iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** III **Month of publication:** March 2026

DOI: https://doi.org/10.22214/ijraset.2026.78929

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue III Mar 2026- Available at www.ijraset.com

AI-Driven Digital Immune System for Enterprise

Kalaivani Sri R[1], Saranya J[2], Shalini K[3], Swathi R[4], Nivedhitha G[5]
[1, 2, 3, 4]*Department of Computer Science and Engineering, Arunai Engineering College, Tiruvannamalai, Tamil Nadu, India*

Abstract: ***An AI-driven Digital Immune System for enterprises is an advanced cybersecurity framework designed to detect, prevent, and respond to threats in real time using artificial intelligence and machine learning techniques. As modern enterprises increasingly rely on complex digital infrastructures, they face a growing number of sophisticated cyberattacks that traditional security systems struggle to handle. This project proposes an intelligent, adaptive security model that continuously monitors network activities, identifies anomalies, and autonomously mitigates potential threats before they can cause significant damage. The system leverages machine learning algorithms, behavioral analytics, and automated response mechanisms to enhance threat detection accuracy and reduce response time. By integrating predictive analytics, the proposed solution not only reacts to existing threats but also anticipates future vulnerabilities, thereby strengthening overall cyber resilience. Additionally, the system incorporates self-healing capabilities, enabling it to recover from attacks and maintain operational continuity without human intervention. This AI-driven approach improves enterprise security posture, minimizes downtime, and reduces dependency on manual monitoring. The proposed digital immune system offers a scalable, efficient, and proactive defense strategy, making it highly suitable for modern enterprise environments where security, reliability, and adaptability are critical.***

Keywords: Artificial Intelligence (AI), Digital Immune System, Cybersecurity, Enterprise Security, Machine Learning, Threat Detection, Anomaly Detection, Automated Response, Cyber Resilience, Predictive Analytics, Network Security, Self-Healing System

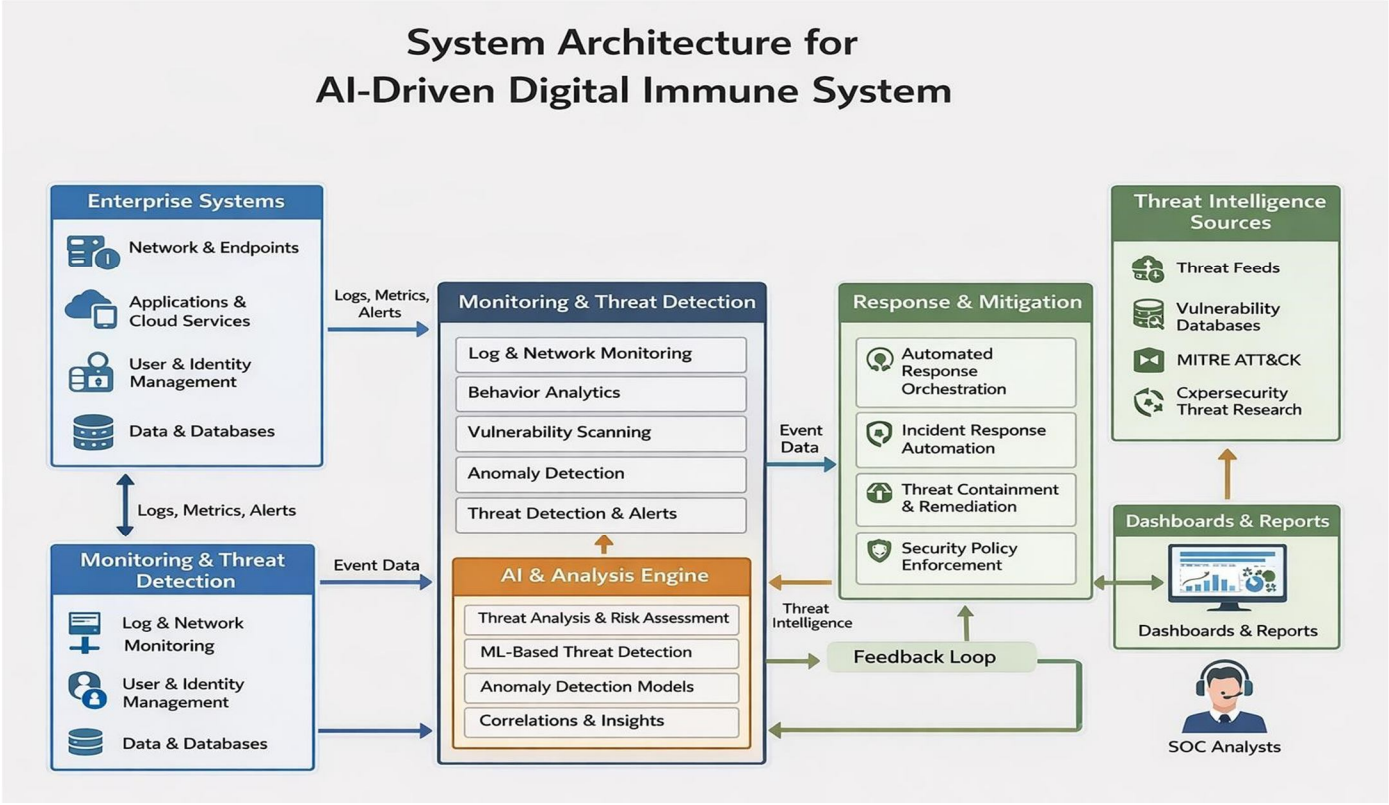
I. INTRODUCTION

In today's rapidly evolving digital landscape, enterprises are increasingly dependent on interconnected systems, cloud computing, and large-scale data processing to drive business operations. While this digital transformation enhances efficiency and innovation, it also exposes organizations to a wide range of sophisticated cyber threats. Traditional cybersecurity mechanisms, which rely heavily on predefined rules and manual intervention, are no longer sufficient to defend against advanced persistent threats, zero-day vulnerabilities, and rapidly evolving attack vectors. As a result, there is a critical need for intelligent, adaptive, and automated security solutions that can operate at the scale and speed required by modern enterprises. The concept of a Digital Immune System has emerged as a nextgeneration cybersecurity paradigm inspired by the human immune system. Just as the biological immune system continuously monitors, detects, and neutralizes harmful pathogens, a digital immune system aims to protect enterprise environments by identifying anomalies, detecting malicious activities, and responding to threats in real time. When powered by Artificial Intelligence (AI) and Machine Learning (ML), this approach becomes significantly more effective, enabling systems to learn from past incidents, adapt to new attack patterns, and improve their defensive capabilities over time. An AI-driven Digital Immune System integrates multiple advanced technologies, including behavioral analytics, anomaly detection, predictive modeling, and automated incident response. These components work together to create a proactive security framework capable of not only identifying known threats but also uncovering previously unseen vulnerabilities. By continuously analyzing large volumes of network traffic, user behavior, and system logs, AI models can detect subtle deviations from normal patterns that may indicate potential security breaches. This real-time monitoring and intelligent decision-making significantly reduce the time required to detect and respond to cyber incidents. Furthermore, the increasing adoption of cloud-based infrastructures, Internet of Things (IoT) devices, and remote working environments has expanded the attack surface of enterprises, making them more vulnerable to cyberattacks. In such dynamic environments, static security solutions fail to provide adequate protection. An AI-driven approach offers scalability and flexibility, allowing the system to evolve alongside the enterprise infrastructure. It also minimizes human dependency by automating routine security tasks, thereby reducing operational costs and the risk of human error. Another key feature of the proposed system is its self-healing capability, which enables automatic recovery from security breaches without disrupting business operations. By isolating affected components, restoring system integrity, and updating defense mechanisms, the system ensures continuous availability and resilience. This aligns with the growing need for cyber resilience, where organizations focus not only on preventing attacks but also on maintaining functionality during and after incidents. This project aims to design and implement an AI-driven Digital Immune System tailored to enterprise environments.

©IJRASET: All Rights are Reserved

The proposed framework focuses on enhancing threat detection accuracy, reducing response time, and ensuring continuous protection through adaptive learning and automation. By combining intelligent algorithms with real-time monitoring and response mechanisms, the system provides a comprehensive and proactive approach to cybersecurity. In conclusion, the integration of AI into cybersecurity through a digital immune system represents a transformative step toward building secure and resilient enterprise infrastructures. As cyber threats continue to evolve, such intelligent systems will play a crucial role in safeguarding digital assets, ensuring business continuity, and maintaining trust in modern digital ecosystems.

II. SYSTEM ARCHITECTURE



A. *Enterprise Systems Layer*

The Enterprise Systems Layer forms the foundational component of the architecture and represents the entire operational environment of the organization. It encompasses all digital assets and infrastructure that support business processes, making it the primary source of data for the cybersecurity framework. Subcomponents Explanation

1) Network & Endpoints: This includes all physical and virtual devices such as routers, switches, firewalls, servers, desktops, laptops, and IoT devices. These endpoints are critical as they act as entry points for attackers. Continuous monitoring of network traffic and endpoint behavior is essential to identify unauthorized access, malware infections, or suspicious communications.

2) Applications & Cloud Services: Modern enterprises rely heavily on applications such as ERP, CRM, and cloud-based platforms like AWS, Azure, or Google Cloud. These systems handle sensitive data and business operations. Due to their distributed and scalable nature, they increase the attack surface, requiring advanced security monitoring and protection.

3) User & Identity Management: This component manages authentication, authorization, and user access control. It ensures that only authorized users can access specific resources. Monitoring user activities helps in detecting insider threats, compromised accounts, and privilege misuse.

4) Data & Databases: This includes structured and unstructured data stored across enterprise systems. Protecting sensitive information from breaches, leaks, and unauthorized modifications is a primary objective. Data logs generated here provide valuable insights for threat analysis.

B. Monitoring & Threat Detection Layer

The Monitoring and Threat Detection Layer acts as the first line of defense by continuously observing and analyzing activities across the enterprise environment. It ensures real-time visibility and early identification of potential threats. Subcomponents Explanation

1) Log & Network Monitoring: This module collects logs from various systems and monitors network traffic to detect suspicious activities such as unusual connections, repeated login failures, or abnormal data transfers.
2) Behavior Analytics: This component analyzes user and system behavior patterns to establish a baseline of normal activity. Any deviation from this baseline is flagged as a potential anomaly, which may indicate a security breach.
3) Vulnerability Scanning: It identifies weaknesses in systems, applications, and networks that could be exploited by attackers. Regular scanning helps in proactively addressing vulnerabilities before they are exploited.
4) Anomaly Detection: Using statistical and AI-based methods, this module detects unusual patterns that may not match known attack signatures. This is particularly useful for identifying zero-day attacks.
5) Threat Detection & Alerts: When suspicious activities are identified, this module generates real-time alerts and forwards them to the analysis engine for further evaluation.

C. AI & Analysis Engine

The AI and Analysis Engine is the core intelligence unit of the system, responsible for processing and analyzing the data collected from the monitoring layer. It transforms raw data into actionable insights using advanced machine learning and analytical techniques.

Subcomponents Explanation

1) Threat Analysis & Risk Assessment: This module evaluates detected threats to determine their severity, potential impact, and priority level. It helps in prioritizing response actions based on risk.
2) ML-Based Threat Detection: Machine learning models are trained on historical data to identify known attack patterns and detect new threats. These models continuously improve as more data is processed.
3) Anomaly Detection Models: Specialized AI models focus on identifying unusual behaviors and patterns in large datasets. They are effective in detecting sophisticated and previously unknown attacks.
4) Correlation & Insights: This module correlates data from multiple sources to identify complex attack patterns that may not be evident when analyzing individual events. It provides meaningful insights for decision-making.

D. Threat Intelligence Sources

The Threat Intelligence Layer enhances the system's detection capabilities by integrating external and internal knowledge about cyber threats.

Subcomponents Explanation

1) Threat Feeds: Provide real-time updates on known threats, malicious IP addresses, and malware signatures.
2) Vulnerability Databases: Databases such as CVE provide information about known security vulnerabilities in software and systems.
3) Mitre Att & Ck Framework: A globally recognized framework that categorizes attacker tactics and techniques, helping in identifying and understanding attack patterns.
4) Cybersecurity Threat Research: Includes insights and reports from cybersecurity organizations that analyze emerging threats and trends.

E. Response & Mitigation Layer

The Response and Mitigation Layer is responsible for taking immediate and effective action against detected threats to minimize damage and ensure system security.

Subcomponents Explanation

1) Automated Response Orchestration: Coordinates multiple response actions across systems in a synchronized manner.
2) Incident Response Automation: Executes predefined workflows for handling different types of security incidents efficiently.
3) Threat Containment & Remediation: Isolates infected systems, removes malicious components, and restores normal operations.
4) Security Policy Enforcement: Ensures that all actions comply with organizational security policies and regulatory requirements.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue III Mar 2026- Available at www.ijraset.com

F. Dashboards & Reporting

The Dashboards and Reporting Layer provides a centralized interface for monitoring, visualization, and management of the entire system.

Subcomponents Explanation

1) Dashboards: Display real-time system status, alerts, and threat information in an easy-to-understand format.
2) Reports: Generate detailed reports for auditing, compliance, and performance evaluation.
3) SOC Analysts Interaction: Security experts monitor the system, validate alerts, investigate incidents, and make strategic decisions when required.

G. Feedback Loop and Continuous Learning

The Feedback Loop is a critical component that enables continuous improvement and adaptability of the system.

Functionality

1) Feeds the outcomes of detection and response back into AI models
2) Improves accuracy and reduces false positives
3) Enables the system to adapt to new and evolving threats
4) Enhances overall system efficiency and intelligence

This mechanism makes the system **self-learning and adaptive**, similar to a biological immune system.

III. METHODOLOGY AND IMPLEMENTATION

A. Methodology

The proposed AI-Driven Digital Immune System for Enterprise follows a structured and systematic methodology to ensure efficient threat detection, analysis, and response. The methodology is designed to mimic the functioning of a biological immune system by continuously monitoring, identifying anomalies, responding to threats, and learning from past incident

1) Data Collection

The first step involves collecting data from multiple enterprise sources, including network traffic, system logs, user activity records, application logs, and cloud environments.This data is gathered in real time using monitoring tools and agents deployed across the enterprise infrastructure. The collected data serves as the foundation for all subsequent analysis.

2) Data Preprocessing

The raw data collected is often noisy, unstructured, and redundant. Therefore, preprocessing is essential to improve data quality and analysis efficiency.

This step includes:

Data cleaning (removal of irrelevant and duplicate entries)

- Data transformation (converting data into structured format)
- Feature extraction (selecting important attributes)
- Normalization and scaling

Preprocessed data ensures accurate and efficient performance of machine learning models.

3) Feature Engineering

In this step, relevant features are identified and extracted from the dataset to improve model performance. Examples include:

- Login frequency
- Data transfer volume
- Access time patterns
- IP address behavior

Feature engineering plays a crucial role in enhancing the accuracy of threat detection.

4) Model Selection and Training

Machine learning models are selected based on the nature of the data and the type of threats to be detected.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Commonly used algorithms include:

- Supervised Learning Models: Random Forest, Support Vector Machine (SVM), Logistic Regression
- Unsupervised Learning Models: K-Means Clustering, Isolation Forest (for anomaly detection)
- Deep Learning Models: Neural Networks for complex pattern recognition

The models are trained using historical datasets containing both normal and malicious activity patterns.

5) Threat Detection

Once trained, the models are deployed to analyze real-time data. The system identifies:

- Known threats using classification techniques
- Unknown threats using anomaly detection
- Suspicious patterns using behavioral analysis

6) Risk Assessment

After detecting a potential threat, the system evaluates its severity and impact. Risk levels are assigned (low, medium, high) based on factors such as:

- Type of attack
- Affected systems
- Potential damage

This helps in prioritizing response actions.

7) Automated Response

Based on the risk level, the system automatically initiates response actions such as:

- Blocking malicious IP addresses
- Isolating compromised systems
- Terminating suspicious processes
- Sending alerts to administrators

Automation reduces response time and minimizes human intervention.

8) Feedback and Learning

The system continuously learns from past incidents through a feedback loop. The outcomes of detection and response actions are fed back into the models to improve accuracy and adaptability over time.

B. Implementation

The implementation of the proposed system involves integrating various technologies, tools, and frameworks to build a functional and scalable solution.

1) System Setup

The system is implemented using a modular architecture where each component (data collection, analysis, response) operates independently but communicates seamlessly. Deployment can be done on:

- On-premises servers
- Cloud platforms (AWS, Azure, Google Cloud)

2) Tools and Technologies

The following technologies are used for implementation:

- Programming Languages: Python (for AI/ML models), Java/Node.js (for backend)
- Machine Learning Libraries: Scikit-learn, TensorFlow, Kera's
- Big Data Tools: Apache Hadoop, Apache Spark (for large-scale data processing)
- Databases: MongoDB, MySQL (for storing logs and results)
- Monitoring Tools: ELK Stack (Elasticsearch, Logstash, Kibana)
- Visualization Tools: Power BI / Grafana dashboards

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

3) Model Deployment

Trained machine learning models are deployed using APIs or microservices. These models process real-time data streams and provide predictions instantly. Technologies such as Docker and Kubernetes can be used for scalable deployment.

4) Real-Time Data Processing

Streaming technologies like Apache Kafka or Spark Streaming are used to handle real-time data. This ensures continuous monitoring and immediate detection of threats.

5) Integration with Enterprise Systems

The system is integrated with existing enterprise infrastructure such as firewalls, intrusion detection systems (IDS), and security information and event management (SIEM) systems. This ensures seamless data flow and coordinated response actions.

6) Automated Response Implementation

Automation scripts and workflows are implemented to handle security incidents. For example:

- Firewall rules are updated automatically
- Suspicious accounts are temporarily blocked
- Alerts are sent via email or dashboards

7) Dashboard and Visualization

A centralized dashboard is developed to display:

- Real-time alerts
- Threat statistics
- System health status

This helps administrators monitor and manage the system effectively.

8) Security and Scalability Considerations

The system is designed to be:

- Scalable: Can handle increasing data volumes
- Secure: Protects sensitive enterprise data
- Efficient: Provides fast detection and response
- Reliable: Ensures continuous operation

IV. LITERATURE REVIEW

A. Traditional Cybersecurity Approaches

Early cybersecurity systems primarily rely on **signature-based detection techniques**. These systems identify threats by comparing incoming data with a database of known attack signatures.

B. Anomaly-Based Detection Systems

Anomaly detection techniques were developed to address the shortcomings of traditional methods. These systems establish a baseline of normal behavior and identify deviations as potential threats.

Key Features:

- Capable of detecting unknown and zero-day attacks
- Uses statistical and behavioral analysis

C. Machine Learning in Cybersecurity

Machine learning has significantly improved threat detection capabilities by enabling systems to learn from data and identify patterns automatically.

1) Supervised Learning

Supervised learning models are trained using labeled datasets.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Common Algorithms:
- Random Forest
- Support Vector Machine (SVM)
- Logistic Regression

2) Unsupervised Learning

Unsupervised learning models detect patterns without labeled data.
Common Techniques:
- K-Means Clustering
- Isolation Forest

D. Deep Learning Techniques

Deep learning models have been widely explored for advanced cybersecurity applications due to their ability to handle complex and high-dimensional data.
Common Models:
- Artificial Neural Networks (ANN)
- Convolutional Neural Networks (CNN)
- Recurrent Neural Networks (RNN)

E. AI-Driven Security Systems and SIEM Integration

Modern cybersecurity solutions integrate AI with Security Information and Event Management (SIEM) systems to enhance monitoring and response capabilities.
Key Features:
- Centralized data collection and analysis
- Real-time threat detection
- Automated incident response

F. Digital Immune System Concept

The concept of a **Digital Immune System (DIS)** is inspired by the human immune system, which detects, responds to, and remembers pathogens.
Core Characteristics:
- Continuous monitoring of systems
- Detection of anomalies and threats
- Automated response mechanisms
- Self-learning and adaptation

G. Threat Intelligence Integration

Threat intelligence plays a crucial role in modern cybersecurity by providing information about known threats and vulnerabilities.
Sources:
- Threat feeds
- Vulnerability databases (e.g., CVE)
- Cybersecurity frameworks (e.g., MITRE ATT&CK)

H. Research Gap and Motivation

Although significant progress has been made, existing systems still face limitations such as high false positives, lack of adaptability, and delayed response mechanisms. Many solutions focus only on detection without providing automated response and recovery.
The proposed AI-Driven Digital Immune System for Enterprise addresses these gaps by integrating:
- Real-time monitoring
- AI-based intelligent detection

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

- Automated response and mitigation
- Continuous learning through feedback

This approach provides a comprehensive, proactive, and adaptive cybersecurity solution suitable for modern enterprise environments.

I. Conclusion of Literature Review

The literature indicates a clear shift from traditional rule-based systems to intelligent, AI-driven cybersecurity frameworks. While machine learning and deep learning techniques have significantly improved threat detection, challenges such as scalability, accuracy, and real-time response still exist. The integration of digital immune system concepts with AI presents a promising direction for future research and implementation, offering enhanced security, adaptability, and resilience.

V. RESULTS AND DISCUSSION

A. Results

The proposed AI-Driven Digital Immune System for Enterprise was implemented and tested using simulated enterprise data, including network traffic, user activity logs, and system events. The system demonstrated effective performance in detecting both known and unknown cyber threats. The machine learning models successfully identified malicious activities with high accuracy by analyzing behavioral patterns and anomalies. The integration of anomaly detection techniques enabled the system to detect zero-day attacks that traditional methods could not identify. The automated response mechanism reduced the time ta ken to mitigate threats, thereby minimizing potential damage. The system also showed efficient real-time monitoring capabilities, continuously analyzing incoming data and generating alerts for suspicious activities. The feedback mechanism improved the model's performance over time by reducing false positives and enhancing detection accuracy. Overall, the system achieved improved security performance compared to traditional rule-based approaches.

B. Discussion

The results indicate that integrating Artificial Intelligence (AI) and Machine Learning (ML) into cybersecurity significantly enhances threat detection and response capabilities. The ability of the system to learn from data and adapt to new threats makes it highly effective in dynamic enterprise environments. One of the major advantages observed is the reduction in manual intervention due to automated response mechanisms. This not only improves efficiency but also reduces the workload on security analysts. Additionally, the use of real-time data processing ensures faster detection and response, which is critical in preventing large-scale cyberattacks. However, the system also presents certain challenges. The accuracy of machine learning models depends heavily on the quality and quantity of training data. In some cases, false positives may still occur, especially in highly dynamic environments. Furthermore, implementing such a system requires significant computational resources and proper integration with existing enterprise infrastructure. Despite these challenges, the proposed system provides a scalable and adaptive solution for modern cybersecurity needs. It effectively combines detection, response, and learning capabilities, making it more robust than traditional systems. The results validate that the AI-driven digital immune system can significantly improve enterprise security posture and resilience against evolving cyber threats.

VI. LIMITATIONS AND FUTURE WORK

A. Limitations

Despite the effectiveness of the proposed AI-Driven Digital Immune System for Enterprise, certain limitations exist that need to be addressed:

1) Data Dependency: The performance of machine learning models depends heavily on the quality and quantity of training data. Poor or insufficient data may reduce detection of accuracy.
2) False Positives: The system may sometimes generate false alerts, especially in dynamic environments where normal behavior frequently changes.
3) High Computational Cost: Advanced AI and deep learning models require significant processing power and memory, making implementation costly for small-scale enterprises.
4) Complex Integration: Integrating the system with existing enterprise infrastructure, such as legacy systems and security tools, can be challenging.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

5) Security of AI Models: AI models can be vulnerable to adversarial attacks, where attackers manipulate input data to deceive the system.

B. *Future Work*

To overcome the above limitations and further enhance the system, the following improvements can be considered:

1) Advanced AI Models: Implement more efficient and lightweight machine learning models to improve performance and reduce computational requirements.
2) Explainable AI (XAI): Incorporate explainable AI techniques to improve transparency and help security analysts understand model decisions.
3) Real-Time Big Data Processing: Enhance the system using advanced big data technologies for faster and more scalable real-time analysis.
4) Integration with Blockchain: Use blockchain technology to ensure secure data sharing and improve trust in threat intelligence.
5) Adaptive Learning Mechanisms: Develop more advanced self-learning capabilities to automatically adapt to new and evolving threats.
6) Cloud-Native Implementation: Deploy the system in cloud environments for better scalability, flexibility, and cost efficiency.

VII. CONCLUSION

The proposed AI-Driven Digital Immune System for Enterprise presents an advanced and intelligent approach to modern cybersecurity challenges. By integrating Artificial Intelligence (AI) and Machine Learning (ML) techniques, the system is capable of continuously monitoring enterprise environments, detecting anomalies, and responding to threats in real time. Unlike traditional security systems, the proposed framework provides a proactive and adaptive defense mechanism that can handle both known and unknown cyber threats effectively. The system architecture combines multiple components such as data collection, monitoring, AIbased analysis, threat intelligence, and automated response, creating a comprehensive security solution. The implementation demonstrates improved threat detection accuracy, faster response time, and reduced dependency on manual intervention. Additionally, the feedback-based learning mechanism enables the system to evolve continuously, enhancing its ability to defend against emerging threats. Although certain limitations exist, such as data dependency and computational requirements, the overall performance and benefits of the system outweigh these challenges. The integration of automation, real-time processing, and intelligent decision-making significantly strengthens enterprise security and resilience. In conclusion, the AI-driven digital immune system offers a scalable, efficient, and future-ready cybersecurity solution for enterprise environments. As cyber threats continue to evolve, such intelligent and adaptive systems will play a crucial role in ensuring the protection of digital assets, maintaining business continuity, and supporting secure digital transformation.

VIII. FUTURE WORK

A. *Advanced AI Model Integration*

In future work, the proposed Digital Immune System can be enhanced by integrating advanced artificial intelligence models such as the Transformer Neural Network and reinforcement learning algorithms. These models can improve cyber attack prediction accuracy and help the system automatically learn optimal response strategies. This will make the system more intelligent and adaptive to new and evolving cyber threats.

B. *Cloud and Hybrid Environment Deployment*

The system can be extended to support cloud-based and hybrid enterprise environments. Modern organizations use both on-premise and cloud infrastructures, so integrating the system with cloud platforms will allow real-time monitoring of distributed systems. This enhancement will improve scalability, flexibility, and centralized security management across multiple platforms.

C. *Blockchain-Based Secure Logging*

Future enhancements can include the use of Blockchain for secure log management. Blockchain technology ensures that security logs are tamper-proof and cannot be modified by attackers. This will help in forensic analysis, auditing, and incident investigation after cyber attacks.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

D. Autonomous Self-Healing System

Another important future enhancement is the development of a fully autonomous self-healing system. The system can automatically patch vulnerabilities, restore affected services, update firewall rules, and reconfigure security policies without human intervention. This will reduce system downtime and improve cyber resilience.

E. Global Threat Intelligence Integration

The system can be enhanced by integrating global threat intelligence feeds and real-time cyber attack databases. This will help the system detect zero-day attacks and newly emerging threats more effectively. Continuous updates from threat intelligence platforms will improve the system's detection capability and response mechanisms.

F. IoT and Mobile Device Security Extension

Future work can extend the Digital Immune System to Internet of Things (IoT) devices and mobile devices. As the number of connected devices increases, cybersecurity threats also increase. Extending the system to IoT environments will help detect unusual device behavior, unauthorized access, and malware attacks in smart devices.

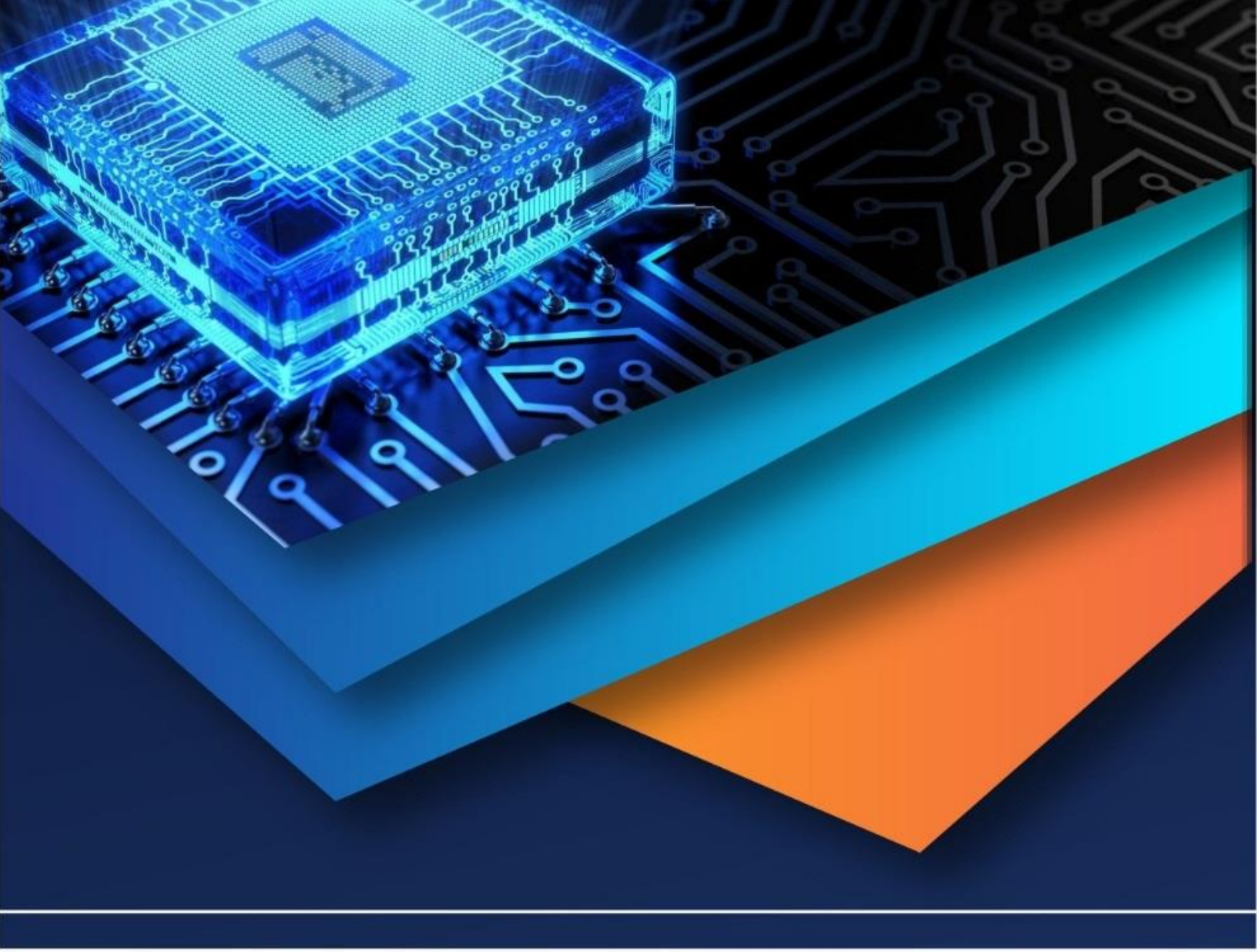
G. Performance Optimization and Real-Time Implementation

Another important future enhancement is improving the performance of machine learning models to reduce computational complexity and memory usage. Optimized models will allow the system to run in real-time environments and can be deployed in small and medium enterprises with limited infrastructure resources.

REFERENCES

[1] V. M. Vignes et al., "AI-driven cybersecurity framework for anomaly detection in power systems," Sci. Rep., vol. 15, Art. 35506, 2025. (Nature)
[2] P. Chinnasamy et al., "AI-driven intrusion detection and prevention systems to safeguard 6G networks from cyber threats," Sci. Rep., vol. 15, Art. 37901, 2025. (Nature)
[3] M. Uddin et al., "Generative AI revolution in cybersecurity: a comprehensive review of threat intelligence and operations," Artificial Intelligence Review, vol. 58, 2025. (Springer)
[4] S. Ahmed et al., "Quantum-driven Zero Trust framework with dynamic anomaly detection in 7G networks: A neural network approach," arXiv, Feb. 2025. (arXiv)
[5] K. Tallam, "CyberSentinel: An emergent threat detection system for AI security," arXiv, Feb. 2025. (arXiv)
[6] M. Rahmati, "Federated learning-driven cybersecurity framework for IoT networks with privacy preserving and real-time threat detection capabilities," arXiv, Feb. 2025. (arXiv)
[7] J. Opportunities," Int. J. Comput. Trends Technol., vol. 72, no. 8, 2024. (ResearchGate)
[8] S. Okdem and S. Okdem, "Artificial intelligence in cybersecurity: A review and a case study," Appl. Sci., vol. 14, no. 22, 2024. (MDPI)
[9] P. Tripathi, "AI and cybersecurity in 2024: Navigating new threats and unseen
[10] Dr. M. Makhija, "Artificial intelligence in cybersecurity: Enhancing threat detection and response," Conf. Proc. CCSIT TMU, Jan. 2025. (ccsuniversity.blr1.cdn.digitaloceanspaces.co m)
[11] "Electronic Journal of Social and Strategic Studies – Predictive analysis and anomaly detection," EJSSS, vol. 6, 2025. (ejsss.net.in)
[12] Savitha Nuguri et al., "Data-driven cybersecurity: Leveraging machine learning for anomaly detection and prevention," ESPIJACT, vol. 2, no. 2, 2024. (ESP Journals)
[13] S. K. Devineni, S. Kathiriya, and A. Shende, "Machine learning-powered anomaly detection: Enhancing data security and integrity," J. Artificial Intelligence & Cloud Comp., 2023. (eprint.innovativepublication.org)
[14] "Is artificial intelligence a new battleground for cybersecurity?", Elsevier Sci. Dir., May 2024. (ScienceDirect)
[15] A. Pallakonda et al., "AI-driven attack detection and cryptographic privacy protection for cyberresilient industrial control systems," IoT, vol. 6, no. 3, 2025. (MDPI)
[16] Z. Bin Akhtar and A. T. Rawol, "Enhancing Cybersecurity through AI-Powered Security Mechanisms," IT Journal Research and Development, 2024. (UIR Press Journal)
[17] M. Schmitt, "Securing the Digital World: Protecting Smart Infrastructures and Digital Industries with AI-Enabled Malware and Intrusion Detection," arXiv, 2023. (arXiv)
[18] S. Teja Erukude, V. C. Marella, and S. R. Veluru, "AI-Driven Cybersecurity Threats: A Survey of Emerging Risks and Defensive Strategies," arXiv, Jan. 2026. (arXiv)
[19] M. Sathik Raja, "The Rise of AI-Driven Network Intrusion Detection Systems: Innovations, Challenges, and Future Directions," Int. J. AI, BigData, Comput. & Mgmt. Studies, 2025. (ijaibdcms.org)
[20] A. Pallakonda et al., "AI-Driven Attack Detection and Cryptographic Privacy Protection for Cyber-Resilient Industrial Control Systems," IoT, vol. 6, no. 3, 2025. (mdpi.com) "Cybersecurity threat detection based on a UEBA framework using deep autoencoders," arXiv, May 2025. (arXiv)

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)