AI-Based Network Intrusion Detection System Using Generative Adversarial Networks. IEEE Internet of Things Journal, 10, 3, 2330-2345. https://doi.org/10.1109/JIOT.2022.3211346.

[28] Sowmya, T., Mary Anita, E. (2023). A comprehensive review of AI-based intrusion detection system. Measurement: Sensors, 28, 100827. https://doi.org/10.1016/j.measen.2023.100827

[29] Dias, F. S., & Peters, G. W. (2020). A non-parametric test and predictive model for signed path dependence. Computational Economics, 56(2), 461-498.