iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** III **Month of publication:** March 2025

DOI: https://doi.org/10.22214/ijraset.2025.67522

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 13 Issue III Mar 2025- Available at www.ijraset.com

AI-Driven Cybersecurity: A Cornerstone of National Security Amidst Emerging Threats and Innovative Solutions

Aastha Bhanushali, Neomi Almeida
KES, Shri. Jayantilal H. Patel Law College, India

Abstract: ***In the current digital environment, cybersecurity has emerged as a key component of national security. Advanced defences have become necessary due to the quick evolution of cyberthreats, such as ransomware, cyberwarfare, and AI-driven attacks. Artificial intelligence (AI) including into cybersecurity systems has transformed security automation, incident response, and threat detection. The influence of AI in cybersecurity, new threats, legal frameworks governing cyber laws, real-world case studies of cyber frauds, and AI-driven cybersecurity solutions are all covered in this research paper. Additionally, policy proposals and statistical trends are examined to offer a strategic perspective on bolstering national cyber defences. This study provides a thorough overview of AI's involvement in digital protection and national security by referencing government rules, cybersecurity reports, and peer-reviewed literature.***

I. INTRODUCTION

The escalating complexity of cyber threats has rendered cybersecurity a critical component of national security. The dynamic nature of cyberattacks frequently makes it impossible for traditional defences to keep up. In this field, artificial intelligence (AI) has become a disruptive force, providing proactive, flexible, and scalable solutions for identifying, stopping, and lessening cyberthreats. To strengthen digital infrastructure and protect national interests, governments and organizations must integrate AI-driven systems. Because of the increased reliance on cyber infrastructure brought about by the digital revolution, entities are now more susceptible to sophisticated cyber assaults. More proactive and intelligent solutions are required since traditional cybersecurity solutions are unable to keep up with the constantly changing nature of cyber threats. By proactively detecting and reducing risks through pattern recognition, malicious activity prediction, and reaction mechanism automation, artificial intelligence (AI) and machine learning have completely changed cybersecurity procedures. This paper examines how AI may improve cybersecurity resilience by going over real-world applications, possible weaknesses, and creative ways to reduce new cyberthreats. Businesses looking for strong protection in an increasingly hostile cyber environment will benefit from the report's strategic recommendations, significant obstacles, and evaluation of current AI cybersecurity implementations

II. METHODOLOGY

The paper's information is gathered through doctrinal investigation. Secondary data sources and references from renowned researchers, official government sources, and the Indian Constitution have been consulted. A qualitative analysis of the available materials has been conducted to investigate data from numerous sources in a flexible and open-ended manner; however, a personal interpretation of the data has also been developed. In order to formulate a hypothesis for the subject and to derive sufficient reasoning from the pertinent facts, deductive reasoning techniques have been examined.

III. UNDERSTANDING CYBERSECURITY: CONCEPTS AND IMPORTANCE

A. Define Cyber Security

Cyber security is the application of technologies, processes, and controls to protect systems, networks, programs, devices and data from cyber-attacks.

It aims to reduce the risk of cyber-attacks and protect against the unauthorised exploitation of systems, networks, and technologies.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue III Mar 2025- Available at www.ijraset.com

B. What is Cyber Security?

Cybersecurity is the protection of digital data, electronic systems, networks, servers, and computers against illegal access, cyber-attacks, damage, theft. It involves implementing technologies, processes, and best practices designed to safeguard information and maintain its confidentiality, integrity, and availability.[1]

C. How does AI Enhance Cybersecurity in National Security?

AI enhances cybersecurity in national security through several critical capabilities:

1) Advanced Threat Detection: AI systems analyze vast amounts of data to detect anomalies and subtle patterns indicative of cyber threats, enabling earlier identification of risks that human analysts might miss.
2) Predictive Intelligence: Predictive Intelligence: National security agencies are able to pre-emptively resolve vulnerabilities by anticipating potential cyber-attacks using machine learning algorithms that analyse historical and real-time data.
3) Automation and Rapid Response: AI enables automation of defensive measures, significantly reducing response times to cyber incidents. This capability is crucial for mitigating damage during critical national security breaches.
4) Enhanced Surveillance and Monitoring: AI continuously monitors network activities and endpoints, providing persistent and comprehensive cybersecurity oversight, essential for protecting critical infrastructure.
5) Adaptive Cyber Defence: AI-driven systems learn continuously, adapting to new threats dynamically, which makes national security frameworks resilient against evolving cyber-attacks.
6) Strategic Decision-Making: AI aids decision-makers by offering insights based on data-driven analytics, allowing informed strategies to counteract national cyber threats effectively.

IV. CYBERSECURITY LAWS AND GOVERNANCE

Cybersecurity laws and governance in India comprise a set of frameworks, regulations, and institutional structures aimed at safeguarding digital infrastructure and data from cyber threats.

Key aspects include:

1) Information Technology Act, 2000 (IT Act)- The Information Technology Act, 2000 (IT Act) is India's primary law governing cybersecurity, digital transactions, electronic governance, and cybercrimes. It was enacted to provide a legal framework for electronic commerce and digital communications while addressing cyber threats in India.[2]
2) IT (Amendment) Act, 2008- The Information Technology (Amendment) Act, 2008 is a significant update to the Information Technology Act, 2000, introduced to address emerging cyber threats, data security concerns, and advancements in digital technologies. The amendment refined existing provisions and added new sections to improve cybercrime regulations, data privacy measures, and national cybersecurity strategies.[3]
3) Indian Penal Code (IPC), 1860- The Indian Penal Code (IPC), 1860 is the primary criminal law in India, covering offenses related to theft, fraud, defamation, and national security. Although originally framed in 1860, several sections of the IPC are used to prosecute cybercrimes alongside the Information Technology (IT) Act, 2000 & IT (Amendment) Act, 2008.[4]
4) National Cyber Security Policy, 2013- The National Cyber Security Policy (NCSP), 2013 was introduced by the Government of India's Ministry of Electronics and Information Technology (MeitY) to enhance cyber resilience, secure digital infrastructure, and protect national cyberspace from growing cyber threats.[5]
5) Personal Data Protection Bill, 2023- The Personal Data Protection Bill (PDPB), 2023, also known as the Digital Personal Data Protection (DPDP) Bill, 2023, is India's latest attempt to regulate data privacy, cybersecurity, and digital rights. It establishes guidelines for collecting, processing, and securing personal data while holding organizations accountable for data breaches and misuse.[6]

6) Institutional Governance Structures

- CERT-In (Computer Emergency Response Team India)**:** Responsible for responding to cyber incidents and providing timely security alerts and guidelines.
- National Critical Information Infrastructure Protection Centre (NCIIPC)**:** Protects critical sectors such as banking, finance, energy, and telecommunications from cyber threats.
- Ministry of Electronics and Information Technology (MeitY)**:** Governs national cybersecurity policies and initiatives

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue III Mar 2025- Available at www.ijraset.com

V. WHY CYBERSECURITY LAWS ARE ENFORCED

Cybersecurity laws exist to:

1) Protect National Security – Prevent cyber espionage and attacks on critical infrastructure.
2) Safeguard Personal Data – Ensure compliance with data protection regulations like GDPR and CCPA.
3) Regulate Digital Transactions – Prevent financial fraud and cybercrimes.
4) Ensure Corporate Security – Mandate compliance for businesses handling sensitive data.
5) Combat Cyber Terrorism – Deter digital warfare and cyberterrorist activities.

VI. CASE STUDIES: CYBER FRAUDS AND HIGH-PROFILE ATTACKS

A. Landmark Cases

Thomson Reuters v. ROSS Intelligence (2025): In February 2025, a Delaware federal court ruled in Thomson Reuters v. ROSS Intelligence, marking a significant decision on the use of copyrighted material to train AI models. The court held that ROSS Intelligence's use of Westlaw headnotes to train its AI-driven legal research tool did not qualify as fair use, emphasizing the need for AI developers to obtain proper licenses for copyrighted content used in training their models.7

Lloyd v. Google LLC (2019): In October 2019, the English Court of Appeal ruled in Lloyd v. Google LLC, concerning Google's alleged misuse of personal data from over 4 million iPhone users through the placement of cookies on the Safari browser. The court's decision opened the door to UK data protection consumer class actions, emphasizing the importance of user consent and transparency in data collection practices.8

Microsoft's Legal Action Against AI Misuse (2025): In February 2025, Microsoft identified and took legal action against four developers accused of circumventing AI guardrails to create illicit content, including celebrity deepfakes. The lawsuit aimed to halt their activities and deter others from misusing AI technology, highlighting the challenges in regulating AI applications and ensuring responsible usage.9

B. Notable Cybersecurity Breaches

1) SolarWinds Cyber Attack (2020)

- Target: U.S. Government Agencies, Tech Companies, and Private Corporations
- Attack Type: Supply Chain Attack
- Impact: The Russian-linked APT29 (Cozy Bear) hackers compromised SolarWinds' software updates, infiltrating U.S. federal agencies, cybersecurity firms, and Fortune 500 companies.
- Estimated Damage: Undisclosed, but considered one of the most sophisticated cyber-espionage operations in history.[10]

2) Colonial Pipeline Ransomware Attack (2021)

- Target: Colonial Pipeline (Critical U.S. Fuel Infrastructure)
- Attack Type: Ransomware Attack
- Impact: Darkside, a ransomware organization, caused panic and gas shortages by upsetting gasoline supplies to the U.S.-East Coast. Colonial Pipeline paid a Bitcoin ransom valued $4.4 million.[11]

3) Equifax Data Breach (2017)

- Target: Equifax (Credit Reporting Agency)
- Attack Type: Data Breach (Exploitation of Software Vulnerability)
- Impact: Personal data of 147 million users (including Social Security Numbers, credit card data) was stolen by hackers allegedly linked to China.
- Lawsuit Settlement: Over $700 million in damages paid by Equifax.[12]

C. AI in Financial and Corporate Cyber Frauds

- AI-Powered Phishing Attacks: Machine learning models generate highly convincing phishing emails to manipulate targets
- Deepfake Fraud: AI-generated deepfake technology is used for corporate scams and identity theft_.
- AI in Insider Threat Detection: Predictive analytics identify anomalies in employee behaviours to detect fraudulent activities

D. Emerging Cybersecurity Threats in the AI Era

- AI-Powered Malware: Self-learning malware that adapts to security defences_.
- Cyber Warfare and Espionage: State-sponsored cyberattacks disrupting national security operations.
- Autonomous Hacking Systems: AI-driven hacking tools capable of executing advanced persistent threats (APTs).
- IoT Vulnerabilities: Increased risk of cyberattacks on smart devices and connected infrastructures.
- AI-Powered Ransomware: Machine learning-enhanced ransomware that dynamically changes its attack strategy.

VII. AI-DRIVEN CYBERSECURITY SOLUTIONS

A. AI in Threat Detection and Prevention

- Machine Learning for Anomaly Detection: AI identifies suspicious activities by analysing patterns.
- Predictive Analytics for Threat Intelligence: AI predicts cyber threats based on historical data.
- Zero Trust Security Models: AI ensures strict access control and identity verification.

B. AI in Automated Incident Response

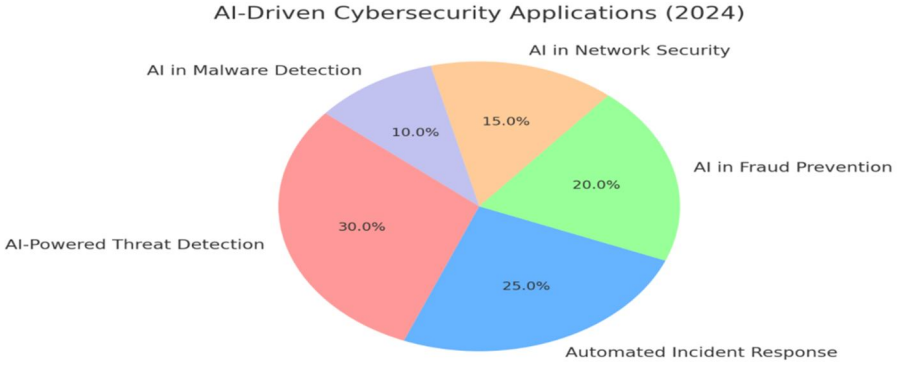
- Security Orchestration, Automation, and Response (SOAR): AI automates threat analysis and incident response.
- Automated Patching and System Updates: AI-driven security frameworks apply security patches in real-time.

C. Blockchain and AI for Cybersecurity

- Decentralized Identity Verification: Blockchain integrated with AI ensures secure authentication.
- Fraud Detection in Financial Transactions: AI-powered blockchain enhances fraud monitoring.

VIII. STATISTICS

1) 150% increase in China-nexus activity across all sectors
2) 442% growth in vishing operations between the first and second half of 2024
3) 51 seconds was the fastest recorded eCrime breakout time
4) 79% of detections were malware-free
5) 26 newly named adversaries in 2024
6) 52% of vulnerabilities observed by CrowdStrike in 2024 were related to initial access
a) AI-Powered Threat Detection (30%) – The largest portion of AI applications in cybersecurity focuses on identifying threats in real-time by analysing vast amounts of network data.
b) Automated Incident Response (25%) – AI automates response mechanisms, reducing reaction times to mitigate cyber threats efficiently.
c) AI in Fraud Prevention (20%) –To identify doubtful transactions, artificial intelligence-powered fraud detection is extensively applied in banking and e-commerce.
d) AI in Network Security (15%) – AI assists in maintaining secure network architectures by monitoring for anomalies and unauthorized access.
e) AI in Malware Detection (10%) – AI enhances antivirus and malware detection by identifying new and evolving cyber threats.



These statistics highlight how AI is revolutionizing cybersecurity by enhancing detection, response, and prevention capabilities.

A. Recommendations for Strengthening AI Cybersecurity

1) Develop AI-Specific Cybersecurity Policies.

- Governments should establish regulatory frameworks for AI applications in cybersecurity.
- AI security policies must address ethics, bias, transparency, and accountability in automated decision-making.
- Industry-wide compliance standards should be enforced to prevent AI misuse in cyber defence systems.

2) Strengthen AI Transparency and Ethics.

- AI models used in cybersecurity should be explainable and interpretable to avoid bias and errors.
- Organizations must conduct regular AI audits to ensure fairness, accuracy, and compliance.
- Implement ethical AI guidelines to prevent AI from being manipulated by cybercriminals.

3) Invest in AI Cybersecurity Workforce Development

- Governments and corporations must train cybersecurity professionals to handle AI-powered security systems.
- Establish AI cybersecurity research centers to encourage innovation and security advancements.
- Encourage public-private partnerships to bridge the skill gap in AI-driven cybersecurity.

4) Enhance AI-Enabled Cyber Threat Intelligence

- AI-driven cyber threat intelligence (CTI) should be used to detect, analyze, and predict cyberattacks.
- Security teams must leverage AI-driven predictive analytics to anticipate future cyber threats.
- AI-powered honeypots and deception technology can be deployed to mislead attackers and collect intelligence.

5) Encourage International Cooperation in AI Cybersecurity

- Governments should collaborate on global threat intelligence sharing to counter cyber warfare and AI-driven attacks.
- Establish international AI governance frameworks to regulate AI cybersecurity applications.
- Countries must work together to combat AI-powered misinformation, cyber espionage, and cyber terrorism.

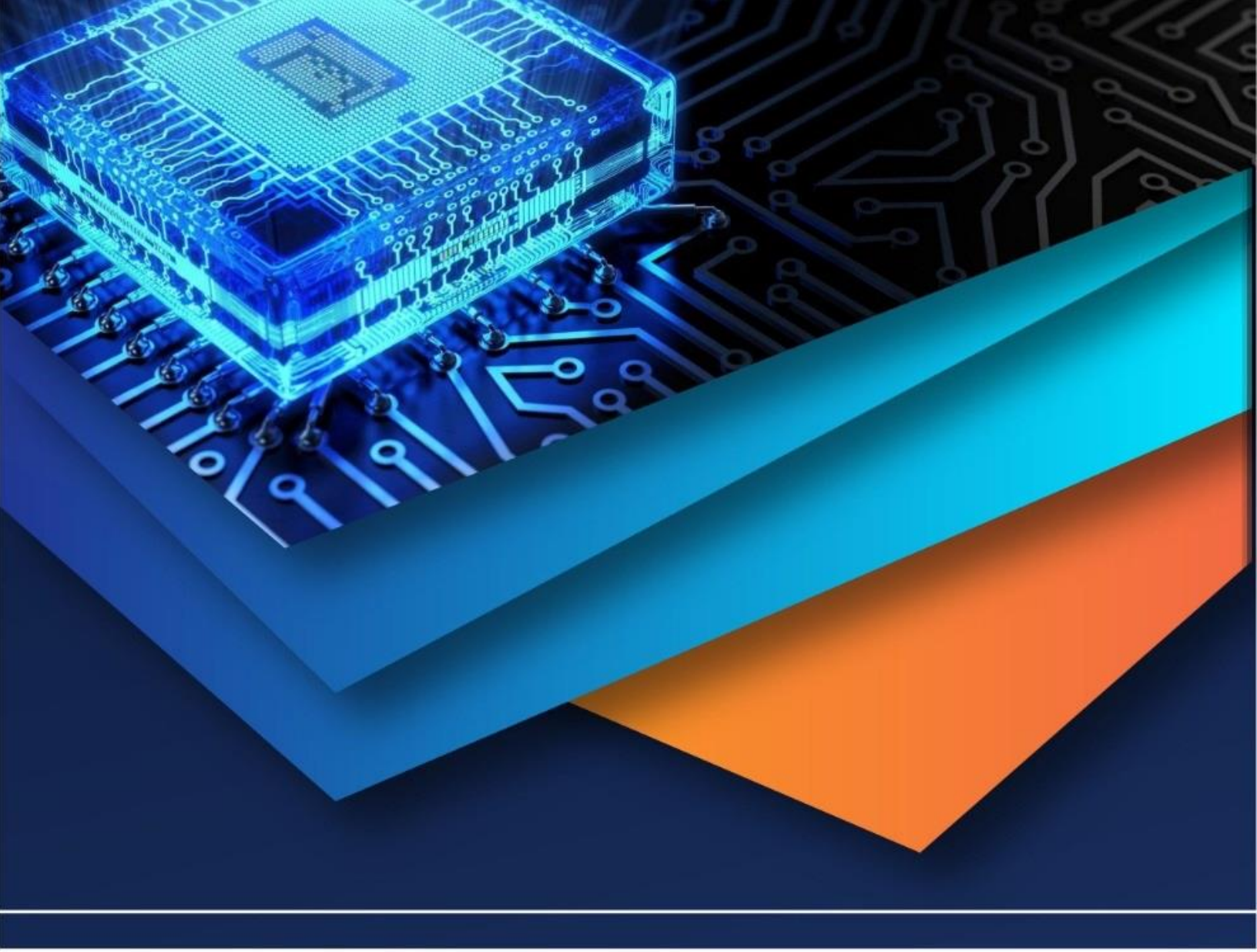
6) Implement AI-Driven Security Audits and Monitoring

- Organizations should deploy continuous AI-based security audits to detect vulnerabilities before exploitation.
- Automated compliance checks should be integrated to ensure security policies are up to date.
- AI should be used for behavioural analytics to identify insider threats and suspicious activities in real time.

IX. CONCLUSION

In conclusion, the utilization of AI and machine learning technologies is becoming increasingly necessary to confront the swiftly changing cybersecurity threat landscape. These sophisticated tools facilitate the more effective management of intricate cyber threats, improve real-time responsiveness, and enhance proactive threat detection. Nevertheless, organizations must exercise caution, incessantly adapting to new threats, refining models to reduce false positives, and addressing ethical and regulatory concerns, despite the unparalleled capabilities that AI offers. Businesses can fortify their defence mechanisms, thereby safeguarding critical infrastructure and assuring resilience, by strategically incorporating AI-driven solutions into cybersecurity frameworks. Undeniably, the future of cybersecurity is contingent upon the complete potential of AI, necessitating continuous investment, innovation, and vigilance to maintain digital security and trust.

WRITTEN BY AASTHA BHANUSHALI AND NEOMI ALMEIDA
***BALLB STUDENT, KES' SHRI. JAYANTILAL H. PATEL LAW COLLEGE*
***BALLB STUDENT, KES' SHRI. JAYANTILAL H. PATEL LAW COLLEGE*



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY