AI-Driven Threat Detection in the Internet of Things (IoT), Exploring Opportunities and Vulnerabilities

Article *in* International Journal of Research Publication and Reviews · November 2024

2 authors, including:

Chris Gilbert
William V. S. Tubman University
29 PUBLICATIONS **321** CITATIONS

SEE PROFILE

WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

AI-Driven Threat Detection in the Internet of Things (IoT), Exploring Opportunities and Vulnerabilities.

[1]Chris Gilbert, [2]Mercy Abiola Gilbert

[1]Professor [2]Instructor

[1]Department of Computer Science and Engineering/College of Engineering and Technology/ William V.S. Tubman University/chrisgilbertp@gmail.com/cabilimi@tubmanu.edu.lr

[2]Department of Guidance and Counseling/College of Education/William V.S. Tubman University/mercyabiola92@gmail.com/ moke@tubmanu.edu.lr

ABSTRACT

The rapid proliferation of the Internet of Things (IoT) has introduced significant security challenges due to the increasing number of connected devices and the complexity of their architectures. This paper explores the role of Artificial Intelligence (AI) in enhancing IoT security through advanced threat detection methodologies. AI-driven techniques, such as machine learning (ML) and deep learning (DL), provide promising solutions for detecting anomalies, mitigating attacks, and managing cyber risks in real-time IoT environments. By leveraging both supervised and unsupervised learning models, the study highlights the potential of AI to identify and counter both known and unknown threats in IoT networks. Reinforcement learning is also examined as a strategy for adaptive security solutions in dynamic IoT ecosystems. Additionally, blockchain technology is employed to verify communication authenticity and safeguard data integrity across IoT devices. The research discusses case studies, such as smart home and industrial IoT setups, and presents an AI-powered framework for securing critical IoT infrastructures. The paper concludes with a call for further exploration of distributed AI-based threat detection architectures and highlights the importance of privacy and security in the future development of AI-driven IoT systems.

Keywords: *AI-driven threat detection, Internet of Things (IoT), machine learning (ML), deep learning (DL), cybersecurity, anomaly detection, supervised learning, unsupervised learning, reinforcement learning, blockchain technology, IoT security, AIoT, cyber-physical systems (CPS), edge computing, privacy, data integrity, AI in IoT.*

1. Introduction

Addressing vulnerabilities in the Internet of Things (IoT) requires developing security measures that can operate effectively within the trust levels of IoT sensors, while also working seamlessly with other components like network topology, smart devices, and processing systems. One challenge is figuring out how to identify IoT devices over multiple interactions, recognize what type of device it is, and link it to its MAC address without needing to alter the hardware. Typically, this kind of problem is handled using learning frameworks, but solving it could revolutionize how MAC architectures manage cyber-physical systems.

The rapid growth of wireless sensor devices has fueled the rise of the IoT revolution, with applications ranging from smart homes to critical infrastructure. However, the wide variety of these devices has introduced new security challenges (Opoku-Mensah et al, 2015). Different protocols, such as those for IPv4 and IPv6, and both older and newer security protocols are used to protect the traffic and devices. This variety makes it difficult to apply a universal security model. As machines and devices in IoT networks increasingly work together, trust issues with sensors can become unclear, complicating strategies to mitigate risks. This has led IoT systems to adopt encryption for communication, databases, and sensors, though this approach still leaves database management systems (DBMS) vulnerable to breaches, even though DBMS and IoT systems are two of the most widely used components in sensor networks.

1.1. Background and Significance

Artificial intelligence (AI) has garnered a lot of attention, especially for its potential to transform various industries, including the Industrial Internet of Things (IIoT). The combination of AI and IoT, often referred to as AIoT, has recently gained significant traction as a driving force behind technological advancements in industrial sectors(Bibri et al., 2024; Gilbert & Gilbert, 2024b). However, securing AIoT systems, especially when it comes to privacy and data integrity, remains a key concern (Aslam, Qureshi & Newe, 2024; Gilbert & Gilbert, 2024i; Rupanetti & Kaabouch, 2024). AI technologies are often vulnerable to cybersecurity threats, such as cloning or imitation of algorithms and software, which can lead to breaches of sensor control data privacy, impacting the effectiveness of industrial systems (Gilbert & Gilbert, 2024c).

AI has been widely used to improve IoT infrastructure by enhancing analytics and automating processes. Today, AI is also being paired with data science to automate data analysis, uncover hidden patterns, and reduce the need for human intervention. These advances help monitor and optimize plant operations, reducing machine failures, repair times, and improving overall productivity. As a result, industries that rely on smart, autonomous systems are placing more trust in networked operations compared to traditional systems, as this new era of IoT continues to evolve (Alterazi et al., 2022).

IoT technology has found applications across a range of industries, including healthcare, agriculture, supply chains, home automation, and industrial automation. As the number of IoT devices increases, they are now commonly used in smart homes, factories, vehicles, and other key infrastructure. IoT has become the foundation of digital transformation, significantly impacting the industrial sector. Industrial automation through IoT (IIoT) improves traditional methods by reducing machine downtime, minimizing errors, and boosting productivity. Previously, industries relied on massive systems like SCADA for data collection, which were slow and costly. In contrast, IIoT provides more reliable, scalable, and real-time data collection solutions, though challenges remain in areas such as reliability, connectivity, and information security (Christopher, 2013; Alabadi, Habbal & Wei, 2022).

The concept of the Cloud of Things (CoT) has emerged as a solution to overcome the current challenges of IIoT. CoT refers to a model that offers the computational and storage resources necessary to make IoT applications more reliable and manageable. Nevertheless, security remains a top concern in the IIoT landscape (Yeboah, Odabi & Abilimi Odabi, 2016; Fadel et al., 2022; Kumar Pandey et al., 2023).

1.2. Research Objectives

The integration of AI and IoT, often referred to as AIoT, needs to gain significant momentum to pave the way for future systems that can handle the challenges of infrastructure development, AI and IoT maturity, and efficient distributed innovation (Aljumah, 2021). AIoT will go beyond just technological advancements, evolving into a broader ecosystem that observes interactions and fosters advanced AI interface development.

This report examines the main contributors to cybersecurity risks in AI and IoT, offering an analysis of state-of-the-art studies and recommendations for improving IoT risk detection techniques. It aims to propose new technologies that address current limitations, while also exploring possible scenarios for cooperation between AI and IoT. The goal is to foster resilient AI-IoT compatibility in the coming years (Ali Talib Al-Khazaali & Kurnaz, 2021; Yeboah, Opoku-Mensah & Abilimi, 2013). The research provides a blueprint for AI integration in specialized environments and focuses on AI security, addressing both visible and emerging challenges.

One of the major problems with IoT technologies is their reliance on complex and diverse architectures, along with the increasing number of outdated or orphaned devices and sensors. These factors, combined with largely unsupervised communication between network devices, create a complicated IoT threat landscape (Kumar Sikder et al., 2018; Yeboah, Opoku-Mensah & Abilimi, 2013). This article will explore the current IoT security challenges and threats, addressing two key research questions to better understand this evolving landscape (Opoku-Mensah, Abilimi & Boateng, 2013).

1.3 Research Approach and methods

The research paper uses several important approaches and methods, which include:

Machine Learning (ML) Techniques: The paper applies supervised learning models to identify security threats in IoT systems, focusing on improving accuracy and reducing false positives for detecting both known and unknown threats. Additionally, unsupervised learning techniques, such as clustering and reconstruction-based models, are utilized to detect anomalies without labeled data. Reinforcement learning is also explored to enable real-time decision-making in complex, dynamic environments.

AI-Based Threat Detection: The research investigates AI-powered systems for identifying and mitigating cyberattacks. This includes the use of machine learning algorithms for automating the detection of potential threats, particularly through anomaly detection and intrusion detection systems (IDS) applied to IoT networks using real-world data sets.

Blockchain Technology: Blockchain technology is employed to secure communication within IoT networks by verifying the authenticity of media files (Gilbert & Gilbert, 2024h). This involves embedding metadata into media, ensuring traceability and validating the source to protect against manipulation and unauthorized access (Gilbert & Gilbert, 2024a).

Data Collection and Analysis: The paper focuses on collecting data from IoT devices and using AI algorithms to analyze that data in real-time. This includes monitoring device behavior, detecting anomalies, and securing the network against potential threats using supervised, unsupervised, and reinforcement learning models.

Simulation and Case Studies: Practical applications of AI in IoT security are demonstrated through simulations and real-world case studies. These examples include smart home systems, industrial IoT setups, and smart city applications to highlight how AI can detect and prevent security threats effectively (Opoku-Mensah, Abilimi & Amoako, 2013).

Security Frameworks: The research proposes AI-driven security frameworks designed for IoT devices. These frameworks include lightweight machine learning models that are built to detect intrusions, identify abnormal activities, and manage threats within IoT environments.

Anomaly Detection Models:The paper explores the use of deep learning architectures like convolutional neural networks (CNN) and recurrent neural networks (RNN) to improve the detection of anomalous activities in IoT networks and devices, focusing on abnormalities in network traffic and device behavior.

Ethical and Legal Evaluation: The research evaluates ethical and legal considerations related to the use of AI in IoT, particularly in regard to privacy, data security, and the implications of AI-powered threat detection systems. It also analyzes existing legal frameworks to ensure compliance with data protection and ethical guidelines.

These approaches form the foundation for exploring how AI can enhance IoT security, while also addressing the vulnerabilities that come with the growing reliance on connected devices and networks.

2. IoT Devices: Vulnerabilities and Security Challenges.

In recent years, there has been a significant rise in the adoption of smart, connected devices across the globe. By 2025, it's anticipated that around 41.6 billion IoT devices will be in use, contributing to a market worth USD 1.1 trillion with a compound annual growth rate (CAGR) of 8.9% (Malhotra et al., 2021). Rather than focusing solely on hardware innovations, exploring user preferences and interaction patterns offers opportunities for more personalized cross-platform activities. However, this growth also brings an increased need for new security mechanisms to manage the broader attack surfaces that these devices introduce.

An access control model has been proposed to enforce and regulate device permissions by leveraging communication patterns within trusted networks. Additionally, a predictive access policy management tool has been developed to securely manage permissions using a Machine Learning model based on user interactions and associated patterns (Al-Shaboti et al., 2019).

The Internet of Things (IoT) employs a wide range of technologies, such as sensors, actuators, networking, and cloud computing, to turn previously "dumb" devices into "smart" ones by connecting them to the Internet and enabling intelligent communication. This has allowed the creation of applications in areas like healthcare, smart homes, smart factories, smart cities, and agriculture (Yang et al., 2021).

However, while the benefits of IoT are clear, this paradigm also introduces numerous security vulnerabilities. Compromised IoT devices can be exploited for various attacks, leading to potential data breaches, financial loss, and system malfunctions. Many of these threats stem from weak or insecure access controls, which attackers can exploit to gain unauthorized access to devices on local area networks (LANs) or the Internet. These threats go beyond denial-of-service (DoS) attacks and packet sniffing, as they can also include man-in-the-middle attacks that cause packet delivery failures or system malfunctions.

In addition to these external threats, IoT systems also suffer from internal vulnerabilities, highlighting the need for secure environments to ensure smooth IoT workflows. Strengthening security measures for critical data in IoT—often referred to as "IoT Security"—is vital, as running IoT systems without proper security measures is akin to driving a vehicle with no brakes, inevitably leading to data breaches and financial losses (see figure below).

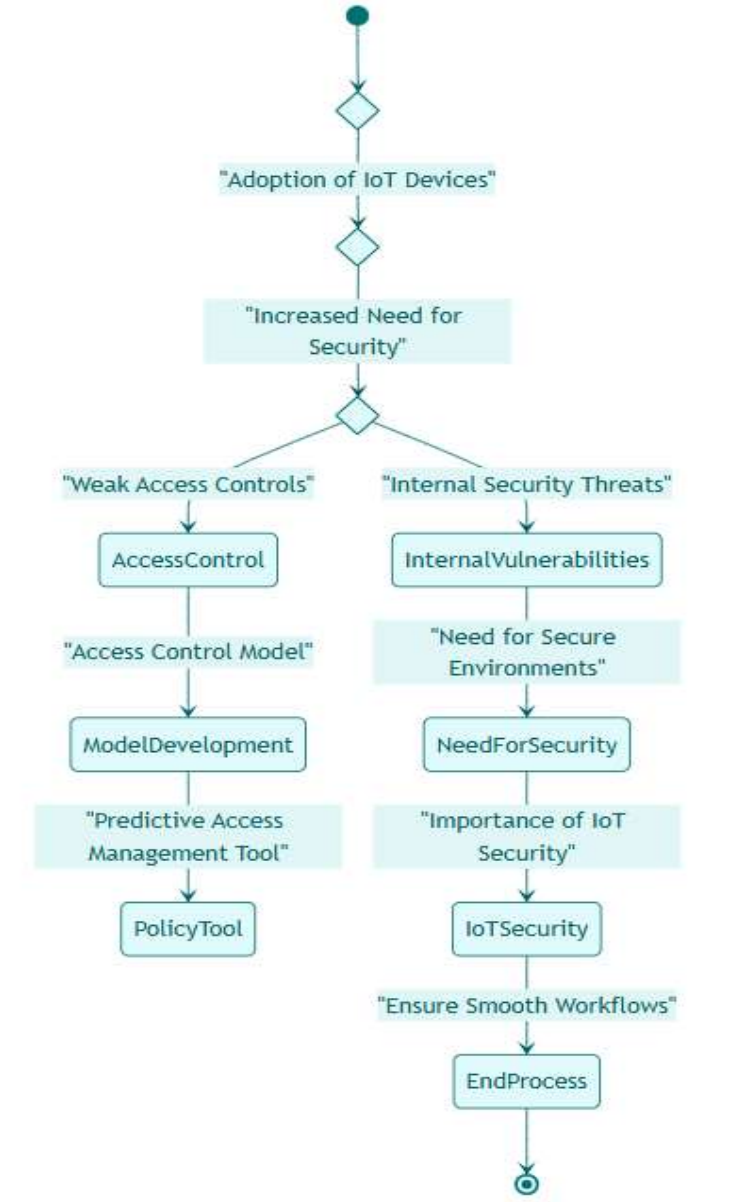

***Figure 1*: IoT Devices vulnerabilities and challenges**

2.1. Overview of IoT Devices

A key feature of IoT devices is their ability to uniquely identify and exchange information with predetermined recipients (Kumar Sikder et al., 2018; Abilimi, Addo & Opoku-Mensah, 2013). Many IoT systems use encryption protocols, such as EPCGlobal (a standard developed by the Auto ID Center), often based on Advanced Encryption Standard (AES) technology, to protect this information. In the case of RFID, a tag (transponder) communicates encrypted data to a reader. However, while this encryption secures the data, it doesn't necessarily guarantee confidentiality, integrity, or availability, especially as wireless communication can still be attacked.

For example, Tapflo's Prosmart, an Industry 4.0 platform, enhances security by connecting systems via high-level protocols, offering resistance against industrial espionage (Kumar Pandey et al., 2023).

The rise of the "smart" paradigm has made technology more pervasive in our daily lives, automating mental and labor-intensive tasks. At the core of this development is the Internet of Things (IoT), which provides unique identification to devices and enables them to communicate autonomously. These devices range from simple motion or temperature sensors to automobiles and industrial machinery, encompassing various technologies such as Radio Frequency Identification (RFID), Near Field Communication (NFC), and micro-electromechanical systems (MEMS).

However, many of these deployed IoT solutions are vulnerable to different types of cyberattacks, underscoring the ongoing need for robust security solutions.

2.2. Common Vulnerabilities in IoT Devices

Many vulnerabilities in the software of IoT devices can undermine the integrity of these systems. Increasingly, these software flaws are at the root of compromises and data breaches. For example, some devices lack proper integrity checks in their secure boot processes, while others leak sensitive data to unauthorized clients. Such vulnerabilities have serious implications, especially in cases where remote attackers can exploit these weaknesses, leading to privacy breaches or enabling attackers to take control of the devices.

One of the major obstacles to securing IoT devices, particularly in military, commercial, and emergency response settings, is the insecurity of the boot process. Many firmware flaws can be exploited to bypass key security mechanisms, even those locked to a secure set of images signed by a trusted key. Attackers with knowledge of these systems can corrupt or modify data, tamper with seed information, and execute rollback or replay attacks, potentially leading to a complete compromise of the device's trusted computing base (Abilimi & Yeboah, 2013). Unauthorized access to device memory has been highlighted in several investigations as a significant security concern. Through forensic analysis of hardware, including firmware inspections and memory dumps, attackers can extract private credentials and sensitive data. This leads to issues such as consumer fraud, mass surveillance, and even unauthorized command execution, allowing attackers to control or manipulate the device.

Common IoT vulnerabilities include physical access to devices, hardware backdoors, and compromised infrastructures. For instance, an attacker who gains physical access to an IoT device can take full control, potentially extracting and modifying the firmware. This is a particular concern for smart home devices that are often left unattended. Another vulnerability arises from the use of insecure default configurations. Many IoT devices still operate with default passwords, unpatched firmware, or hardware backdoors, making them prime targets for remote attacks. Notorious examples include the Mirai botnet and the 2015 revelation of a certified software backdoor in customer premises equipment (CPE) deployed globally.

Network-based attacks are also a significant threat. Attackers often use Man-in-the-Middle (MitM) techniques to intercept unencrypted communications or tamper with data integrity during transmission (Malhotra et al., 2021). These vulnerabilities underscore the importance of strengthening IoT security measures across physical, software, and network layers (see table and figure below).

Table 1

IoT Device Vulnerabilities

Vulnerability	Frequency	Percentage
Insecure Boot Processes	25	25%
Unauthorized Access	21	21%
Data Leakage	17	17%
Insecure Default Configurations	13	13%
Physical Access	13	13%
Network-Based Attacks	8	8%
Firmware Flaws	4	4%

Interpretation of IoT Device Vulnerabilities

The chart on IoT device vulnerabilities categorizes common security risks by frequency of occurrence, highlighting areas where these devices are particularly vulnerable:

i. **Insecure Boot Processes (25%)**: The most frequent vulnerability in IoT devices, insecure boot processes indicate that many devices lack the ability to verify the integrity of their software upon startup, leaving them open to tampering and unauthorized modifications. This gap in security makes it easier for attackers to compromise device functions from the beginning (Fortinet, 2023; Sternum IoT, 2023).

ii. **Unauthorized Access (21%)**: Unauthorized access is the second-most common vulnerability, emphasizing the inadequacy of access controls in many IoT devices. This weakness exposes devices to exploitation, particularly if default credentials or poor authentication methods are in place, making it easier for attackers to bypass basic security (BeyondTrust, 2023; Venafi, 2023).

iii. **Data Leakage (17%)**: IoT devices often process sensitive information but lack adequate protection measures, leading to data leakage vulnerabilities. This can occur if data encryption or secure transmission protocols are not properly implemented, posing privacy and security risks (Sternum IoT, 2023).

iv. **Insecure Default Configurations & Physical Access (13% each)**: These two vulnerabilities are moderately common. Many devices retain insecure default settings out of the box, which can easily be exploited if not changed by the user. Physical access vulnerabilities, on the other hand,

indicate that devices lack sufficient protections against direct tampering or unauthorized access, especially when deployed in public or unsecured areas (Fortinet, 2023; BeyondTrust, 2023).

v. **Network-Based Attacks (8%)**: Though less common than other issues, network-based attacks still pose a risk, particularly if IoT devices communicate over insecure networks or lack protection against interception. This vulnerability is commonly exploited in attacks like man-in-the-middle or denial-of-service (Venafi, 2023).

vi. **Firmware Flaws (4%)**: Firmware flaws are the least prevalent but remain significant, as outdated or insecure firmware can serve as an entry point for attackers. Firmware vulnerabilities are particularly dangerous as they may provide persistent access or be difficult to patch (Fortinet, 2023).

vii. These findings underscore the importance of implementing robust security measures in IoT devices, from secure boot processes to strict access controls and secure configurations.

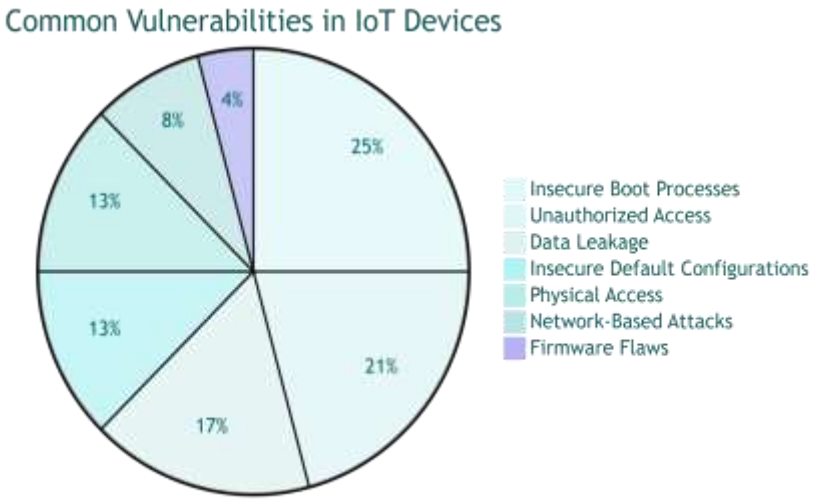

Figure 2:The rate of common vulnerabilities in IoT devices

3. Role of AI in Threat Detection

Machine learning (ML) techniques, especially those using supervised learning algorithms, have proven to be effective in threat detection within IoT networks (Haji & Ameen, 2021). The vast amount of data and its varied nature in IoT environments present significant challenges, including uncertainty, noise, missing data, and complexity. However, these challenges also create opportunities to harness the power of ML algorithms. Over the past few years, ML and AI-specific methods have been increasingly applied to improve security in information systems (Haji & Ameen, 2021; Gilbert, Oluwatosin & Gilbert, 2024; Abilimi & Adu-Manu, 2013). As explained by various researchers, IoT devices that incorporate appropriate technologies can help reduce security vulnerabilities in the IoT landscape. Moreover, ML-based algorithms are both efficient and effective in these environments (Neto et al., 2023).

The application of ML algorithms in detecting congestion or source-based attacks in IoT networks is especially promising. These methods are also useful for verifying the overall security of IoT networks (Neto et al., 2023). IoT networks face a multitude of security challenges due to their complex structure, lack of standardized secure architectures, and limited energy capacity. For instance, efficient feature selection is critical in developing Intrusion Detection Systems (IDS) such as SeN-IDS, which uses a combination of features identified through methods like chi-squared feature selection (KIFS).

Research in this area has explored the use of fixed-model ASIC-based real-time intrusion detection systems for cyber-physical systems (CPS), focusing on detecting and isolating security vulnerabilities. One proposed approach includes using a lightweight permutation-based machine-learning algorithm. Python libraries such as scikit-learn, TensorFlow, and radial basis functions have been employed to design machine learning classifiers. These classifiers have been tested using the mal-detectCNN model, which has demonstrated a high detection rate with low latency.

The diversity in classifier design has enabled the use of clustering predictions before making final intrusion detection decisions, which boosts confidence in the detection rate. In particular, the DWmalCNN model has shown its ability to accurately detect attacks by verifying whether predicted intrusions are real. It has been tested on both synthetic and real-world malware datasets, such as the Mirai and c2-shell types, confirming its effectiveness in distinguishing between true and false attacks in IoT networks (see ***Figure 3***).

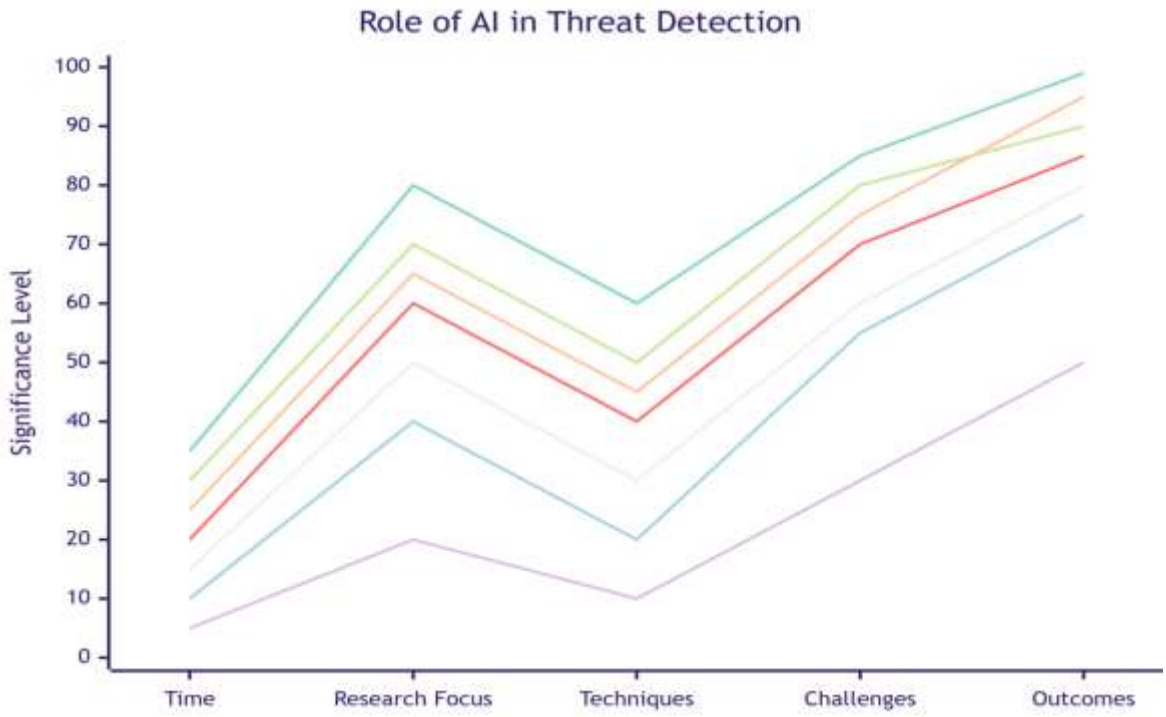

***Figure 3*: Role of AI in thread Detection (George, 2024)**

- There's a big jump in significance from **Time** to **Research Focus**, which suggests that as AI's role has grown, it's also become a major area of study and investment.
- The highest significance score is for **Techniques**, meaning that the specific methods used in AI-powered threat detection are at the heart of its success.
- **Challenges** and **Outcomes** are also high, indicating that while AI is producing valuable results, there are also big obstacles that need addressing.

3.1. Machine Learning and AI in Security

In efforts to reduce the time it takes to detect signal modulations like BaPSK, QPSK, 8PSK, 16QAM, and 64QAM within IoT environments, recurrent deep learning models such as Bidirectional LSTM (Long Short Term Memory), GRU (Gated Recurrent Units), and BLSTM-attention have been employed (Almohamad et al., 2021). These models help improve accuracy in self-learning AI systems used to secure IoT environments. Additionally, to decrease the complexity of MLA-BDL models, dilated convolutional blocks have been incorporated into traditional CNN architectures, creating a hybrid model that outperforms previous approaches, particularly in noise control and industrial protocol detection(Almohamad et al., 2021; Kwame, Martey & Chris, 2017). To further distinguish between signal and noise, models such as Convolutional Wavelet Transform (CWT) and recreated CNNs have been proposed. However, many widely used benchmark datasets—like NSL-KDD, CICIDO, CICIDS2017, KDD'99, ISCX, and AWS—are outdated or have limitations due to privacy concerns, making them less suitable for future security protocol implementations.

Machine learning (ML) and AI are essential for building more accurate analytical models that reduce false alarms in IoT attack and anomaly detection. Various ML techniques are being used to detect intrusions in real time and classify malicious activities. In the context of encrypted traffic, minimizing overhead while identifying the root causes of network events is crucial. To address ML limitations, deep learning (DL) techniques have been introduced and analyzed within IoT security. These include convolutional, recurrent, and attention-based models that enhance detection accuracy. For example, a shallow CNN model has demonstrated high classification accuracy, ranging from 85% to 98%, when identifying normal traffic versus denial-of-service (DoS) attacks (Chen et al., 2022). The figure below illustrate that.

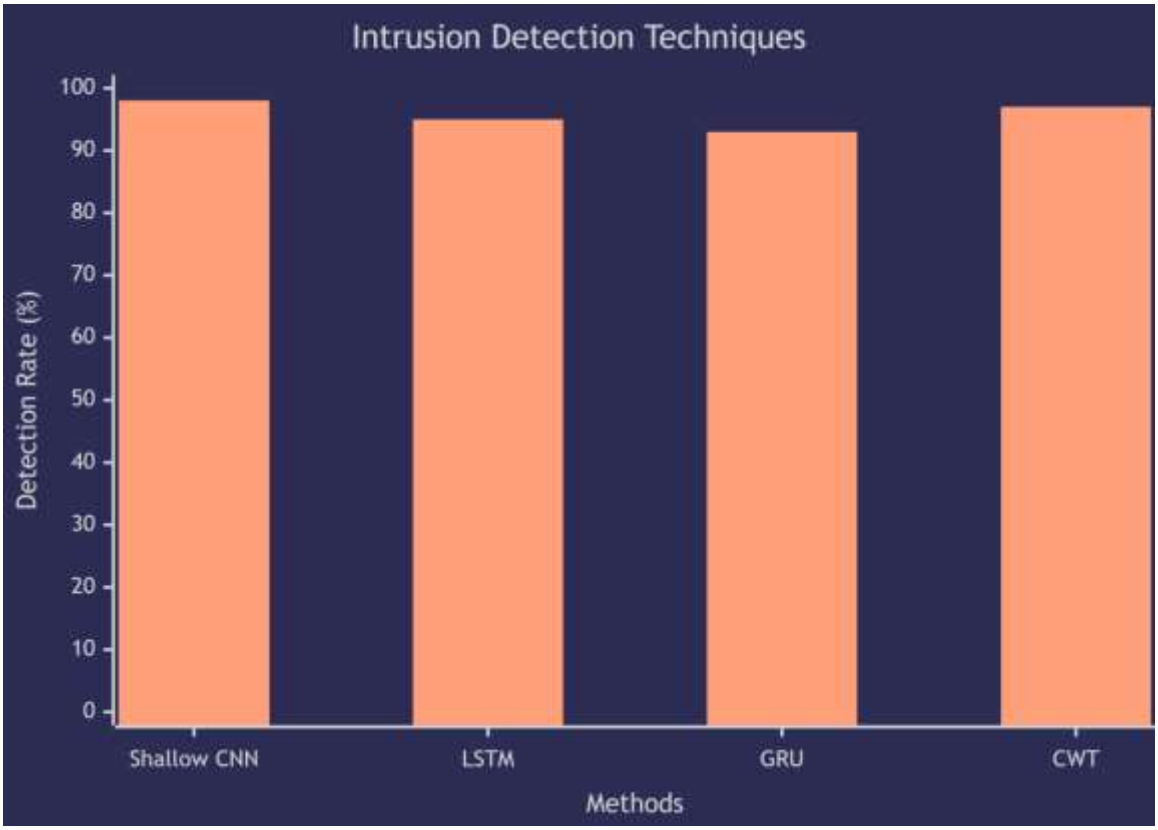

Figure 4:**Instruction detection Technique**

The chart(*Figure 4*) shows a comparison of four intrusion detection techniques: Shallow CNN, LSTM, GRU, and CWT. Each method achieves a high detection rate, nearly reaching 100%, which suggests that all of them are highly effective at identifying intrusions.

3.2. Benefits of AI in Threat Detection

The increasing deployment of connected devices across various regions has heightened the risks posed by cyber attackers, who can now coordinate attacks on millions of unsecured devices. These attackers exploit numerous vulnerabilities through the large-scale deployment of malicious software, enabling them to perform harmful activities like spying on users, creating command channels, or launching distributed denial-of-service (DDoS) attacks. For example, in the Internet of Things (IoT) ecosystem, data generated by the healthcare sector can be highly valuable to hackers, who may sell it on the dark web. To protect IoT devices from such attacks, the two main defense strategies are protection mechanisms and anomaly detection.

Traditional signature-based methods can recognize common attack patterns but are limited to identifying only known threats. They struggle to detect new, previously unseen attacks, which is where artificial intelligence (AI) comes into play(Gilbert & Gilbert, 2024d). There is a pressing need for an autonomous threat detection system capable of analyzing current and historical data to predict future security events. AI excels in making estimates, predictions, and suggestions, making it an ideal tool for developing predictive intrusion detection systems (IDS).

AI algorithms are particularly effective in identifying future trends in cyberattacks and detecting unusual behaviors. With the growing volume of data, traditional techniques are becoming less effective, creating a demand for AI-driven solutions. AI techniques, such as clustering, use various learning strategies—supervised, unsupervised, reinforcement, and semi-supervised learning. By combining these methods, the accuracy and reliability of predictions are enhanced, allowing the system to become more efficient and faster at detecting intrusions, a significant challenge for online intrusion detection systems.

4. AI-Driven Threat Detection Techniques

As previously mentioned, traditional threat detection methods, such as signature-based Intrusion Detection Systems (IDS), are not particularly effective at detecting subtle, complex, or hidden attacks that are common in IoT environments (Aljumah, 2021). Anomaly detection has emerged as a more promising strategy, as it can identify both known and unknown threats by utilizing existing models. In recent years, many machine learning-based techniques have been developed to detect anomalies in IoT data, making it possible to identify unusual activities more accurately and quickly (Hafsa Rafique et al., 2024).

Despite their flexibility and ability to evolve, machine learning-based anomaly detection algorithms still have significant room for improvement. One major challenge lies in dealing with the complexity and high dimensionality of IoT data. More accurate and generalizable tools are needed to effectively detect unknown or zero-day attacks. To strike a balance between complexity and accuracy, recent studies have suggested combining both deep learning and machine learning techniques to enhance results. Several researchers have recommended a hybrid approach for IoT intrusion detection, integrating both deep learning and machine learning algorithms for better performance (Malhotra et al., 2021).

4.1. Supervised Learning

In Figure below, we presented a block diagram outlining our approach to integrating several key system components from the fields of computer architecture, CGRA (Coarse-Grained Reconfigurable Architecture), secure machine learning, and system security into the LDIoT LSI system-on-chip. This design aims to provide lightweight security, intrusion detection, isolation, and adaptive resilience mechanisms (Yeboah & Abilimi, 2013). The innovation in this approach lies in combining various analysis techniques to address cybersecurity challenges from a systems research perspective. Specifically, we are focusing on securing monorail cyberspace, its environment, and monorail cybersecurity systems from the viewpoint of Cyber-Physical Systems (CPS). We have proposed the PRISM framework as a novel lightweight security architecture for ICPTCySy (Integrated Cyber-Physical Transportation Cybersecurity Systems) within the transportation sector.

This work also extends into economic security, aiming to optimize privacy, mobility, and security of lightweight IoT systems integrated on SoC (System-on-Chip) architectures, IoT networks, and blockchain technologies (Gilbert & Gilbert, 2024e).

We validated our empirical research by demonstrating how malicious activities, particularly Type A and Type B abnormal events, could negatively impact IoT cyber-physical systems. We also demonstrated how existing datasets can be expanded for evaluating lightweight machine learning and deep learning models in these contexts. Notably, this study is the first to introduce SDL_IPCL, a new open software architecture designed for lightweight, reliable streaming deep learning intrusion prediction within IoT firmware. SDL_IPCL uniquely demonstrates the potential of using sparse, open-ended deep reinforcement learning for cyber-physical systems, helping to prevent costly security breaches and malicious events (see figure below).

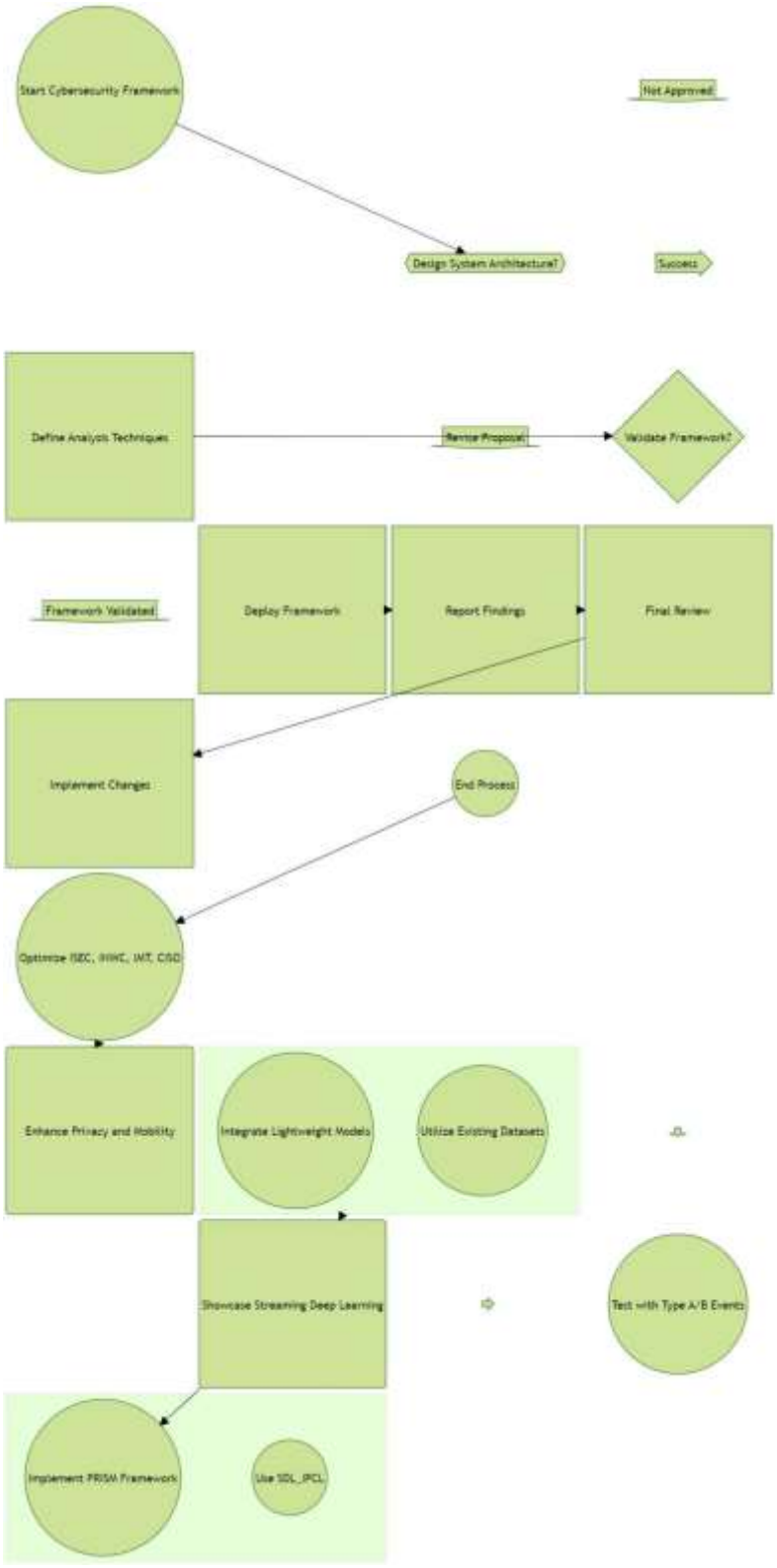

***Figure 5*: Cybersecurity framework for IoT using advanced analysis techniques.**

4.2. Unsupervised Learning

Unsupervised learning is a model that can learn to recognize normal system behavior and detect anomalies without relying on labeled data. We use two unsupervised learning techniques for anomaly detection: clustering and reconstruction-based methods. In this unsupervised model, without using labels, the ANN (Artificial Neural Network) or DBN (Deep Belief Network) models can detect various types of attacks, including abnormal BIND attacks, FTP attacks, multi-hop attacks, network partition issues, and node replication attacks. According to Table III, the accuracy rates for goodput with ANN and

DBN are 85.9% and 93.9%, respectively. The table also highlights the execution costs for these models. From this, we can infer that DBN offers a better balance between accuracy and computational cost.

A key consideration here is the difference in resources, power consumption, and secure hardware that can be implemented for a node to improve its place within an IoT provider's security strategy. In terms of computational memory and time cost, DBN provides an efficient trade-off between performance and computational expense when compared to other machine learning methods. Additionally, Table VI shows that the new wave of attacks could affect goodput, but both ANN and DBN models are capable of dynamically learning from the application profile content, including intrusion techniques, to mitigate these threats (Hugelmeyer, 2023).

Anomaly detection can be classified into two main approaches: supervised learning and unsupervised learning (M. Fadel et al., 2022). Virtual Intrusion Detection Systems in IoT are often trained using labeled datasets and are usually considered supervised anomaly detection methods. However, identifying all IoT attacks is not feasible. It is also impractical to rely solely on supervised algorithms to detect new, unknown attacks because IoT systems are frequently targeted at specific time intervals with changing sensors or attack methods. This makes unsupervised anomaly detection approaches more appealing for IoT security solutions (Shahnawaz Ahmed & Mehraj Shah, 2022).

4.3. Reinforcement Learning

The learning content can be gathered offline and applied across the entire organization in a camouflage context, isolating the loop within local domains for one or more episodes to allow the intrusion to reveal its location. Developing effective solutions requires a detailed understanding of how real-time security defenses can collaborate with legacy machine learning concepts to manage these attacks, especially when dealing with zero-sum games. Centralizing functions to establish global policies and empowering agents to act in parallel can lead to more consistent policies. This approach significantly improves decision-making efficiency without sacrificing accuracy, as permanent policy agents are tasked with making the right decisions at the right time (Ahmad et al., 2020).

Another major challenge associated with AI-driven threat detection in IoT networks is the limited availability of data for intrusion detection. Security frameworks must be tested on large datasets and in different environments because false positives, accuracy issues, and detection time are critical for success in adversarial network environments. Remote-controlled attacks at the physical layer can have severe consequences. Detecting these attacks with minimal false negatives and within a reasonable timeframe remains a significant challenge that IoT networks have yet to overcome. Additionally, data authentication presents difficulties due to the high volume, speed, and diversity of IoT data. Anomaly detection is another key issue in distributed systems.

As cyber-physical systems, IoT networks require multiple layers of security to defend against advanced persistent threats (APTs). The evolving nature of malware-based attacks demands adaptable and agile security systems, qualities that AI solutions can inherently provide. Reinforcement learning (RL) in AI-driven threat detection for IoT must address the "infinite horizon" problem seen in online MDP (Markov Decision Process) models. Effective security solutions at the agent level must continuously learn in real time, even when making decisions in complex, dynamic, and unpredictable environments. Distributed RL system architectures are capable of handling multiple attack scenarios with a global policy. These architectures can also detect zero-day attacks by leveraging knowledge from past and present states using knowledge banks, establishing an intruder-specific permanent policy for the entire network.

5. Case Studies and Examples

Several use case scenarios and prototypes for AI-driven distributed threat detection methodologies have been introduced by various industrial actors. These include projects such as energy automation for photovoltaic and energy storage systems (EMS), lightweight concrete (LWC) used for digitally reinforced mobility (OLYMPUS), and optimized operation and maintenance of railway bridges (OORT). Additional examples involve worker support in robot-driven flexible pipe production (FlexHub) and Industry 4.0 maintenance, covering the full lifecycle from prescription to end-of-life (RESOLVIT). Other research project cases include the development of trustworthy condition monitoring and interference control for last-mile services in mobility (Cross4Health), a 360° environmental assessment for elderly-friendly city initiatives (City4Age), and ensuring resilient operations for water authorities (RESOLVD) (Xu et al., 2021; Saeed Alzahrani & Waselallah Alsaade, 2022).

This section presents case studies and examples drawn from survey findings, with nine in-depth interviews conducted with key stakeholders. Interviewees included a public service provider in a megacity, a manufacturing company, a German research project supervisor specializing in networked systems, an Argentinian IoT tech company, as well as project managers in fields such as senior care, urban air quality, and process monitoring. Additionally, interviews were held with a German SME mechanical researcher and two manufacturers of industrial embedded system hardware and services. Each participant shared insights from either real-world scenarios or prototype applications utilizing AI-driven threat detection in IoT systems. The research project interview partners also discussed their methodology proposals and shared preliminary results from the German national research data hub, which aims to become a national provider of application layers for smart cities.

5.1. Real-World Applications of AI in IoT Security

In smart home ecosystems, the IoT gateway is the most vulnerable interface to electronic attacks due to its higher processing power, making it an attractive target. This concept extends to smart city edge computing nodes, where similar vulnerabilities exist. AI-ML tools can detect abnormal data behavior and

communicate with the cloud to mitigate attacks by leveraging flowchart-based reliability (Kumar Jagatheesaperumal et al., 2022). AI is particularly beneficial in smart home environments, such as in the kitchen, where it can predict the quantity of food needed, generate heat maps for cooking, and even prevent accidents like the door closing on a user's hands. Additionally, AI's predictive capabilities linked to recall sensors can anticipate failures; for example, AI can identify interactions with certain materials that may lead to patient hospitalizations, thus providing valuable preventive insights.

Artificial intelligence is already well-integrated into various industries, including healthcare, finance, and energy. Now, researchers are focusing on combining AI with the Internet of Things (IoT) to create smart objects with enhanced security features (Xu et al., 2021; Gilbert & Gilbert, 2024g). However, IoT networks using protocols like Zigbee, Bluetooth, and LPWAN are particularly susceptible to distributed denial of service (DDoS) attacks and man-in-the-middle attacks. AI can be deployed to monitor these networks, even when the data is encrypted, and predict potential electronic attacks on edge devices. Flowchart analyses further illustrate how AI integrates cybersecurity measures, such as firewalls, into smart home ecosystems. AI can identify unauthorized devices attempting to join the network, while the firewall implements zero-trust management to ensure secure communication among devices.

6. Future Trends and Risks

The coming years are expected to present significant challenges due to the high probability of unpredictability, rapid changes, and conflicts in the operational activities of IoT technologies (Sobb,Turnbull & Moustafa, 2020). As a result, addressing the future security issues and threats in AIoT (Artificial Intelligence of Things) is critical, especially for government and national infrastructure security(Gilbert & Gilbert, 2024j; Alaba et al., 2024). While AIoT is considered more reliable than its predecessors, several issues remain, such as inadequate AI-based attack management paradigms and the lack of trust, authentication methods, and security protocols for handling the data and objects generated by these systems. AIoT's introduction of machine learning and intelligent computing has also raised uncertainties, as these technologies require continuous risk-free analyses, and they often present non-deterministic outcomes (Xu et al., 2024). Furthermore, systems use real-life images and sensors to train AI models to predict thermal patterns and temperature ranges, which can help prevent stress-related abnormal incidents before they escalate into catastrophic events.

Despite advances in current technologies, many challenges remain in integrating AIoT technologies to create practical, affordable, and innovative solutions. This is a difficult task, given that advancements in AI, IoT, sensor networks, and wireless body-area networks (WBAN) often produce both beneficial and disruptive effects. Cyber-physical systems (CPS) and IoT devices have introduced new threats, including data storage attacks, communication breakdowns, denial-of-service (DoS) attacks, black market activities, and even robotic threats(Rani et al., 2024; Snehi, Bhandari & Verma, 2024). It is essential to update the state-of-the-art security measures, develop flexible defense strategies, and implement policies to handle these attacks and ensure secure AIoT operations (Adi et al., 2020).

Cyber-attacks are expected to have an increasingly severe impact on the global economy due to the growing number of IoT devices and the emergence of sophisticated malware and botnets (Kumar Pandey et al., 2023). In recent years, fog and cloud-based AI-empowered systems have demonstrated the ability to predict trends in the marketplace with remarkable accuracy, highlighting the effectiveness of AI methods in AIoT systems (Lifelo et al., 2024; Mishra et al.,2024). These systems, enhanced by cloud, fog, and dust computing, rely on top communication technologies like 5G, sensor networks, and WBANs (Yaghoubi, Ahmed & Miao, 2022). However, some commodity electronic healthcare devices still lack the technology necessary to regulate essential variables, raising concerns about their security and effectiveness (See the ***Figure 6 & 7***).

Figure 6:Future trends and risks in AIoT

This chart (Figure 6) illustrates the projected impact levels of trends and risks in AIoT (Artificial Intelligence of Things) from 2024 to 2028.

- **Trend**: The impact level rises steadily each year, indicating that AIoT's influence and associated risks are expected to grow.
- **Breakdown**: Each bar is divided into segments, likely representing different categories or types of impacts. As the years progress, the size of each segment generally increases, suggesting that multiple factors are contributing to the overall rise in impact.

Overall, the chart shows that by 2028, the impact of AIoT trends and risks will be at its highest, emphasizing the need for careful monitoring and management of these evolving technologies.

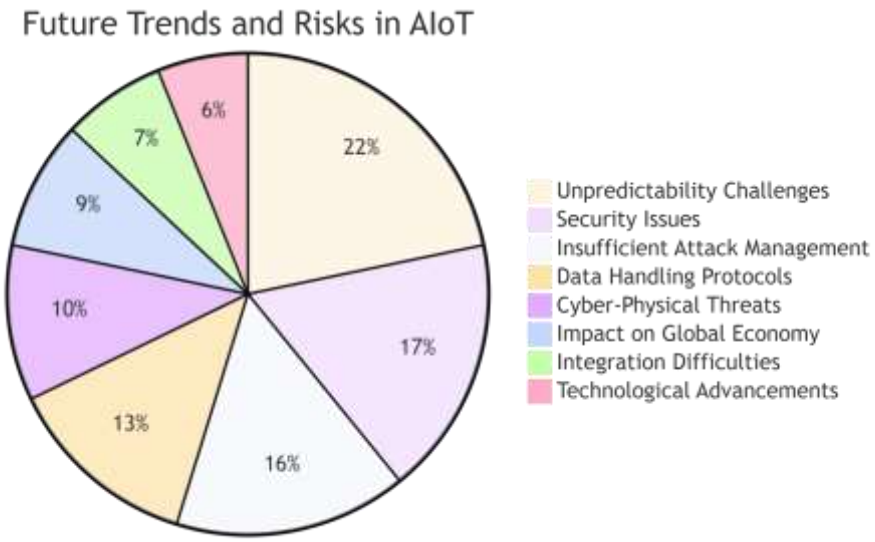

***Figure 7*: Future trends and risks in AIoT in a pie chart**

This pie chart (***Figure 7***) breaks down the main future trends and risks in AIoT, showing each one's impact level.

- **Unpredictability Challenges (22%)**: The biggest concern, highlighting the difficulty of predicting and managing AIoT systems.
- **Security Issues (17%)**: Security is a major risk, stressing the need for strong protective measures.
- **Insufficient Attack Management (16%)**: Points to the lack of effective tools and strategies to handle potential attacks on AIoT systems.
- **Data Handling Protocols (13%)**: Reflects concerns about managing and securing the large amounts of data generated by AIoT.
- **Cyber-Physical Threats (10%)**: Risks related to how AIoT systems interact with the physical world.
- **Impact on Global Economy (9%)**: Shows that AIoT could significantly affect the economy, both positively and negatively.
- **Integration Difficulties (7%)**: Highlights the challenges of integrating AIoT into existing systems.
- **Technological Advancements (6%)**: The smallest slice, suggesting that while advancements are crucial, they pose less direct risk compared to other issues.

In summary, unpredictability and security stand out as the most pressing concerns, indicating areas where extra attention is needed in the development of AIoT.

6.1. Emerging Technologies in IoT Security

To effectively address current and future IoT security threats, new strategies must be implemented in both network and cloud infrastructures (El Kafhali, El Mir & Hanini, 2022). According to Omolara et al.(2022), although some software and hardware security solutions have improved previously insecure areas, they are not universally adopted due to factors such as limited usability, high costs, and other drawbacks. In this context, AI-based solutions offer a valuable trade-off between performance and cost. AI-driven security, particularly using machine learning algorithms, has been extensively researched and applied, providing robust security solutions that enhance the efficiency and security of IoT processes (Abed & Anupam, 2023).

Traditional security methods in IoT environments have proven insufficient (Malhotra et al., 2021). Recent cyberattacks targeting IoT systems are especially concerning, as many of these systems perform critical functions, sometimes even life-dependent. When discussing IoT, the main issue that arises is the extensive security vulnerabilities these systems face and the wide range of protocols required to secure IoT communications (Kumar Pandey et al., 2023).

6.2. Potential Risks of AI in Threat Detection

AI-based intrusion detection systems (IDS) have shown vulnerabilities in terms of reduced precision for detecting attacks, which may be attributed to adversarial machine learning attacks. These attacks manipulate the AI models by introducing seemingly harmless but flawed data inputs, which negatively affect the model's performance (Aljumah, 2021). Recent studies highlight that AI-centered systems are becoming primary targets for attackers, especially through methods like poisoning machine learning models by injecting perturbed data that appears ordinary but contains deceptive elements. While domains like Computer Vision (CV) have received media attention for their vulnerabilities, cybersecurity concerns within AI systems remain less emphasized (Bernardez Molina et al., 2023; Xu et al., 2024).

AI has significantly enhanced the ability to detect cyberattacks, especially in the area of intrusion detection systems, by predicting and identifying network traffic anomalies. While early research on AI-based IDS has primarily focused on how effectively these systems detect distributed attacks, there is also a growing need to evaluate the reliability of these methods. As our reliance on AI for cybersecurity increases, we must recognize that AI systems themselves can be targets of exploitation. Therefore, it is crucial to understand the various types of cyberattacks that can take advantage of vulnerabilities in AI-based IDS (Aljumah, 2021; Bernardez Molina et al., 2023; Xu et al., 2024).

7.Summary of Key Findings

An AI-based system operates without manual intervention, making precise predictions that can identify both known and previously undiscovered attacks. Following this detection, automatic notifications and control measures are implemented to mitigate the effects of these attacks (Salayma, 2023). AI-driven threat detection works on both the sender's and receiver's ends since communication occurs between these two points. As real-time data continuously flows to controller nodes, anonymization algorithms and AI-based identification mechanisms utilize sensor and controller data to manage the threat detection process. This model proves to be both practical and robust, addressing a key challenge in ensuring the security of a diverse and reliable ecosystem.

The rise of AI-driven threat detection is increasingly prominent due to the widespread integration of artificial intelligence, machine learning, and deep learning technologies across critical IoT operations (Ali Talib Al-Khazaali & Kurnaz, 2021). With the rapid growth of data and the need for scalable algorithms, managing large datasets has become a significant challenge for IoT systems. To address this, anomaly detection and deep learning techniques can be employed to automate threat detection processes (Zhang & Tao, 2020). Given the numerous attack points across various platforms and applications, implementing AI-based threat detection is crucial for accurately identifying threats and enhancing personal security. Additionally, AI can reduce human errors in managing security processes, further strengthening system integrity.

7.1. Conclusion

The trend of cryptographic defense in IoT architectures, particularly to prevent man-in-the-middle attacks, has been highlighted in literature. This defense mechanism is crucial as many commercial IoT models do not support published APIs or ecosystem integration, which pushes them towards autonomous architectures that cannot depend on third-party cloud-based security solutions. However, local or edge configurations, like the "SunBlock" architecture, have shown potential by using more advanced machine learning (ML), deep learning models, fuzzy logic, and explainable AI (XAI) techniques. These methods enhance feature learning and anomaly detection patterns. The SunBlock architecture, with its feature extraction techniques, aims to provide simplified and potentially adversarial-proof systems against universal attacks. Future research should explores deeper into evaluating embedded AI systems, such as reinforcement learning for adaptive security responses that can go beyond basic rule-based filters (Vardhan et al., 2022).

This review of IoT threat detection, focusing on AI-driven sensors, indicates that there is a lack of comprehensive studies analyzing the specific risks, limitations, and vulnerabilities at the edge of IoT networks. More research is needed to address the challenges and explore the opportunities for secure, AI-driven architectures that protect consumer IoT devices. The emerging distributed AI-based threat detection systems present a promising area for further exploration. Securing privacy-protective AI at the edge is becoming a key factor in safeguarding commercial IoT systems (Safronov et al., 2024; Gilbert & Gilbert, 2024f).

7.2. Implications for Future Research

Several key areas should be explored to address the security and efficiency implications highlighted by this research (Malhotra et al., 2021). As smart devices are permitted to learn and evolve in real-time, they can inadvertently expose data across networks, heightening privacy and security risks (Gilbert & Gilbert, 2024f). Additionally, the growing number of AI-driven attacks, as outlined in the IoTDevice Twinning subsection, is a pressing concern. As the number of IoT devices rapidly increases and more individuals entrust them with sensitive and private information, the likelihood of cyber threats also rises. Without robust privacy and security measures in place, these vulnerabilities could be exploited. A risk-aware cybersecurity analysis for IoT, focusing on understanding, predicting, and assessing these vulnerabilities, is necessary. This can aid in the design, safety, and defense of IoT systems, unifying AI and IoT through a framework that incorporates a triple-study approach combining technologies and paradigm applications (Gilbert & Gilbert, 2024f).

The rapid advancements in IoT environments have led to the collection and transmission of vast amounts of data. However, there are currently too few devices capable of effectively analyzing these massive datasets. One potential solution is to explore how AI capabilities can be integrated at the resource-constrained edge of networks (Zhang & Tao, 2020). In cases involving surveillance cameras, smart sensors, or health-monitoring devices used at home,

it is not feasible to fully integrate AI locally without a loss of quality and efficiency. Ideally, machine learning models should be trained on powerful, on-site systems. But when device resources and energy constraints prevent running advanced algorithms locally, the machine learning models must be executed remotely in a way that optimizes performance at the edge.

The security implications of AI-driven threat detection within IoT systems have been discussed in detail. However, the potential for utilizing machine learning techniques to improve recognition bandwidth efficiency, reduce dependency on high-energy cloud services, and develop more secure devices in the future presents exciting opportunities.

References

1. Abed, A. K., & Anupam, A. (2023). Review of security issues in Internet of Things and artificial intelligence-driven solutions. *Security and Privacy*, *6*(3), e285.
2. Abilimi, C. A., Addo, H., & Opoku-Mensah, E. (2013). Effective Information Security Management in Enterprise Software Application with the Revest-Shamir-Adleman (RSA) Cryptographic Algorithm. In *International Journal of Engineering Research and Technology*, 2(8), 315 – 327.
3. Abilimi, C. A., & Yeboah, T. (2013). Assessing the challenges of Information and Communication Technology in educational development in High Schools in Ghana. In *International Journal of Engineering Research and Technology*,2(11), 60 - 67.
4. Abilimi, C. A., & Adu-Manu, K. S. (2013). Examining the impact of Information and Communication Technology capacity building in High School education in Ghana. In *International Journal of Engineering Research and Technology*,2(9), 72- 78
5. **Adi, E., Anwar, A., Baig, Z., & Zeadally, S.** (2020). ***Machine learning and data analytics for the IoT*** PDF.
6. **Ahmad, I., Shahabuddin, S., Kumar, T., Harjula, E., Meisel, M., Juntti, M., Sauter, T., & Ylianttila, M.** (2020). ***Challenges of AI in wireless networks for IoT*** PDF.
7. **Ahmed, M. S., & Shah, S. M.** (2022). ***Unsupervised ensemble-based deep learning approach for attack detection in IoT network*** PDF.
8. **Aljumah, A.** (2021). ***IoT-based intrusion detection system using convolution neural networks***. Retrieved from ncbi.nlm.nih.gov
9. Alaba, F. A., Jegede, A., Sani, U., & Dada, E. G. (2024). Artificial Intelligence of Things (AIoT) Solutions for Sustainable Agriculture and Food Security. In *Artificial Intelligence of Things for Achieving Sustainable Development Goals* (pp. 123-142). Cham: Springer Nature Switzerland.
10. Alabadi, M., Habbal, A., & Wei, X. (2022). Industrial internet of things: Requirements, architecture, challenges, and future research directions. *IEEE Access*, *10*, 66374-66400.
11. **Al-Khazaali, A. T. A., & Kurnaz, S.** (2021). ***Study of integration of blockchain and Internet of Things (IoT): An opportunity, challenges, and applications as medical sector and healthcare***. Retrieved from ncbi.nlm.nih.gov.
12. Almohamad, T. A., Salleh, M. F. M., Mahmud, M. N., Karaş, İ. R., Shah, N. S. M., & Al-Gailani, S. A. (2021). Dual-determination of modulation types and signal-to-noise ratios using 2D-ASIQH features for next generation of wireless communication systems. *IEEE Access*, *9*, 25843-25857.
13. **Alterazi, A. H., Kshirsagar, P. R., Manoharan, H., Selvarajan, S., Alhebaishi, N., Srivastava, G., & Lin, J. C.-W.** (2022). ***Prevention of cyber security with the Internet of Things using particle swarm optimization***. Retrieved from ncbi.nlm.nih.gov
14. **Al-Shaboti, M., Chen, A., & Welch, I.** (2019). ***Automatic device selection and access policy generation based on user preference for IoT activity workflow*** PDF.
15. **Alzahrani, M. S., & Alsaade, F. W.** (2022). ***Computational intelligence approaches in developing cyberattack detection system***. Retrieved from ncbi.nlm.nih.gov
16. Aslam, A., Qureshi, K. N., & Newe, T. (2024). Future Privacy and Trust Challenges for AIoT Networks. In *Artificial Intelligence of Things (AIoT)* (pp. 198-216). CRC Press.
17. **Asam, M., Khan, S. H., Akbar, A., Bibi, S., Jamal, T., Khan, A., Ghafoor, U., & Bhutta, M. R.** (2022). ***IoT malware detection architecture using a novel channel boosted and squeezed CNN***. Retrieved from ncbi.nlm.nih.gov
18. **Bernardez Molina, S., Nespoli, P., & Gómez Mármol, F.** (2023). ***Tackling cyberattacks through AI-based reactive systems: A holistic review and future vision*** PDF.
19. BeyondTrust. (2023). *Top IoT Security Vulnerabilities*. Available at: BeyondTrust
20. Bibri, S. E., Krogstie, J., Kaboli, A., & Alahi, A. (2024). Smarter eco-cities and their leading-edge artificial intelligence of things solutions for environmental sustainability: A comprehensive systematic review. *Environmental Science and Ecotechnology*, *19*, 100330.
21. **Blinowski, J. G., & Piotrowski, P.** (2020). ***CVE-based classification of vulnerable IoT systems*** PDFPDFPDF.
22. **Chen, Z., Liu, J., Shen, Y., Simsek, M., Kantarci, B., Mouftah, H. T., & Djukic, P.** (2022). ***Machine learning-enabled IoT security: Open issues and challenges under advanced persistent threats*** PDF.

23. Christopher, A. A.(2013). Effective Information Security Management in Enterprise Software Application with the Revest-Shamir-Adleman (RSA) Cryptographic Algorithm.International Journal of Engineering Research & Technology (IJERT),ISSN: 2278-0181,Vol. 2 Issue 8, August - 2013.

24. **El Kafhali, S., El Mir, I., & Hanini, M. (2022).** Security threats, defense mechanisms, challenges, and future directions in cloud computing. ***Archives of Computational Methods in Engineering***, ***29***(1), 223-246.

25. **Fadel, M. F., El-Ghamrawy, S. M., Ali-Eldin, A. M. T., Hassan, M. K., & El-Desoky, A. I.** (2022). ***The proposed hybrid deep learning intrusion prediction IoT (HDLIP-IoT) framework***. Retrieved from ncbi.nlm.nih.gov.

26. Fortinet. (2023). *Top IoT Device Vulnerabilities: How To Secure IoT Devices*. Available at: Fortinet.

27. George, A. S. (2024). Emerging Trends in AI-Driven Cybersecurity: An In-Depth Analysis. *Partners Universal Innovative Research Publication*, *2*(4), 15-28.

28. Gilbert, C. & Gilbert, M.A.(2024a).Unraveling Blockchain Technology: A Comprehensive Conceptual Review. International Journal of Emerging Technologies and Innovative Research (www.jetir.org | UGC and ISSN Approved), ISSN:2349-5162, Vol.11, Issue 9, page no. ppa575-a584, September-2024, Available at : http://www.jetir.org/papers/JETIR2409066.pdf.

29. Gilbert, C. & Gilbert, M.A.(2024b).Strategic Framework for Human-Centric AI Governance: Navigating Ethical, Educational, and Societal Challenges. International Journal of Latest Technology in Engineering Management & Applied Science, 13(8), 132-141. https://doi.org/10.51583/IJLTEMAS.2024.130816.

30. Gilbert, C. & Gilbert, M.A.(2024c).The Impact of AI on Cybersecurity Defense Mechanisms: Future Trends and Challenges.Global Scientific Journals.ISSN 2320-9186,12(9),427-441. https://www.globalscientificjournal.com/researchpaper/The_Impact_of_AI_on_Cybersecurity_Defense_Mechanisms_Future_Trends_and_Challenges_.pdf.

31. Gilbert, C. & Gilbert, M.A. (2024d). The Convergence of Artificial Intelligence and Privacy: Navigating Innovation with Ethical Considerations. *International Journal of Scientific Research and Modern Technology*, *3*(9), 9-9.

32. Gilbert, C. & Gilbert, M.A.(2024e).Transforming Blockchain: Innovative Consensus Algorithms for Improved Scalability and Security. International Journal of Emerging Technologies and Innovative Research (www.jetir.org), ISSN:2349-5162, Vol.11, Issue 10, page no.b299-b313, October-2024, Available :http://www.jetir.org/papers/JETIR2410134.pdf.

33. Gilbert, C. & Gilbert, M.A. (2024f). *Future Privacy Challenges: Predicting the Agenda of Webmasters Regarding Cookie Management and Its Implications for User Privacy*. International Journal of Advanced Engineering Research and Science, ISSN (Online): 2455-9024,Volume 9, Issue 4, pp. 95-106.

34. Gilbert, C., & Gilbert, M. A. (2024g). Navigating the Dual Nature of Deepfakes: Ethical, Legal, and Technological Perspectives on Generative Artificial Intelligence (AI) Technology. *International Journal of Scientific Research and Modern Technology*, *3*(10). *https://doi.org/10.38124/ijsrmt.v3i10.54*.

35. Gilbert, C., & Gilbert, M. A. (2024h).*Revolutionizing Computer Science Education: Integrating Blockchain for Enhanced Learning and Future Readiness*. International Journal of Latest Technology in Engineering, Management & Applied Science, ISSN 2278-2540, Volume 13, Issue 9, pp.161-173.

36. Gilbert, C. & Gilbert, M.A. (2024i). *Unlocking Privacy in Blockchain: Exploring Zero-Knowledge Proofs and Secure Multi-Party Computation Techniques*. Global Scientific Journal (ISSN 2320-9186) 12 (10), 1368-1392.

37. Gilbert, C. & Gilbert, M.A. (2024j).The Role of Artificial Intelligence (AI) in Combatting Deepfakes and Digital Misinformation.International Research Journal of Advanced Engineering and Science (ISSN: 2455-9024), Volume 9, Issue 4, pp. 170-181.

38. Gilbert, M.A., Oluwatosin, S. A., & Gilbert, C.(2024). An investigation into the types of role-based relationships that exist between lecturers and students in universities across southwestern nigeria: a sociocultural and institutional analysis. Global Scientific Journal, ISSN 2320-9186, Volume 12, Issue 10, pp. 263-280.

39. Haji, S. H., & Ameen, S. Y. (2021). Attack and anomaly detection in iot networks using machine learning techniques: A review. *Asian J. Res. Comput. Sci*, *9*(2), 30-46.

40. **Hafsa Rafique, S., Abdallah, A., Musa, N. S., & Murugan, T.** (2024). ***Machine learning and deep learning techniques for Internet of Things network anomaly detection—Current research trends***. Retrieved from ncbi.nlm.nih.gov

41. **Hugelmeyer, C.** (2023). ***Inscribed squares and relation avoiding paths*** PDF.

42. **Jagatheesaperumal, S. K., Pham, Q. V., Ruby, R., Yang, Z., Xu, C., & Zhang, Z.** (2022). ***Explainable AI over the Internet of Things (IoT): Overview, state-of-the-art and future directions*** PDF.

43. **Kumar, N. P., Kumar, K., Saini, G., & Mishra, A. K.** (2023). ***Security issues and challenges in cloud of things-based applications for industrial automation***. Retrieved from ncbi.nlm.nih.gov

44. **Kumar, P. S., Yanambaka, V. P., & Abdelgawad, A.** (2022). ***Internet of Things: Security and solutions survey***. Retrieved from ncbi.nlm.nih.gov

45. **Kumar, A. S., Petracca, G., Aksu, H., Jaeger, T., & Uluagac, A. S.** (2018). ***A survey on sensor-based threats to Internet-of-Things (IoT) devices and applications*** PDF.

46. Kwame, A. E., Martey, E. M., & Chris, A. G. (2017). Qualitative assessment of compiled, interpreted and hybrid programming languages. *Communications on Applied Electronics*, *7*(7), 8-13.

47. **Lifelo, Z., Ding, J., Ning, H., & Dhelim, S. (2024).** Artificial Intelligence-Enabled Metaverse for Sustainable Smart Cities: Technologies, Applications, Challenges and Future Directions.

48. **Malhotra, P., Singh, Y., Anand, P., Bangotra, D. K., Singh, P. K., & Hong, W. C.** (2021). ***Internet of Things: Evolution, concerns and security challenges***. Retrieved from ncbi.nlm.nih.gov.

49. **Mishra, A. K., Ravinder Reddy, R., Tyagi, A. K., & Arowolo, M. O. (2024).** Artificial Intelligence-Enabled Edge Computing: Necessity of Next Generation Future Computing System. In ***IoT Edge Intelligence*** (pp. 67-109). Cham: Springer Nature Switzerland.

50. Neto, E. C. P., Dadkhah, S., Sadeghi, S., Molyneaux, H., & Ghorbani, A. A. (2023). A review of Machine Learning (ML)-based IoT security in healthcare: A dataset perspective. *Computer Communications*.

51. **Omolara, A. E., Alabdulatif, A., Abiodun, O. I., Alawida, M., Alabdulatif, A., & Arshad, H. (2022).** The internet of things security: A survey encompassing unexplored areas and new insights. ***Computers & Security***, ***112***, 102494.

52. Opoku-Mensah, E & Boateng, F.O.,Abilimi,C.A., Asante, M., (2015).Testing for Randomness in Pseudo Random Number Generators Algorithms in a Cryptographic Application.Computer Engineering and Intelligent Systems 6(9), 12-16.

53. Opoku-Mensah, E., Abilimi, C. A., & Boateng, F. O. (2013). Comparative analysis of efficiency of fibonacci random number generator algorithm and gaussian Random Number Generator Algorithm in a cryptographic system. Comput. Eng. Intell. Syst, 4, 50-57.

54. Opoku-Mensah, E., Abilimi, A. C., & Amoako, L. (2013). The Imperative Information Security Management System Measures In the Public Sectors of Ghana. A Case Study of the Ghana Audit Service. International Journal on Computer Science and Engineering (IJCSE), 760-769.

55. **Rani, S., Kataria, A., Kumar, S., & Karar, V. (2024).** A New Generation Cyber-Physical System: A Comprehensive Review from Security Perspective. ***Computers & Security***, 104095.

56. **Rupanetti, D., & Kaabouch, N. (2024).** Combining Edge Computing-Assisted Internet of Things Security with Artificial Intelligence: Applications, Challenges, and Opportunities. ***Applied Sciences***, ***14***(16), 7104.

57. **Safronov, V., Mandalari, A. M., Dubois, D. J., Choffnes, D., & Haddadi, H.** (2024). ***SunBlock: Cloudless protection for IoT systems*** PDF.

58. **Salayma, M.** (2023). ***Risk and threat mitigation techniques in Internet of Things (IoT) environments: A survey*** PDF.

59. **Sangeetha, K. B. S., Mani, P., Maheshwari, V., Jayagopal, P., Kumar, M. S., & Allayear, S. M.** (2022). ***Design and analysis of multilayered neural network-based intrusion detection system in the Internet of Things network***. Retrieved from ncbi.nlm.nih.gov

60. **Saxena, R., Gayathri, E., & Kumari, L. S.** (2023). ***Semantic analysis of blockchain intelligence with proposed agenda for future issues***. Retrieved from ncbi.nlm.nih.gov

61. **Schmitt, M.** (2023). ***Securing the digital world: Protecting smart infrastructures and digital industries with artificial intelligence (AI)-enabled malware and intrusion detection*** PDF.

62. **Sobb, T., Turnbull, B., & Moustafa, N. (2020).** Supply chain 4.0: A survey of cyber security challenges, solutions and future directions. ***Electronics***, ***9***(11), 1864

63. **Snehi, M., Bhandari, A., & Verma, J. (2024).** Foggier skies, clearer clouds: A real-time IoT-DDoS attack mitigation framework in fog-assisted software-defined cyber-physical systems. ***Computers & Security***, ***139***, 103702.

64. Sternum IoT. (2023). *Top 10 IoT Vulnerabilities and How to Mitigate Them*. Available at: Sternum IoT

65. **Vardhan, H., Timalsina, U., Volgyesi, P., & Sztipanovits, J.** (2022). ***Data-efficient surrogate modeling for engineering design: Ensemble-free batch mode deep active learning for regression*** PDF.

66. Venafi. (2023). *Top 10 Vulnerabilities that Make IoT Devices Insecure*. Available at: Venafi

67. **Xu, H., Li, Y., Balogun, O., Wu, S., Wang, Y., & Cai, Z.** (2024). ***Security risks concerns of generative AI in the IoT*** PDFPDFPDF.

68. **Xu, Y., Liu, X., Cao, X., Huang, C., Liu, E., Qian, S., ... Zhang, J.** (2021). ***Artificial intelligence: A powerful paradigm for scientific research***. Retrieved from ncbi.nlm.nih.gov

69. **Yaghoubi, M., Ahmed, K., & Miao, Y. (2022).** Wireless body area network (WBAN): A survey on architecture, technologies, energy consumption, and security challenges. ***Journal of Sensor and Actuator Networks***, ***11***(4), 67.

70. **Yang, W., Wang, S., Sahri, N. M., Karie, N. M., Ahmed, M., & Valli, C.** (2021). ***Biometrics for Internet-of-Things security: A review***. Retrieved from ncbi.nlm.nih.gov.

71. Yeboah, T., Opoku-Mensah, E., & Abilimi, C.A..(2013). A Proposed Multiple Scan Biometric-Based Registration System for Ghana Electoral Commission. *Journal of Engineering, Computers & Applied Sciences (JEC&AS)*, *2*(7).

72. Yeboah, D. T., Odabi, I., & Abilimi Odabi, M. C. A. A. (2016). *Utilizing divisible load scheduling theorem in round robin algorithm for load balancing in cloud environment*.

73. Yeboah, T., Opoku-Mensah, E., & Abilimi,A. C. (2013). A Proposed Multiple Scan Biometric-Based Registration System for Ghana Electoral Commission. *Journal of Engineering, Computers & Applied Sciences (JEC&AS)*, *2*(7).

74. Yeboah T. & Abilimi C.A. (2013).*Using Adobe Captivate to creative Adaptive Learning Environment to address individual learning styles: A Case study Christian Service University*, International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181,www.ijert.org, "2(11).

75. **Zhang, J., & Tao, D.** (2020). ***Empowering things with intelligence: A survey of the progress, challenges, and opportunities in artificial intelligence of things*** PDF