ARTIFICIAL INTELIGENCE IN CYBER SECURITY

Abstract

Artificial Intelligence is like smart guard that helps protecting data and computer system from bad people. Instead of replying solely on humans to detect and stop cyber threats, AI user advanced algorithms and machine learning to learn from past attacks, detect suspicious activities, and respond quickly to keep systems safe. It works like a super-fast detective which helps a lot in detecting hidden patterns and potential threats. This strengthens security and helps in keeping cyber criminals away.

Not only have there been a lot more cyber attacks in recent year, but they have also gotten much more advanced. In the event of a cyberattack, traditional security measures are in sufficient to prevent data leaks. Cyber criminals have mastered the use of cutting-edge methods and powerful tools for data intrusion, hacking, and assault. Fortunately, applications of AI technology the creation of intelligent models for securing system against attackers. In order to identify malware attacks, AI – based systems are capable of providing efficient phishing and spam emails, network intrusions, and data breaches capabilities and alert the security during the impact.

Introduction

Artificial intelligence involves the use of learnings algorithms and AI techniques to enhance cyber securities measures, detect threats, and responds more effectively to cyber-attacks. By analyse the big data, AI systems can identify anomalies, predict potential threats, and responds to incidents in real time. AI-powered cyber security solutions offer benefits such as improved threat detection accuracy, faster incident response times, and reduced human error.

Nowadays AI is increasingly becoming an important tool in securing digital assets and mitigating cyber risks. AI is an intriguing tool that can provide analytics and intelligence to protect against even evolving cyberattacks by swiftly analysing millions of events and tracking a white variety of cyber threats to anticipate and act in advance of the problem. The flourishing field of cybersecurity and the numerous studies to solve problems related to the identification, protection, detection, response and recovery from cyberattacks.

The role of Artificial Intelligence in cyber security: Enhance threats detection and prevention

Nowadays cybersecurity is becoming increasingly and challenging to combat in digital landscape.

AI is revolutionising the field of cyber security by significantly improving threats detection and prevention capabilities. We will explore the role of AI in cybersecurity and how it is reshaping the way we safeguard our digital assets.

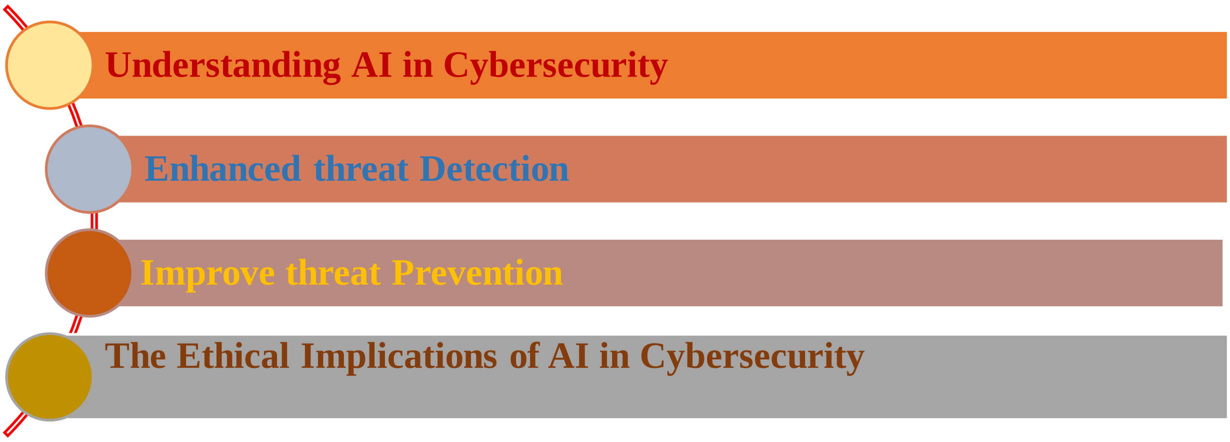
Understanding AI in Cybersecurity
Enhanced threat Detection
Improve threat Prevention
The Ethical Implications of AI in Cybersecurity

Figure 1: Role of AI in Cybersecurity

I. Understanding AI in cybersecurity:

Artificial Intelligence refers to the ability of machines to perform task that typically require human intelligence, such as problem-solving patterns recognition, and decision making. In cyber security, AI systems are designed to analyse big amount of data, identify patterns and make informed decision in real time to detect and mitigate potential threats.

II. Enhanced threat detection:

Artificial Intelligence through its ability to enhance threat detection mechanisms. Unlike traditional signature-based method that struggle to keep pace with rapidly evolving threats, AI powered solution utilise machine learning algorithms to identify anomalies and suspicious activities that may indicate a cyberattack. By continuously learning from historical data and adapting new threats, Artificial Intelligence systems can accurately detect even previously unknown or zero-day attacks.

III. Improved threat prevention:

Artificial Intelligence plays a vital role in preventing cyberattack by identifying vulnerabilities in systems and recommending appropriate security measures This proactive approach reduces the window of opportunity for potential attackers and enhance overall cybersecurity.

IV. The Ethical Implications of AI in cybersecurity:

However, it is crucial to navigate the ethical consideration surrounding AI use in cybersecurity, ensuring transparency, fairness, and privacy protection. By staying proactive and embracing the power of AI, we can effectively combat cyber threats and safeguard our digital assets in an ever-changing digital landscape.

Opportunities of AI in cyber security:

AI has the potential revolutionize the cybersecurity landscape by automating and enhancing various security processes.

i. **Threat detection and prevention:** Artificial Intelligence algorithms can analyse big amount of data and detect patterns that may indicate a cyber threat. By automating threat detection and prevention, organization can enhance their security posture and respond more quickly to threats.
ii. **Vulnerability Management:** Artificial Intelligence can analyse vulnerabilities and prioritize them based on their severity, enabling organization to allocate there resources more efficiently.
iii. **Incident response:** AI can also be used to automate incident response processes, such as identifying the source of an attack and containing it. It can reduce the time it takes to respond to a cyber incident and minimize its impact.
iv. **Fraud detection:** AI can be used to detect fraudantly activity, such as phishing attempts and social engineering attacks, by analysing user behaviour and identifying anomalies.

Challenges of AI in Cybersecurity:

Artificial Intelligence offers many opportunities in cybersecurity, it also presents some challenges.

i. **Bias:** AI algorithms may be biased if they are trained on a limited data set or if the data used to train them contains inherent biases.
ii. **Complexity:** AI algorithms can be complex and difficult to understand, making it challenging to troubleshoot and debug them.
iii. **Cyber Attacks:** AI algorithms can also be vulnerable to cyber-attacks.

iv. **Legal and Ethical concerns:** The use of AI in cyber security raises legal and ethical concern, such as privacy and data protection issues.

Organization	Challenge	AI-power cybersecurity to the rescue
Google	Android malware bypassing security and infecting multiple application on google play store.	Google's bouncer, an automated system, scans app for malicious code, gather app data, feeds it into deep neural network, and identifies harmful behaviour.
Apollo Hospital	No real-time quantified view of risk posture and breach likelihood of their critical assets that store patient data.	Enterprise-wide, unified, and real-time cybersecurity & digital business risk quantification platform to quantify infrastructure security risk and measure adherence to international compliance.

ED&F MAN	Minor server (non-data) breach highlighting the firm's low defence against crypto-mining scams.	Modern security operation centre implements networks and endpoint detection and response platform with privileged access analytics that drills down the crypto miner threats actor in time.

Table 1 :Challenge of AI in Cybersecurity

The human-AI partnership in cybersecurity

The limitation of AI, Humans should always be thr final decision makers, while using AI to speed up the process. Companies may use AI to be presented multiple options and then key decision makers can act quickly, thus AI will supplement, but not replace, human decision-making. Together, AI anf humans can accomplish more than then they alone.

Table 2: Human-AI Partnership

Artificial Intelligence	Humans
• Learn from data and patterns • Can mimic creativity but lack genuine emotion • Rapid processing and analysis • Virtually unlimited memory storage • Can scale to handle massive datasets • Lacks true self – awareness • Devoid of genuine empathy	• Learn from experience and adapt over time • Exhibit creativity and emotional understanding • Limited speed compared to AI • Limited memory capacity • Cannot easily scale certain tasks • Exhibit self-awareness and consciousness • Express empathy and emotional connection

The use of Artificial Intelligent to curb Cyber crime in India

Cyber crime

The phrase "cybercrime" has no definition under Indian law. In reality, even after being amended by the information Technology Act, the Indian Cyber never refers to "cybercrime" at any time.

Cyber terrorism refers to planned, politically motivated attacks in information, computer system, and computer networks programmes and information that result in act of violence against people, government, and property.

The need to handle cybercrime in India and the potential of India in doing so:

- Cybercrime is becoming more of a problem in India, as it is in many other nations across the world. The risk of cyber attacks and other cybercrime has grown along with the usage of technology and the internet. These crimes can have major economics and social effects, including money losses, reputational damage, and loss of personal data.
- In recent year, India has seen a number of high-profile cybercrime instance, including data breaches, phishing attacks, ransomware assaults, and online fraud.
- Using artificial intelligence might be one way to reduce cybercrime. AI has the ability to identify and respond to threats more rapidly and efficiently, as ell as assist in detecting and stopping cyber-attacks before they happen.
- AI may also be used to automate task related to cybersecurity, such as threat detection and response. Security team may be able to concentrate on more difficult problem as a result, increase productivity may also be used to create better secure systems and find holes before thieves can exploit them.

Current State of Cybercrime in India

In India, the national Crime Records Bureau (NCRB) has seen a sharp rise in cybercrime in recent year. There were 44,546 document incidences of cybercrime in India in 2019, according according to the NCRB's most recent report on crime data in the nation. This is an increase 63.5% from the prior year.

1. **Types of cybercrimes in India:**

- **Financial fraud:** They comprise phishing schemes, credit\debit card fraud, and internet banking frauds.
- **Hacking:** Gaming unauthorized access to a computer system is known as hacking.

- **Cyber stalking and harassment:** Stalking, bulking, and harassment committed online or through social media are all considered to be cyber stalking and harassment.
- **Identify theft:** Identify theft is the theft of a person's name, address, social security number, among other personal data.

2. **The effect of cybercrime**

- **Financial loss:**
  The hacker's will be target financial Information. Cyber crime cause Financial loses for both people and corporation.
- **Damage to reputation:**
  Cybercrime have the potential to cause long-lasting harm to the reputation of a person or an organization.
- **Information losses:**
  Cybercrimes are capable of stealing sensitive data, including financial or personal information, which can result in fraud and identify theft.

- **Legal repercussions:**
  Cybercrimes are illegal, and anyone found guilty they have to deal with the legal repercussions.

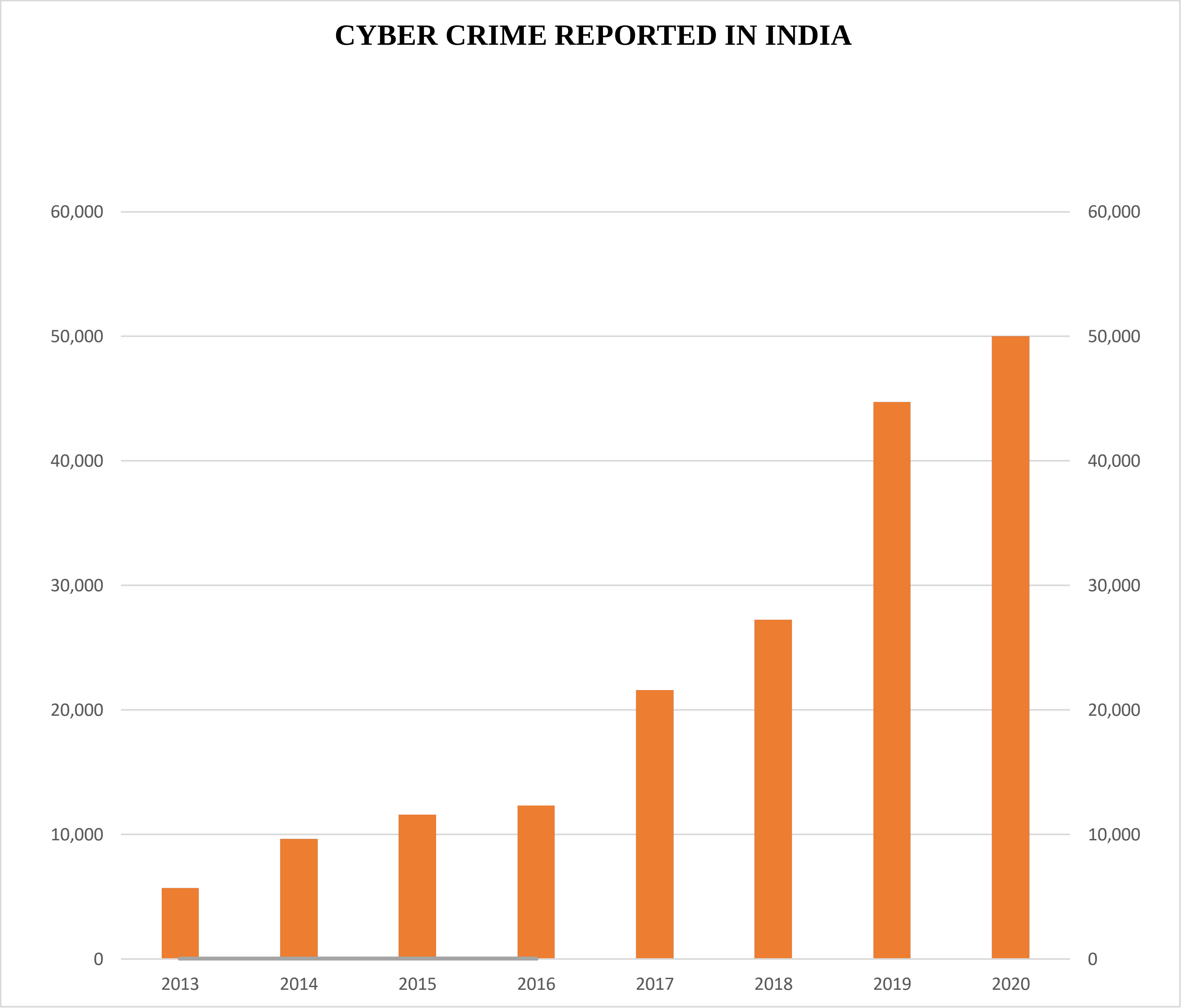

Figure 2: Cyber-crime Reported in India

Application of AI in cybersecurity

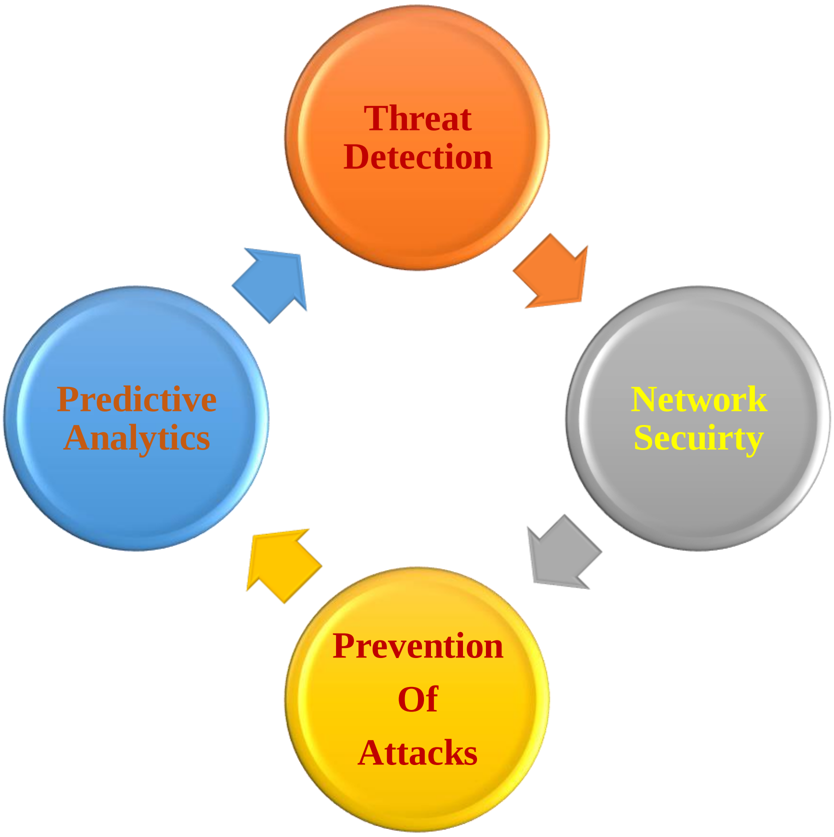

Figure 3: Application of AI in Cybersecurity

Threat Detection

AI and advanced machine learning algorithms assist organization in identifying threats, intrusion, and any malicious activities. Using AI software to detect threats is not new, as most cyber security firms deployed AI algorithms and identify indicators of attacks, Real-time detection of deviations and change in behaviour help organization to respond faster and intelligently.

Network Security

AI-enabled software is used at the network level to ensure better network security. As AI tools can read patterns and identify patterns, they are fast enough to detect hundreds of objects, including files, IP addresses, link to identify theft, and large amount of data. AI is faster than human detection, as human can scan million of sites and addresses. Moreover, real-time detection and automated processes help companies respond faster and more efficiently.

Prevention Of Attacks

Business can use AI to reduce the risk of cyber-attacks. In traditional ways, it can take days or even months to find a breach and take action to respond. By using AI-driven security measures, companies can develop a more automated. Also, it is an effective way to prevent an attack before it happens rather than do something after potential damage. AI algorithms process large amount of data per second, which is not possible for humans.

Predictive Analytics

AI can help analyse user behaviour. With this capability, algorithms can learn user behaviour and create patterns about usage, timing, and platforms. AI-powered tools constantly monitor real-time data and can quickly detect errors in data or behaviour, reducing the possibilities of potential damage.

State-Wise Cyber Crime Recorded in India

The incident of cyber crime in India have been increasing at a rapid pace and jumped by nearly nine times between 2013 and 2020, official data showed. As per the latest 'Crime in India' report, cyber crimes in India increased to 50,693 cases reported in 2013. Further, as per the data analysed by CNN-News18, between 2018 and 2020, the cases have jumped by nearly 85 percent. In 2018, India recorded 27,248 cases related to cybercrime.

Also, the cases reported in 2020 were nearly 12 percent more than the recorded in 2019 – 44,725 cases. Of the cyber crimes reported in 2020, over 60 percent (30,098 cases) were done with a motive of fraud. While most of the state have reported a jump in cyber crime in 2020, when compared to 2019, state including Uttar Pradesh, Karnataka, Mizoram, Rajasthan and Sikkim have recorded a drop in the cases, the data showed. Also, among all the state and union territories, Sikkim is the only state that recorded zero cases of cybercrime last year.

Up Tops List Followed by Karnataka, Maharashtra

In 2020, Uttar Pradesh recorded the most cases of cybercrime-11,085 - followed by Karnataka with 10,731 cases, Maharashtra (5,469 cases) and Telangana (5,015 cases) stood next, the data showed. The state that has recorded massive jump in the cases of cyber-crimes between 2019 and 2020 were Arunachal Pradesh (from 7 to 30); Assam (2,231 to 3,530); Chhattisgarh (175 to 294); Goa (17 to 30); Gujarat (781 to 1,243); Manipur (4 to 79) and Telangana (2,691 to 5,024).

In Bihar and Telangana, cases of cyber-crimes have increased by over four time, while in Uttar Pradesh, there has been an increase of over 75 percent since 2018.

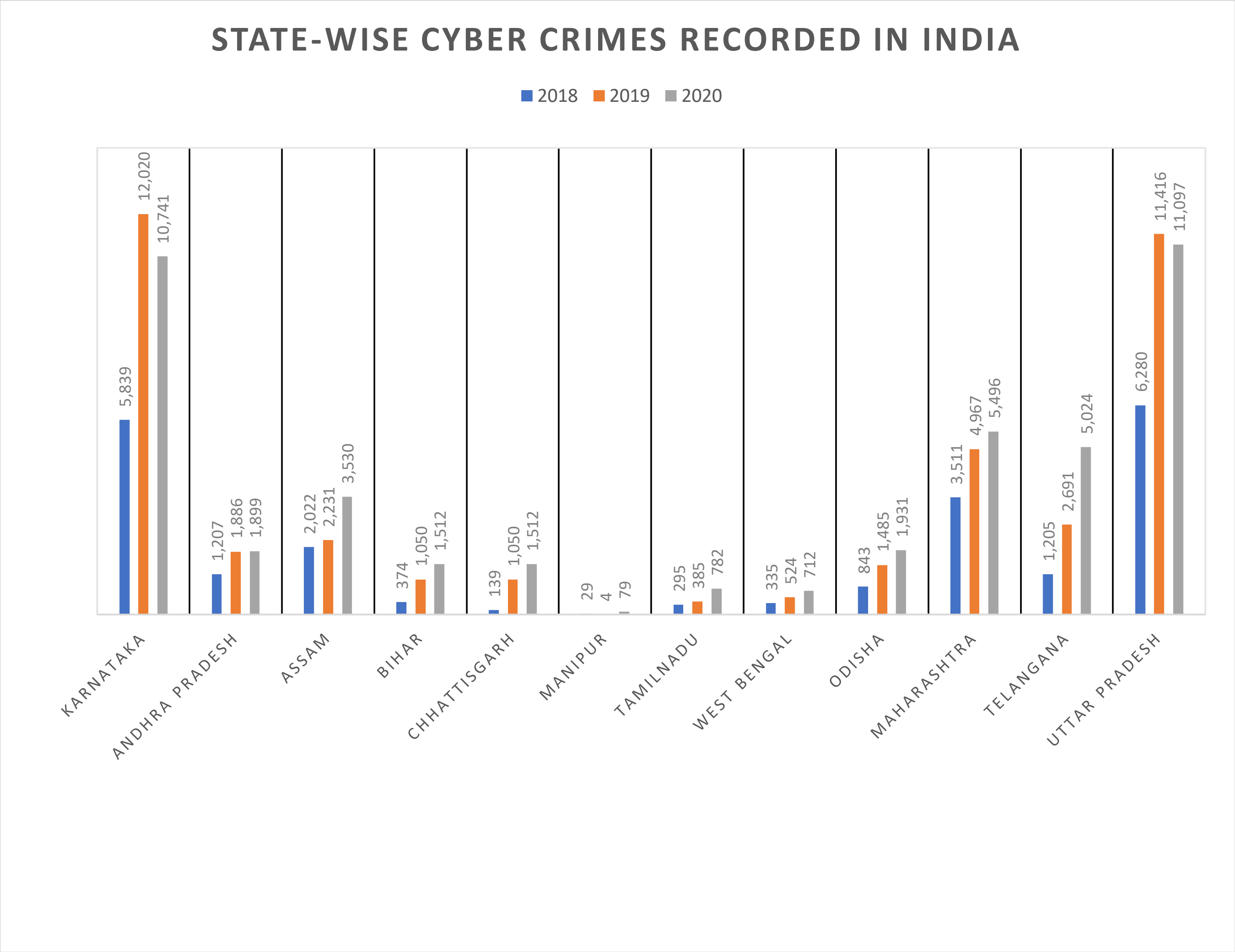

Figure 4: State-Wise Cyber Crimes Recorded In India

The total rate of cyber crime per one lakh population increased to 3.5 in 2020 from 3.1 a year ago. For union territories, this is 0.9, while for states it is 3.8 states that reported the highest rate of cyber crime in 2020 were Karnataka (16.1), Assam (10.1), Uttar Pradesh (4.7), Meghalaya (4.3), Maharashtra (4.3) and Odisha (4.1).

Conclusion

Artificial Intelligence (AI) is a game-changer in cybersecurity, significantly enhancing threats detection and prevention capabilities. By analysing big amount of data, AI systems can detect anomalies, identify potential vulnerabilities, and recommend appropriate security measures. However, it’s crucial to address ethical consideration surrounding AI use, ensuring transparency, fairness, and privacy protection. By embracing AI while remaining vigilant, we can effectively combat cyber threats and safeguard our digital assets in today's everchanging digital landscape.

AI offers a lot of potential for reducing cybercrime in India. Using AI's capacity to identify, prevent, and respond to cybercrime quickly and effectively is crucial given the growth in their frequency. Deep learning, machine learning, and other AI based tools may all be used find patterns, abnormalities, and other signs of cyber-attacks. It analyses enormous amount of information to find suspicious activity, and forecasts and stop potential assaults.

Reference

https://ieeexplore.ieee.org/document/10085175

https://www.sciencedirect.com/science/article/pii/S1566253523001136

https://www.linkedin.com/pulse/role-artificial-intelligence-cybersecurity-enhancing-threat

https://www.cyberneticsearch.com/blog/the-role-of-ai-in-cybersecurity--opportunities-and-challenges/

https://www.netscribes.com/ai-in-cybersecurity/

https://www.digicert.com/blog/the-future-role-of-ai-in-cybersecurity

https://www.news18.com/news/india/cyber-crimes-in-india-spiked-nearly-nine-times-since-2013-up-topped-chart-in-2020-data-4210703.html

https://codestoresolutions.com/artificial-intelligence/the-role-of-artificial-intelligence-in-cyber-security/

https://www.legalserviceindia.com/legal/article-11906-the-use-of-artificial-intelligence-to-curb-cyber-crimes-in-india.html#google_vignette

https://www.news18.com/news/india/cyber-crimes-in-india-spiked-nearly-nine-times-since-2013-up-topped-chart-in-2020-data-4210703.html

Submitted by:

Author- Mr Rishu Raj, Mr Aman Kumar Gupta

Co- Author- Ms Manisha Jain – Assistance Professor SGVU