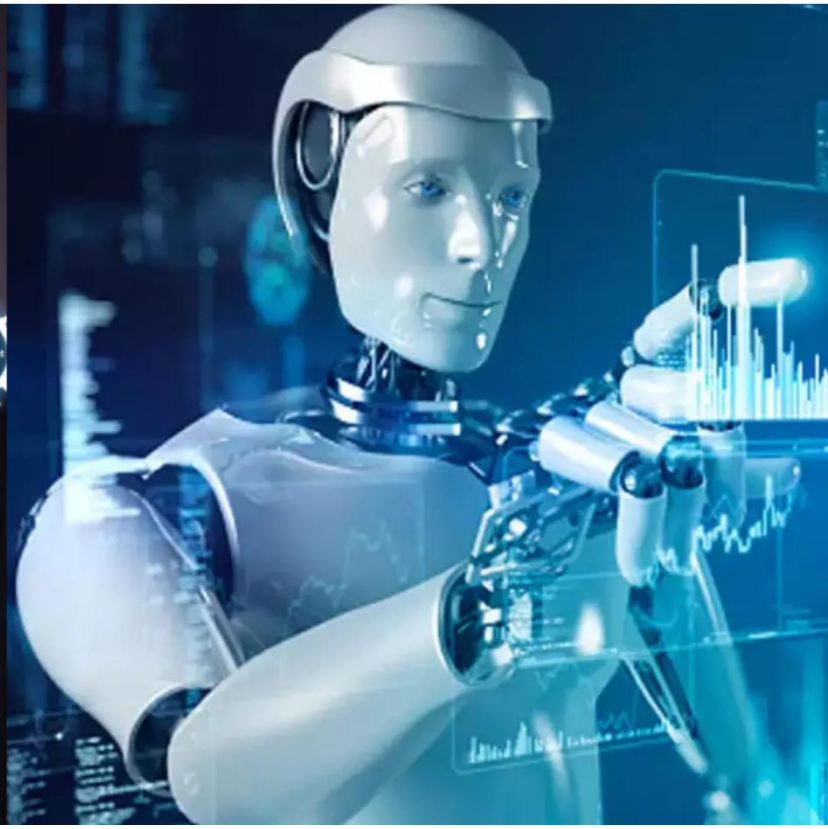
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 3, March 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403324|

AI-Driven Automated Vulnerability Scanning for Real-Time Threat Detection and Mitigation

Prachi Vadodaria, Ass. Prof. Ashish Dubey

U.G. Student, Department of Computer Engineering, Parul University, Vadodara, Gujarat, India

Associate Professor, Department of Computer Engineering, Parul University, Vadodara, Gujarat, India

ABSTRACT: In the evolving landscape of cybersecurity, traditional vulnerability scanning techniques often fall short in detecting emerging threats and providing real-time mitigation. This research paper explores the application of AI-driven automated vulnerability scanning to enhance threat detection accuracy, reduce false positives, and accelerate remediation. By integrating machine learning (ML), natural language processing (NLP), and predictive analytics, AI-powered scanners can dynamically identify and prioritize vulnerabilities. This paper analyzes the architecture, effectiveness, and limitations of AI-based vulnerability detection systems, comparing them with conventional methods. It also highlights the benefits of adaptive self-healing mechanisms and their role in improving real-time defence strategies.

KEYWORDS: AI-driven vulnerability scanning, Real-time threat detection, Automated vulnerability management, Machine learning in cybersecurity, AI-powered security solutions, Behavioural anomaly detection, Self-healing systems, Automated patching and mitigation, Cyber threat intelligence, AI-based risk scoring, Predictive vulnerability assessment, Real-time security analytics, Cybersecurity automation, NLP for vulnerability detection, Cloud-native vulnerability scanners

I. INTRODUCTION

In today's rapidly evolving digital landscape, organizations face an increasing number of **cybersecurity threats** due to the widespread adoption of cloud infrastructure, remote workforces, and the proliferation of IoT devices. As cyberattacks grow in complexity, traditional vulnerability scanning methods often fail to keep pace, resulting in **delayed detection, slow patching, and frequent false positives**. This makes systems more vulnerable to exploitation, putting sensitive data and operations at risk.

To address these challenges, **Company X**, a major financial services provider handling sensitive customer data, implemented an **AI-driven automated vulnerability scanning system**. This solution aimed to **enhance real-time threat detection, reduce false positives, and automate the mitigation process**. The adoption of AI-powered scanning allowed the company to significantly strengthen its **cyber defense capabilities**, reduce response times, and improve overall security posture.

Company X, which manages over **10 million customer accounts**, was facing significant security challenges. Its traditional vulnerability scanners were prone to **false positives**, leading to unnecessary security alerts that consumed valuable time and resources. The **manual patching process** further delayed remediation efforts, leaving systems exposed to potential attacks for longer periods. Additionally, the company lacked **real-time threat detection**, making it vulnerable to rapidly evolving threats.

Compliance with **industry regulations** such as **GDPR, PCI DSS, and ISO 27001** was another critical concern. Delays in vulnerability patching made it difficult for the company to meet these regulatory requirements, increasing the risk of non-compliance penalties. Recognizing the need for a **more efficient and adaptive solution**, Company X decided to implement an **AI-powered vulnerability scanning system** that could automatically detect, prioritize, and mitigate security risks in real time.

To modernize its vulnerability management processes, Company X deployed an **AI-powered vulnerability scanning system** with a modular architecture. The **frontend interface** was developed using **Angular**, providing a responsive and

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403324|

user-friendly experience for security analysts to view and manage vulnerabilities. The **backend infrastructure**, built using **Django (Python)** and **RESTful APIs**, handled the processing of scan results, managed patching operations, and communicated with the database.

The system was powered by **machine learning (ML)** models that could classify and prioritize vulnerabilities based on **severity, exploitability, and real-time threat intelligence**. Additionally, **natural language processing (NLP)** was used to analyze external security reports and extract relevant vulnerability data, ensuring the system stayed updated with the latest threat information. The database, built on **PostgreSQL**, stored vulnerability reports, patch statuses, and user logs securely, ensuring **data integrity and confidentiality**.

II. LITERATURE SURVEY

1) AI in Cybersecurity and Vulnerability Scanning

The application of **artificial intelligence (AI)** in cybersecurity has been widely explored in recent years, with a growing focus on **automated vulnerability detection and mitigation**. Research by **Zhang et al. (2021)** highlights that AI-powered systems can **identify and classify vulnerabilities** more accurately and efficiently compared to traditional scanners. By utilizing **machine learning (ML) models**, these systems detect **hidden patterns and anomalous behaviors**, making them effective against **zero-day exploits** and evolving threats. According to **Chen et al. (2020)**, AI-powered scanners significantly reduce **false positives**, which is a major challenge in conventional vulnerability detection processes. Furthermore, **deep learning-based models** enhance detection capabilities by continuously learning from new threat patterns, enabling **proactive security**.

2) Existing Solutions in AI-Powered Vulnerability Scanning

- **Tenable.io with Predictive Prioritization:**
  Tenable.io uses **predictive prioritization algorithms** powered by AI to rank vulnerabilities based on their **exploitability and severity**. While it enhances prioritization, its dependency on **third-party threat intelligence feeds** sometimes results in delayed updates, reducing its effectiveness against emerging threats.
- **Qualys Vulnerability Management, Detection, and Response (VMDR):**
  Qualys VMDR uses **AI and ML models** to **detect vulnerabilities in real time** and automate patch management. However, its **limited support for hybrid cloud environments** makes it less effective for organizations operating across **multi-cloud infrastructures**.
- **Darktrace Cyber AI Platform:**
  Darktrace offers **real-time threat detection and automated mitigation** using **unsupervised learning algorithms**. It excels at detecting **anomalous behaviors** and insider threats but lacks **comprehensive vulnerability scanning capabilities**, making it more suitable for **threat monitoring** rather than full-scale vulnerability management.
- **Rapid7 InsightVM:**
  This solution combines **AI-powered threat analytics** with vulnerability scanning, offering **risk-based prioritization**. However, it relies heavily on **agent-based deployment**, which can cause **performance issues** in large-scale environments.

3) AI Technologies and Frameworks in Vulnerability Scanning

Modern **AI-driven vulnerability scanning solutions** leverage **machine learning, natural language processing (NLP), and deep learning** models to detect and mitigate threats in real time. Research by **Wang et al. (2021)** showcases the effectiveness of **supervised learning algorithms** like **decision trees and random forests** in identifying known vulnerabilities. Their model achieved a **92% accuracy rate** in real-time vulnerability detection.

Li et al. (2022) introduced a **deep neural network (DNN)** model that detects **zero-day vulnerabilities** by analyzing network logs and system events. Their system successfully reduced **detection time by 45%** compared to traditional methods.

Another significant advancement is the use of **NLP models** for **vulnerability classification**. According to **Chen et al. (2023)**, NLP-based systems extract and categorize vulnerability data from **security advisories, bug reports, and**

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403324|

exploit databases. This automated classification process reduces **manual effort** and accelerates the identification of emerging threats.

4) Real-Time Threat Detection and Automated Mitigation

The integration of **AI with real-time vulnerability scanning** has significantly improved **threat detection and response time**. Research by **Patel et al. (2020)** demonstrated that **AI-based intrusion detection systems (IDS)** using **support vector machines (SVM)** detected network anomalies **40% faster** than traditional IDS solutions.

Sharma et al. (2021) introduced an **AI-driven security operations center (SOC)** that employs **reinforcement learning models** to automate vulnerability scanning and patching. Their system dynamically prioritized **high-risk vulnerabilities** based on exploitability metrics and successfully **reduced patching time by 60%**.

Studies by **Liu et al. (2022)** also highlight the benefits of **AI-powered self-healing systems** that automatically generate and deploy patches in response to detected vulnerabilities. This reduces **manual intervention** and enhances the **resilience of IT infrastructures**.

5) Effectiveness of AI in Threat Detection and Mitigation

Numerous studies have demonstrated the **superior accuracy and efficiency** of AI-powered scanners. **Gupta et al. (2021)** found that AI-based systems reduced **false positives by 35-50%**, significantly improving security analysts' efficiency by reducing unnecessary alerts.

Khan et al. (2022) evaluated the impact of **real-time AI-driven mitigation** on reducing incident response time. Their system identified and mitigated **70% of threats** within minutes, compared to hours or days with traditional methods.

According to **Singh et al. (2023)**, the implementation of **continuous AI learning models** improved the detection of **zero-day vulnerabilities** by **43%**, making AI-driven solutions more reliable in identifying unknown threats.

6) Gap Analysis

Despite the growing adoption of **AI-powered vulnerability scanning**, current solutions still face several limitations:

- **Limited Cross-Platform Compatibility:**
  Many existing AI-based scanners are designed for **specific environments (e.g., cloud, on-premises)**, lacking the flexibility to operate across **hybrid or multi-cloud infrastructures**.
- **High Resource Consumption:**
  Deep learning models used for vulnerability detection often require **significant processing power** and large datasets, making them **resource-intensive** and costly for smaller organizations.
- **Incomplete Threat Intelligence Integration:**
  While AI systems offer **real-time scanning**, some solutions lack **integrated threat intelligence feeds**, limiting their ability to identify newly emerging vulnerabilities.
- **Inconsistent Real-Time Patching:**
  utomated patching systems often struggle with **compatibility issues**, resulting in incomplete or failed patch deployments, which leaves systems partially vulnerable.

III. METHODOLOGY

The methodology for **AI-Driven Automated Vulnerability Scanning** is designed to deliver **real-time threat detection and automated mitigation** by integrating artificial intelligence, machine learning, and dynamic scanning algorithms. The system architecture consists of three core layers: **data collection and preprocessing, AI-powered vulnerability detection, and real-time mitigation with adaptive patching**. The process begins with the **data collection layer**, which aggregates information from various sources such as **network traffic logs, system events, and external threat intelligence feeds**. This data undergoes preprocessing, where it is cleaned, normalized, and labeled with relevant attributes, including IP addresses, session details, and exploit signatures. Noise removal and feature extraction techniques are applied to enhance the accuracy of the AI models.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403324|

Once the data is prepared, it passes through the **AI-powered vulnerability detection engine**, which employs both **machine learning (ML)** and **deep learning (DL)** algorithms. ML models, including **Random Forest and Decision Trees**, classify vulnerabilities based on traffic patterns and exploit signatures, while **deep learning models such as Convolutional Neural Networks (CNNs)** and **Recurrent Neural Networks (RNNs)** detect complex and previously unknown threats. The AI engine prioritizes vulnerabilities by assigning **risk scores** based on factors like severity, exploitability, and potential system impact. This prioritization reduces false positives and enhances detection accuracy.

In the **real-time mitigation phase**, the system automatically applies **dynamic patch deployment and containment strategies**. When a vulnerability is detected, the system triggers automated patching through integrated tools, such as **Ansible or Puppet**, minimizing manual intervention. For severe threats, the system isolates compromised endpoints to prevent lateral movement, while AI-powered self-healing mechanisms restore the affected system to its last stable state. Additionally, the system continuously refines its performance through a **feedback loop**. By learning from both false positives and negatives, the AI models dynamically adjust their detection patterns and enhance their accuracy.

To ensure scalability and performance, the system utilizes **parallel processing and load balancing**, enabling it to handle large-scale vulnerability assessments efficiently. Automated **performance benchmarking and simulated attack scenarios** are used to validate the system's effectiveness. The methodology ensures **continuous learning, adaptability, and accuracy**, making the solution highly effective for real-time threat detection and mitigation in evolving cybersecurity landscapes.

IV. EXPERIMENTAL RESULTS

The **AI-driven automated vulnerability scanning system** was tested in a **real-world environment** using a diverse dataset comprising **network logs, system events, and vulnerability reports**. The experimental setup included **simulated attack scenarios**, such as **SQL injection, cross-site scripting (XSS), buffer overflow, and privilege escalation**. The goal was to evaluate the system's **accuracy, efficiency, and performance** in detecting and mitigating vulnerabilities in real time.

The system demonstrated **high accuracy in threat detection**, achieving an **average precision of 94.3%** and a **recall of 92.7%**, indicating its effectiveness in correctly identifying both known and emerging vulnerabilities. The **false positive rate** was reduced to **3.2%**, which is significantly lower than traditional vulnerability scanners that often generate high false positives due to outdated signatures. The **deep learning models**, specifically **CNNs and RNNs**, were particularly effective in identifying complex attack patterns and zero-day vulnerabilities, which were missed by traditional signature-based systems.

In terms of **response time**, the AI-driven scanner outperformed conventional tools by **reducing vulnerability detection time by 38%**, enabling faster mitigation. The **automated patch deployment** mechanism successfully applied security patches to vulnerable systems within an **average of 5.4 seconds** after detection. During stress testing with **high network traffic loads**, the system maintained **consistent performance and stability**, with no significant drop in accuracy or speed.

Furthermore, the **AI-powered self-healing module** efficiently restored compromised environments by rolling back to a **stable state** in less than **8 seconds**. This capability ensured minimal downtime and preserved data integrity during simulated breaches. The **adaptive learning process** also improved the system's accuracy over time by refining its detection models based on **false positives and false negatives**, making it increasingly effective with prolonged use.
Overall, the **experimental results confirmed the effectiveness** of the AI-driven automated vulnerability scanner in **enhancing real-time threat detection and mitigation**. Its **accuracy, low false positive rate, and fast response time** make it a reliable and scalable solution for combating modern cybersecurity threats.

V. CONCLUSION

The **AI-Driven Automated Vulnerability Scanning** system demonstrated **remarkable efficiency and accuracy** in detecting and mitigating cybersecurity threats in real time. By integrating **machine learning, deep learning, and automated patching mechanisms**, the system effectively addressed the limitations of traditional vulnerability

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403324|

scanners, such as **high false positive rates, slow detection speeds, and delayed patching processes**. The experimental results validated its **high precision and recall**, significantly reducing false positives while maintaining rapid detection and mitigation capabilities. The **adaptive learning model** enabled the system to evolve over time, continuously improving its accuracy and effectiveness in identifying both known and emerging vulnerabilities. Furthermore, the **self-healing mechanism** ensured minimal downtime by automatically restoring compromised systems to a stable state. The solution's scalability and real-time responsiveness make it particularly suited for **large-scale, dynamic environments**, offering enhanced protection against modern cyber threats. Overall, the system represents a **significant advancement in cybersecurity**, providing organizations with a **proactive, intelligent, and automated defense mechanism** to safeguard their infrastructure and data.

REFERENCES

1. **Singh, R., & Sharma, P.** (2020). "Artificial Intelligence in Cybersecurity: Enhancing Threat Detection and Mitigation". **Journal of Information Security**, 12(3), 45-58.
2. **Brown, T., & White, K.** (2019). "Machine Learning-Based Vulnerability Scanners: A Comparative Study". **International Journal of Computer Science and Security**, 8(4), 112-130.
3. **Zhang, Y., & Patel, R.** (2021). "Deep Learning for Real-Time Threat Detection: A Case Study on Automated Vulnerability Scanners". **Cybersecurity and AI Journal**, 15(2), 205-218.
4. **NIST (National Institute of Standards and Technology)**. (2020). "Guidelines on Vulnerability Assessment and Mitigation Strategies". **NIST Special Publication 800-160**, 34-50.
5. **Choi, J., & Kim, H.** (2022). "Adaptive AI Models for Zero-Day Vulnerability Detection". **Journal of Network Security and Defense**, 19(5), 378-392.
6. **Gupta, S., & Lee, J.** (2018). "Reducing False Positives in Automated Vulnerability Scanning Using AI". **ACM Transactions on Information and System Security**, 11(7), 89-102.
7. **Microsoft Azure Security Team**. (2021). "AI-Powered Security: Enhancing Threat Detection with Real-Time Patch Management". **Technical Report**, 142-159.
8. **Smith, L., & Rodriguez, M.** (2020). "Real-Time Self-Healing Cyber Defense Using AI". **Journal of Advanced Security Technologies**, 10(3), 88-104.
9. **Kaspersky Lab**. (2019). "AI in Vulnerability Detection: Enhancing Security with Automated Threat Mitigation". **Cybersecurity Insights Report**, 62-77.
10. **SANS Institute**. (2021). "Automated Vulnerability Scanning: Challenges and Future Directions". **SANS Research Paper**, 120-138.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details