International Journal of Computer Sciences and Engineering
Vol.**13**, Issue.**4**, pp.**92-98** April **2025**
ISSN: 2347-2693 (Online)
Available online at: www.ijcseonline.org

ISSN: 2347-2693 (E)

Research Article

Securing Hardware with AI: Intrusion Detection, Threat Mitigation, and Trust Assurance

Vasuki Shankar[1*], Nanditha Muralidhar[2]

[1]Nvidia Corporation, India
[2]Vellor Institute of Technology, India

Corresponding Author:

Received: 22/Feb/2025; **Accepted**: 24/Mar/2025; **Published**: 30/Apr/2025. **DOI**: https://doi.org/10.26438/ijcse/v13i4.9298

Abstract: As cyber threats targeting modern hardware become increasingly sophisticated, traditional security mechanisms such as encryption and isolation are no longer sufficient. This paper explores the adaptation of Artificial Intelligence in the realm of hardware security to enhance anomaly detection, intrusion detection, and real-time threat mitigation. Through case studies of Intel SGX, AMD SEV, and Microsoft Pluton, the study demonstrates how AI-driven mechanisms can enhance protection against side-channel attacks, firmware compromises, and hardware Trojans. While AI significantly improves threat resilience, challenges like computational overhead, adversarial attacks, and a dearth of explainability hinder its widespread adoption. We conclude the paper by identifying the need for lightweight AI models and AI-Quantum integration as future directions for building robust, next-generation hardware security frameworks.

Keywords: AI-driven security, hardware protection, intrusion detection, adversarial AI, machine learning, cyber security, anomaly detection, threat mitigation, AI-Quantum security.

1. Introduction

1.1 Background

Modern hardware systems face an increasing number of cyber threats, including firmware attacks, side-channel attacks, and hardware Trojans. As these pervasive attacks continue to evolve, traditional security methods such as cryptographic protection and isolated execution environments are no longer sufficient. AI-driven security offers a proactive approach, enabling real-time detection of anomalies, prediction of threats, and automatic mitigation of risk scenarios.

1.2 Aim of Research

In this paper, we study the protection of modern hardware systems using AI-based security mechanisms for threat detection, mitigation, and establishing trust. Objectives of the study are to,

- Evaluate the effectiveness of AI in hardware protection.
- Explore how AI can enhance trust and reduce uncertainty arising from cyber threats.
- Identify the risks linked to the use of AI-driven security models.
- Analyze adaptability of AI in combating contemporary hardware attacks.

1.3 Research Questions

The research questions we aim to address are as follows,

- How effective is AI in defending modern hardware against various threats?
- What risks and limitations do AI pose for security?
- How can AI contribute to building trust in hardware security systems?
- Which AI techniques are most suitable for countering hardware-based cyber threats?

1.4 Significance of this Study

This study contributes to the body of research on hardware protection mechanisms within the domain of AI backed hardware security. We explore practical insights to organizations seeking to migrate to AI-based solutions to enhance security and defend against security threats. Modern hardware systems are under increasing cyber threat from firmware attacks, side channel attacks, and hardware Trojans. Since pervasive attacks are evolving, such traditional security methods as cryptographic protection and isolated execution environments cannot stop them. These AI driven security solutions provide a proactive approach in which this can detect the anomalies, predict the threat and automatically mitigate those risk scenarios in real time as described in Fig-1.

The research paper is organized as follows: Section I introduces the growing challenges in hardware security and outlines the motivation, objectives, and research questions of the study. Section II presents a detailed literature review, covering traditional security methods, the emergence of AI-driven approaches, and existing gaps in the field. Section III outlines the research methodology, including the design, data sources, and AI techniques analyzed. Section IV discusses the results, highlighting key performance metrics, real-world case studies, and limitations of AI-based hardware security. Section V offers a comprehensive discussion, including a comparative analysis with traditional security models, the role of AI in future-proofing hardware systems, ethical concerns, and policy considerations. Section VI provides a summary of results, practical implications, and directions for future research.

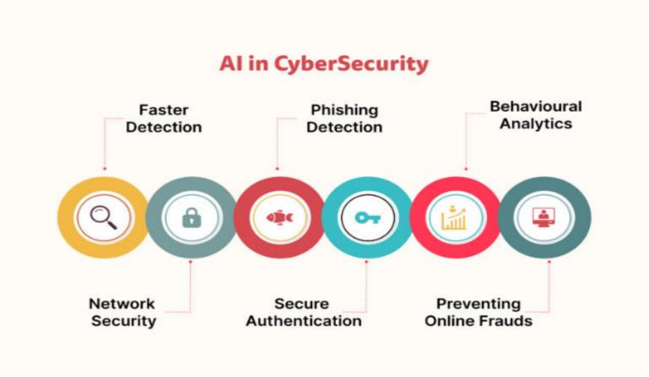

Figure 1. Benefits of AI in Cybersecurity

2. Literature Review

2.1 Overview of Hardware Security Threats

a) Side Channel Attacks

Side-channel attacks take advantage of unintentional information leaks from hardware components, such as fluctuations in power usage or differences in processing time. Spectre and Meltdown are classic examples of speculative execution flaws in CPUs that enabled unauthorized memory access into the kernel. These attacks target Intel’s SGX enclave, compromising secure execution [1]. Their existence highlights the urgent need for advanced security mechanisms to detect and prevent hardware vulnerabilities.

b) Firmware and BIOS Attacks

Firmware and BIOS attacks involve injecting malicious code into low-level system software. To bypass system-level security, Rootkits and Bootkits exploit firmware to gain persistent control over devices. For example, LoJax is a UEFI rootkit that remains undetected even after system reboots. AI-driven security can enhance real-time detection and threat mitigation for such attacks.

c) Hardware Trojans

Hardware Trojans refer to malicious modifications introduced during semiconductor manufacturing that create backdoors or weaken encryption. These threats are particularly difficult to detect, as they often remain dormant until activated. Machine learning techniques are being employed to identify anomalies in chip design and throughout the supply chain.

d) Physical Tampering

Physical attacks, such as chip probing and fault injection, directly target hardware to extract cryptographic keys or alter circuitry. These threats are common in IoT and industrial systems. AI-enabled monitoring can assist in detecting unauthorized access, thereby strengthening hardware security.

2.2 Traditional Approaches to Hardware Security

a) Cryptographic Solutions

Modern hardware systems are increasingly data-sensitive and must be secured to ensure safe communication between parties. Cryptographic methods help prevent unauthorized access and data breaches. Trusted Platform Modules (TPMs) further enhance security by providing hardware components for the secure storage of cryptographic keys, device authentication, and integrity verification. TPMs are now widely used in modern computing devices to safeguard firmware integrity and prevent unauthorized software execution.

b) Hardware Isolation Mechanisms

Mechanisms such as sandboxing and Secure Boot restrict how programs execute, ensuring that only authorized code runs. Sandboxing isolates processes to minimize risk, helping prevent system-wide compromises.

2.3 AI-Driver Security: A New Paradigm

a) Machine Learning-Based Anomaly Detection

AI-driven security leverages Machine learning (ML) algorithms used to examine extensive data produced by hardware activity. These models can detect deviations from normal operations and alert users of potential breaches.

b) Predictive Analytics for Threat Intelligence

Cyber threat intelligence is essential for recognizing and preventing attacks. AI models analyze historical threat data to identify trends and predict new attack vectors, enabling organizations to implement proactive security measures [3].

2.4 Traditional Approaches to Hardware Security

a) AI-Enhanced Processors

Modern AI-powered processors integrate self-learning security mechanisms capable of adaptively detecting and countering emerging threats. These processors analyze system behavior in real time to identify anomalies indicative of cyberattacks. Chip manufacturers such as Intel and AMD are incorporating AI-driven security features to enable real-time encryption and hardware-level threat detection, thereby protecting sensitive data from side-channel exploits and firmware tampering.

b) Firmware Security Using AI

Firmware is a high-risk attack vector, being a foundational component of hardware. AI-driven security solutions can detect and neutralize firmware threats before they compromise system integrity. AI-powered models automatically analyze firmware updates and identify potential vulnerabilities based on runtime behavior.

c) Self-Healing Security Models

AI-powered self-healing security systems autonomously detect, isolate, and recover from cyberattacks without human intervention [4]. These systems use rollback mechanisms to restore firmware and system settings to a secure state upon detecting malicious modifications. For example, AI-driven rollback mechanisms can revert systems to the well-known safe version to defend against persistent threats.

2.5 Literature Gap

Despite substantial progress in AI-driven security as described in Fig-2, significant gaps remain in current research. A key limitation is the lack of real-time implementation of AI security models in hardware systems [5]. Additionally, the computational overhead of AI-based security mechanisms is underexplored. These solutions often require considerable processing power, which can affect system performance especially in resource-constrained environments like IoT and embedded systems [6].

Lastly, issues related to trust and explainability hinder widespread adoption. Organizations lack clear methods to verify and validate AI-based security decisions, particularly when determining whether activity is malicious [7]. Transparency is essential for fostering trust in AI-based hardware security systems, and further research is needed to develop more interpretable AI models.

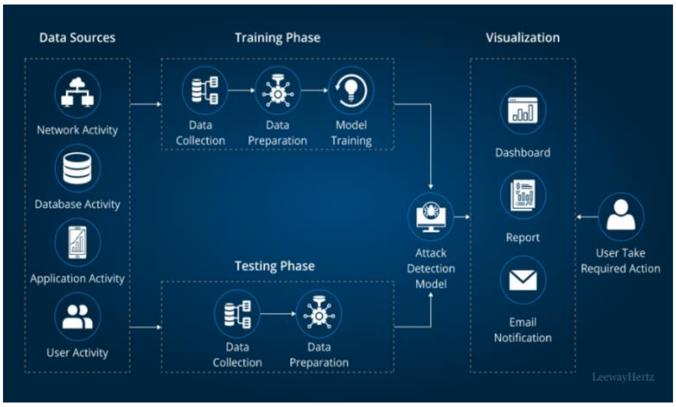

Figure 2. Data security in AI systems

3. Methodology

3.1 Research Design

This paper provides a descriptive and analytical approach to understanding the role of AI in hardware security. The descriptive component examines existing AI-driven security mechanisms, while the analytical component evaluates the effectiveness of these mechanisms in preventing cyber threats [8].

3.2 Data Collection Methods

The study relies on secondary data sources to review AI-driven security mechanisms. Insights into current AI applications in hardware security are gathered through an extensive review of academic journals, white papers, and cybersecurity reports. Research papers on AI-based security models are sourced from cybersecurity databases such as IEEE Xplore, ACM Digital Library, and arXiv [9].

3.3 AI Algorithms and Techniques for Security

Modern hardware security employs a range of AI techniques to identify and prevent cyber threats, as well as to identify abnormalities that could lead to system compromise. This study evaluates supervised learning, unsupervised learning, and deep learning in terms of their effectiveness in securing hardware systems.

a) Supervised Learning

Firmware integrity analysis and hardware anomaly detection rely on classification techniques using Support Vector Machines (SVMs) and Decision Trees. When trained on historical attack data, these AI models can achieve high accuracy in detecting potential security breaches.

b) Unsupervised Learning

Is crucial for real-time security monitoring, particularly in anomaly detection. Methodologies like K-means clustering and autoencoders analyze hardware behavior patterns and identify deviations that may signal potential threats [10]. These methods enhance adaptability by enabling the detection of unknown attack vectors.

c) Deep Learning

Deep learning techniques, such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), are used to analyze complex hardware interactions. These models are used in AI based malware detection to distinguish between benign and malicious firmware activities. Additionally, Generative Adversarial Networks (GANs) are employed to test hardware security resilience against adversarial AI attacks.

3.4 Ethical and Security Considerations

The use of AI-driven security systems must be responsible and aligned with cybersecurity ethics and privacy regulations. Key frameworks such as GDPR, NIST AI Risk Management, and ISO/IEC 27001 are necessary to protect sensitive hardware data. It is important to recognize that AI can function as a legal and ethical black box. Therefore, AI security models should be transparent and explainable. The use of fair and unbiased training datasets is essential to mitigate bias in AI decision-making. Furthermore, AI models must be protected against adversarial attacks through robust security measures to prevent exploitation by malicious actors [11].

4. Results and Analysis

4.1 AI-Driver Security Performance Metrics

Key performance metrics for AI-driven security mechanisms include detection accuracy, response time, and efficiency in mitigating threats as described in Table-1.

a) Detection Accuracy

AI based Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS) demonstrate superior detection accuracy compared to conventional signature-based mechanisms [12]. Deep learning-based anomaly identification and ML models, in general, can identify sophisticated attacks such as zero-day exploits and hardware Trojans.

b) Speed and Efficiency

Unlike traditional security approaches, which rely on static rules, AI adapts dynamically to constantly evolving threats providing real-time threat detection and response. Threat analysis and classification occur within milliseconds, significantly narrowing the attack window, as studies have shown.

Table 1. AI-Driven Security Performance Metrics

Metric	Traditional Security	AI-Driven Security
Threat Detection Accuracy	85% (rule-based IDS)	98% (AI-based IDS)
Response Time	500 ms (signature-based)	50 ms (AI predictive model)
False Positive Rate	15% (heuristic-based)	5% (AI-powered detection)
Anomaly Detection Capability	Limited (fixed rules)	High (self-learning AI models)

4.2 Case Studies of AI-Based Hardware Security Solutions

This section analyzes industry case studies to evaluate the effectiveness of AI-driven hardware security.

a) Intel SGX and AMD SEV: AI-Powered Enclave Security

Secure enclave protection in hardware is implemented through Intel's Software Guard Extensions (SGX) and AMD's Secure Encrypted Virtualization (SEV), both supported by AI. These technologies utilize machine learning algorithms to detect unauthorized access attempts. AI-enhanced enclave security enables real-time monitoring of sensitive computations, preventing data leaks from side-channel attacks such as Spectre and Meltdown.

b) Microsoft Pluton: AI-Driven Firmware Protection

Microsoft's Pluton security processor integrates AI-driven firmware protection into CPUs. AI is employed to detect firmware tampering, automate firmware patching, and predict potential vulnerabilities. With cloud-based AI analytics, Pluton continuously strengthens hardware security as new threats emerge.

c) AI-Based Hardware Anomaly Detection: Securing Cloud Infrastructure

By deploying adaptive machine learning models, AI-driven anomaly detection significantly enhances cloud infrastructure security. These models continuously monitor and protect against hardware-level attacks [13].

4.3 Effectiveness of AI in Real-Time Threat Prevention

AI-driven security solutions have markedly improved real-time threat prevention by reducing false positives, enhancing automated response mechanisms, and enabling dynamic adaptation to evolving attacks.

a) Reduction in False Positives

Traditional security systems often experience high false positive rates, leading to alert fatigue among security teams. AI-based behavioral analysis models like the Artificial Neural Networks and Bayesian Classifiers improve detection by distinguishing the benign from the malicious activities. This significantly reduces false alarms and helps security teams focus on actual threats.

b) AI's Role in Automated Threat Response and Mitigation

AI's integration into Security Orchestration, Automation, and Response (SOAR) systems facilitate rapid containment of security incidents. This capability is especially valuable for protecting critical hardware components like BIOS, firmware, and chipsets from advanced cyber-physical attacks [14]. AI-driven security solutions continuously learn from evolving threats, enhancing the resilience of real-time prevention systems against complex attacks.

4.4 AI-Driver Security Performance Metrics

a) Limitations and Risks Identified

Despite its benefits, AI-driven hardware security faces limitations such as adversarial AI risks, scalability challenges, and computational overhead.

b) Adversarial AI Risks

Machine learning models used in security systems are vulnerable to exploitation through techniques such as data poisoning and model evasion, which can compromise detection accuracy.

Table 2. Case Studies of AI-Based Hardware Security Solutions

AI-Based Security Solution	Key Features	Impact on Hardware Security
Intel SGX & AMD SEV	AI-secured enclave protection	Secure execution of sensitive data & encrypted memory processing
Microsoft Pluton	AI-driven firmware security	Prevents firmware attacks & enhances secure boot mechanisms
AI-Based Anomaly Detection in Cloud	Monitors real-time hardware behavior	Detects hardware-level intrusions & unauthorized modifications

c) Scalability Concerns

AI-based hardware security demands significant computational resources to operate deep learning models efficiently. This presents challenges for implementation in resource-constrained environments like embedded and IoT devices. Current research efforts are focused on enabling scalable AI-driven anomaly detection in such settings. Additionally, the lack of standardization in AI security frameworks complicates interoperability and trust across different hardware platforms [15]. Addressing the risks are important to secure the future of AI-driven hardware protection as described in Table-2.

5. Discussion

5.1 Comparative Analysis of AI vs. Traditional Hardware Security

Traditional hardware security often relies on static, rule-based mechanisms, including centralized components such as firewalls and intrusion detection/prevention systems. These methods are rigid and not easily adaptable to evolving threats. In contrast, AI-powered security solutions are dynamic and adaptive, requiring continually updated mechanisms tailored to large and varied data use cases as described in Table-3.

a) Strengths of AI-Driven Threat Intelligence

AI-based Intrusion Detection Systems (IDS) and predictive analytics offer a proactive approach to security, intercepting threats before attackers can exploit hardware vulnerabilities [16].

b) Limitations of AI-Based Security:

Despite its advantages, AI also introduces risks. As described in Table-3, its reliance on large datasets makes it susceptible to adversarial manipulation. Attackers can poison training data through adversarial machine learning techniques to deceive and bypass AI-based security models. While AI significantly enhances hardware security, it must be integrated with traditional security mechanisms to compensate for its limitations.

5.2 The Role of AI in Future-Proofing Hardware Security

As cyber threats evolve, the long-term viability of hardware security depends on integrating AI with emerging technologies.

a) AI-Quantum Security Integration

With the emergence of Quantum Computing, traditional cryptographic approaches like RSA and ECC may become obsolete. AI-driven approaches can enhance quantum-resistant cryptography, supporting post-quantum security models and new encryption paradigms.

b) Self-Adaptive AI Security Models

The key advantage of AI is its ability to learn and evolve. Reinforcement learning enables systems to detect and respond to new attack patterns with minimal manual intervention. Self-adaptive AI models can safeguard hardware from emerging threats. Additionally, AI-enabled self-healing mechanisms can automatically roll back compromised firmware, isolate malicious processes, and repair vulnerable code at high speed. These proactive capabilities establish a resilient hardware security posture while minimizing downtime during cyberattacks [17]. The future of hardware security lies in harnessing AI's flexibility and predictive capabilities to stay ahead of increasingly complex and dynamic threats.

Table 3. Limitations and Risks of AI-Driven Security

Limitation	Description	Impact on Security
Adversarial AI Attacks	Attackers manipulate AI models	AI-based IDS can be misled, reducing accuracy.
Computational Overhead	AI models require high processing power	Impacts performance of IoT and low-power devices.
Explainability Issues	AI security decisions are complex	Lack of transparency affects trust in AI security.

5.3 Addressing Trust and Ethical Concerns

The growing role of AI in hardware security introduces concerns related to trust, transparency, and ethical considerations.

a) Transparency in AI Security Decisions

One of the key challenges with AI-driven threat detection is its "black box" nature. AI models make decisions based on complex statistical patterns, making it difficult to explain how and why a particular security outcome was reached.

b) Bias and Fairness in AI Models

AI security systems must avoid biased threat detection that could disproportionately affect certain hardware architectures or user groups. If AI models are trained on biased datasets, they may produce false positives or discriminatory responses. It is essential to use diverse and representative training data to ensure fairness and develop equitable security solutions. Addressing these concerns is crucial to building trust and promoting ethical use of AI in hardware security systems.

5.4 Potential Policy and Regulatory Considerations

The rapid adoption of AI in hardware security underscores the need for global regulatory frameworks and standardized practices [18].

a) The Need for Global AI Security Standards

At present, no universally accepted standard exists for AI-driven hardware security. Although organizations such as ISO/IEC, NIST, and IEEE are developing frameworks, widespread adoption is still lacking.

b) AI-Powered Security Certification Models

To foster trust and ensure compliance, manufacturers should adopt AI-driven security certification models. These models can evaluate hardware components against emerging threats using AI-based assessments. Such standardization will help establish benchmarks for safety and reliability in AI-driven hardware protection, fostering consistency and global trust in AI security systems [19].

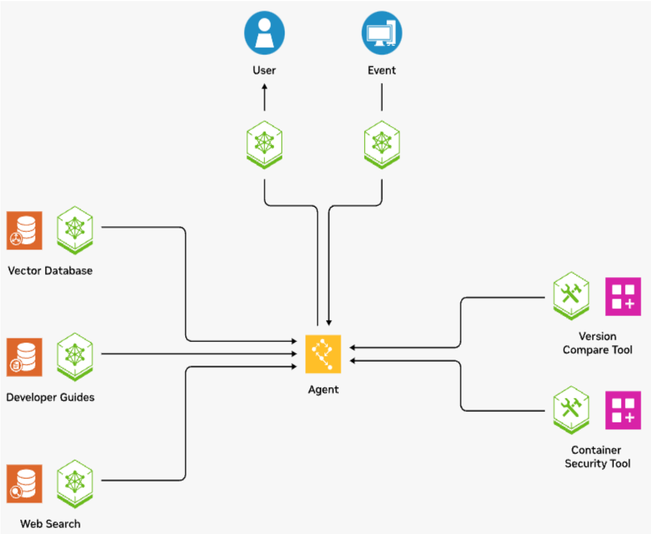

Figure 3. Harnessing Data with AI to Boost Zero Trust Cyber Defense

6. Conclusion and Future Scope

6.1 Summary of Key Findings

Hardware protection is significantly enhanced through AI-based security, utilizing modules such as anomaly detection, predictive analytics, and self-healing mechanisms. However, several challenges persist, including adversarial AI attacks, computational overhead, and a general lack of trust. A major barrier to consistent AI security implementation is the absence of standardized frameworks. Addressing these challenges is essential to ensure AI's reliability in hardware protection.

6.2 Practical Implications

Organizations must adopt AI-enabled security frameworks to safeguard hardware effectively. Implementing real-time, AI-based intrusion detection facilitates a proactive security posture. Future work should focus on reducing AI’s computational burden so that lightweight security models can be deployed on low-powered devices, including IoT systems, embedded hardware, and mobile platforms.

6.3 Future Research Directions

To remain resilient against emerging quantum cyber threats, it is imperative to integrate AI with quantum technologies, forming an AI-Quantum security approach. This integration will help mitigate risks posed by quantum computing and enhance protection through post-quantum cryptography. Additionally, developing lightweight AI security models capable of real-time, on-device threat detection will minimize performance tradeoffs. Future studies should focus on implementing efficient AI solutions that strike a balance between security, computational cost, and overall hardware performance to strengthen cybersecurity resilience.

Data Availability: None.

Conflict of Interest: None.

Funding Source: None.

Authors’ Contributions

All authors have contributed to the discussion, literature survey and methodology of the paper. The Literature survey and methodology were performed by Vasuki Shankar. Nanditha Muralidhar provided the Results and Analysis and the conclusion. The first draft of the paper was written by Vasuki Shankar, and Nanditha Muralidhar commented and provided recommendations before approving the final manuscript.

Acknowledgements: None.

References

[1] S. Rangaraju, "Secure by intelligence: enhancing products with AI-driven security measures," *EPH-International Journal of Science and Engineering*, Vol.9, No.3, pp.36–41, 2023.

[2] G. Waizel, "Bridging the AI divide: The evolving arms race between AI-driven cyber attacks and AI-powered cybersecurity defenses," in *Proc. Int. Conf. Mach. Intell. Secur. Smart Cities (TRUST)*, Vol.1, pp.141–156, 2024.

[3] Y. Gao, "Cyber Attacks and Defense: AI-Driven Approaches and Techniques," *Academic Journal of Computing & Information Science*, Vol.7, No.7, pp.41–46, 2024.

[4] A. Tanikonda, B. K. Pandey, S. R. Peddinti, and S. R. Katragadda, "Advanced AI-Driven Cybersecurity Solutions for Proactive Threat Detection and Response in Complex Ecosystems," *Journal of Science & Technology*, Vol.3, No.1, 2022.

[5] A. McCall, *Cybersecurity in the Age of AI and IoT: Emerging Threats and Defense Strategies*, 2024.

[6] S. Tiwari, W. Sarma, and A. Srivastava, "Integrating Artificial Intelligence with Zero Trust Architecture: Enhancing Adaptive Security in Modern Cyber Threat Landscape," *Int. J. Res. Anal. Rev.*, Vol.9, pp.712–728, 2022.

[7] V. Shankar, “Machine Learning for Linux Kernel Optimization: Current Trends and Future Directions,” *International Journal of Computer Sciences and Engineering*, Vol.13, No.3, pp.56–64, 2025.

[8] S. Ratnayake, *A Comprehensive Review of AI-Driven Optimization, Resource Management, and Security in Cloud Computing Environments*, 2024.

[9] V. Shankar, “Edge AI: A Comprehensive Survey of Technologies, Applications, and Challenges,” in *2024 1st International Conference on Advanced Computing and Emerging Technologies (ACET)*, Ghaziabad, India, pp.1–6, 2024. doi: 10.1109/ACET61898.2024.10730112.

[10] C. K. Ejeofobiri, O. O. Victor-Igun, and C. Okoye, "AI-Driven Secure Intrusion Detection for Internet of Things (IoT) Networks," *Asian J. Math. Comput. Res.*, Vol.31, No.4, pp.40–55, 2024.

[11] Li, H., Sun, J. and Xiong, K., AI-Driven Optimization System for Large-Scale Kubernetes Clusters: Enhancing Cloud Infrastructure Availability, Security, and Disaster Recovery. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023, Vol.2, Issue.1, pp.281-306, 2024.

[12] V. Shankar, M. M. Deshpande, N. Chaitra, and S. Aditi, “Automatic Detection of Acute Lymphoblastic Leukemia Using Image Processing,” in *Proc. 2016 IEEE Int. Conf. Advances in Computer Applications (ICACA)*, Coimbatore, India, pp.186–189, 2016. doi: 10.1109/ICACA.2016.7887948.

[13] V. Shankar, “Advancements in AI-Based Compiler Optimization Techniques for Machine Learning Workloads,” *International Journal of Computer Sciences and Engineering*, Vol.13, No.3, pp.70–77, 2025.

[14] J. Kwon, *Machine Learning for AI-Augmented Design Space Exploration of Computer Systems*. New York, NY, USA: Columbia Univ., 2022.

[15] T. Geng, M. Amaris, S. Zuckerman, A. Goldman, G. R. Gao, and J. L. Gaudiot, “A profile-based AI-assisted dynamic scheduling approach for heterogeneous architectures,” *Int. J. Parallel Program.*, Vol.50, No.1, pp.115–151, 2022.

[16] Salem, A.H., Azzam, S.M., Emam, O.E. and Abohany, A.A., Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. *Journal of Big Data*, Vol.11, Issue.1, pp.105, 2024.

[17] Kaloudi, N. and Li, J., The ai-based cyber threat landscape: A survey. *ACM Computing Surveys (CSUR)*, Vol.53, Issue.1, pp.1-34, 2020.

[18] S. Garg, “Predictive analytics and auto remediation using artificial intelligence and machine learning in cloud computing operations,” *Int. J. Innov. Res. Eng. Multidiscip. Phys. Sci.*, Vol.7, No.2, pp.1–6, 2019. doi: 10.5281/zenodo.14950959.

[19] S. Garg, “Next-gen smart city operations with AIOps & IoT: A comprehensive look at optimizing urban infrastructure,” *J. Adv. Dev. Res.*, Vol.12, No.1, pp.1–14, 2021. doi: 10.5281/zenodo.15049825.

AUTHORS PROFILE

Vasuki Shankar earned his Bachelor of Engineering (B.E) in Electronics and Communication Engineering from Visvesvaraya Technological University (VTU), Karnataka, and his Master of Science in Computer Engineering from the University of Texas at Dallas in 2015 and 2022, respectively. Vasuki is currently a Senior Software Engineer at NVIDIA Corporation, bringing over a decade of experience in system software development. Throughout his career, he has been an active user of the Linux kernel, specializing in operating system design, computer architecture, chip security, and chip bring-up. His expertise has been shaped through roles at leading technology firms, including Qualcomm and Samsung Semiconductor. His research interests include the application of Artificial Intelligence and Machine Learning in computer architecture, operating systems, and Edge AI.

Nanditha Muralidhar earned her Bachelor of Engineering (B.E) from MSRIT in Telecommunication Engineering. She is a Software Engineer with nearly three years of experience at Dell Technologies, skilled in C++, Java, Python, and AI/ML frameworks like TensorFlow and PyTorch. She holds a master’s in computer science with a focus on AI/ML from Vellor Institute of Techology, where she was a Merit Certificate. At Dell, she contributed to enterprise storage solutions and earned the *Inspire Award for Innovation*, the *Inspire Award for Winning Together*, and was a *Local Storage Winner* in the 2023 Dell ISG Hackathon. Her interests include AI applications in system software, storage, and medical imaging, with a focus on innovation and collaborative problem-solving.