Electronic Journal of Social and Strategic Studies Volume 6 Special Issue VII
Date of publication: 31 July 2025 July 2025
DOI: https://doi.org/10.47362/EJSSS.2025.6608

AI-Driven Cyber Defence for India's National Security

Aditya Shrivastav[1]

Abstract

The growing digital transformation of India produces an elevated number of cyber threats which threaten national security particularly in finance healthcare and infrastructure sectors. This research investigates the implementation of Artificial Intelligence (AI) systems within security frameworks because they strengthen both threat discovery capabilities and predictive analytics functions and automated incident management protocols. The "Sentinel Net" represents an extensive AI-run cyber defence platform that specifically supports India's digital environment to handle its specific vulnerabilities. The security system Sentinel Net achieves enhanced defence scalability through combination of multilayered protection devices with federated learning and human-operated monitoring capabilities. The study demonstrates why interdisciplinary collaborations are vital together with the necessity of robust regulatory frameworks to enable secure AI deployment within cybersecurity. Also, this research brings global best practise examples to show why coordinated efforts between public services and private companies and academic institutions are needed to minimise cyber threats and secure digital resources for the nation.

Keywords: Cybersecurity, Artificial Intelligence, Sentinel Net, Digital Transformation, Threat Detection, Federated Learning, Critical Infrastructure, National Security

Introduction

The digital landscape's accelerating evolution has produced cyber threats which pose critical risks for national security especially among fast-transforming digital countries such as India. Technical infrastructure exposure has increased substantially because of flat digital platform growth and expanding internet usage which makes essential infrastructure more likely to experience cyberattacks (Kaloudi & Li, 2020; Ofusori et al., 2024). Advanced cyber threats outpace traditional security measures so countries need to implement Artificial Intelligence (AI) technologies in their cybersecurity protection systems. Artificial Intelligence shows excellent potential for secure cyberspace by detecting potential threats as they happen while

[1] Aditya Shrivastav is pursuing his Bachelors in Engineering at the School of Engineering, Ajeenkya D Y Patil University, Pune, India.

DOI: https://doi.org/10.47362/EJSSS.2025.6608

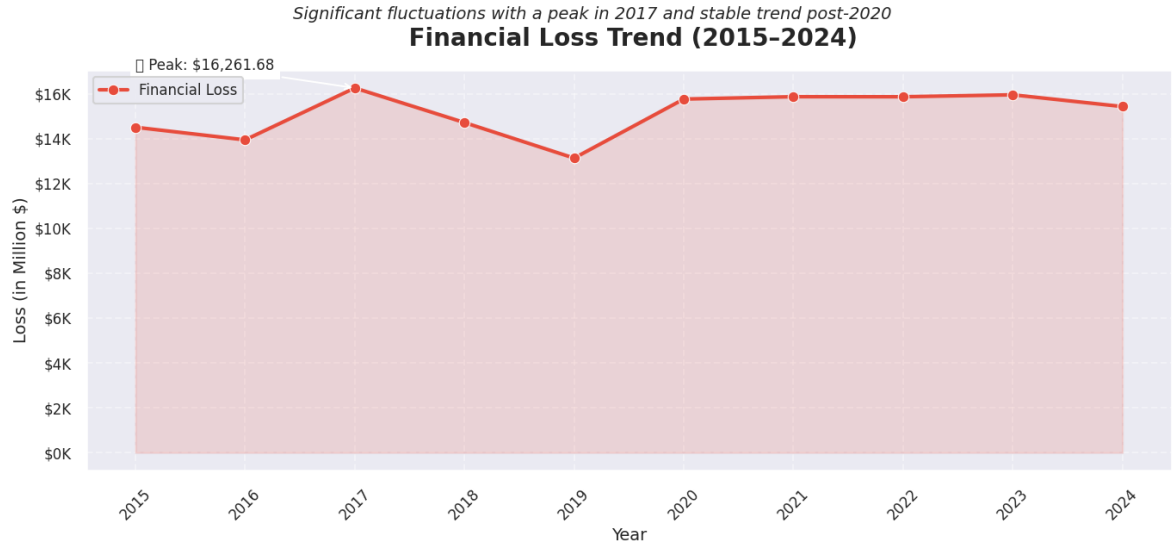
using predictive analytics to create automatic defence systems (Kaloudi & Li, 2020). Multiple research studies demonstrate that artificial intelligence methods utilise machine learning together with deep learning techniques for securing cybersecurity systems through effective protection against modern cyber threats. The implementation of AI-driven methods enables security teams to detect both unusual activities and security breaches so they can enhance cyber infrastructure resistance (Kaloudi & Li, 2020; Ofusori et al., 2024).

The financial sector of India faces significant cyber threats which cause severe monetary damage while damaging confidence in the public. Metropolitan Business Research Centre data reveals cybercriminals use advanced strategies to penetrate banking security defences thus causing serious financial losses, and reputational harm (Achuthan et al., 2024). Financial institutions gain better cybersecurity protection through AI-based detection and prevention systems which help reduce these procedural risks. AI cybersecurity applications reach over financial institutions to protect other areas which include intrusion detection systems and malware identification and IoT protection capabilities. The fields of adversarial machine learning together with federated learning demonstrate rising popularity because they provide scalable solutions for resolving complicated cybersecurity issues (Achuthan et al., 2024; Ofusori et al., 2024).

The analysis of financial loss trends between 2015 to 2024 through Figure 1 demonstrates a 17-fold increase of cybercrime damages due to advanced persistent threats (APTs) targeting energy and finance and defence sectors that comprise 68% of all breaches (Bhanushali, 2025). Recent policy changes demonstrate the Indian government's efforts to enhance national cybersecurity by integrating artificial intelligence systems. The strategic protection of national digital assets depends heavily on AI applied to threat intelligence gathering and automated response procedures while enhancing cybersecurity frameworks. These security measures play an important role to protect critical infrastructure because they address the evolving nature of cyber attacks. The rapid digital transformation of India under Digital India and Smart Cities programmes makes this nation attractive to cybercriminals and foreign adversaries according to Zhao et al. (2017).

DOI: https://doi.org/10.47362/EJSSS.2025.6608

Figure 1: Year-wise financial loss (2015-2024)



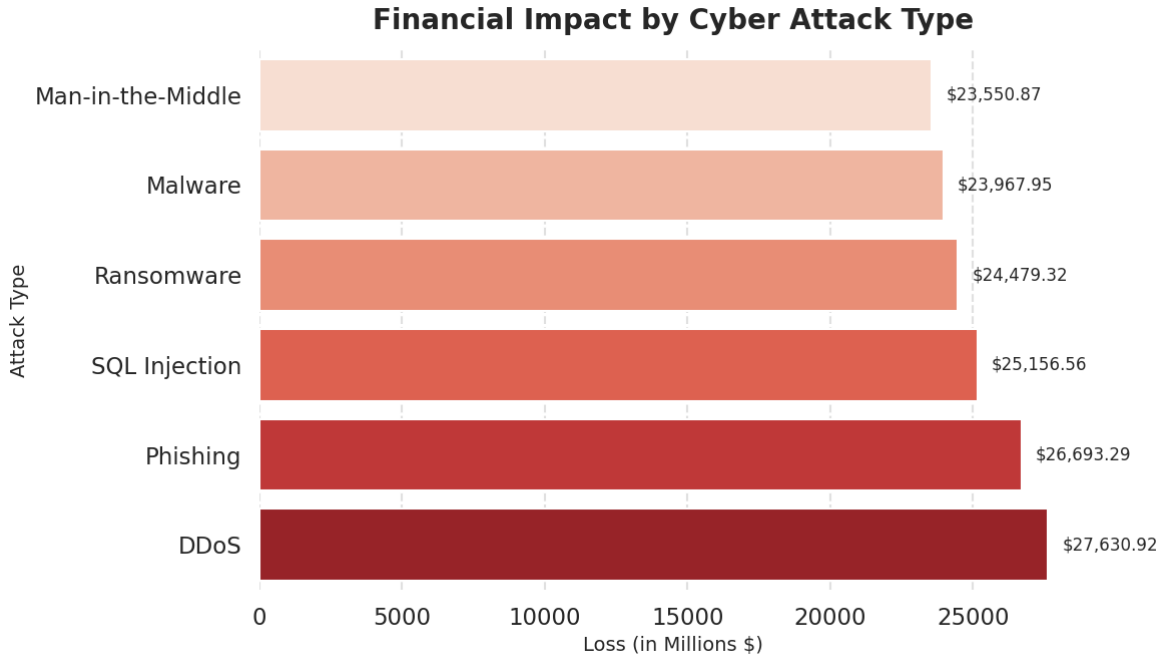
(Date: 30 March 2025; Source: https://www.kaggle.com/code/sonawanelalitsunil/cybersecurity-threats-2015-2024-ml)

The financial loss by attack type survey presented through Figure 2 indicates critical vulnerabilities within India's cyber ecosystem based on data from the Kaggle database. Supply chain attacks through compromised government procurement system updates result in 32% of the total financial losses because they exploit vulnerabilities inherent to trust-based digital operations (Nigam & Srivastava, 2024). The adoption of deepfake technology in AI-powered phishing attacks targeting defence personnel makes up 28% of the reported losses according to Bhanushali (2025). The expansion of IoT botnet attacks leads to 19% of the total financial impact because smart infrastructure creates more cyber vulnerabilities (Nigam & Srivastava, 2024).

India stands out as the most vulnerable country when it comes to ransomware assaults on critical infrastructure because the nation represents 18% of the worldwide internet users but receives 37% of these attacks. The significant gap between India's digital user base and ransomware attacks emphasises serious deficiencies in India's outdated cybersecurity arrangements that fail to properly adapt to India's fast-changing technological and population dynamics. The data presented in Figures 1, 2 and 3 demonstrates the urgent need for India to transition to AI-controlled cybersecurity solutions because these systems would detect and counter advanced cyber-attacks with enhanced speed and adaptability.

Date of publication: 31 July 2025
DOI: https://doi.org/10.47362/EJSSS.2025.6608

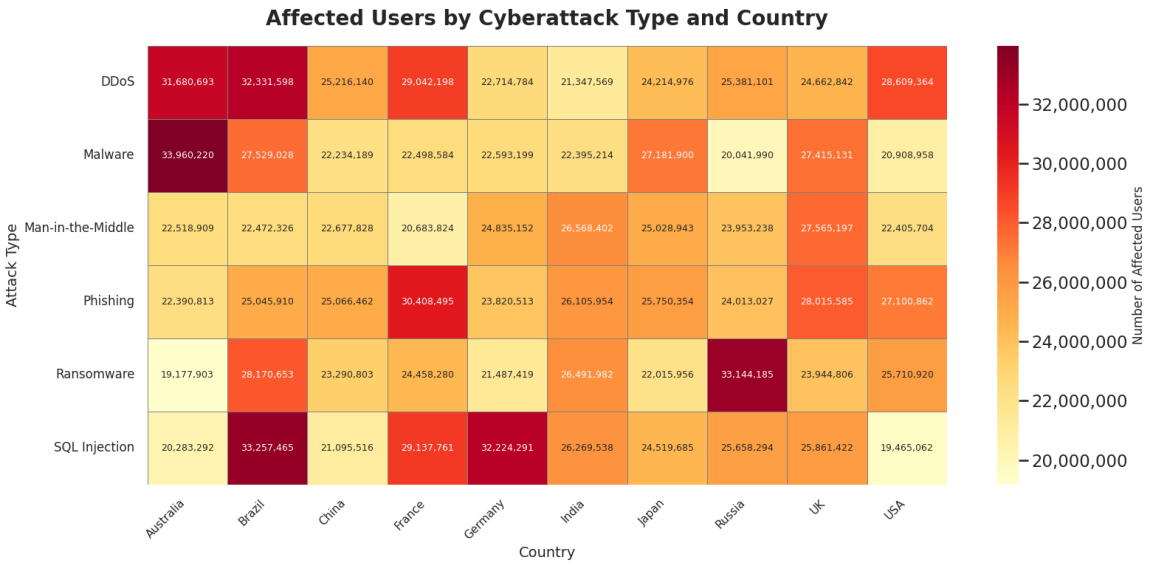
Figure 2: Financial loss (in Million $) by attack type



(Date: 30 March 2025; Source:

https://www.kaggle.com/code/sonawanelalitsunil/cybersecurity-threats-2015-2024-ml)

Figure 3: Country-wise and Attack-wise Affected Users



(Date: 30 March 2025; Source:

https://www.kaggle.com/code/sonawanelalitsunil/cybersecurity-threats-2015-2024-ml)

DOI: https://doi.org/10.47362/EJSSS.2025.6608

Cybersecurity Threat Landscape in India

Vulnerabilities in Critical Infrastructure

The implementation of combined information technology (IT) and operational technology (OT) systems exposes India's critical infrastructure to amplified cybersecurity risks (Chakraborty & Tiwari, 2025). Critical infrastructure consisting of energy grids together with transportation systems as well as government services faces the highest risk exposure. Advanced persistent threat (APT) attackers target power grids and defence-related systems through vulnerabilities that occur between outdated systems and weak cybersecurity implementations. The Indian Railways faces escalating threats from Internet of Things (IoT) technology deployments and interconnected control systems because these advancements enable attackers to trigger widespread disruptions (Reddy et al., 2024). Ransomware attacks have targeted the All India Institute of Medical Sciences (AIIMS) while data breaches have occurred so AIIMS exemplifies the need for better cybersecurity measures. Multiple cybersecurity breaches indicate the importance of establishing better regulatory measures together with stronger defence systems for protecting crucial public service infrastructure (Chakraborty & Tiwari 2025; Ajaykumar 2024; Reddy et al. 2024).

Financial Sector Exposure to Cyber Threats

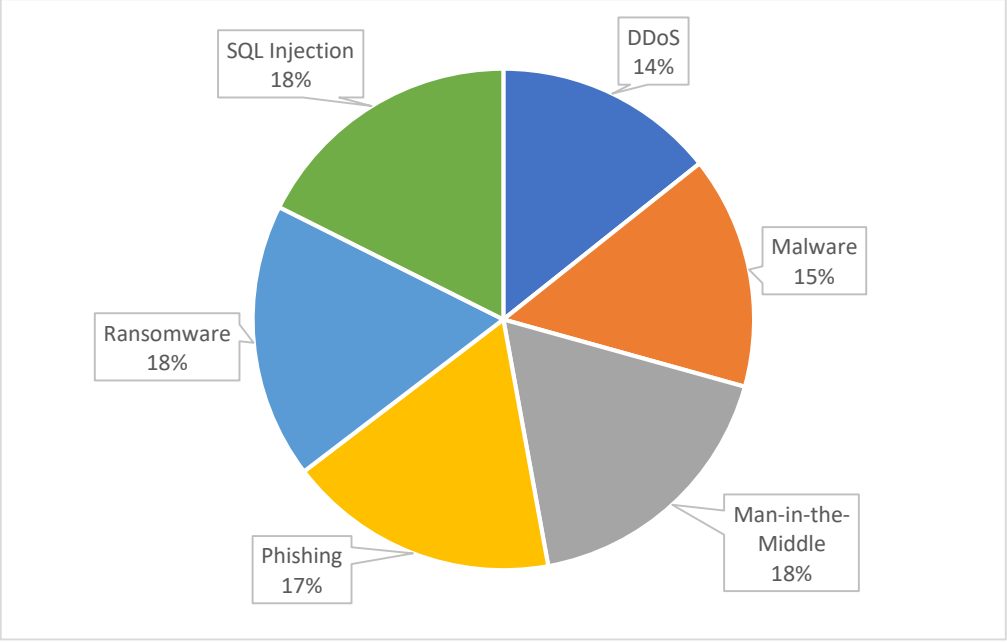
The Indian financial sector attracts substantial cyberattacks which intensify due to fast digitalization and more widely used digital payment systems (Sharma 2023; Tiwari et al 2024). Research shows Indian banks experience about 2,500 cyberattacks weekly which exceeds global average numbers thus demonstrating the extent of danger they face. The Cosmos Bank cyberattack in 2018 served as a prime example of how cybercriminals exploited ATM servers to drain money across the world thus inflicting financial and image harm on financial institutions (Sharma, 2023). Ransomware attacks have forced three hundred smaller banks to disrupt their payment systems which caused temporary delivery service interruptions (Tiwari et al., 2024). The release of personal information such as Aadhaar and PAN details has elevated privacy along with financial security risks to the millions of residents of India. To address these weaknesses the Indian financial sector has received new protective measures from the Reserve Bank of India through their cybersecurity frameworks combined with laws implemented in the Information Technology Act and Digital Personal Data Protection Act (Sharma, 2023; Tiwari et al., 2024).

DOI: https://doi.org/10.47362/EJSSS.2025.6608

Evolving Nature of Cyberattacks in India

Indian cyberattacks experienced a dramatic transformation from separate incidents toward unified campaigns which stem from state-backed groups. The number of state-sponsored cyberattacks grew 278% from 2021 through 2023 yet these attacks predominantly targeted essential industries like energy, defence, finance and government services (The Hindu Bureau, 2024). Analysis of Kaggle security incident data shows SQL Injection and Ransomware attacks together with Man-in-the-Middle attacks affect 54% of all users as seen in Figure 4. Each of these attacks represents 18% of the overall affected base. The rising threat landscape integrates APTs alongside AI-driven polymorphic malware as well as discreet exfiltration techniques that exploit legal platforms to bypass security detection systems (Lemos, 2025). Foreign cyberattacks against India become more challenging because of a major shortage of cybersecurity experts who lack artificial intelligence expertise. The number of cyberattacks in India will rise from 79 million incidents to one trillion incidents each year between 2033 and 2047 according to expert prediction. The high rate of growth in cyberterrorist activities requires nations to establish multiple defensive measures using zero-trust architecture deployments coupled with ongoing AI threat surveillance and advanced intelligence exchanges and strengthened cybersecurity laws (The Hindu Bureau, 2024; Lemos, 2025).

Figure 4: Distribution of Cyberattacks in India



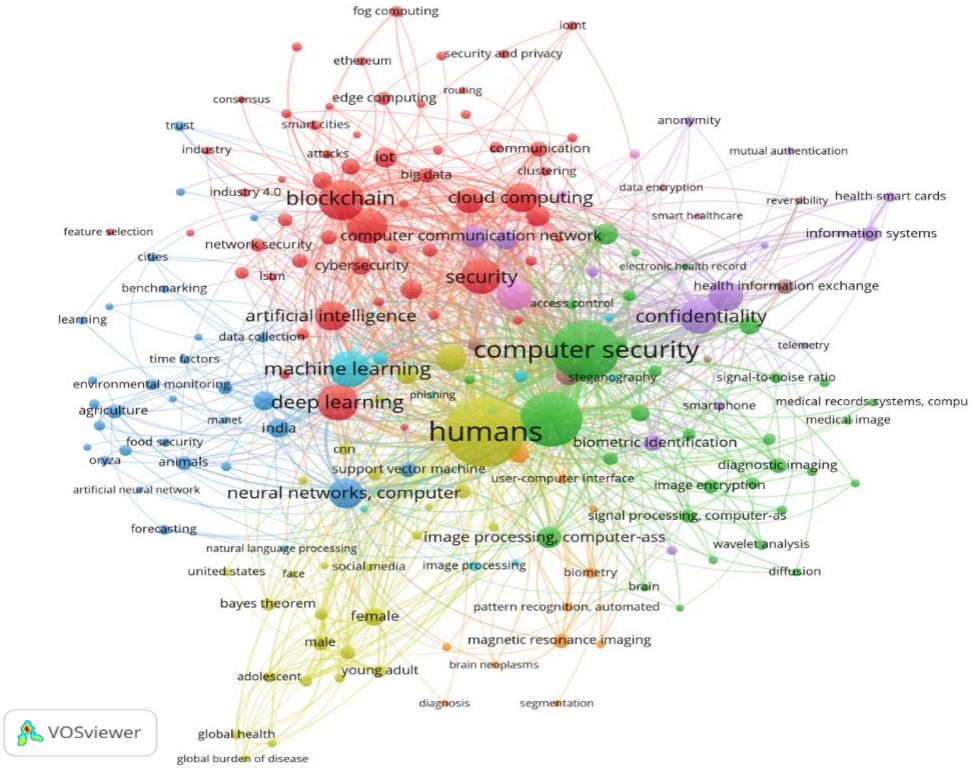
(Date: 30 March 2025; Source: https://www.kaggle.com/code/sonawanelalitsunil/cybersecurity-threats-2015-2024-ml)

DOI: https://doi.org/10.47362/EJSSS.2025.6608

Bibliometric Analysis of Cybersecurity Research Trends

A bibliometric analysis (Figure 5) of cybersecurity research connected to emerging technologies in India was carried out by analysing PubMed database outputs. The visualisation developed by VOS viewer software displays cooperative research relationships between cybersecurity concepts "computer security" and "machine learning" as well as emerging technologies such as "blockchain", "cloud computing" and "deep learning" with traditional security concepts "confidentiality" and "network security" and "data encryption." The results display meaningful interdisciplinary research crossover areas between artificial intelligence cybersecurity implementations and blockchain security systems alongside health informatics privacy protection research. Human-focused security solutions are major focal points of modern cybersecurity because "humans" and "computer security" terms lead the network's central clusters. A bibliometric mapping reveals the immediate need for AI, IoT and security field integration while underscoring India needs unified cross-disciplinary cybersecurity strategies.

Figure 5: Bibliometric map showing cybersecurity research clusters across AI, blockchain, deep learning, and healthcare



(Date: 24 March 2025; Source: https://pubmed.ncbi.nlm.nih.gov/?term=AI+in+ccybersecurity ; created using VOSviewer).

DOI: https://doi.org/10.47362/EJSSS.2025.6608

The cyber risk environment in India experienced fast-paced changes because of national digital transformation programmes together with wide technology adoption and increasing adversary complexity. Ransomware together with data breaches, phishing and hacktivist activities make India one of the country's most frequently targeted by cyber threats worldwide. This section reviews the prevalence of attacks along with their corresponding vulnerabilities by analysing recent empirical data and real-world case examples (Vinoth, 2024; Gupta & Ciso, 2025).

Prevalent Attack Types and Key Vulnerabilities

Among all cyber threats India faces today ransomware attacks represent the most severe problem affecting financial systems as well as banking institutions and healthcare facilities and government departments and information technology corporations. The main strategy of ransomware attackers involves data encryption of vital information which damages business functionality and forces companies to pay exorbitant fees for data retrieval (ETtech, 2024). Collectively known as double or triple extortion service, contemporary threat actors now tend to double down by demanding payment for data decryption as well as threatening to share or attack the stolen information with customers or business partners (Vinoth, 2024).

Phishing operates as an established and highly successful method of digital attack which targets individual and organisational targets. Accompanying the modern sophistication of phishing attacks are deceiving emails combined with fake websites and social media-based impersonations. Financial institutions alongside healthcare providers generate the majority of phishing targets because of their holding sensitive data (Solutions, 2024). Phishing attacks start by granting digital access to systems which then enables attackers to deploy malware or further penetrate target systems. Both public and private organisations experience heightened negative effects from Distributed Denial-of-Service (DDoS) attacks which have become more complex while appearing more frequently. The widespread implementation of cloud-native designs along with APIs has created fresh security vulnerabilities which resulted in API-focused DDoS attacks becoming more frequent than standard web-based incidents (Gupta & Ciso, 2025). Data breaches continue to threaten organisations since adversaries find and take advantage of technical system vulnerabilities along with human mistakes to extract confidential information from phone service providers and banking institutions and healthcare facilities. Cloud infrastructure adoption at a fast pace across India led to new security risks because poorly secured and misconfigured resources enable attackers to access the network (ETtech, 2024).

DOI: https://doi.org/10.47362/EJSSS.2025.6608

Deepfake technology together with AI-assisted attacks have become dominant security threats. Various cybercriminals use artificially created AI content in their phishing attempts as well as their fraud schemes and their activities involving false impersonation. Deepfake technology has committed high-level executive deceit which facilitated fraudulent fund transfers and controlled public opinion during elections according to Desk (2025). India faces cyber-attacks due to three primary reasons which range from financial profit to geopolitical priorities alongside ideological activism. Politically motivated hacktivists perform synchronised attacks against websites during national holidays along with sensitive times which leads to large-scale website defacement and service disturbances (Ajmera, 2025).

The Role and Impact of Cryptocurrency-Enabled Ransomware

Cryptocurrency has revolutionised ransomware attacks in India because it serves as both a payment tool and money laundering method for criminal profits. The ransom requests from cybercriminals now use cryptocurrencies mainly because of their anonymous features which makes it harder for law enforcement to follow money trails. The increasing adoption of mobile ransomware programmes now directs their ransom payments toward privacy-enhanced cryptocurrencies like Monero because Bitcoin offers insufficient hiding capabilities (Ajmera, 2025).

Ransomware perpetrators execute two main actions during an attack by encrypting data files while locking systems before demanding cryptocurrency payments with decryption keys as part of the extortion process. The advanced variant of ransomware actively steals cryptocurrency wallet keys from victimised environments while pursuing data extortion strategies (Ajmera 2025). Ransomware-as-a-Service (RaaS) technology transformed the cybercriminal landscape by building infrastructure for complex attacks which then became reachable to novice attackers through service provider leased systems (Team, 2025; Cisomag, 2021). During 2024 a major hacking attack was reported to have taken place at WazirX which operates as one of India's largest cryptocurrency exchange platforms. Attacks against multi-signature wallets revealed intrinsic vulnerabilities that enabled cybercriminals to steal approximately $230 million worth of assets from the platform (Ajmera 2025, Greig 2024). The crypto platform trust declined substantially after this incident while it demonstrated significant digital asset ecosystem vulnerabilities to public audiences(Ajmera 2025; Team, 2025; Cisomag, 2021).

DOI: https://doi.org/10.47362/EJSSS.2025.6608

Ransomware attackers hit C-Edge Technologies Ltd. with an attack that left the UPI service and Aadhaar-based systems inoperable while cutting off 150-200 cooperative and regional rural banks from their customers and services according to ETtech (2024). The healthcare sector together with manufacturing and IT services continue to battle constant ransomware attacks by attackers who implement double and triple extortion strategies (Khaitan, 2024). The technological anonymity provided by cryptocurrencies drives criminal behaviour through a network of criminal activities that includes ransom payments for stolen data along with dark web marketplaces and illicit information sales. The recurrence of operational disruptions in critical services combined with a decline in public trust persists as a result of these attacks (Barlow, 2024).

Recent Trends in Financial Losses Caused by Cyberattacks

The number of financial losses from cyberattacks in India shows historic heights. The total amount of losses from cyber fraud exceeded ₹1,770 million (equivalent to USD 20 million) in fiscal year 2024 which represented a fourfold increase over previous year figures (Bfsi, 2025). During the first four months of 2024 more than 740,000 cyber fraud cases emerged leading to ₹11,333 crore worth of losses throughout the nine-month period. Statistics indicate that cyber fraud losses will surpass ₹1.2 lakh crore in 2025 and may represent almost 0.7% of India's GDP according to Bhavsar (2025).

Notable cyber incidents in 2024 included:

- The security breach at Bharat Sanchar Nigam Limited (BSNL) led to 278 GB of sensitive data being exposed (ETtech, 2024).
- The cyberattack on Angel One's systems exposed customer information from eight million accounts (ETtech, 2024).
- The WazirX cryptocurrency exchange suffered a security breach resulting in the theft of assets worth $230 million (Ajmera, 2025; Greig, 2024).
- Ransomware attacks against Motilal Oswal Financial Services and Polycab India Ltd. led to operational disruptions and forced ransom payouts (Khaitan, 2024).
- The healthcare provider Star Health Insurance faced a data breach that exposed records from 31 million customers while hackers demanded prices up to $150,000 from dark web marketplaces (Bhavsar 2025).

DOI: https://doi.org/10.47362/EJSSS.2025.6608

Data breaches made worse through illicit sales of stolen information led to increased financial crime and identity theft which magnifies the original economic damage.

Role of Artificial Intelligence in Cyber Defence

Enhancing Threat Detection and Incident Response

AI has revolutionised cyber defence operations through its ability to enhance immediate threat perception together with automated response capabilities that lower the response period to cyber threats (Salem et al., 2024). Security Information and Event Management (SIEM) systems lead this transformation by incorporating machine learning (ML) algorithms to process large security event data continuously from various sources extending to network traffic and system logs and endpoint activity. Forged by AI technology SIEM platforms uses advanced behaviour analytics along with pattern recognition to detect anomalous behaviour from regular activity thereby surpassing traditional signature-based or manual analysis methods (Pulyala, 2024).

SIEM systems receive support from Security Orchestration Automation and Response (SOAR) solutions that use AI technology to enhance incident response workflows (Subudhi, 2024). The AI/ML system within SOAR platforms helps identify alerts then decides their importance through contextual risk analysis to either automate threat resolution procedures with asset isolation or direct serious incidents to human analysts or execute predefined security rules instantly (Subudhi, 2024; Radiant Security, 2024). Human experts dedicate their expertise to complex investigations as well as strategic threat hunting because SOAR platforms automate several regular security tasks such as validation and ticket generation. AI-integrated SOAR solutions reduce response time performance to the point where they can stop or minimise attacks before detection hours pass (Radiant Security, 2024).

AI-driven cybersecurity tools enable the extension of SIEM and SOAR capabilities to create proactive cyber defence methods (Gudimetla & Kotha, 2024). The combination of deep learning (DL) models with advanced analytics enables these tools to identify and categorise new security threats including polymorphic malware and phishing schemes and APTs and botnets during real-time operations at high precision while generating few false alerts (Salem et al., 2024). An intelligent adaptive framework with high scalability exists for today's cyber operations because it provides organisations with an effective speedy defence against evolving attacker strategies (Ofusori et al., 2024).

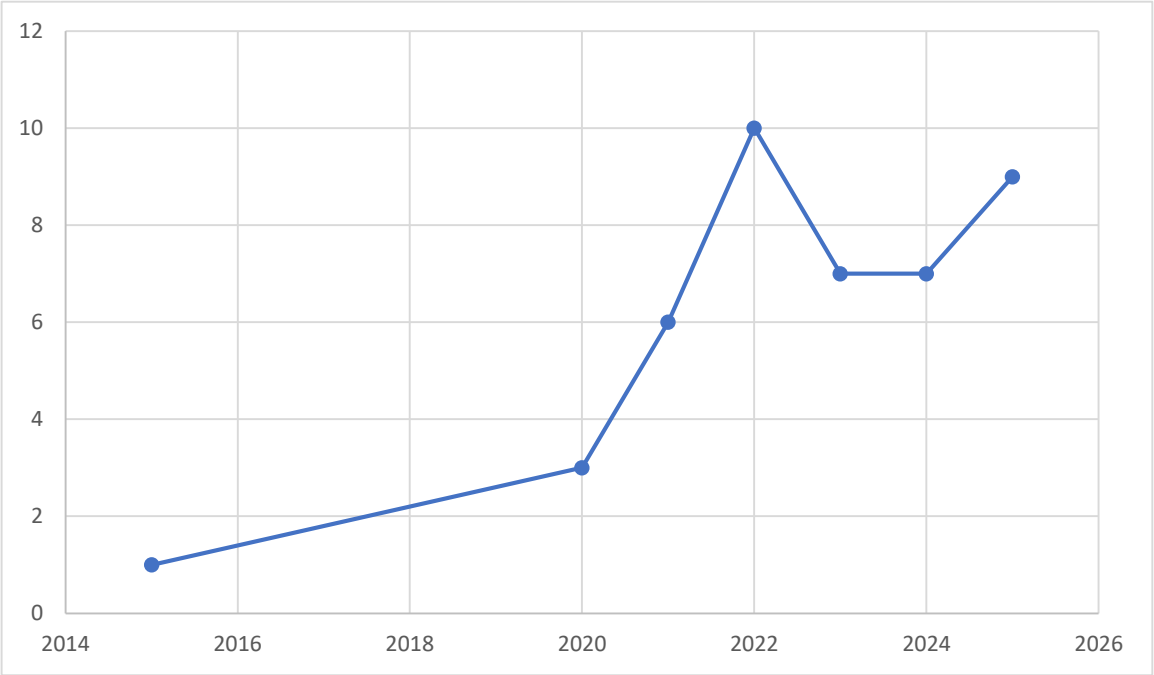
DOI: https://doi.org/10.47362/EJSSS.2025.6608

Predictive Analysis and Anomaly Detection

The combination of predictive modelling and machine learning with cyber defence practises has enabled organisations to adopt preventive security strategies instead of merely reacting to vulnerabilities (Salem et al., 2024). The analysis of historical cybersecurity patterns through ML algorithms helps designers identify potential attack vectors and system vulnerabilities before exploitation (Madala et al., 2023). Through predictive analytics organisations gain predictive capabilities by creating mathematical models from multiple threat intelligence and network data sources which enables them to establish proactive defence mechanisms and optimised cybersecurity resource distribution (Samia et al., 2024). Organisations evolving their cybersecurity approach through anomaly detection implement supervised and unsupervised learning models to discover network or user behavioural deviations from pre-established norms. Rule-based detection methods fall short in stopping new or complex attacks since their signature-based and heuristic analysis proves insufficient (Edozie et al., 2025). AI-based anomaly detection extends its ability to learn from evolving high-dimensional datasets which enables the discovery of multiple malicious activities including insider threats and lateral movement and botnets and network intrusions (Salem et al., 2024). Long Short-Term Memory (LSTM) networks and autoencoders demonstrate exceptional performance in detecting anomalies of voluminous real-time sequential data that telecom and enterprise networks typically generate. The LSTM autoencoder enables users to identify both cyberattacks and system failures through its ability to understand typical temporal patterns in vast network traffic data (Edozie et al., 2025). The combination of traditional machine learning algorithms with deep architecture components through hybrid and ensemble techniques allows enhanced attack detection performance and resilience during detection of persistent and stealthy threats. AI anomaly detection technologies serve as essential components when identifying insider security risks and stopping data theft by detecting human patterns beyond human oversight capacities (Salem et al., 2024). The growing interest in AI cybersecurity research during the past years indicates both the expanding cyber threat environment and the necessity of defensive systems that combine intelligence with adaptability. The number of indexed publications in PubMed about "Artificial Intelligence" and "Cybersecurity" shows a steep increase in Figure 6 through 2025 especially starting from 2020. Machine learning and predictive analytics continue to enter practical security operations while this trend matches the industry analysis provided previously.

Date of publication: 31 July 2025
DOI: https://doi.org/10.47362/EJSSS.2025.6608

Figure 6: Trend of PubMed-indexed publications (2014-2025) mentioning "Artificial Intelligence" and "Cybersecurity," showing rising research focus.



(Date: 24 March 2025; Source:
https://pubmed.ncbi.nlm.nih.gov/?term=AI+in+ccybersecurity)

Emerging Technologies: Adversarial and Federated Learning

Cyber defence research faces new directions coupled with emerging AI paradigms including adversarial machine learning and federated learning (Liu et al., 2022). The field of adversarial machine learning reveals faults in machine learning and AI components through the creation of specialised inputs called adversarial examples which fool advanced deep learning models used for malware detection and biometric authentication and intrusion detection systems (Xi, 2020). The implementation of adversarial samples reduces the predictive capabilities of neural network-based malware detectors by 85% through invisible changes to user or traffic authentication systems (Liu et al., 2022). These findings expose serious security risks with AI defence systems because the models for improved detection easily become targets for advanced evading methods. The development of secure defence mechanisms including adversarial training combined with model assembling and defensive distillation and adversarial input detection has happened in response. Most countermeasures lead to performance reductions or impaired model generalisation and make defence and attack tactics engage in an endless battle (Liu et al., 2022).

DOI: https://doi.org/10.47362/EJSSS.2025.6608

Federated learning (FL) functions as a collaborative decentralised AI methodology which enables multiple entities such as organisations and data centres or edge devices to train ML models collectively by sharing model updates instead of sending raw sensitive data between them (Liu et al., 2022). FL proves suitable for cyber defence applications that limit data aggregation because it allows entities to collaborate through model transfer instead of sharing raw sensitive information (Muzammal et al., 2024). FL maintains privacy by transmitting model updates (weights or gradients) since it enables distributed intelligence access from worldwide data sets that boosts threat detection robustness and generalisation abilities. FL allows security operation centres from several organisations to work together on malware and URL threats through collaborative efforts with no disclosure of sensitive information (Ferrag et al., 2021). The implementation of FL encounters multiple obstacles like poisoning attacks on data and models as well as inference attacks and backdoor insertions and communication overhead. FL deployment requires dependable aggregation protocols as well as differential privacy schemes and continuous auditing mechanisms to achieve security and trustworthiness (Liu et al., 2022).

Critical Cyber Incidents and AI-Based Defense Strategies in India

Since 2015, India was already experiencing various major cyberattacks, which have demonstrated serious weakness of its digital infrastructure. One of the most famous ones was the example of Cosmos Bank cyberattack in 2018, there the organized collective threat showed its high level of sophistication. This type of sophisticated strategy was employed against Cosmos Bank, a large cooperative financial organization, in August 2018, when cybercriminals every debit card cloned and, using these copies, performed more than 12,000 fraudulent actions with ATMs in 28 countries, losing some 94 crores (roughly 13.5 million) in this process in only a few hours. The attackers also made unrecommended SWIFT payments to pipe money to other countries thus forcing the bank to put its ATM and online banking services on hold. This operation entailed colossal downtime to its operations and a dent in its reputation (Odeleye et al., 2022). Some key vulnerabilities were cited as being the reason behind the success of this attack. We can assume that the malware allowed the hackers to access the inside network of the bank, and they managed to remain hidden in the system, working unnoticed during a long flow of time. They were able to hack into the ATM switch server, and therefore they could create and deploy cloned cards without the backend fraud detection systems getting to know about it. Furthermore, inadequate segmentation on the network and the absence of real-time

DOI: https://doi.org/10.47362/EJSSS.2025.6608

monitoring allowed transferring to the sideways within the network and controlling the traffic of approving transactions (Odeleye et al., 2022).

This incident could have been countered had AI-powered cybersecurity systems, including the hypothetical Sentinel Net in place. Real time anomalous transaction behavior discovery that could have been detected by artificial intelligence, e.g. a sharp increase in high-value withdrawals in various countries, was possible. The capability of AI to find a relationship between seemingly dissimilar data, like anomalous network behaviour and transaction anomalies could have helped reveal the orchestration of the attack at an initial stage. Moreover, the real-time automated action of isolating compromised systems or denying suspicious transactions would have saved a considerable amount of money and prevented the spread of the infection before it is too late (Rajyalakshmi & Lakshmanna, 2024; Perumallaplli, 2025).

In November 2022, another important cyber incident took place, as All India Institute of Medical Sciences (AIIMS) in Delhi became a target of a ransomware attack. This hack blocked some of the most important servers compromising the ability to work in the sphere of digital healthcare like billing, patient registration, and medical records. Consequently, the hospital had to work manually, at least temporarily, which seriously affected patient care and even revealed the personal health of millions to third parties (Hijji & Alam, 2021). Their exploits enabled them to access five servers out of 100 by use of weak network partitioning and negligible endpoint security. The unavailability of the real-time detection and automated defense systems enabled the ransomware to spread across and encrypt the bulk of sensitive information. Moreover, its prolonged recovery process indicated the inadequacy of the institution in incident response planning as well as data backup policies (Hijji & Alam, 2021).

In such a case, cybersecurity tools powered by AI may have been crucial to prevent. AI-driven real-time anomaly detectors would detect suspicious file encryption activities, and lateral movement between systems in the early stages of the attack. With the help of correlation between the alerts on endpoints, network shifts, and behavioral patterns of users, AI systems might have smoked out the threat and placed it into context so that the threat is identified prior to gaining critical mass. Furthermore, automated alert systems, i.e., quarantining of infected systems, launching information recovery with the use of uncompromised, secure backups, etc., would have helped tremendously in reducing the activity lost in the operational processes and protecting the integrity of the patients information (Rajyalakshmi & Lakshmanna, 2024; Perumallaplli, 2025).

DOI: https://doi.org/10.47362/EJSSS.2025.6608

The situation described in these Indian case studies emphasizes the necessity to consider the implementation of better, AI-based cybersecurity systems that could reveal, contextualize, and eliminate threats in real-time. The need to be more secure is associated with the increasing complexity and destructive activities occurred in cyberattacks, so traditional security systems are not enough anymore. The ability of AI to learn tirelessly, identify patterns quickly, and act on its own volition should make this type of software a vital tool in the fight against contemporary cybercrime.

Development of an AI-Driven Cyber Defence Framework for India

Framework Architecture and Design Principles

Digital transformation in India's financial sector along with healthcare services and defence systems and energy infrastructure requires an immediate implementation of powerful adaptive cybersecurity architecture. This research presents Sentinel Net (SentinelOne, 2025; Gargiulo et al., 2020; Guo et al., 2021) as a new architectural approach for developing an AI-Governed Cybersecurity Nervous System which defends national infrastructure. The structural and responsive nature of biological neural networks energised Sentinel Net to integrate automated defence layers alongside human-assistance models which protect national crucial infrastructure (Guo et al., 2021).

The proposed architectural system consists of five fundamental components. At the core of the architecture stands the Data Acquisition and Harmonisation Layer which combines different system telemetry from essential infrastructure elements. Standardised API protocols normalise the data while providing secure methods for its transmission. The Adaptive Threat Analysis Layer builds its foundation by using federated learning models which both distribute threat detection of new patterns between institutions and preserve each organisation's data sovereignty (Daram, 2024). The learning procedure happens locally with specific sector data while transferring only new model components to a global system enabling more efficient and private operations. The Interactive AI Command Layer of Sentinel Net functions differently by avoiding autonomous decision-making. Through dialogue-based interfaces the system presents best responses to human operators and predicts outcome possibilities and enhances its capabilities through operator feedback (Ronaldo, 2022). The system enables both explainable procedures and operation accountability. The Autonomous Response Orchestration Layer deploys pre-approved and conditional responses such as dynamic honeypots and micro-segmentation and automated forensic triaging while it depends on AI assurance scores and

DOI: https://doi.org/10.47362/EJSSS.2025.6608

vetted approval from humans (Achuthan et al., 2024). The Self-Healing and Reinforcement Layer enables continuous change management by implementing reinforcement learning frameworks. The defence models receive continual update on distributed nodes via reinforcement learning when the system identifies anomalies or specific breaches (Jaiswal & Mishra, 2024).

The architecture of Sentinel Net prioritises four core principles which are scalability, explainability, interoperability and ethical governance. A national-scale modular deployment system makes Sentinel Net scalable through microservices architecture (Das & Sandhane, 2021). The system places explainability at its core by linking all AI-triggered alerts with clear explanations along with models that maintain transparency for operator confidence (Ronaldo, 2022). Open cybersecurity standards STIX and TAXII are strictly followed to build interoperability which enables protected threat intelligence exchange features (Daram, 2024). The framework includes ethical governance principles that protect users because they both enforce AI ethics regulations and cybersecurity law (Achuthan et al., 2024).

The new Sentinel Net architecture offers a complete, five-layer AI-based cybersecurity framework that would enhance India in strengthening its digital security in carrying out business to its citizens in the key sectors of healthcare, banking, and industrial infrastructure. Data Collection and Preprocessing is the first layer, which is essential to the operation of Sentinel Net. It collects data of a broad scope such as network logs, endpoint sensors, IoT devices, cloud services, and SCADA systems. The collected data becomes structured and relevant to further analysis after exploiting AI-driven means normalizing it and mitigating noise content. Notably, the layer uses federated learning and privacy-preserving technologies, allowing training a model with sensitive data without sharing raw data in the central infrastructure. It does not only increase the adherence to the national regulations but also scalability (Malik et al., 2025; Achuthan et al., 2024). In Indian perspective, this ability is imperative towards facilitating real-time monitoring of hospital networks, banking systems and industrial control infrastructures. This kind of visibility is important in the early identification of ransomware, fraudulent transaction, and SCADA-associated threats (Benmalek, 2024). Anomaly detection in healthcare and finance is also facilitated by the architecture, which creates the contextual datasets, and it is also consistent with the guidelines of CERT-IN on breach reporting and the IT Act in terms of data protection, privacy, and audit trails (Gupta et al., 2023; Kashyap & Chaudhary, 2023).

DOI: https://doi.org/10.47362/EJSSS.2025.6608

The second module, Threat Detection, uses powerful AI models, both supervised, unsupervised, and deep learning such as CNNs, RNNs, and DNNs in detection of intrusions, malware classification and behavioral anomaly detection (Achuthan et al., 2024). Explainable AI (XAI) incorporation is also included as a means of achieving transparent decision-making, which will promote confidence in the decision and lead to high triaging rates of human analysts. These algorithms are dynamic, and keep getting updated in real-time to identify zero-day attacks and advanced persistent threats (APTs). In the Indian cybersecurity ecosystem, the ability of detecting ransomware and lateral movement is hospital networks as observed during the AIIMS hack. It is also crucial in fighting phishing and fraud, which are common in the banking industry in India, and reviewing SCADA systems to identify unknown commands or protocol execution, (Okdem & Okdem, 2024). The outputs of the detectors are relayed to CERT-IN to coordinate threat responses on the national level and sharing of the intelligence. In addition, the AI-generated logs can be audited and comply with the IT Act, which contributes to the legality of admissibility and regulatory transparency (Gupta et al., 2023; Kashyap & Chaudhary, 2023).

Response Coordination is the third layer that coordinates and streamlines incident response techniques. Reinforcement learning is used to automate containment, eradication and recovery operations depending on the type of attack vectors. Such a layer ensures this coordination of the communication between national Security Operations Centers (SOCs) and sectoral CERTs, as well as between these centres and local IT teams, so that a prompt and collective response occurs. Ransomware, banking fraud, and SCADA playbooks allow distributing the standard antidotes in such situations swiftly (Malik et al., 2025). This is especially useful in India, where the healthcare endpoints should be rapidly quarantined during ransomware attack to avoid creating inconveniences in delivering healthcare services to patients. Multi-bank coordination in banks prevents concomitant fraud attempts that increase the systemic risk (Okdem & Okdem, 2024). On the critical infrastructure, the framework enables real-time drills and breach response in protection of SCADA systems (Benmalek, 2024). Incident escalation and notification to CERT-IN as per national policies are also automated in this component and incident logs that are necessary to comply with IT Act are maintained in this component (Gupta et al., 2023; Kashyap & Chaudhary, 2023).

The fourth element, called Policy Enforcement, guarantees the ongoing compliance with regulations and operations by use of AI in them. It controls access control and network segmentation and risk-based observance through adaptive algorithms. It also protects

DOI: https://doi.org/10.47362/EJSSS.2025.6608

vulnerable areas such as finance and healthcare by introducing zero-trust ideas and continuous authentication algorithms. Automated policy compliance reporting is a technology that monitors policy compliance at all sectors (Malik et al., 2025). In practice, this may mean avoiding unauthorized access to the hospital information and track of records which is commonly used as an attack factor and implementing Reserve Bank of India (RBI) procedures to minimize the chances of frauds or insider attacks. The advantages of SCADA systems are that they can introduce sector-specific controls that represent the execution of commands by authorized staff members only (Benmalek, 2024). Policy enforcement systems are directly linked to CERT-IN advisory and IT act requirements and produce evidence that can be used during audits and litigation (Kashyap & Chaudhary, 2023).

Lastly, the fifth layer is the Continuous Learning Loop that positively guarantees that Sentinel Net keeps up with the threat environment. Response and detection models are retrained on new data continuously to reinforce them using federated and reinforcement learning methods to enable them to be adaptive. Feedback and post-incident analysis are also combined within the human loop to enhance precision and minimize false positives, and adversarial machine learning allows the detection and prevention of the development of new attack vectors (Malik et al., 2025; Achuthan et al., 2024). This cycle of learning is essential to adjust to new variants of ransomware attacking Indian hospitals, to come up with fraud models based on the emerging scams in the banking system, and to enhance SCADA security against the new methods of intrusion (Okdem & Okdem, 2024; Benmalek, 2024). Newer models and lessons are also communicated to CERT-IN to drive a countrywide demonstration of threat intelligence activities, and detection systems are constantly updated to ensure they do not violate the growing provisions of the IT Act (Gupta et al., 2023; Kashyap & Chaudhary, 2023).

In conclusion, a Sentinel Net is a high quality, scalable and context-based framework of cybersecurity that fits the Indian digital eco-sphere. Besides the proactive defense and fast incident response, its modular design precondition continuous consistency with the national policies and regulatory requirements. It has the potential to be a central component used to secure India in the future through implementing AI at all stages, including collection of data and non-stop learning.

Integration with National Critical Infrastructure

A strong operational method needs to be developed to implement Sentinel Net successfully in India's cyber defence field as you can refer Table 1. This paper introduces the Public-Private-

DOI: https://doi.org/10.47362/EJSSS.2025.6608

Academic Integration Strategy (PPAIS) as a mechanism to deploy the solution at scale. The model requires National Critical Infrastructure Nodes (NCINs) to instal Sentinel Net agents as monitoring and defensive solutions. The strategy establishes Federated Coordination Centres (FCCs) that exist at national and sectoral levels for managing AI model updates while conducting federated learning aggregation along with coordinating cross-sectoral incident responses (Daram, 2024).

Secure Human-AI Interaction Consoles (SHAICs) would provide human oversight capability through their deployment at control centres. Real-time AI system collaboration would be enabled by these interfaces which allow human personnel to maintain control while making better strategic decisions (Ronaldo, 2022). Sentinel Net agents can identify irregular patterns signals that suggest possible cascading power failures stemming from cyberattacks in the power grid. The system would provide recommendations to operators regarding the best isolated steps to stop power grid-wide failure patterns (Jaiswal & Mishra, 2024). The integration process requires protective data agreements, end-to-end encryption systems and repeated red-teaming evaluations for rigorous adversarial threat tests on AI models. Identification of system weaknesses combined with data collection through these exercises supports the continuous betterment of system performance (Marda, 2018).

Table 1: India's 'Sentinel Net': Comparative Advantages (Amandeep, 2025)**.**

Feature/Dimension	**Global Best Practices (US, Israel, UK, Singapore)**	**Sentinel Net (India)**
Architecture	Modular, layered, containerized	Modular, context-aware, sector-adaptive
AI Methods	Deep learning, hybrid detection, explainability	Deep learning, real-time, explainable AI
Sectoral Scalability	Cloud-native, scalable, but often sector-specific	Designed for multi-sector, pan-India scaling
Context Awareness	Generalized, global threat models	Tailored to India's digital, linguistic, and regulatory diversity
Regulatory Alignment	Aligned with local laws (GDPR, NIS, etc.)	Explicitly mapped to IT Act, CERT-IN, Indian sectoral regulations
Explainability/Transparency	SHAP, LIME, visual analytics	SHAP, LIME, enhanced for regulatory audits

DOI: https://doi.org/10.47362/EJSSS.2025.6608

(Date: 8 April 2024; Source: http://dx.doi.org/10.22214/ijraset.2025.72761).

Case Studies and Comparative Analysis

Global Best Practices in AI Cyber Defence (USA, EU) - United States

The United States maintains a leading position in implementing Artificial Intelligence (AI) strategies for cybersecurity protection. The Department of Homeland Security (DHS) stresses that AI regulations need to align with international partners because split policies generate potential weak points. During his time as DHS chief Alejandro Mayorkas expressed concerns about worsened European-tech company relationships because they could compromise global AI regulatory efforts thus creating areas where security vulnerabilities could emerge (Criddle & Kinder, 2024). Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger highlighted how AI exists in a contradictory position regarding cybersecurity issues. The deployment of AI-based solutions in critical infrastructure requires thorough risk evaluations and standards definition before implementation due to its dual nature of offering advantages alongside significant security concerns (Graff, 2024).

European Union

European Union institutions have taken a rigid regulatory position toward AI technology in cybersecurity frameworks. The Artificial Intelligence Act of the EU provides a multi-faceted legal framework for AI which concentrates on risk management systems alongside provisions for transparency and human control and accountability measures. The EU systematically develops a regulatory foundation which integrates trust enhancement measures for AI technologies alongside human rights protection mechanisms. European Union military expenditures now include substantial funds for developing AI-enhanced communication networks and constructing autonomous combat drones. The European Defence Fund plans to use €1.1 billion in 2024 for projects that boost European military strength and defend its industry against changing global security risks (Zorloni, 2024).

Lessons for India from International Implementations

India can learn multiple beneficial approaches to AI-driven cybersecurity from both United States and European Union cybersecurity strategies.

DOI: https://doi.org/10.47362/EJSSS.2025.6608

- EU regulatory frameworks place premium value on complete AI legislation because they help create balanced protocols to nurture innovation within ethical boundaries. India needs to establish equivalent platforms for managing AI applications in cybersecurity which will uphold both accountability along with transparency.
- The United States maintains effective cybersecurity through its aggressive approach to AI research coupled with major funding for development and continued innovation. India needs to allocate funding toward research of AI technology to build homegrown solutions which solve its individual cybersecurity difficulties.
- India should engage in international cybersecurity dialogue and cooperation activities regarding AI regulations and standards since cyber threats operate at a global scale. India's cyber resilience will improve through worldwide cybersecurity best practise adoption alongside expansion of knowledge sharing possibilities.

Strategies implemented in this manner will fortify India's cyber defence structures powered by artificial intelligence which will protect from modern evolving cyber hazards.

The Sentinel Net framework presents a flexible modular platform for cybersecurity which understands the growing complexities found in India's digital environment. The framework achieves its goal of detecting and mitigating different cyber threats such as phishing and ransomware attacks together with advanced persistent threats (APTs) via combination of AI analytics and predictive modelling along with real-time threat intelligence. Existing research demonstrates the ability of Sentinel Net to defend against a wide range of attack targets. The authors of Omerovic et al. (2019) explain that risk identification methods need customization since traditional one-fits-all cybersecurity models do not match the intricate requirements of smart power grids and other complex structures. Their research proves the need for customised security solutions so the Sentinel Net framework delivers this through its adaptable structure that includes context-sensitive functions.

Binyamini et al. (2021) developed an automated system for creating models about cyberattack approaches using vulnerability details to showcase the importance of adaptive real-time defence technologies. The fundamental design principle of Sentinel Net emphasises the need for cybersecurity frameworks to constantly adapt to emerging threats while confirming this requirement. A modular design of the Sentinel Net system allows for simple additions to existing infrastructure therefore supporting both staged implementation and expansion capabilities. Central infrastructure sectors can adopt AI-defence capabilities through gradual

DOI: https://doi.org/10.47362/EJSSS.2025.6608

implementation steps which prevent disruptive infrastructure changes. Organisations can apply model-based risk analysis methods like CORAS method according to Omerovic et al. (2019) to validate the theoretical framework. CORAS enables structured risk modelling which Sentinel Net applies to its risk analysis and mitigation functions to build a strong security environment that identifies and plans responses to potential cyber threats. The work by Binyamini et al. (2021) demonstrates how predictive features reinforce artificial intelligence's vital role in optimising threat recognition and incident response functions. Similar to Sentinel Net's function the integrated machine learning algorithms predict possible weaknesses and enemy actions so organisations can defend proactively instead of responding to threats (Binyamini et al., 2021). The feasibility aspects for deployment in actual revolutionary settings are clearly established. The implementation of Sentinel Net fulfils the current research criteria while resolving issues related to system interoperability and resource management and compliance requirements. The implementation of layered security with predictive intelligence serves to decrease detection delays while improving response precision and strengthening national cyber defences (Guo et al., 2021).

AI Integration into India's Cybersecurity Legal and Regulatory Frameworks: The Role of Sentinel Net

The potential of AI technologies in strengthening the cybersecurity infrastructure of India is enormous once these technologies combine with the legal provisions (and consequently the existing systems) that the country already has like the Information Technology (IT) Act, 2000 and the operating guidelines of CERT-IN. Automated incident detection is one of the most significant uses of AI. The AI-powered systems are capable of examining large volumes of network traffic, system logging and behavioural data in real time to detect anomalous patterns, zero-day exploits and other advanced threats that are proving difficult to detect to actualize them through conventional system such as. Machine learning algorithms enable that proactive threat classification occurs, that containment protocols are run automatically, and that intelligent alerts are issued to human analysts, and it saves a lot of time before human analysts can reduce or even mitigate the damage done in the initial phase of an attack (Choudhary, 2024). Such a system as Sentinel Net might combine those functions to allow uninterrupted adaptive monitoring of both secure and insecure networks and meet the mandate of CERT-IN to organize timely responses to cyber incidents (Yang et al., 2022).

DOI: https://doi.org/10.47362/EJSSS.2025.6608

Besides the threat detection, another important way AI can be used is through the guarantee of regulatory compliance in real-time, especially with clauses like Section 70B of the IT Act where it requires timely reporting of cybersecurity breaches to CERT-IN. They can also have embedded regulatory logic in AI systems that can keep track of compliance requirement, detect notifiable incidents and automatically produce structured reports within the legal threshold. Systems such as the Sentinel Net minimize the element of human error and increase the capability that an organization will strive to meet the statutory timelines by automating the reporting workflow. This capability is especially relevant considering the context of the evolving Indian cybersecurity regulations including the introduction of the Digital Personal Data Protection (DPDP) Act, 2023 and updated CERT-IN guidelines aimed at enhancing the timeliness of the breach notification and highly standards of data privacy and security (Jaiswal & Mishra, 2024).

The sharing of threat intelligence is also boosted by AIs which allows real-time, structured and anonymized exchange of threat information between organisation and even at a national level with the CERT-IN. Such tools as Natural Language Processing (NLP) and AI-based data normalization allow extracting actionable data out of a variety of unstructured data sources, clean them to eliminate personally identifiable information (PII), and convert them into standardized formats to share securely. The AI-based systems may be used to fully automate the process of collecting, correlating, and distributing threat intelligence, thus increasing the collective defense potential of the nation. A network of this nature, e.g. Sentinel Net, may institutionalize such processes since it creates a pattern of information flow between sectors, establishing safe lines of interactions, and at the same time adopts the concept of privacy-by-design to adhere to principles of data minimisation, consent, and limitation of purpose in line with the stipulations outlined in the DPDP Act (Jaiswal & Mishra, 2024).

Dynamic risk classification is another essential use of AI because it would make sure that risk assessment is regularly updated due to the emergence of new threats and changes in regulation. Based on regulatory changes, threat feeds and sector-specific contextual data, AI-powered risk engines are able to ingest risk dimensions and clusters them to ensure efficiency in ranking vulnerabilities and the ways to mitigate them. It is also optional to include legal taxonomies, compliance lists, and audit trails within these systems in order to guarantee all risk assessments are written within the confines of the current law, especially as India considers the introduction of the proposed Digital India Act, and national increases in protection of important infrastructure and sensitive personal information. In that regard, Sentinel Net may start playing

DOI: https://doi.org/10.47362/EJSSS.2025.6608

the role of the compliance-aware cybersecurity platform providing real-time dashboards and automated compliance reporting capabilities to regulators and other stakeholders as well (Jaiswal & Mishra, 2024).

Through the case model of Sentinel Net, it is possible to illustrate the ways in which AI can maximise efficiency, scalability, and legal-consistency of the cybersecurity strategy in India. Upon efficiency, the automatization based on AI reduces the amount of manual labor and speeds up incident handling, thus enabling organizations to respond quickly to new threats (Choudhary, 2024; Yang et al., 2022). Its scalable architecture enables endless surveillance of genuinely huge, confusing, and dispensed systems, which is an essential need in India because India is in a period of rapid digital growth (Yang et al., 2022). Legally, the embedding of the compliance modules to the Sentinel Net satisfies provision as all the steps under the cybersecurity procedures, including detection, classification, reporting, and sharing intelligence, comply with the legal requirements in India according to IT Act, CERT-IN advisories, and DPDP Act (Jaiswal & Mishra, 2024).

However, legal and strategic issues should be accessed to propose responsible and successful implementation of AI in cybersecurity. Although the IT Act, 2000 and CERT-IN guidelines provide a legal basis, they do not contain specific aspects of the law that target AI-related issues like algorithm bias, explainability and accountability of autonomous decisions. The DPDP Act makes the concept of consent, limitation of purpose, and data minimization critically important and must be enabled within the scope of AI algorithms (cybersecurity application examples). Periodic auditing of AI systems is also becoming increasingly desirable as an enforcement mechanism in terms of fairness, accountability, and transparency. Moreover, there is a need to ensure the harmonization of India across the sectoral regulatory entities, such as, finance, healthcare and critical infrastructure, to eliminate patchy obligations and establish a unified, national body of cybersecurity policy (Jaiswal & Mishra, 2024).

Finally, the opportunity to incorporate AI technology into the cybersecurity regulation mechanism in India can be described as groundbreaking. The legal and ethical flexibility that such frameworks as Sentinel Net might provide will likely present not just the technological but also the legal ethical strength that India might need to face the next wave of cyber threats in a robust and regulatory-savvy manner.

DOI: https://doi.org/10.47362/EJSSS.2025.6608

Conclusion

The changing digital environment of India brings forward exceptional chances alongside substantial security challenges within the cybersecurity domain. National digital advancement projects like Digital India and Smart Cities create growing cyber threats which require a strong and flexible cybersecurity defence system. The rapid increase of cybercriminal activities that cause financial losses in finance and healthcare and infrastructure sectors means there is an immediate need for modern security solutions to combat sophisticated adversarial methods. Using AI for cybersecurity defence constitutes an essential step towards solving modern security challenges. National digital security takes a groundbreaking turn through AI which delivers instant threat spotting as well as predictive abilities to handle incidents automatically. The forward-thinking "Sentinel Net" framework applies AI analytics with human involvement to build resilient cyber defence through an innovative structure. The Sentinel Net framework achieves its purpose to defend India's diverse digital architecture with its combination of multi-tier defences and learning mechanisms that enable a resilient response to regional vulnerabilities.

The bibliometric analysis identifies expanding interest in AI cybersecurity topics as researchers understand their mutual importance and acknowledge the necessity of multidisciplinary team cooperation. The framework must incorporate design principles of scalability with explainable capabilities while maintaining interoperability standards along with ethical governance strategies because they advance trust-based practises and regulatory compliance. The Public-Private-Academic Integration Strategy (PPAIS) proposed for implementation enhances the framework's potential because it brings public-private and academic partnership to achieve comprehensive national cybersecurity solutions. India must learn important lessons about its cyber risks from global best practises which specifically focus on American and European Union approaches. The combination of integrated regulatory systems with development research funding and global partnerships will supply India with essential guidance for improving its AI-automated cybersecurity measures. India will build its resistance against modern cyber-attacks through these adopted strategies thus protecting both national infrastructure security and public trust. The implementation success of Sentinel Net combined with the new policies depends on unified dedication from all stakeholders consisting of public agencies alongside private sector representatives along with academic organisations. Through innovation along with collaboration and continuous improvement India will make its way to lead the cybersecurity field while securing its digital future. India's path to defend a digital

DOI: https://doi.org/10.47362/EJSSS.2025.6608

environment continues indefinitely as it becomes a powerful nation to face complex cyber threats with effective strategic measures.

References

Achuthan, K., Ramanathan, S., Srinivas, S., & Raman, R. (2024). Advancing cybersecurity and privacy with artificial intelligence: current trends and future research directions. *Frontiers in Big Data*, *7*.

Ajaykumar, S. (2024). Securing India's critical infrastructure: Prioritising cybersecurity in chemical facilities.

Ajmera, V. (2025). Shocking Rise in Hacktivist Cyber Attacks in India & What It Means for 2025! *Cloudsek White Papers and Report*.

Amandeep. (2025). CyberSentinel AI: An intelligent cybersecurity framework using artificial intelligence. *International Journal for Research in Applied Science and Engineering Technology*, *13*(6), 2679–2686.

Barlow, E. (2024). Cyber Security in India- Concerns & Actions.

Barth, S., De Jong, M. D., Junger, M., Hartel, P. H., & Roppelt, J. C. (2019). Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and Informatics*, *41*, 55–69.

Benmalek, M. (2024). Ransomware on cyber-physical systems: Taxonomies, case studies, security gaps, and open challenges. *Internet of Things and Cyber-Physical Systems*, *4*, 186–202.

Bfsi, E. (2025). Cyber fraud cases jumped over four-fold in FY2024, caused ₹175 crore losses: Govt data. *ETBFSI.com*. Retrieved from

Bhanushali, A. (2025). AI-Driven cybersecurity: a cornerstone of national security amidst emerging threats and innovative solutions. *International Journal for Research in Applied Science and Engineering Technology*, *13*(3), 1265–1269.

Bhavsar, R. (2025). India’s major cybersecurity incidents of 2024: What lies ahead in 2025 - 63SATS Cybertech.

Binyamini, H., Bitton, R., Inokuchi, M., Yagyu, T., Elovici, Y., & Shabtai, A. (2021). A Framework for Modeling Cyber Attack Techniques from Security Vulnerability Descriptions. *In Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery & Data Mining*, 2574–2583.

Chakraborty, A., & Tiwari, S. (2025). An analytical study on challenges and gaps in India’s cyber security framework. *International Journal of Criminal Common and Statutory Law*, *5*(1), 04–07.

DOI: https://doi.org/10.47362/EJSSS.2025.6608

Choudhary, S. (2024). AI and Cyber Security with Reference to Information Technology Act, 2000 and other Laws in India. *International Journal for Research in Applied Science and Engineering Technology*, *12*(1), 720–723.

Cisomag. (2021). Indian organizations among most targeted for ransomware; most pay ransom. *CISO MAG | Cyber Security Magazine*.

Criddle, C., & Kinder, T. (2024). US Homeland Security chief warns EU over effort to police AI. *Financial Times*.

Daram, S. (2024). Securing the Future: AI-Driven cyber defenses in a hyperconnected world. *International Journal of Computer Trends and Technology*, *72*(10), 173–182.

Das, R., & Sandhane, R. (2021). Artificial intelligence in cyber security. *Journal of Physics Conference Series*, *1964*(4), 042072.

Desk, T. (2025, April 9). Crypto poses cybersecurity risks to India's financial sector: Digital Threat Report 2024. *The Indian Express*.

Edozie, E., Shuaibu, A. N., Sadiq, B. O., & John, U. K. (2025). Artificial intelligence advances in anomaly detection for telecom networks. *Artificial Intelligence Review*, *58*(4).

ETtech. (2024). Year ender 2024: Biggest cyberattacks in India. *The Economic Times*.

Ferrag, M. A., Friha, O., Maglaras, L., Janicke, H., & Shu, L. (2021). Federated Deep Learning for Cyber Security in the Internet of Things: concepts, applications, and experimental analysis. *IEEE Access*, *9*, 138509–138542.

Gandhi, P., & Pahwa, S. (2024). All India Institute of Medical Sciences (AIIMS), Delhi: Cyberattack Puts Digitalisation Under Scanner. *IMIB Journal of Innovation and Management*.

Gargiulo, M., Dell'Aglio, D. a. G., Iodice, A., Riccio, D., & Ruello, G. (2020). Integration of Sentinel-1 and Sentinel-2 data for land cover mapping using W-Net. *Sensors*, *20*(10), 2969.

Graff, G. M. (2024). Anne Neuberger, a top White House cyber official, sees the "Promise and peril" in AI. *WIRED*. Retrieved from

Greig, J. (2024). Indian crypto platform WazirX confirms $230 million stolen during cyberattack.

Gudimetla, S. R., & Kotha, N. R. (2024). ENHANCING THREAT DETECTION AND RESPONSE STRATEGIES. *International Research Journal of Modernization in Engineering Technology and Science*.

Guo, M., Yu, Z., Xu, Y., Huang, Y., & Li, C. (2021). ME-NET: a deep convolutional neural network for extracting mangrove using Sentinel-2A data. *Remote Sensing*, *13*(7), 1292.

Gupta, M., Akiri, C., Aryal, K., Parker, E., & Praharaj, L. (2023). From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy. *IEEE Access*, *11*, 80218–80245.

Gupta, R., & Ciso, E. (2025, March 5). The growing threat of cyberattacks in India's tier-2 markets. *ETCISO.in*.

DOI: https://doi.org/10.47362/EJSSS.2025.6608

Hijji, M., & Alam, G. (2021). A multivocal literature review on growing social engineering based Cyber-Attacks/Threats during the COVID-19 Pandemic: Challenges and Prospective Solutions. *IEEE Access*, *9*, 7152–7169.

Jaiswal, A., & Mishra, P. C. (2024). Artificial intelligence (ai) and cybersecurity law: legal issues in ai-driven cyber defense and offense. *ShodhKosh Journal of Visual and Performing Arts*, *5*(6).

Jaiswal, A., & Mishra, P. C. (2024). ARTIFICIAL INTELLIGENCE (AI) AND CYBERSECURITY LAW: LEGAL ISSUES IN AI-DRIVEN CYBER DEFENSE AND OFFENSE. *ShodhKosh Journal of Visual and Performing Arts*, *5*(6).

Kaloudi, N., & Li, J. (2020). The AI-Based cyber threat landscape. *ACM Computing Surveys*, *53*(1), 1–34.

Kashyap, A. K., & Chaudhary, M. (2023). Cyber security laws and safety in e-commerce in India. *Law And Safety*, *89*(2), 207–216.

Khaitan, A. (2024). The Top 15 Cyberattacks that Rocked India in 2024. *The Cyber Express*.

Lemos, R. (2025). India Is Top Global Target for Hacktivists, Regional APTs. *Dark Reading*.

Liu, P., Xu, X., & Wang, W. (2022). Threats, attacks and defenses to federated learning: issues, taxonomy and perspectives. *Cybersecurity*, *5*(1).

Madala, R., Vijayakumar, N., N, N., Verma, S., Chandvekar, S. D., & Singh, D. P. (2023). Automated AI Research On Cyber Attack Prediction And Security Design. *International Conference on Contemporary Computing and Informatics*, 1391–1395.

Malik, A., Arshid, K., Noonari, N., & Munir, R. (2025). Artificial Intelligence-Driven Cybersecurity Framework using machine learning for advanced threat detection and prevention. *Scholars Journal of Engineering and Technology*, *13*(06), 401–423.

Marda, V. (2018). Artificial intelligence policy in India: a framework for engaging the limits of data-driven decision-making. *Philosophical Transactions of the Royal Society a Mathematical Physical and Engineering Sciences*, *376*(2133), 20180087.

Muzammal, S. M., Bibi, R., Waseem, H., Din, S. N. U., Jhanjhi, N. Z., & Tayyab, M. (2024). Federated Learning for Collaborative Cyber Defense. In *Advances in digital crime, forensics, and cyber terrorism book series* (pp. 1–28).

Nigam, S., & Srivastava, V. (2024). Exploring the impact of artificial intelligence on Indian national security dynamics. *International Journal of Law Management & Humanities*, *7*(5), 2161–2178.

Odeleye, B., Loukas, G., Heartfield, R., Sakellari, G., Panaousis, E., & Spyridonis, F. (2022). Virtually secure: A taxonomic assessment of cybersecurity challenges in virtual reality environments. *Computers & Security*, *124*, 102951.

Ofusori, L., Bokaba, T., & Mhlongo, S. (2024). Artificial intelligence in cybersecurity: a comprehensive review and future direction. *Applied Artificial Intelligence*, *38*(1).

Okdem, S., & Okdem, S. (2024). Artificial intelligence in Cybersecurity: A review and a case study. *Applied Sciences*, *14*(22), 10487.

Omerovic, A., Vefsnmo, H., Erdogan, G., Gjerde, O., Gramme, E. and Simonsen, S. (2019). A Feasibility Study of a Method for Identification and Modelling of Cybersecurity Risks in

DOI: https://doi.org/10.47362/EJSSS.2025.6608

the Context of Smart Power Grids. In *Proceedings of the 4th International Conference on Complexity, Future Information Systems and Risk - COMPLEXIS*; ISBN 978-989-758-366-7; ISSN 2184-5034, SciTePress, pages 39-51.

Perumallaplli, R. (2025). AI in Real-Time Cybersecurity: Enhancing Threat Detection in Dynamic Networks. *SSRN Electronic Journal*.

Pulyala, S. R. (2024). From detection to prediction: AI-powered SIEM for proactive threat hunting and risk mitigation. *Türk Bilgisayar Ve Matematik Eğitimi Dergisi*, *15*(1), 34–43.

Radiant Security. (2024). AI-Driven Incident Response: definition and components..

Rajyalakshmi, V., & Lakshmanna, K. (2024). SentinelGuard Pro: Deploying Cutting-Edge FusionNet for unerring detection and enforcement of wrong parking incidents. *International Journal of Network Management*, *35*(1).

Reddy, C. S., Babu, G. A., Prasad, T. D., & Reddy, P. M. (2024). Cyber security challenges and best practices for protecting critical infrastructure in india: a comprehensive study. *International Journal of Applied and Advanced Scientific Research*, (1), 79–86. journal-article.

Ronaldo, S. (2022). The Role of AI in Securing Critical Infrastructure: A Data-Driven Approach to Cyber Defense.

Salem, A. H., Azzam, S. M., Emam, O. E., & Abohany, A. A. (2024). Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. *Journal of Big Data*, *11*(1).

Samia, N., Saha, S., & Haque, A. (2024). Predicting and mitigating cyber threats through data mining and machine learning. *Computer Communications*, *228*, 107949.

SentinelOne. (2025). SentinelOne, AI-Powered Enterprise Cybersecurity Platform.

Sharma, S. (2023). 13 lakh cyber attacks hit Indian banks in 10 months; Who is behind them? *India Today*.

Solutions, P. (2024). Cyber Attacks in India: A Comprehensive and In-Depth analysis.

Subudhi, S. (2024). Effectiveness of AI/ML in SOAR (Security Automation and Orchestration) Platforms. *International Journal of Science and Research (IJSR)*, *13*(8), 201–206.

Team, C. (2025, February 5). 35% Year-over-Year Decrease in Ransomware Payments, Less than Half of Recorded Incidents Resulted in Victim Payments.

The Hindu Bureau. (2024). Incidents of cyberattacks on India may reach 17 trillion by 2047: Study.

Tiwari, M., Gandhar, A., Gandhar, S., Kumar, S. B., Rehalia, A., Priyadarshi, P., & Gupta, S. (2024). A survey of cybersecurity threats and countermeasures in the Indian financial sector. *Journal of Information and Optimization Sciences*, *45*(2), 507–514.

Vinoth. (2024). Ransomware attacks in India - Gokulam seek IAS Academy.

Xi, B. (2020). Adversarial machine learning for cybersecurity and computer vision: Current developments and challenges. *Wiley Interdisciplinary Reviews Computational Statistics*, *12*(5).

DOI: https://doi.org/10.47362/EJSSS.2025.6608

Yang, M., Chen, L., Wang, J., Msigwa, G., Osman, A. I., Fawzy, S., Rooney, D. W., & Yap, P. (2022). Circular economy strategies for combating climate change and other environmental issues. *Environmental Chemistry Letters*, *21*(1), 55–80.

Zhao, R., John, S., Karas, S., Bussell, C., Roberts, J., Six, D., Yue, C. (2017). Design and evaluation of the highly insidious extreme phishing attacks. *Computers & Security*, *70*, 634–647.

Zorloni, L. (2024). Europe is pumping billions into new military tech. *WIRED*.

DOI: https://doi.org/10.47362/EJSSS.2025.6608

Additional Readings

Arif, A., Khan, M. I., Khan, A. R. A., Anjum, N., & Arif, H. (2025). AI-Driven Cybersecurity Predictions: Safeguarding California's digital landscape. *International Journal of Innovative Research in Computer Science & Technology*, *13*(1), 74–78.

Bharadiya, J. P. (2023). AI-Driven Security: How Machine learning will shape the future of Cybersecurity and Web 3. *American Journal of Neural Networks and Applications*.

Bonagiri, K., S, N. M. V., Gopalsamy, M., A, I., R, R. H. H., & J, S. S. (2024). AI-Driven Healthcare Cyber-Security: Protecting Patient Data and Medical Devices. *Second International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI), Coimbatore*, 107–112.

Dinu, A., Vasile, P. C., & Georgescu, A. (2024). AI-driven solutions for cybersecurity: comparative analysis and ethical aspects. *Revista Română De Informatică Şi Automatică*, *34*(3), 35–48.

Guembe, B., Azeta, A., Misra, S., Osamor, V. C., Fernandez-Sanz, L., & Pospelova, V. (2022). The emerging threat of AI-driven cyber-attacks: a review. *Applied Artificial Intelligence*, *36*(1).

Jimmy, F. (2021). Emerging threats: the latest cybersecurity risks and the role of artificial intelligence in enhancing cybersecurity defenses. *International Journal of Scientific Research and Management (IJSRM)*, *9*(02), 564–574.

Khan, M. I., Arif, A., Khan, A. R. A., Anjum, N., & Arif, H. (2025). The dual role of artificial intelligence in cybersecurity: enhancing defense and navigating challenges. *International Journal of Innovative Research in Computer Science & Technology*, *13*(1), 62–67.

Malatji, M., & Tolah, A. (2024). Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI. *AI And Ethics*.

Ojo, N. B., & Aghaunor, N. C. T. (2024). AI-driven cybersecurity solutions for real-time threat detection in critical infrastructure. *International Journal of Science and Research Archive*, *12*(2), 1716–1726.

DOI: https://doi.org/10.47362/EJSSS.2025.6608

Keywords and Definitions

1. Cybersecurity: It refers to the practice of protecting systems, networks, and programs from digital attacks, and unauthorized access. It involves technologies, processes, and controls designed to safeguard information integrity, confidentiality, and availability.
2. Artificial Intelligence: It is a branch of computer science focused on creating systems capable of performing tasks that typically require human intelligence.
3. Sentinel Net: It is a conceptual or actual cybersecurity framework or system that uses AI and distributed computing to monitor, detect, and respond to cyber threats in real time.
4. Digital Transformation: It is the integration of digital technologies into all aspects of business and government operations, fundamentally changing how organizations operate and deliver value to stakeholders.
5. Threat Detection: It is the process of identifying malicious activity or unauthorized access attempts within a network or system.
6. Federated Learning: It is a decentralized approach to machine learning where models are trained across multiple devices or servers holding local data samples, without exchanging the actual data.