International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 11 | Nov - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Utilization of AI in System Security

Atharva M. Humane[1], Soham N. Harane[2]

Under the guidance of

Prof. Snehal Vastrad (Mentor)

MCA Department – Zeal Institute of Business Administration Computer Application & Research, Pune

---

Abstract - This research explores the role of Artificial Intelligence (AI) in strengthening system security by examining AI-driven intrusion detection, real-time threat evaluation, and automated response mechanisms. Findings indicate that AI-based security frameworks consistently outperform conventional rule-dependent tools, with machine learning (ML), deep learning (DL), and natural language processing (NLP) proving effective in identifying anomalies and predicting potential threats. The study further highlights market trends that fuel the adoption of AI, outlines core AI principles, and identifies major challenges—including adversarial attacks and the need for Explainable AI (XAI). Results demonstrate that AI delivers higher accuracy, improved responsiveness, and enhanced predictive capability, making it a reliable cybersecurity solution across sectors such as finance, defense, and healthcare. Ethical concerns, data privacy issues, and robustness against adversarial manipulation remain key considerations. Ultimately, the research concludes that integrating automated AI technologies with human expertise provides a comprehensive and resilient defense against emerging cyber threats.

Key Words: Artificial Intelligence (AI), System Security, Cybersecurity, Machine Learning (ML), Deep Learning (DL), Intrusion Detection Systems (IDS), Threat Detection, Anomaly Detection

1. INTRODUCTION

Modern society relies heavily on digital systems, network infrastructures, and online platforms for essential operations. This dependency has led to a notable rise in cyberattacks, including ransomware, phishing, malware infiltration, identity theft, and denial-of-service assaults. Traditional security frameworks—such as firewalls, signature-based antivirus software, and rule-based intrusion detection systems—often prove insufficient against these advanced and continuously evolving threats.

Artificial Intelligence (AI) has emerged as a transformative force in cybersecurity. With the support of ML, DL, and NLP, AI-enabled systems can process large datasets, recognize hidden behavioural patterns, and adapt to newly observed attack techniques. Unlike traditional security measures, AI can analyse massive security logs, detect irregularities in real time, and predict intrusions before they occur.

Given the growing number and complexity of cyberattacks, the incorporation of AI into security systems has become a necessity rather than an option. This research evaluates the contribution of AI to security enhancement, identifies its operational benefits, acknowledges its shortcomings, and explores future developments in cybersecurity.

A. Statement of the Research Problem:

This study examines how AI technologies can substantially strengthen system security by improving threat identification, prevention, and response, while also analyzing the limitations and challenges associated with AI-based protection mechanisms.

B. Objectives of the study:

- To analyse how AI contributes to strengthening cybersecurity systems.
- To examine diverse AI strategies applied in cybersecurity operations.
- To explore the application of AI in intrusion detection, malware analysis, phishing mitigation, and authentication.
- To evaluate the performance of AI-driven security tools compared to conventional models.
- To identify challenges and limitations associated with AI implementation in system security.
- To assess future prospects for AI in cybersecurity.

C. Hypothesis of the Study:

1. AI-enhanced security systems achieve greater accuracy and faster anomaly detection than conventional rule-based approaches.

2. The incorporation of AI in system security reduces the chances of undetected cyber intrusions and reinforces overall network protection.

D. Significance of the Study:

Cyber threats pose critical risks for individuals, organizations, and governments. As attackers adopt increasingly sophisticated strategies, traditional security models become less effective. Understanding AI's role in improving cybersecurity is therefore essential.

This research provides insight into how AI-based technologies transform traditional cybersecurity into adaptive, intelligent, and automated security systems. From an academic standpoint, this study enriches existing literature on AI and cybersecurity, offering a strong foundation for future studies.

E. Data Collection Source:

1. Primary data: Based on previously published research papers directly relevant to the study topic.

2. Secondary data: Collected from credible online articles, websites, and resources related to AI and cybersecurity.

3. Data Analysis: Data were systematically analysed using percentage analysis and graphical interpretation.

F. Scope of Study:

1. Geographical Scope - Focuses on the Narhe region.

2. Topical Scope - Restricted to studying AI's influence on system security.

3. Analytical Scope - Limited to the study's objectives and includes methods such as data classification and comparative analysis.

4. Functional Domain - Encompasses proposing effective strategies for system security.

G. Validity of Study:

- The study reflects the current landscape of system security.

- It aims to raise awareness regarding cyber risks, vulnerabilities, and necessary preventive practices.

2. Body of Paper

In today's digital environment, cyber threats have become a critical challenge for individuals, enterprises, and government bodies. Advancements in technology have also enabled attackers to devise sophisticated methods, rendering traditional security systems inadequate. Consequently, the integration of AI into security frameworks has become crucial.

This research highlights how AI facilitates an intelligent, adaptive, and automated shift in cybersecurity practices. It demonstrates how AI assists in early threat identification, rapid incident response, and continuous monitoring. The study also emphasizes AI's role in advancing academic discourse in AI and cybersecurity, serving as a reference for researchers and practitioners.

2.1 Introduction

The conceptual foundation of AI in security describes the principles and theoretical models that clarify how AI technologies influence modern security systems. This section outlines the evolution of AI, its functioning mechanisms, and its growing relevance within physical and digital security structures.

2.2 Concept of Artificial Intelligence

Artificial Intelligence refers to the ability of machines to execute tasks typically associated with human cognition, including learning, decision-making, and pattern recognition. Initially conceptualized in the mid-20th century, AI has evolved into a multifaceted domain comprising ML, DL, NLP, computer vision, and other advanced components. In security, AI is increasingly adopted to automate surveillance, predict intrusions, and enhance decision-making through data-driven insights.

2.3 Theoretical Framework of AI in Security

Several theoretical frameworks help to explain the use of AI in the security division.

2.3.1 Socio-Technical Design Perspective

This framework examines the interaction between humans and technologies. In security contexts, AI operates alongside human analysts, ensuring efficient threat detection and response while maintaining appropriate levels of human oversight and technological autonomy.

2.3.2 Systems Theory

Systems theory views security infrastructures as interconnected units working toward a common goal. AI enhances these interactions by integrating data from cameras, sensors, and databases to enable coordinated and intelligent incident handling.

2.3.3 Decision Theory

Decision theory provides analytical and predictive foundations for AI systems. In cybersecurity, AI applies this theory to evaluate risks, recognize threats, and identify the most suitable mitigation strategies under uncertain circumstances.

2.4 Evolution of AI in Security

AI applications in security have evolved significantly. Early systems relied on rigid rule-based mechanisms. With the emergence of machine learning, security solutions became capable of identifying complex patterns and adapting to new threats. Recent developments in deep learning and neural networks allow AI to analyze large volumes of unstructured data—such as video feeds and network logs—making AI a proactive tool for threat prediction and prevention.

2.5 Key Concepts Related to AI Security Systems

There are several key concepts that essentially mark the role of AI in modern security systems:

• Machine Learning (ML): Enables systems to learn from data and improve performance without explicit programming.

• Deep Learning (DL): Utilizes neural networks to detect intricate patterns, particularly for video and image analysis.

• Computer Vision: Allows machines to interpret visual data for applications such as surveillance and facial recognition.

• Natural Language Processing (NLP): Assists in phishing detection, spam filtering, and log interpretation.

• Finally, predictive analytics uses past and current data to forecast potential security incidents.

2.6 Relationship Between AI and Security Systems

AI and security systems complement one another. Security mechanisms supply vast data streams, while AI analyses this information to identify threats, automate decision-making, and enhance response strategies. This partnership strengthens the adaptability and responsiveness of modern security infrastructures.

2.7 Conceptual Model of AI-Driven Security Systems

AI-enabled security systems typically comprise:

1. **Data Acquisition Layer:** Collects input from sensors, cameras, and system logs.
2. **Intelligence Processing Layer:** Utilizes AI algorithms for analytics, pattern recognition, and predictions.
3. **Decision and Response Layer:** Initiates automated or human-assisted actions such as alerts or countermeasures.

2.8 Summary

This chapter demonstrates that AI's contribution to security is rooted in both theoretical and technological foundations. Through cognitive computing, predictive modelling, and pattern recognition, AI enhances real-time monitoring and rapid incident response, shaping the future of security in both digital and physical environments.

Data Analysis & Interpretation

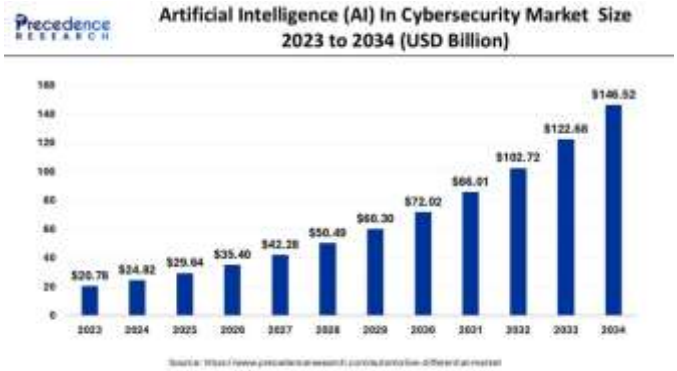

Chart 1: AI in Cybersecurity Market Size 2023-2024 (USD Billion)
[Source: Link]

Interpretation:

Analysis indicates a substantial upward trajectory in the global market for AI-driven cybersecurity solutions. The market rises from $20.78 billion in 2023 to $146.52 billion in 2034, showing sustained year-to-year expansion. Notably, growth accelerates significantly in later years, signaling a sharp rise in the adoption of AI-centered security technologies.

Implications:

Initial and Final Market Values:
The AI cybersecurity market is projected to grow substantially, rising from **$20.78 billion in 2023** to **$146.52 billion by 2034**. This significant increase reflects the rapid shift toward AI becoming the predominant technology driving cybersecurity solutions.

Consistent Annual Growth:
The market demonstrates steady year-over-year expansion. Between 2023 and 2030, the market value nearly triples—from **$20.78 billion** to **$72.02 billion**—indicating strong and sustained adoption of AI-based security tools.

Increasing Growth Momentum:
Although the expansion progresses consistently, the most notable surge occurs in the later years. In particular, from **2032 ($102.72 billion)** to **2034 ($146.52 billion)**, the market grows by approximately **$20–$25 billion**, signalling a sharp acceleration in the demand and integration of AI technologies within cybersecurity.

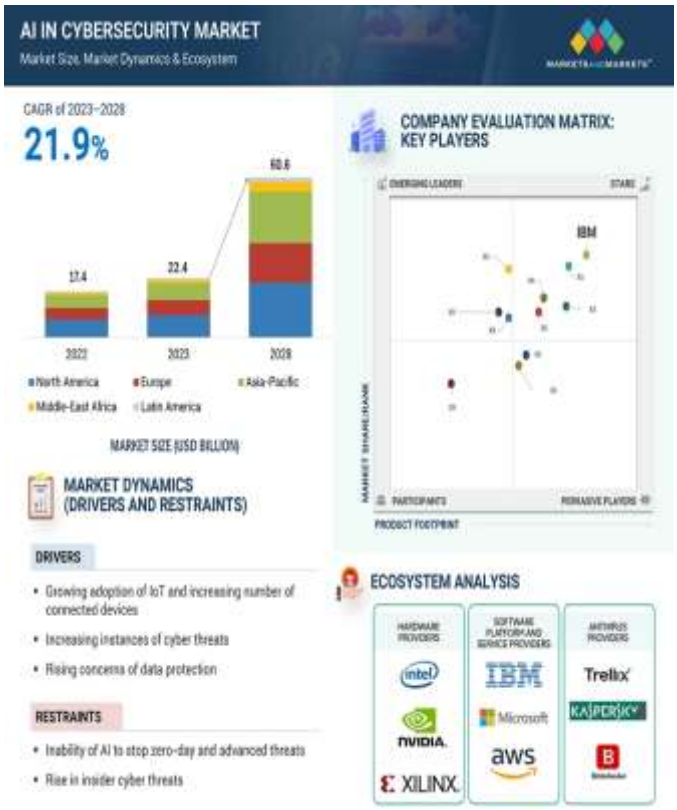

Chart 2: AI in Cybersecurity Market Analysis (2022–2028) [Source: Link]

Interpretation:

The AI cybersecurity market shows strong growth potential, with a CAGR of 21.9% from 2023 to 2028. Market value is projected to nearly triple, reaching $60.6 billion by 2028. North America and Europe dominate market share, while Asia-Pacific remains a rapidly growing region. Key drivers include expanding IoT deployments, rising cyberattacks, and heightened data-security requirements. Major constraints include limitations in AI's detection capacity for zero-day threats and increasing insider attacks.

1. Market Growth & Size (CAGR 2023–2028)

Compound Annual Growth Rate (CAGR):
The AI cybersecurity sector is expected to expand at a **21.9% annual growth rate** from 2023 to 2028. This strong CAGR indicates that the rapid momentum currently observed in the market will continue, reflecting sustained and increasing demand for AI-powered security solutions.

Market Size Forecast:
Projections show that the market will rise from **$22.4 billion in 2023** to **$60.6 billion in 2028**. This threefold increase over just five years demonstrates how essential AI technologies have become in addressing the fast-changing landscape of cyber threats.

Regional Distribution (2028 Outlook):
By 2028, **North America and Europe** are expected to hold the largest shares of the market, reflecting their mature cybersecurity infrastructure and high adoption rates. Meanwhile, the **Asia-Pacific region** is anticipated to experience rapid expansion, signaling rising demand and significant future growth potential in emerging economies.

2. Market Dynamics (Drivers and Restraints)

Drivers (Factors Promoting Growth)

Expansion of IoT and Connected Devices:
As the number of IoT devices increases, organizations generate far more data and face a broader attack surface. AI becomes essential for managing, analysing, and securing these large-scale and diverse data environments.

Escalating Cyber Threats:
The growing sophistication and frequency of cyberattacks—such as ransomware and phishing—compel organizations to adopt advanced AI tools capable of proactive detection and swift incident response.

Rising Data Protection Requirements:
Stringent data privacy regulations (e.g., GDPR) and the high financial impact of data breaches encourage companies to integrate AI solutions to strengthen data protection and maintain regulatory compliance.

Restraints (Factors Limiting Growth)

AI Limitations in Handling Zero-Day and Highly Advanced Attacks:
Current AI systems are not fully capable of identifying threats they have never encountered. Zero-day attacks can bypass AI trained only on historical data, highlighting the continued need for human expertise to interpret anomalies and make informed decisions.

Increase in Insider Threats:
Some cyber risks originate from within an organization, and AI systems may struggle to differentiate between normal internal activities and malicious insider behaviour. This inability to reliably detect insider threats can reduce the effectiveness of AI-driven security tools.

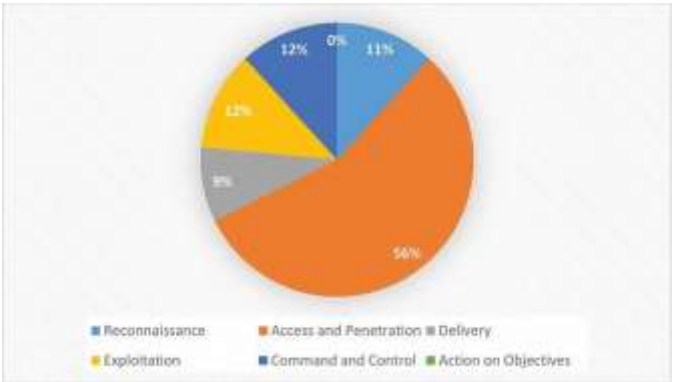

Chart 3: Identified AI-Driven Attack Techniques

The chart highlights frequent use of AI during the Access and Penetration stage of cyberattacks (56%), suggesting attackers leverage AI primarily to automate initial compromise attempts. AI is also heavily utilized in exploitation, exfiltration, and command-and-control activities. The absence of AI in the final "Action on Objectives" stage suggests attackers still rely on manual execution for critical operations.

This pie chart presents the distribution of AI-assisted cyberattack techniques across the various stages of the attack kill chain. The data shows that AI is most heavily applied during the **Access and Penetration** phase, accounting for **56%** of the identified methods. This suggests that attackers rely on AI predominantly to streamline and automate initial entry into a system or network—often through advanced phishing strategies, automated vulnerability discovery, or intelligent evasion of existing security defences.

The chart further highlights the significant involvement of AI during the **Implementation** stage, where **50%** of techniques employ AI-driven tools.

AI commonly facilitates the automated exploitation of system weaknesses, enabling attackers to gain entry more efficiently using technologies such as intelligent exploitation frameworks.

AI also plays a notable role in the **Exfiltration** phase (**20%**), where it assists in maintaining unauthorized access and bypassing data protection mechanisms, thereby enabling the extraction of sensitive information with reduced risk of detection. In the **Exploitation** phase (**12%**), AI enhances the execution of malicious payloads, increasing the effectiveness and sophistication of attack operations. Additionally, AI is used during the **Command-and-Control** phase (**12%**) to create stealthy communication channels between attackers and compromised devices, making it harder for defenders to identify or block malicious activity.

In the **Reconnaissance** stage (**11%**), AI is employed for automated information gathering—such as mapping systems, identifying potential weaknesses, and profiling targets—allowing attackers to prepare efficiently for subsequent actions.

AI is also used in the **Delivery** phase (**9%**), where it supports the distribution of malicious content to victims through optimized targeting techniques.

Interestingly, the **Action on Objectives** stage shows **0% AI utilization**, indicating that while AI significantly enhances preparation and execution phases, attackers often carry out the final objective—such as data theft or system sabotage—manually or through direct intervention.

Overall, the chart demonstrates that adversaries primarily leverage AI to automate, strengthen, and accelerate the **early and middle stages** of a cyber intrusion, rather than the final execution stage.

3. CONCLUSIONS

AI has become a critical component of modern security systems and is widely adopted across sectors such as finance, defense, and healthcare. It enhances intrusion detection, malware analysis, and phishing identification through ML and DL techniques. Computer vision improves surveillance capabilities, while predictive analytics assists in forecasting potential risks. AI supports fraud detection, identity verification, and large-scale threat monitoring. Healthcare organizations rely on AI to secure patient information and ensure regulated access to digital records.

Suggestions

These are the Practical Recommendations and Suggestions to Enhance AI Programs for Security.

A. Enhance Data Quality and Diversity

AI models require diverse and updated datasets to ensure accurate detection and reduce false alarms.

B. Implement Explainable AI (XAI)

XAI improves transparency, helping analysts understand AI-generated decisions and strengthening trust.

C. Integrate Human Expertise

AI should complement human decision-makers. Hybrid systems combining automated detection with human verification achieve higher accuracy.

D. Continuous Model Updates

AI security systems must be regularly retrained to keep up with evolving cyber threats.

E. Consolidate Adversarial Robustness

Defensive strategies such as adversarial training and anomaly detection layers can protect AI from manipulation.

F. Apply AI Across All Security Layers

Extending AI to network monitoring, access control, endpoint protection, and behavioral analysis creates a multi-layered defense.

G. Ensure Ethical and Privacy-Compliant AI Use

AI systems should follow data privacy regulations through measures such as anonymization, consent management, and transparent data practices.

ACKNOWLEDGEMENT

We extend our sincere gratitude to our faculty mentor Prof. Snehal Vastrad, for their guidance, encouragement, and support throughout this research. We also thank the MCA Department of Zeal Institute of Business Administration, Computer Application & Research, Pune, for providing the resources and academic environment essential for this study. Our appreciation goes to the authors and researchers whose work contributed to our understanding of AI and cybersecurity. Lastly, we thank our friends and family for their continuous support during the preparation of this manuscript.

REFERENCES

1. Artificial intelligence for system security assurance: A systematic literature review
Shao-Fang Wen
University of South-Eastern Norway
Ankur Shukla
Institute for Energy Technology
Basel Katt
Norwegian University of Science and Technology

2. Artificial Intelligence in Cyber Security
License CC BY-NC-SA 4.0
Md. Fazley Rafy
West Virginia University

3. Statista. (2024). Artificial Intelligence in Cybersecurity Market Size Worldwide (2023–2034). Retrieved from https://www.statista.com/

4. AI Market Dynamics
https://www.marketsandmarkets.com/PressReleases/artificial-intelligence-ai-cyber-security.asp

5. AI in Cybersecurity Market
https://www.precedenceresearch.com/artificial-intelligence-in-cybersecurity-market

4. www.wikipedia.com