A Systematic Review of AI-Based Security Solutions for IoT Operating Systems

Retaj Baaqeel, Razan Almalki, Wafaa Alawadhi, Elaf Sultan, Raghad Alowaybidi
Department of Cybersecurity, Umm Al-Qura University, Kingdom of Saudi Arabia
{ }@uqu.edu.sa

Abstract— **While the proliferation of Internet of Things (IoT)-connected devices has greatly enhanced connectivity, it has also made them susceptible to significant security risks[22]. The applications of artificial intelligence (AI) to the security of Internet of Things operating systems are reviewed in the current article. The effectiveness of AI approaches, like as machine learning and anomaly detection, in detecting and thwarting threats like Distributed Denial of Service (DDoS) attacks has been evaluated using systematic review methodologies[22]. We also look at the potential of blockchain technology in terms of data integrity[19]. Our survey findings demonstrate that AI-based security measures can successfully boost IoT networks' resistance to attacks. In order to build a robust, intelligent security architecture that can outsmart the risk of assaults in a connected world as technology advances, we emphasized the significance of ongoing research and collaborations.**

Keywords: Operating Systems Security; Internet of Things; Artificial Intelligence; Threats; Machine Learning; Intrusion Detection Systems; Real-Time Monitoring.

1 INTRODUCTION

The Internet of Things (IoT) represents a network of interconnected devices that communicate and exchange data with one another. These devices range from household items like smart refrigerators, smart thermostats: Nest, and health-tracking monitors to sophisticated industrial machinery, which are embedded with sensors and software that enable them to operate autonomously and efficiently However, the rapid proliferation of IoT devices brings with it significant security challenges[15]. With the number of connected devices growing exponentially, they have become prime targets for cyberattacks, exposing vulnerabilities that can threaten data integrity, privacy, and operational continuity[13]. Many IoT devices are not built with strong security measures, as manufacturers often prioritize usability and features over robust protections. Once compromised, these devices can be manipulated to steal sensitive information, conduct distributed denial-of-service (DDoS) attacks, or in- filtrate broader network systems. To address these pressing security concerns, our research focuses on enhancing the security of IoT operating systems through the integration of Artificial Intelligence (AI) and machine learning techniques. These tech- neologises offer advanced solutions that go beyond traditional security mechanisms, addressing complex threats like device authentication, intrusion detection, denial of service (DoS) attacks, and malware detection. Thus, artificial intelligence not only shows threat detection and provides response in real time but also learns from past events to face emerging threats. our survey aims to systematically review existing AI- based solutions for securing IoT operating systems, providing an in-depth analysis of their effectiveness and implementation frameworks. our surevy pinpoints main weaknesses in IoT systems and illustrates using AI and machine learning for risk mitigation, hence the path to inventive security measures that guarantee safety and integrity of connected devices. as IoT devices become deeply integrated into both daily life and industrial processes, ensuring their security is critical. Our study aims to systematically review existing AI-based solutions designed to secure IoT operating systems, offering a detailed analysis of their effectiveness and implementation frameworks[7][20].

Three focal questions inform our research: RQ1: What are the recent advancements and future trends in leveraging AI and blockchain technologies to tackle security challenges in IoT systems? This question delves into how the integration of AI and blockchain technologies is evolving to address the growing security concerns within IoT environments. The focus is on identifying cutting-edge innovations and emerging trends that enhance the security and reliability of IoT systems, exploring how these technologies are reshaping the future of IoT security.

RQ2: How can AI-driven techniques improve the security of IoT operating systems by addressing vulnerabilities and emerging threats? This question examines the role of AI techniques, such as machine learning and deep learning, in strengthening IoT operating systems. By focusing on how AI can proactively detect and counteract vulnerabilities, the goal is to understand how these techniques enhance resilience against emerging threats and provide more robust security for IoT systems.

RQ3: What are the key components of a machine learning-based security framework for IoT systems? This question centers on identifying the critical elements that make up a comprehensive machine learning-based security framework for IoT. The aim is to explore what components are essential for real-time threat detection, mitigation, and overall scalability, guiding the design of next-generation solutions that can adapt to the dynamic threat landscape of IoT systems.

By focusing on these three research questions we provide a comprehensive investigation into the Internet of Things operating system and Artificial Intelligence. By exploring these questions in detail, we aim to obtain a clearer grasp

of the difficulties, prospects, and developing trends in this important topic by thoroughly examining these concerns. Our research is structured as follows: Section 2 discusses the transformative impact of IoT across industries, highlighting unique security vulnerabilities such as weak encryption and design flaws. Section 3 details our research approach, including the formulation of key research questions that explore advancements in AI and blockchain for IoT security. Section 4 discusses the main themes in current research, integration of Artificial Intelligence (AI) and blockchain technologies to enhance the security of Internet of Things (IoT) operating systems. It discusses current advancements in AI-driven threat detection, the core components of machine learning security frameworks and section 5 suggests future research directions to address limitations in scalability, model efficiency, and bias within these systems. Finally, the conclusion summarizes our key findings and highlights promising directions for future research.

By organizing this paper's sections, questions, and importance, we ensure a structured approach that guides the reader through a logical sequence. and that will help the reader to clearly follow the progression of ideas and understand how each question is addressed in a coherent manner. As a result, the answers to the questions will be presented in a way that is easy to comprehend, leading to a deeper understanding of the solutions and insights offered throughout the paper.

2 BACKGROUND

The Internet of Things (IoT) refers to a network of interconnected physical devices, such as sensors, appliances, or wearable technology, that communicate and share data over the internet. These devices can range from home thermostats to industrial machinery, all connected to monitor and automate processes. IoT systems rely on the collection, exchange, and processing of data, making them susceptible to numerous security threats [17], [18].

An operating system (OS) is software that manages hardware and software resources on a device, providing essential services to applications and users. IoT operating systems are specialized versions of OS designed to manage the constraints of IoT devices, such as limited computing power, memory, and energy resources. These operating systems are lightweight, efficient, and optimized for the specific needs of IoT environments [15].

IoT systems are composed of several layers, each with its unique functions and security challenges (potential weak spots that attackers can exploit):

- The perception layer consists of physical devices and sensors (devices that detect physical changes in the environment, such as temperature, humidity, or motion) that collect data from the environment. These sensors, while critical for IoT functions, are often susceptible to physical tampering, where an attacker might damage the device or manipulate the data it captures [17].
- The network layer is responsible for transmitting the data collected by the perception layer to other devices or cloud servers. However, this layer is vulnerable to data interception attacks, such as man-in-the-middle (MitM) attacks. In a MitM attack, malicious actors intercept or alter communications between devices, making it possible for sensitive information to be stolen or manipulated. This is particularly dangerous in IoT environments because encryption protocols may be weak or outdated, allowing attackers to easily intercept the data [16].
- The application layer processes data and provides the interface that users interact with. This layer is often targeted by malware (malicious software designed to infect systems, compromise data, or disrupt normal operations). Ensuring the security of this layer is essential to prevent the spread of attacks throughout the system [17].

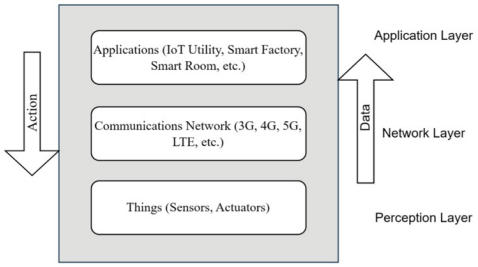


Fig. 1. Layers of the assumed IoT architecture[17].

One major threat to IoT systems is a Distributed Denial of Service (DDoS) attack. In this type of attack, compromised devices (often part of a botnet, which is a network of infected computers or devices controlled remotely by attackers) are used to flood a target with an overwhelming amount of traffic. This causes the target to slow down or become completely unresponsive, preventing it from functioning properly [18]. Another common issue is weak encryption, which allows attackers to easily intercept and decrypt sensitive information [15].

To combat these vulnerabilities, several technologies have been proposed. Machine Learning (ML), a subset of Artificial Intelligence (AI), allows systems to learn from data patterns and detect anomalies (unusual or abnormal behaviors) in real-time, which is particularly useful in identifying unusual behaviors in IoT networks that may signal an attack [18]. Deep learning, an advanced form of ML, uses artificial neural networks to improve decision-making and threat detection. Meanwhile, Natural Language Processing (NLP) enables machines to understand human language, which can be applied to analyze threat reports or detect phishing attempts [16].

Anomaly detection, driven by AI, is a key technique in IoT security, as it helps identify deviations from normal system behavior that could indicate a security breach. Threat intelligence refers to the process of gathering and analyzing data to predict, detect, and respond to emerging security threats.

AI-powered models can process large amounts of data to enhance threat intelligence and even automate responses to

identified risks [16].

In addition to AI, blockchain technology is being explored for IoT security. Blockchain is a decentralized, distributed ledger that provides a secure method for device-to-device communication by ensuring the data being shared remains trustworthy and unchangeable [17]. Software-Defined Networking (SDN) offers another layer of protection by separating the control of the network from the physical devices, allowing for centralized management that can quickly adapt to new threats [16].

For IoT operating systems (OS), AI-driven approaches have been developed to manage devices more efficiently. One such approach is Over-the-Air (OTA) updates, which allow for the remote updating of IoT devices without the need for physical access. This ensures that devices stay up-to-date with the latest security patches [15].

In terms of communication between IoT devices, protocols like the Constrained Application Protocol (CoAP) and Lightweight M2M (LWM2M) are designed specifically for devices with limited resources. CoAP is a specialized web transfer protocol that is lightweight and efficient, making it suitable for low-power devices like sensors. It functions similarly to HTTP but is optimized for constrained environments, ensuring secure and efficient data transfer between devices and servers. On the other hand, LWM2M (Lightweight Machine to Machine) is a protocol that facilitates the management of IoT devices, providing remote control, software updates, and monitoring capabilities. LWM2M is designed to operate efficiently in low-power environments, allowing for secure communication and device management with minimal resource usage. These protocols ensure that IoT systems maintain performance while also safeguarding the data being transmitted [15].

Despite these advances, IoT operating systems remain vulnerable to cyberattacks, such as brute-force attacks and Denial of Service (DoS) attacks. Machine Learning (ML) techniques have been proposed to detect such threats by analyzing system behavior in real-time and flagging suspicious patterns as potential attacks [18].

However, there are challenges in using AI for IoT security. Data quality refers to the accuracy and completeness of the data that AI models rely on to make decisions. Poor data quality can lead to incorrect predictions or failures in detecting threats. Additionally, model training requires large amounts of high-quality data, which can be difficult to obtain in IoT environments. Another risk is adversarial attacks, where attackers intentionally feed misleading data into AI models to trick them into making incorrect decisions. Ensuring that AI models are robust enough to resist these attacks is a major focus of ongoing research [16].

IPv6, the latest version of the Internet Protocol (IP), plays a crucial role in enabling the growing number of IoT devices to communicate with each other over networks. IPv6 offers a vastly larger address space than its predecessor, IPv4, and includes built-in security features that improve data encryption and authentication. This protocol is essential for IoT environments, where the number of connected devices is rapidly expanding [15].

Future research directions are exploring the development of explainable AI, especially in critical applications like IoT security. Additionally, researchers are investigating the integration of lightweight cryptographic methods, which are encryption techniques optimized for low-power IoT devices. The convergence of AI, blockchain, and SDN is also being studied to create more secure, adaptable, and scalable IoT security systems [17].

3 Methodology

We have selected this topic due to the increasing prominence of the Internet of Things (IoT), particularly following the widespread adoption of IPv6. The IoT has become a critical aspect of modern life, significantly enhancing convenience and efficiency in various domains. However, this technological advancement also raises important questions regarding security. As we embrace the benefits of IoT, it is essential to explore effective strategies for safeguarding these systems to ensure they remain both user-friendly and secure.

- **RQ1: What are the current advancements and future trends in utilizing AI and blockchain technologies to address security challenges in IoT systems?**
- **RQ2: How can AI-driven approaches enhance the security of IoT operating systems by addressing vulnerabilities and emerging threats?**
- **RQ3: What are the core components of a machine learning security framework for IoT systems?**

We identified research questions focused on exploring advancements in AI and blockchain technologies to address IoT security challenges. The study aims to identify tools and technologies based on AI and blockchain that can enhance IoT system security, as well as the key components required for a machine learning-based security framework to ensure better protection of IoT operating systems.

After defining these questions, We identified three sets of terms related to AI, operating systems, and IoT, which were combined using Boolean searches to create search strings. The focus was on papers published between 2018 and 2024, using Google Scholar to gather relevant studies at the intersection of AI, operating systems, and IoT. The search terms included:

Artificial Intelligence OR Machine Learning OR Deep Learning AND Operating System OR OS Security OR Kernel Security AND Internet of Things OR IoT Security

We started with an initial set of around 50 papers focused on the intersection of AI, operating systems (OS), and IoT. To refine the selection, we applied specific inclusion and exclusion criteria as follows:

IC	Inclusion criteria
1	Peer-reviewed papers – Only peer-reviewed papers were included.
2	Relevance to AI-OS-IoT security – Papers had to discuss AI techniques enhancing OS and IoT security.
3	Publication date – Only papers published between 2018 and 2024 were considered.
EC	**Exclusion criteria**
1	Duplicate removal – Only the latest or most detailed version of each study was retained.
2	Language – Only papers written in English were considered.
3	Limited scope – Papers that focused on unrelated topics were excluded.
4	The paper cover IoT Shortly
5	The paper page is less than four

TABLE I

INCLUSION AND EXCLUSION CRITERIA .

As a result, 20 papers aligned with our criteria and fell within the scope of our research. The excluded papers only briefly mentioned the relevant terms but did not thoroughly explore the intersection of AI, OS, and IoT security.

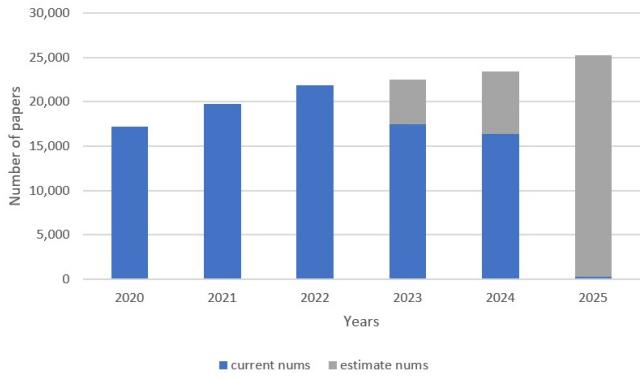
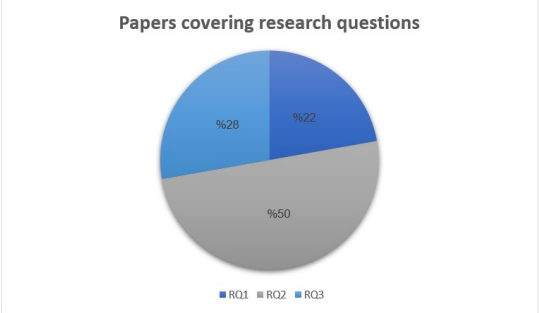


Fig. 2. Number of papers related to securing IoT operating systems with AI.

We began by analyzing the content of each paper to classify it according to the research questions. This involved reading the keywords, abstract, introduction, and conclusion, as well as highlighted titles within the papers to determine their coverage. Each team member was tasked with summarizing their assigned paper, identifying its main points, solutions, challenges, strengths, and limitations. After completing these individual summaries, we compiled the findings to create a comprehensive study. This allowed us to identify common themes, compare the papers, and produce an accurate literature review that supports our research objectives.

Paper Analysis The Main Venues Figure 2 depicts the number of research papers related to securing IoT operating systems with artificial intelligence. From 2020 to 2022, there is a noticeable increase in the number of papers. However, in 2023, a slight decline was observed. Estimates for 2024 and 2025 indicate steady growth, reflecting continuous advancement in research. Overall, the chart suggests expectations for



increased interest and innovation in this field.[9]

Conference Distribution the chart illustrates the distribution of conferences and the number of associated research papers. ARES and ICSE are the leading conferences, each with 26 published papers. This distribution highlights the diversity of research areas and interests in securing IoT operating systems with artificial intelligence, emphasizing the key role these conferences play in advancing research in this field.[8]

Conference	Papers
ARES	26
ICSE	26
CH	17
Nss	14
Middlewere	11
Eurosys	10
Icimmi	10
Asia ccs	9
css	9
CoNext	8

TABLE II

CONFERENCES DISTRIBUTION

4 Discussion

RQ1: What are the current advancements and future trends in utilizing AI and blockchain technologies to address security challenges in IoT systems?

The fusion of Artificial Intelligence (AI) and blockchain technologies is driving significant advancements in securing Internet of Things (IoT) systems. With IoT networks continually expanding, the need for robust security frameworks has intensified. Current research has explored how AI can enhance real-time threat detection and response, while blockchain offers a decentralized security infrastructure to improve data integrity and reliability across IoT ecosystems.

Blockchain for Decentralized Security Frameworks Blockchain technology provides a decentralized and secure data management solution for IoT systems. Unlike traditional centralized systems, which are vulnerable to attacks on single points of failure, blockchain ensures that data is securely distributed across multiple nodes. [1] discusses how blockchain can create a tamper-proof ledger for IoT data, which helps mitigate risks related to data integrity and unauthorized access.

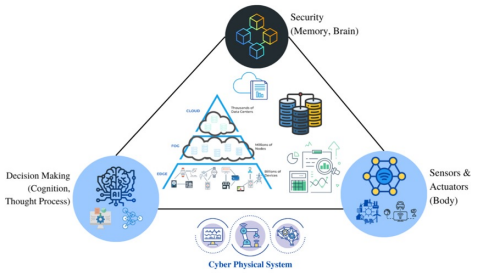


Fig. 3. Convergence of blockchain, AI towards secured IoT[1].

AI-Driven Threat Detection and Response AI enhances IoT security by employing machine learning algorithms to detect and respond to threats in real-time. Through pattern recognition, AI can autonomously identify abnormal behaviors that may indicate security risks, enabling prompt actions. Zhang et al.[2], underscore the role of AI in improving IoT security, particularly through predictive analysis and anomaly detection models, which enhance threat response capabilities within IoT systems. Aljabri et al. [18] further demonstrate the effectiveness of AI, specifically machine learning models, in detecting IoT attacks like Flood DoS and Brute Force. By employing models such as Gradient Boosting and Decision Trees, they achieved accuracy rates of up to 95.94% for detecting these attacks. This high accuracy supports the potential of AI to autonomously identify and respond to threats in real time, which is crucial for the rapidly expanding IoT landscape. The study's focus on supervised ML techniques complements existing advancements in AI-driven security, emphasizing the ability of these models to accurately detect abnormal behaviors in IoT traffic. Fu-

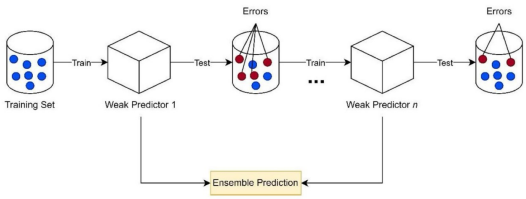


Fig. 4. The Gradient Boosting Procedure[18].

ture Trends in AI-Blockchain Convergence the convergence of AI and blockchain is anticipated to shape future IoT security frameworks, emphasizing autonomous, intelligent, and decentralized protection. Gupta et al.[3] describe future trends where smart contracts on the blockchain, driven by AI analytics, can execute security protocols automatically, reducing human intervention. This approach enables IoT networks to manage security collaboratively, sharing threat intelligence securely and optimizing real-time threat response across interconnected devices.

In response to the question, research indicates that AI and blockchain technologies jointly address IoT security challenges by combining decentralized data management with intelligent threat detection. Blockchain provides a secure, immutable platform for data sharing among IoT devices, while AI facilitates real-time threat identification and response. As these technologies evolve, future trends suggest the potential for creating distributed IoT networks where AI-driven devices autonomously manage and share security intelligence through blockchain. This fusion of technologies promises a more resilient and adaptive IoT security framework, capable

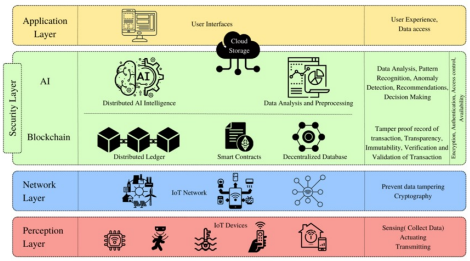


Fig. 5. Architectural framework Blockchain and AI for secured IoT[1].

of responding to the dynamic security needs of modern IoT ecosystems.

RQ2: How can AI-driven approaches enhance the security of IoT operating systems by addressing vulnerabilities and emerging threats?

AI-driven approaches, especially machine learning and deep learning, have been lately addressed as a promising solution to enhance the security of IoT operating systems. These approaches can analyze vast amounts of data from IoT devices and predict potential security threats [10].First, let's address some AI-driven techniques: ML (Machine Learning) is employed for analyzing network traffic, device logs and to find out potential security vulnerabilities. Deep Learning (DL) is also deployed to perform data profiling and feature extraction for anomaly detection and threat identification on difficult datasets. Supervised Learning, on the other hand, allows models to be trained in labeled datasets and learn from known threats and identify new ones, while Unsupervised Learning enables pattern identification or unknown threat detection as it handles unlabeled data [11] [12].By integrating AI-driven approaches with existing security solutions, IoT devices can be better protected from emerging threats and vulnerabilities Now let's explore how AI-driven approaches can enhance the security of IoT operating systems by addressing two main points: vulnerabilities and emerging threats. AI algorithms can predict potential vulnerabilities in IoT operating systems by analyzing code and configuration files, such as buffer overflows, SQL injection, and cross-site scripting In addition, these algorithms can also recognize trends and anomalies that do not align with the normal state. Trained on known vulnerabilities and coding patterns, AI models can discover potential security problems in IoT devices. This was in terms of vulnerability [13].As for emerging threats we are addressing Anomalies which are the crucial aspect of IOT Security that detects and identifies new patterns or behavior shown by devices, which can be an indication of a threat. In IoT systems, the detection of anomalies can be performed using AI-powered methodolo-

gies like Machine Learning (ML) and Deep Learning (DL). Here's how: Training ML models, Normal behavior data coming off IoT devices can power the training for machine learning algorithms to detect patterns and trends. The training data may be sensor readings, network traffic or system logs. Detecting deviant behavior: A well-trained ML model can also be employed to analyze fresh, unseen data from connected devices building further on this information. If the model identifies something different from a normal pattern, it can tell you in an alert that this is happening [14]. There are several different types of anomalies that AI can detect, such as Point Anomalies: A single instance of data is anomalous if it's too far off from the rest. Contextual anomalies: It is the data that are anomalies in a specific context, but not necessarily in others, Collective anomalies: These are a collection of data instances that are anomalous when compared to the rest. Also when in The machine learning field there are some efficient threat detection techniques such as, Dyna-Q: Suitable with a reinforcement technique, this algorithm can learn and adapt over time that could make it ideal to identify potential threats being enforced by the IOTs(rule set) as well challenge detonate one, Q-Learning: Is a Reinforcement learning algorithm that can be used in educational scenario where it could help IoT devices learn from past interactions with the environment and decide strategically to block attacking IP from entering or causing security breach, Multivariate Correlation Analysis: A statistical approach to assessing the relationships between a set of variables with potential patterns and anomalies in IoT data [13].

Therefore, Machine Learning and Deep Learning are AI-based approaches, which with the right programming can elevate security measures for IoT OS by efficiently dealing with loopholes and real time threats. They can ingest data on a scale from IoT devices and use the vast amounts of telemetry available to predict potential security threats but also work with existing security solutions. They also might be able to find or respond to deviations from the norm, identify previously undetectable threats and mitigate security breaches. This capability enables IoT operating systems to identify and mitigate vulnerabilities (like buffer overflow, SQL injection), by even prefilling them which can help in preventing zero-day attacks. Plus, AI-driven methodologies can train from more data and adapt to new situations while taking decisions based on the best possible information that helps in securing a stronger IoT landscape. Moreover, such methods allow us to constantly provide threat intelligence and facilitate IoT operating systems in responding rapidly to any new potential threats as they arise [14] [11] [12].

RQ3: What are the core components of a machine learning security framework for IoT systems?

The core components of a machine learning security framework for IoT systems encompass data collection and preprocessing, anomaly detection, behavioral analysis, and threat prediction and prevention. These components work synergistically to enhance IoT security by continuously monitoring device and network activities, detecting and responding to threats, and using historical data to anticipate potential risks.

Data Collection and Preprocessing the foundation of the framework is data collection from IoT devices and networks, which provides the raw inputs for analysis. Preprocessing this data—such as filtering noise, normalizing values, and handling missing information—is essential to maintain data quality, which directly impacts the accuracy of machine learning models. [4] emphasizes that effective preprocessing is crucial for building reliable threat detection models that can differentiate between normal and malicious activity.

Anomaly detection is the framework's primary tool for identifying potential security threats in IoT environments. By leveraging supervised and unsupervised learning algorithms, the framework can recognize patterns in data that deviate from typical behavior, signaling a potential security issue.[5] highlights how machine learning-based anomaly detection is vital for identifying threats such as unauthorized access or unusual data transmissions within IoT systems.

Behavioral Analysis to enhance detection accuracy, the framework includes a behavioral analysis component that profiles the normal operations of IoT devices and networks over time. This allows for the identification of subtle changes in behavior that may not be evident through anomaly detection alone. [6] describes how behavioral analysis can differentiate between benign and suspicious activities, offering an additional layer of security.

Threat Prediction and Prevention using historical data, the machine learning models within this framework can predict future security incidents and enable proactive measures to prevent them. This capability allows the system to recognize patterns associated with known threats and intervene before an attack can occur. [7] underscores the importance of predictive capabilities in enhancing IoT security, as it allows for a more resilient and adaptable defense strategy.

The integration of these components into a machine learning security framework provides a comprehensive approach to IoT security. By combining real-time monitoring, advanced threat detection, and proactive threat prediction, this framework can effectively protect IoT systems from various security challenges, ensuring a more secure and resilient network environment.

Main Themes and Trends in Current Research the main trend in OS security research, particularly in IoT environments, is the use of AI techniques such as machine learning and deep learning for real-time threat detection and anomaly detection. Blockchain is also gaining attention for providing decentralized security frameworks to ensure data integrity and prevent attacks. Current studies explore how AI-driven systems can adapt to emerging threats, learning from data and continuously improving security mechanisms.

AI and Blockchain for IoT Security several studies have explored the integration of AI and blockchain technologies to enhance IoT security. Blockchain offers a decentralized security framework that ensures data integrity and prevents unauthorized access by distributing data across multiple nodes, eliminating single points of failure. For example,

the study by Nalband et al. [1] emphasizes the strength of blockchain in creating tamper-proof ledgers for IoT data, which mitigates risks related to data integrity and data breaches[5][7][3][12].

On the other hand, AI focuses on real-time threat detection and anomaly detection. Studies like Zhang et al.[2] highlight AI's ability to analyze large volumes of IoT data, recognize patterns, and identify abnormal behaviors that may indicate a security threat. AI-driven techniques such as machine learning (ML) and deep learning (DL) allow for predictive analysis and anomaly detection, enhancing the response capabilities of IoT operating systems.

The convergence of these two technologies—AI for intelligent detection and blockchain for secure data management—promises to offer comprehensive security solutions. However, while they both aim to secure IoT environments, the focus of each technology is different: blockchain addresses the structural integrity of data, and AI provides dynamic threat monitoring and response capabilities.

Approaches to Threat Detection AI techniques like machine learning and deep learning are commonly applied for analyzing vast amounts of IoT data to detect threats. Studies show that ML models can be trained on device logs and network traffic to predict potential security threats and vulnerabilities (e.g., buffer overflows or SQL injection). Techniques such as anomaly detection are vital in this domain, with different types of anomalies being detected—point, contextual, and collective anomalies.

In contrast, blockchain-based approaches do not directly detect threats. Instead, they ensure the security of data transactions within the IoT ecosystem. By distributing data across a network of devices, blockchain minimizes the risk of data manipulation and unauthorized access. For example, smart contracts within blockchain systems can automatically enforce security protocols based on predefined conditions[18].

Strengths and Weaknesses of Current Approaches The biggest strength of AI and ML in OS security is their ability to quickly process large amounts of data, making them highly effective for spotting potential threats early. AI-driven anomaly detection has shown great promise, especially in identifying unknown threats that more traditional methods might miss.

On the other hand, these AI models have limitations. They require high-quality data to function well, and can sometimes produce false positives, where harmless activities are flagged as threats. Moreover, AI is not always adaptable to brand-new, unseen types of attacks, which can pose a problem for rapidly changing threat landscapes[16].

Blockchain is great for securing communications by ensuring data integrity, but its downside lies in the latency it introduces. The computational requirements to process transactions can slow down systems, making it less ideal for environments where speed is crucial, like in real-time IoT systems[3].

Gaps and Inconsistencies one major gap is the scalability of these solutions. Many AI models require substantial computing power and large datasets, which may not always be feasible for small or low-powered IoT devices. Moreover, while blockchain enhances data security, its integration with AI in practical applications is still in its infancy. Many studies overlook the potential high cost and energy requirements of maintaining blockchain infrastructures across vast IoT networks[10].

Broader Implications for OS Security the findings from this survey highlight the increasing complexity of securing modern operating systems. OS security is no longer just about protecting individual machines; it now involves securing entire networks, monitoring user behavior, and ensuring compliance with regulations.

Integrating technologies like AI and blockchain into OS security frameworks introduces new challenges, particularly around privacy and ethical considerations. As AI systems become more widespread, issues like data privacy, bias, and regulatory compliance (such as the General Data Protection Regulation or GDPR) become more critical. These broader concerns are just as important as the technical aspects of OS security[21].

5 Future Work

Unexplored Areas or Unanswered Questions in OS Security AI Model Efficiency for Resource-Constrained IoT Devices: Most AI models require significant computational resources, which are not always available in small IoT devices. Future research could focus on developing lightweight AI models that can function effectively with limited processing power and energy. Blockchain Scalability in IoT Networks: Blockchain is effective for ensuring data integrity but is not fully scalable in IoT environments due to its computational overhead. Further research is needed to explore blockchain alternatives or modifications that allow it to scale in realtime systems. AI Bias in Threat Detection: While AI models are excellent at pattern recognition, they can sometimes exhibit bias based on the datasets used for training. Investigating methods to reduce bias in AI-driven OS security systems would be beneficial.

New Methodologies or Technologies to Advance Research Federated Learning for Decentralized AI Training: Instead of relying on centralized data to train AI models, federated learning allows for training across distributed IoT devices without transferring sensitive data. This methodology could advance the development of more secure and privacy-conscious AI models. AI-Blockchain Integration for Autonomous Systems: Research could explore AI-powered smart contracts that autonomously manage security protocols in real time across distributed IoT networks. These contracts could use AI to detect anomalies and trigger automated responses while being secured through the blockchain's decentralized nature[1][6].

Addressing the Limitations of Current Research improving the Accuracy of AI Models: To address the problem of false positives and adaptability in AI-based threat detection, future research could focus on integrating context-aware AI models. These models could use contextual data, such as user behavior or device conditions, to make more

informed decisions. Optimizing Blockchain for Real-Time IoT Security: Research into lightweight consensus algorithms (e.g., Proof of Stake or Proof of Authority) or layer-2 solutions like sidechains and state channels could reduce the latency and computational demands of blockchain in IoT networks. Additionally, exploring hybrid approaches where time-critical data is handled outside of blockchain but anchored to it for verification could offer a solution to the latency issue[2]. Energy Efficiency: Another limitation is the high energy consumption of both AI models and blockchain. Future work could investigate energy-efficient algorithms or explore the use of renewable energy sources to support the infrastructure[2][13].

Interdisciplinary Approaches Human-Computer Interaction (HCI): Incorporating HCI into OS security research can lead to the development of more user-friendly and intuitive security solutions. For instance, research into how users interact with AI-driven security systems could help optimize threat detection processes without overwhelming users with false alarms. CrossDomain Applications: AI and blockchain can benefit from collaboration with fields like edge computing, autonomous systems, and cloud computing. Research on how these technologies interact and enhance security could lead to more comprehensive solutions for IoT-based OS security.

The limitations that we faced could influence, the overall quality and comprehensiveness of the findings. Understanding these constraints is crucial for developing effective strategies to mitigate their influence. The following table outlines key constraints encountered during research, their associated impacts, and proposed solutions to address these challenges. This structured approach not only enhances the research process but also fosters a deeper understanding of how to navigate potential obstacles effectively.

Constraint	**Impact and Solution**
Language Constraints	Missing important studies due to focusing on English papers. Solutions included seeking translations and using translation tools.
Lack of Research Experience	Inability to apply methodologies correctly due to lack of experience. Solutions involved pursuing online courses and relevant literature.
Time Constraints	Hasty decisions due to time pressures. A timetable was established to manage tasks effectively.
Limited Access to Academic Resources	Hindrance in research due to lack of access. Solutions included utilizing university libraries and joining research groups.

TABLE III

SUMMARY OF CONSTRAINTS AND THEIR IMPACTS AND SOLUTIONS IN RESEARCH.

6 CONCLUSIONS

Our survey systematically investigates the state of operating systems security (OS), highlighting significant insights into current practices and future directions, particularly with emerging technologies like blockchain, IoT, and artificial intelligence (AI). A key takeaway from our findings is the increasing integration of AI-driven techniques for threat prediction, vulnerability management, and anomaly detection. AI has shown success in identifying known and unknown threats using deep learning, supervised as well as unsupervised mechanisms that can constantly learn against an ever-changing security landscape. The blockchain model for decentralized security, is one of the takeaways from our survey because it eliminates traditional single points-of-failure and ensures data integrity. our survey underscores how the convergence of these technologies can foster a more secure and adaptable OS environment, especially for IoT-connected systems. Future work in this area should focus on refining AI models for security by improving the accuracy of anomaly detection systems and expanding predictive analytics to an- ticipate and mitigate potential risks. Additionally, exploring the integration of decentralized technologies like blockchain can further strengthen OS security frameworks, particularly in distributed environments. With security threats maturing on a non-stop, 24×7 basis nowadays systems profiting multidisciplinary approach united of AI and blockchain beside the normal classical set- tings becomes mandatory. While this survey serves as something of a roadmap for future research, the very present need is clear: we must continue to innovate in AI-driven and blockchain-supported security solutions.. We encourage collaboration between researchers and practitioners to effectively tackle the dynamic landscape of OS security, ultimately enhancing the resilience and integrity of interconnected systems.

References

[1] A. H. Nalband, et al., "Exploring the Joint Potential of Blockchain and AI for Securing Internet of Things," *ResearchGate*, 2024. [Online]. Available: https://www.researchgate.net. [Accessed: Oct. 12, 2024].

[2] Y. Zhang, et al., "Operating System and Artificial Intelligence: A Systematic Review," *School of Software Technology, Zhejiang University*, 2024.

[3] V. Gupta, et al., "Integrating Blockchain with Artificial Intelligence to Secure IoT Networks: Future Trends," *MDPI*, 2022. [Online]. Available: https://www.mdpi.com. [Accessed: Oct. 12, 2024].

[4] Author(s), "Artificial Intelligence for Securing IoT Services in Edge Computing: A Survey," *Wiley*, 2020. [Online]. Available: https://www.wiley.com. [Accessed: Oct. 12, 2024].

[5] Author(s), "A Machine Learning Security Framework for IoT Systems," *IEEE*, 2020. [Online]. Available: https://www.ieee.org. [Accessed: Oct. 12, 2024].

[6] Author(s), "Security and Privacy Concerns in AI Enabled IoT Educational Frameworks: An In-Depth Analysis," *Kuey*, 2020. [Online]. Available: https://www.kuey.com. [Accessed: Oct. 12, 2024].

[7] Author(s), "Machine Learning-Based Solutions for IoT Security: A Survey," *ScienceDirect*, 2020. [Online]. Available: https://www.sciencedirect.com. [Accessed: Oct. 12, 2024].

[8] ACM Digital Library, "[All: securing IoT operating systems with AI] AND [E-Publication Date: (01/01/2019 TO 12/31/2024)] : Search," 2019. [Online]. Available: https://dl.acm.org/action/doSearch?AllField=Securing+IoT+operating+systems+with+AI+&startPage=&AvailableFormat=lit%3Aimage&AfterYear=2019&BeforeYear=2024&queryID=52/7737484228. [Accessed: Oct. 12, 2024].

[9] Google.com, "Google Scholar," 2024. [Online]. Available: https://scholar.google.com. [Accessed: Oct. 12, 2024].

[10] T. Mazhar, D. B. Talpur, T. Al Shloul, Y. Y. Ghadi, I. Haq, I. Ullah, K. Ouahada, and H. Hamam, "Analysis of IoT Security Challenges and Its Solutions Using Artificial Intelligence," *Brain Sciences*, vol. 13, no. 4, p. 683, Apr. 2023. doi:10.3390/brainsci13040683. *Keywords: IoT Security, Artificial Intelligence, Challenges, Solutions.*

[11] H. El-Sofany, S. A. El-Seoud, O. H. Karam, and B. Bouallegue, "Using machine learning algorithms to enhance IoT system security," *Scientific Reports*, vol. 14, no. 1, pp. 12077, 2024. *Keywords: Machine Learning, IoT Security, Algorithms, Enhancement.*

[12] N. Ghaffari, S. Jelodari, N. Pouralish, N. Derakhshanfard, and B. Arasteh, "Securing internet of things using machine and deep learning methods: a survey," *Cluster Computing*, vol. 27, no. 1, pp. 9065–9089, 2024. *Keywords: IoT Security, Machine Learning, Deep Learning, Survey.*

[13] M. A. Al Kabir, W. Elmedany, and M. S. Sharif, "Securing IoT Devices Against Emerging Security Threats: Challenges and Mitigation Techniques," *Journal of Cyber Security Technology*, vol. 7, no. 4, pp. 199–223, Jul. 2023. *Keywords: IoT Devices, Security Threats, Mitigation Techniques.*

[14] D. Rupanetti and N. Kaabouch, "Combining Edge Computing-Assisted Internet of Things Security with Artificial Intelligence: Applications, Challenges, and Opportunities," *Applied Sciences*, vol. 14, no. 7104, Aug. 2024. *Keywords: Edge Computing, IoT Security, Artificial Intelligence, Applications.*

[15] A. Antony and S. S., "A Review on IoT Operating Systems," *International Journal of Computer Applications*, vol. 176, no. 24, pp. 33-40, May 2020.

[16] F. Tao, M. S. Akhtar, and Z. Jiayuan, "The Future of Artificial Intelligence in Cybersecurity: A Comprehensive Survey," *EAI Endorsed Transactions on Creative Technologies*, vol. 8, no. 28, pp. e3, 2021.

[17] zzcvvvvvvvvvvM. Adam, M. Hammoudeh, R. Alrawashdeh, and B. Alsulaimy, "A Survey on Security, Privacy, Trust, and Architectural Challenges in IoT Systems," *IEEE Access*, vol. 12, pp. 57128-57144, 2024. doi:10.1109/ACCESS.2024.3382709.

[18] M. Aljabri, A. Shaahid, F. Alnasser, A. Saleh, D. Alomari, M. Aboulnour, W. Al-Eidarous, and A. Althubaity, "IoT Attacks Detection Using Supervised Machine Learning Techniques," *HighTech and Innovation Journal*, vol. 5, no. 3, pp. 534-550, 2024. doi:10.28991/HIJ-2024-05-03-01.

[19] M. Humayun, N. Tariq, M. Alfayad, M. Zakwan, G. Alwakid, and M. Assiri, "Securing the Internet of Things in Artificial Intelligence Era: A Comprehensive Survey," *IEEE Access*, vol. 12, pp. 25469–25486, Feb. 2024.

[20] M. R. Islam and K. M. Aktheruzzaman, "An Analysis of Cybersecurity Attacks against Internet of Things and Security Solutions," *Journal of Computer and Communications*, vol. 08, no. 04, pp. 11–25, 2020.

[21] A. K. Abed and A. Anupam, "Review of security issues in Internet of Things and artificial intelligence-driven solutions," *Security and Privacy*, vol. 6, no. 3, pp. e285, Nov. 2022, doi: 10.1002/spy2.285.

[22] S. Zaman, K. Alhazmi, M. A. Aseeri, M. R. Ahmed, R. T. Khan, M. S. Kaiser, and M. Mahmud, "Security Threats and Artificial Intelligence Based Countermeasures for Internet of Things Networks: A Comprehensive Survey," *IEEE Access*, vol. 9, pp. 1–35, Jun. 2021, doi: 10.1109/ACCESS.2021.3089681.