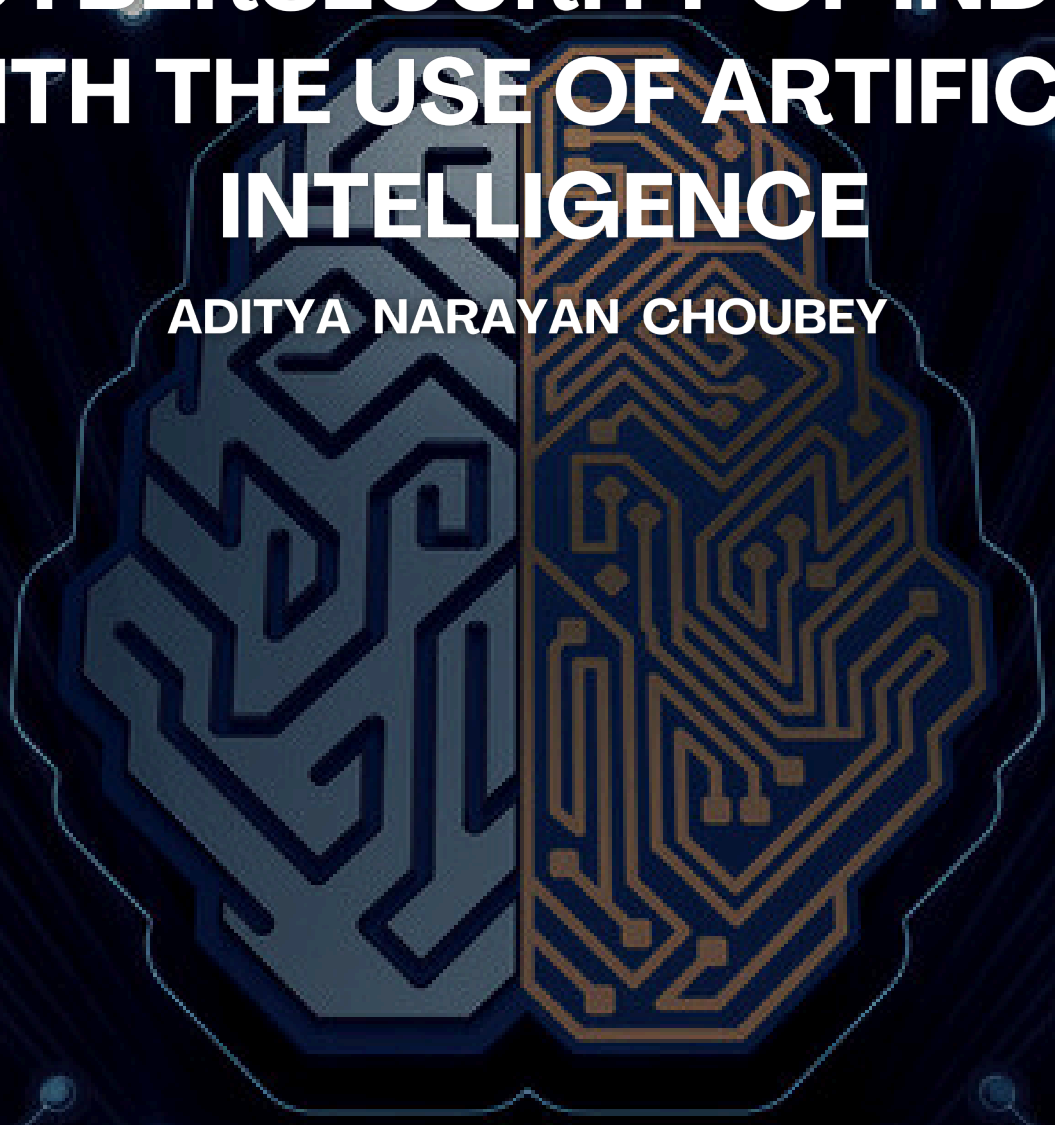
CENJOWS

WEB ARTICLE
WA/20/24

# STRENGTHENING NATIONAL CYBERSECURITY OF INDIA WITH THE USE OF ARTIFICIAL INTELLIGENCE

ADITYA NARAYAN CHOUBEY



www.cenjows.in

CENTRE FOR JOINT WARFARE STUDIES

CENJOWS

# STRENGTHENING NATIONAL CYBERSECURITY OF INDIA WITH THE USE OF ARTIFICIAL INTELLIGENCE

**Aditya Narayan Choubey** is a Research Intern at CENJOWS, New Delhi.

## Introduction

The Fourth Industrial Revolution (IR4) provided us with the cyber domain. Since then, the internet networks have flourished and there has been a boom in the virtual domain. Computers have become the new powerhouses of data allowing their easy sharing. This has shrunk boundaries between nations and allowed internet technologies and internet communications to play a pivotal role in bringing technological globalization.[1] Such an evolution has made corporations, nations and individuals to rely on huge chunk of data on a near daily basis. As a result, digital data has become important as it can be used to derive new insights making it the 'new oil'. Like oil, today, data is valuable, but if unrefined, it cannot provide the best insights.[2] This 'oil' needs protection as it can be used to help in retaining customers, upselling, create new revenue models, increase advertising, etc.[3] Thus, it is natural that in this data-rich era where information flows like an endless river, there are high risks and vulnerabilities because of the value this data possesses.

Since the data was found to be the 'next-oil', cyber threats through acts of stealing, compromising, or unauthorised access of this data emerged. Such cyber threats as

malicious acts emerged as a driving factor for corporations, nations and individuals to resort to certain 'cybersecurity' measures that can eliminate these cyber threats. As per CISA (Cybersecurity and Infrastructure Security Agency), "Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information".[4] Major threats that exist in the cyberspace include use of worms and viruses that tend to compromise the CIA (Confidentiality, Integrity and Availability) triad of cybersecurity systems.[5] Accordingly, national cybersecurity systems across the globe have been improving over the time because of history of attacks starting right from the creeper virus of 1971 to ransomware attacks of 2017.[6] With the advent of emerging technologies like Artificial Intelligence, a lot more can be done to enhance the domain of cyber. It is with this understanding that this article attempts to explore the use of Artificial Intelligence (AI) for enhancing national cybersecurity in the Indian context.

**Indian Cyberspace**

Indian Cyberspace evolved exponentially and independently because of the "Snowden's Revelations".[7] Documents leaked by Snowden indicate that much of NSA's (National Security Agency) surveillance was focused on Indian cyberspace thereby exposing a lot of vulnerabilities in the Indian cyber-domain.[8] Even while Indian cyberspace was found to be vulnerable the 'Cambridge Analytica' scandal shows how matured democracies like UK and USA are also vulnerable to cyber manipulation.[9]

Post Snowden's revelations, digitisation in India occurred at a tremendous pace with India becoming the second fastest digitising economy after Indonesia.[10] Moreover, since many of the CIIs (Critical Information Infrastructure) of India are heavily reliant on the virtual domain, the security of this data becomes critical thereby necessitating a robust cybersecurity framework. However, the existing cybersecurity is found to be currently lacking given the fact that the Indian cyberspace has been breached successfully at regular intervals.[11] As per the DSCI's (Data Security Council of India) cyber threat report on India for 2023, as many as 400 million malware were detected, with ransomware attacks topping the list[12] and most of the attacks on individuals to 'Vishing' (Call-based Phishing attacks).[13]

With AI enabled cybersecurity, since most of the mundane activities of cybersecurity specialists can be reduced through automation, they would be able to focus better on addressing prospective threats.[14] Simply put, Artificial Intelligence can analyse a

dataset having signatures that are genuine to those identified as attacks and rejecting the ones that do not comply automatically, thereby reducing the load on the cybersecurity specialist.

Having understood the Indian cyberspace and the need for Cybersecurity for this cyberspace, let us now explore the possible use of AI in developing cybersecurity to strengthen the existing and ever evolving Indian cyberspace.

**Leveraging Artificial Intelligence in Cybersecurity**

Before the advent of AI, traditional cybersecurity relied heavily on signature-based detection systems, which worked by comparing the incoming traffic to a database of threats or malicious code signatures. If a match was found, the system would trigger an alert to take action and block the threat. Moreover, approaches such as manual analysis and rule-based detection systems were also part of traditional cybersecurity. While these served their purpose for the known threats, these were not adequate for the unknown or new threats, making new cybercriminals easy to bypass the security.[15] These new and unknown threats require a cybersecurity measure that addresses them with the passage of time.

In contrast to the above discussed ways, AI is useful in providing cybersecurity measures that are robust. Since AI-based solutions involve the use of machine learning algorithms, the threats can be detected and mitigated in real-time. The ability of AI to adapt and learn continuously is what makes this approach unique.[16] Some of the common ways in which AI can be utilised are as follows:

- **Malware Detection:** AI can be utilised to enhance malware detection. AI based solution can learn on machine learning algorithms, analyze huge data (labelled and unlabelled) and identify anomalies and patterns which are not easily detected by the humans. The identification of malware can be both static and dynamic. In static process, AI uses characteristics of file (size, structure, code) whereas the dynamic one processes maliciousness during execution part.[17] An AI-based dynamic malware detection model is discussed in the figure below (Figure 1). Herein, when training files are available (for the ML-model), features are extracted using a feature extraction module. These features are then used to train a deep learning model on a server or PC, resulting in a trained model. Thus, when a test file is provided, existing pattern-based antivirus software examines it. If the pattern is in the database, the antivirus determines if the file is malicious. If the pattern is not recognized, the antivirus reports its uncertainty.

The suspect file is then passed to the feature extraction module for AI-based malware detection. Relevant features are extracted, and the trained deep learning model on the user's PC determines if the file is malicious.[18]

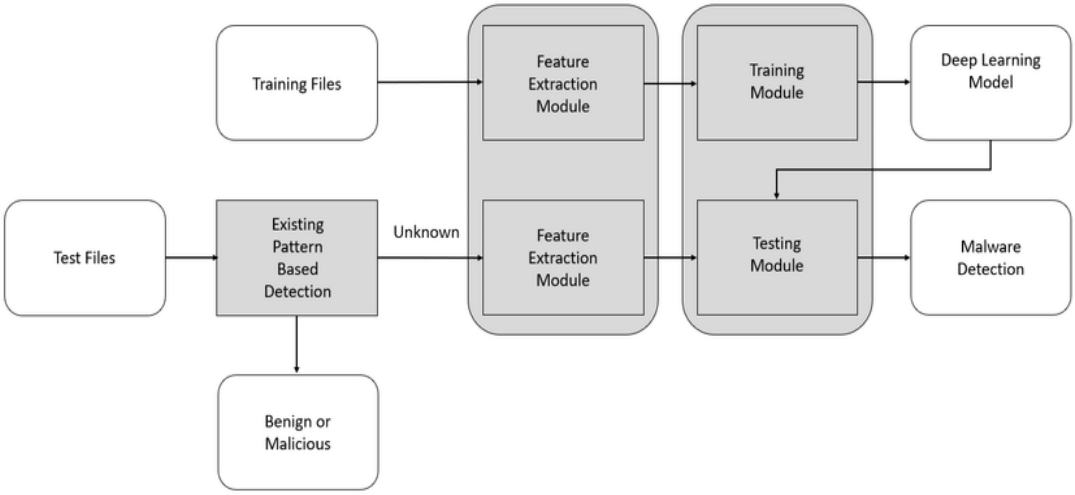



Figure 1: A machine learning model to detect malware[19]

- **<u>Phishing Detection:</u>** Most mails that we receive on a daily basis are spams. It is sometimes hard to distinguish between a genuine one and one that is malicious. AI analyses the content and structure of email to identify potential phishing threats.[20] Google Mail is already using AI to detect potential threats. Given below is an ML-model that can be used to detect phishing mails. A dataset is provided to train a machine learning model to predict whether the traffic is a phishing attack or legitimate. Continuous evaluation of the testing datasets with the training data set can be done in order to enhance the phishing detection.[21]

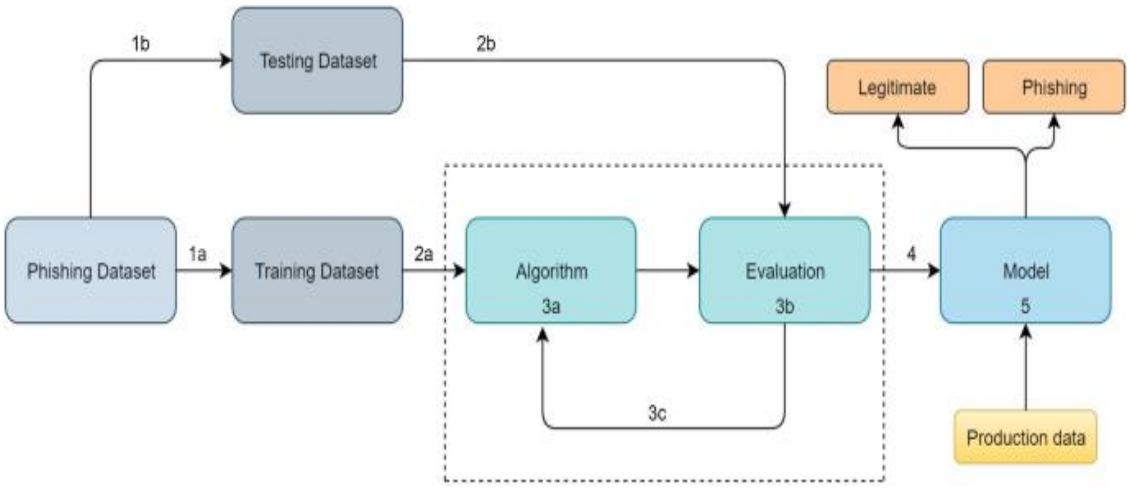



Figure 2: A machine learning model designed to detect Phishing attacks[22]

- **Intelligent Anti-Virus Softwares:** AI enabled anti-virus softwares are the future. They provide enhanced threat detection, fast scanning and high success rate due to its potential to scan large data within seconds and identify patterns that they exhibit. Instances for the same are given below:
    (a) Endpoint detection: AI sifts through massive data to spot threats, like finding attack patterns in computer logs that humans might miss.[23]
    (b) Advanced Malware Detection: AI acts like a code detective, scrutinizing files for sneaky malware. By analyzing file behaviour and code patterns, it can spot ransomware trying to encrypt data, stopping it before your files get locked.[24]
- **Network Traffic Regulation:** DDoS (Distributed Denial of Service) attacks flood website with malicious traffic, making the access to the same unavailable to the genuine users.[25] Here, machine learning algorithms can help in analysing the traffic and detect anomalies or malicious behaviour. Moreover, the devised model can take necessary steps to mitigate the risks.

**Current Efforts and Future Recommendations**

As on date, the Indian government has taken certain initiatives and framed policies that aim to protect the Indian cyberspace. The National Cybersecurity Policy, 2013 lays down the framework which aims to protect Indian cyberspace and the CIIs. Moreover, the CERT-In (Indian Cybersecurity Emergency Response Team) plays a pivotal role in controlling cybercrimes and coordinate response activities.[26] But still the Indian cyberspace cannot be referred to as the most secure one as of today given the fact that cyber-attacks take place in a huge numbers in India when compared to other nations.[27]

Given the potential AI has in the domain of cybersecurity, AI can be leveraged to create secure cyberspace that addresses the cyber threats that exist now. Such recommendations include:

- **Formulating an AI based National Cyber Security Strategy:** The current policy needs to inculcate use of emerging technologies like AI to enhance robustness of the cyberspace, especially for the CIIs. Using AI to enhance threat detection and generation of response can improve cybersecurity of CIIs. For instance, the response for a DDoS attack (which are quite common nowadays on the Indian government sites[28]) can be done efficiently with AI as it can identify the malicious pattern by apt analysis and the shutting off the traffic if required.[29]

- **Fraud Detection:** Financial frauds in India are at an all-time high, with as much as 800 financial frauds being reported on a daily basis.[30] It is another area where AI can help. Deepfakes have been up on the list since Generative-AI came into existence. Here, AI can be used to identify the authenticity of the person. Large data sets can help AI in analysing the pattern of deepfakes and thus prevent such incidents from taking place. Truecaller just came out with an AI call scanner that can identify potential calls that are fake.[31] Taking such steps can mitigate the risks of fraud.
- **Threat Intelligence**: As AI models have the tendency to evolve by using bigger datasets, large chunks of data can help in creating AI-powered threat intelligence solutions that can zero in on the potential threats and offer early warnings around new type of attacks.[32] This can come in handy for the CERT-In to generate early warnings, address possible loopholes that exist in the virtual domain and generate appropriate response.

**Conclusion**

The cyberspace has been continuously evolving with the introduction of new technologies. With it, cyber-threats are also evolving with induction of new technologies in the cyber-domain. Having a robust cybersecurity is essential in present times. Cybersecurity policies that adapt to these evolving threats should be formulated, and here AI can play a key role. AI has the ability to transform security systems and bring robustness to the CIIs, provide better threat perception and give out adequate response accordingly. A proper roadmap for investing, and formulating such cybersecurity models is required. To emphasise the importance of this requirement, the present work has looked at the cyberthreat in the Indian context and the possibility of using AI to address the growing menace of cyberthreat.

## Endnotes

[1] 'What Is Globalization: Pros, Cons, and History | Definition from TechTarget', CIO, https://www.techtarget.com/searchcio/definition/globalization.

[2] Nisha Talagala, 'Data as The New Oil Is Not Enough: Four Principles For Avoiding Data Fires', Forbes, accessed 27 June 2024, https://www.forbes.com/sites/nishatalagala/2022/03/02/data-as-the-new-oil-is-not-enough-four-principles-for-avoiding-data-fires/.

[3] Ibid.

[4] CISA, "What Is Cybersecurity?", Cybersecurity and Infrastructure Security Agency CISA, February 1, 2021, https://www.cisa.gov/news-events/news/what-cybersecurity.

[5] 'What Is the CIA Triad and Why Is It Important?', Fortinet, accessed 1 July 2024, https://www.fortinet.com/resources/cyberglossary/cia-triad.

[6] 'The Evolution of Cybersecurity | ManageEngine Blogs', accessed 1 July 2024, https://www.manageengine.com/log-management/cyber-security-awareness/evolution-of-cybersecurity.html.

[7] Ashok Kumar and Vipul Anekant, *Challenges to Internal Security of India*, 3rd ed. (2019; repr., Chennai: McGraw Hill Education (India) Private Limited, 2021), 9.6-9.7.
[8] Ibid.

[9] Sam Meredith, 'Here's Everything You Need to Know about the Cambridge Analytica Scandal', CNBC, 21 March 2018, https://www.cnbc.com/2018/03/21/facebook-cambridge-analytica-scandal-everything-you-need-to-know.html.

[10] 'India's the Second Fastest Digitising Economy in the World: McKinsey', *The Times of India*, 31 March 2019, https://timesofindia.indiatimes.com/business/startups/trend-tracking/indias-the-second-fastest-digitising-economy-in-the-world-mckinsey/articleshow/68652913.cms.

[11] 'India Witnesses 15% Rise in Cyber Attack Cases in 2023; Emerges as 2nd Most Targeted Nation', https://www.livemint.com/news/india/india-witnesses-15-rise-in-cyber-attack-cases-in-2023-emerges-as-2nd-most-targeted-nation-11705939863447.html; Business Standard, 'Ransomware Attacks Continue to Loom Large over Indian Cyberspace: Kaspersky', 3 April 2024, https://www.business-standard.com/industry/news/ransomware-attacks-continue-to-loom-large-over-indian-cyberspace-kaspersky-124040300868_1.html; PTI, 'Indian Cyberspace Seeing Incidents at Higher Rate than Global Average: National Cybersecurity Coordinator', *The Hindu*, 19 November 2023, sec. Technology, https://www.thehindu.com/sci-tech/technology/indian-cyberspace-seeing-incidents-at-higher-rate-than-global-average-national-cybersecurity-coordinator/article67550840.ece.

[12] 'India Cyber Threat Report 2023', Data Security Council of India, https://www.dsci.in/resource/content/india-cyber-threat-report-2023.

[13] 'What Is A Phishing Attack? | IBM', 17 May 2024, https://www.ibm.com/topics/phishing.

[14] 'What Is the Role of AI in Security Automation?', Palo Alto Networks, https://www.paloaltonetworks.com/cyberpedia/role-of-artificial-intelligence-ai-in-security-automation.

[15] Sonya Moisset, "How Security Analysts Can Use AI in Cybersecurity," freeCodeCamp.org, May 24, 2023, https://www.freecodecamp.org/news/how-to-use-artificial-intelligence-in-cybersecurity/.

[16] Ibid.

[17] Sonya Moisset, "How Security Analysts Can Use AI in Cybersecurity," freeCodeCamp.org, May 24, 2023, https://www.freecodecamp.org/news/how-to-use-artificial-intelligence-in-cybersecurity/.

[18] Sunoh Choi et al., 'Attention-Based Automated Feature Extraction for Malware Analysis', Sensors 20 (20 May 2020): 2893, https://doi.org/10.3390/s20102893.

[19] Choi et al.

[20] Ibid.

[21] Abdul Basit et al., 'A Comprehensive Survey of AI-Enabled Phishing Attacks Detection Techniques', Telecommunication Systems 76, no. 1 (1 January 2021): 139–54, https://doi.org/10.1007/s11235-020-00733-2.

[22] Basit et al.

[23] Abhishek Pratap Singh, 'AI in Cybersecurity: What You Need to Know', Analytics Vidhya (blog), 1 February 2023, https://www.analyticsvidhya.com/blog/2023/02/ai-in-cyber-security/.

[24] Dmitry Dontov, "Ransomware Detection Using Machine Learning Algorithms," Spin.ai, December 24, 2019, https://spin.ai/blog/ransomware-detection-using-machine-learning/.

[25] 'What Is a DDoS Attack? | IBM', 7 October 2022, https://www.ibm.com/topics/ddos.

[26] 'Government Initiatives in India: Tackling Cybersecurity Challenges', Cybersecurity Centre of Excellence (CCoE), https://ccoe.dsci.inthe-role-of-government-initiatives-in-tackling-cybersecurity-challenges-in-india.

[27] PTI, "Indian Cyberspace Seeing Incidents at Higher Rate than Global Average: National Cybersecurity Coordinator," The Hindu, November 19, 2023, sec. Technology, https://www.thehindu.com/sci-tech/technology/indian-cyberspace-seeing-incidents-at-higher-rate-than-global-average-national-cybersecurity-coordinator/article67550840.ece#:~:text=Nair%20said%20the%20Indian%20cyberspace.

[28] www.ETCISO.in, 'DDoS Attacks Strike Indian Airports. Here's How the Threat Was Mitigated - ET CISO', ETCISO.in, https://ciso.economictimes.indiatimes.com/news/cybercrime-fraud/ddos-attacks-strike-indian-airports-heres-how-the-threat-was-mitigated/99461876; '16 Lakh "DDos" Attacks per Minute on G20 Website during Summit: Govt - Hindustan Times', https://www.hindustantimes.com/technology/16-lakh-ddos-attacks-per-minute-on-g20-website-during-summit-govt-101704293255773.html; 'During G20 Summit, Delhi Police Website Hit by 3-4 Cyber Attacks', *The Indian Express* (blog), 12 September 2023, https://indianexpress.com/article/cities/delhi/delhi-police-website-attacked-by-hackers-cyber-attacks-police-probe-8935656/; www.ETCIO.com, 'Bangladeshi Hacktivist Group Targeting Indian Govt Websites, Servers - ET CIO', ETCIO.com, https://cio.economictimes.indiatimes.com/news/digital-security/bangladeshi-hacktivist-group-targeting-indian-govt-websites-servers/94448475.

[29] Sonya Moisset, "How Security Analysts Can Use AI in Cybersecurity," freeCodeCamp.org, May 24, 2023, https://www.freecodecamp.org/news/how-to-use-artificial-intelligence-in-cybersecurity/.

[30] 'India Sees Nearly 800 Online Financial Frauds Daily, Reports Show', Times Now, 25 June 2024, https://www.timesnownews.com/business-economy/personal-finance/india-sees-nearly-800-online-financial-frauds-daily-reports-show-article-111259033.

[31] Amith Raj, 'True caller Launches AI Call Scanner, the AI Voice Scam Detection System', *World Business Outlook* (blog), 30 May 2024, https://worldbusinessoutlook.com/truecaller-launches-ai-call-scanner-the-ai-voice-scam-detection-system/.

[32] slandau, 'How Artificial Intelligence Is Revolutionizing Cyber Security', CyberTalk, 9 April 2024, https://www.cybertalk.org/2024/04/09/how-artificial-intelligence-is-revolutionizing-cyber-security/.