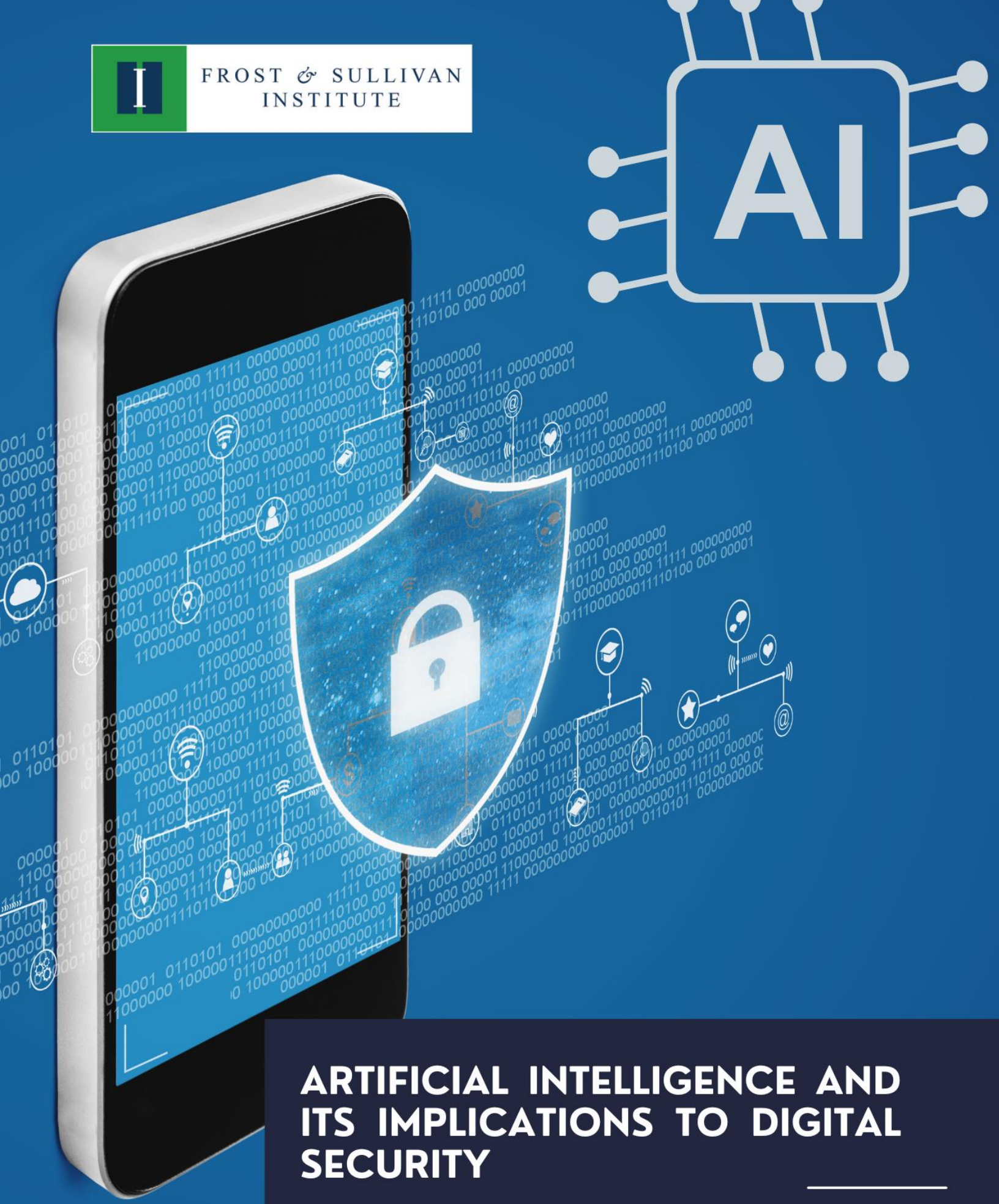
FROST & SULLIVAN INSTITUTE



ARTIFICIAL INTELLIGENCE AND ITS IMPLICATIONS TO DIGITAL SECURITY

Article by Shreya Ghimire,
Research Analyst, Frost & Sullivan Institute

Artificial Intelligence and Its Implications to Digital Security

With the advancement of artificial intelligence, machines have become adept at understanding the information they are fed about humans. It is now more crucial than ever to comprehend the potential impact of AI on our digital security, as the risks associated with its use evolve daily.

Artificial intelligence, or AI, encompasses the development of computer systems capable of performing tasks traditionally requiring human intelligence, such as problem-solving, learning, perception, and analysis. The rapid adoption of AI is driven by various factors, including improved computing power, which enables the rapid processing of extensive datasets essential for AI algorithms. Furthermore, AI's integration across industries and its automation capabilities attracts businesses seeking competitive advantages and operational efficiencies. Additionally, advancements in natural language processing broaden the scope of AI applications, thereby enhancing user experiences. The combined influence of these factors has led to widespread and enhanced integration of AI technologies across diverse sectors.

In today's world dominated by rapid advancements in artificial intelligence (AI), the integration of these technologies into our lives brings about unparalleled opportunities and, also, a host of security challenges. Problems like deepfake, phishing scams, and increasing privacy concerns are some negative implications of AI on our digital security. The active use of artificial intelligence leads to the need to resolve several ethical and legal problems. The ethical framework for the application and use of data today is highly blurred, which poses great risks in ensuring data confidentiality[1]. From the vulnerability of AI systems to concerns surrounding data privacy and biases, the security landscape is evolving.

[1] International Journal of Cyber Criminology . Jul-Dec2019, Vol. 13 Issue 2, p564-577. 14p.

Navigating the Security Landscape of Artificial Intelligence

Machine learning models are susceptible to adversarial attacks, wherein malicious entities manipulate input data to deceive the model, leading to inaccurate predictions or classifications. This vulnerability arises due to the dependence of AI on algorithms and human input. Furthermore, the utilization of large datasets for training AI models raises significant concerns regarding data privacy. Protecting sensitive information within these datasets is essential to prevent unauthorized access or misuse.

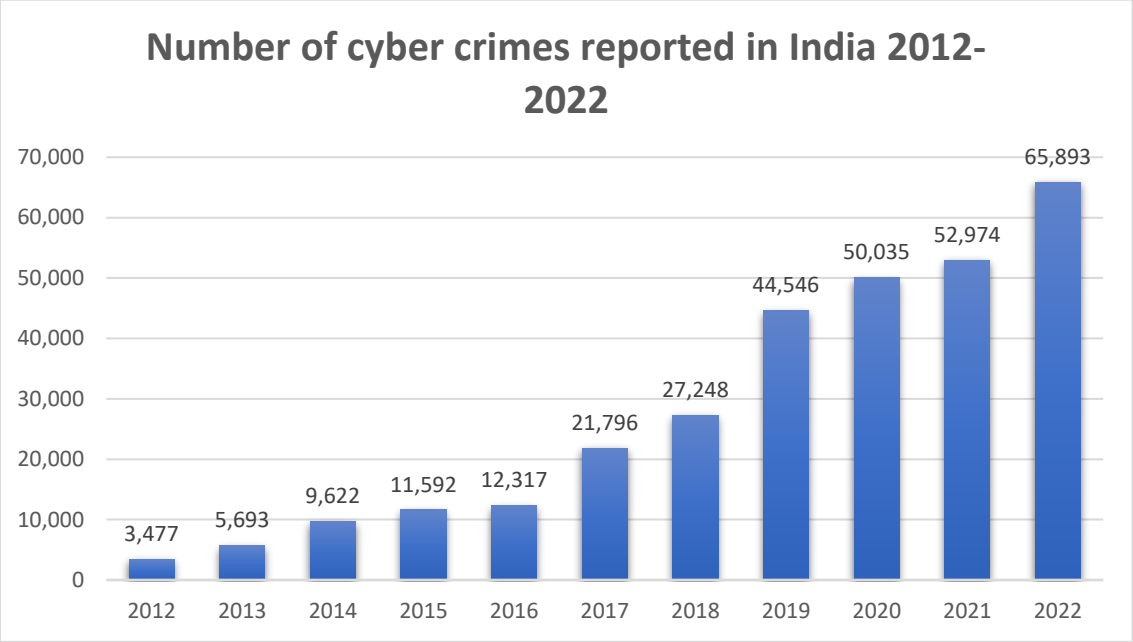
Additionally, the lack of transparency in AI decision-making processes, particularly in complex models like deep neural networks, presents a security challenge. Understanding how AI arrives at specific decisions is crucial for accountability and identifying potential vulnerabilities in outcomes. Moreover, AI systems have the potential to amplify biases present in the training data, resulting in discriminatory outcomes. Addressing bias in AI algorithms is vital for ensuring fair and equitable security practices, particularly in sensitive domains such as law enforcement and finance.

The increasing sophistication of AI technology also gives rise to concerns about its potential misuse for malicious purposes. This includes the creation of realistic deepfakes, convincing phishing attacks, and the automation of cyberattacks, posing significant security threats. Furthermore, the dynamic nature of AI technology presents an ongoing challenge in staying ahead of potential security threats. As AI continues to evolve and enhance its capabilities, security measures must evolve in tandem. Moreover, the intersection of AI with other emerging technologies, such as the Internet of Things (IoT) and 5G networks, complicates security considerations further. Navigating this complex landscape requires fostering a culture of responsible AI development and promoting transparency. Doing so will be instrumental in building trust and ensuring the long-term security of AI applications across diverse sectors.

Implications of AI on Digital Security

In 2021, globally, 323,972 internet users fell victim to phishing attacks. This was despite Google’s cyber security measures blocking 99.9% of phishing attempts from reaching their users. On an average of $136 lost per phishing attack, this amounts to $44.2 million stolen by cyber criminals

through phishing attacks in 2021[2]. This shows just how large the treat AI poses, and it is only going to grow since hackers are deploying AI of their own.



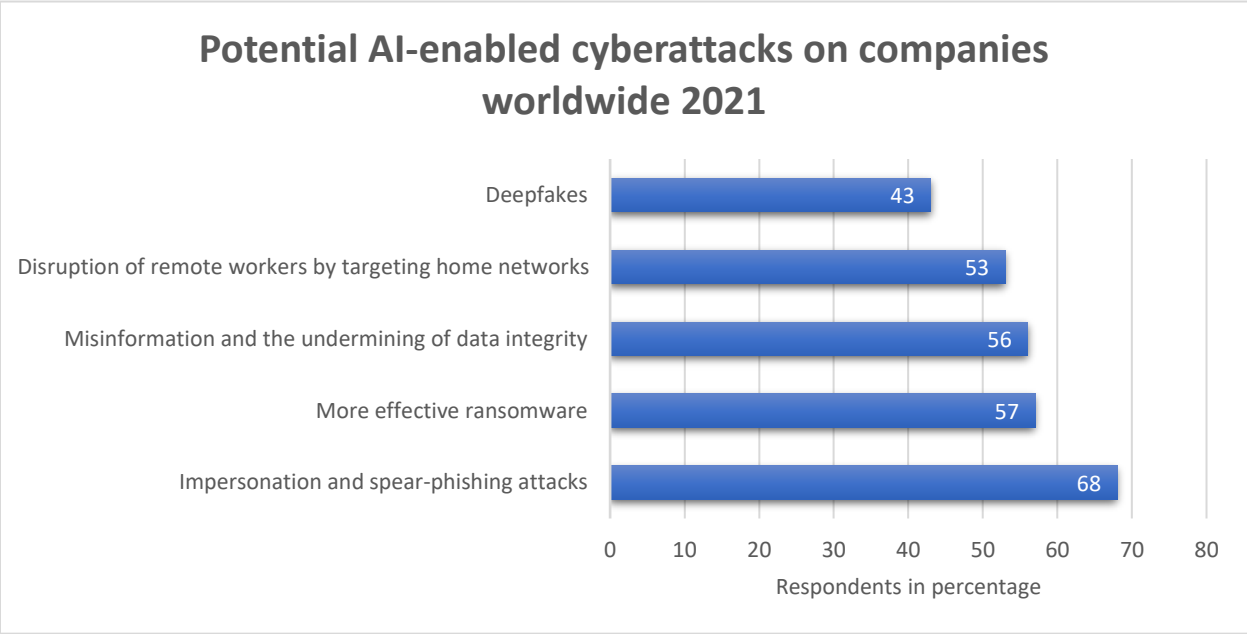
Source: NCRB (India)

As per the findings of a McAfee study, a staggering 83% of Indian victims of AI voice scams have reported monetary losses, with nearly half of them (48%) losing more than ₹50,000. While Artificial Intelligence offers enormous possibilities, it can also be exploited by cybercriminals for malicious making scams even more convincing[3].

A study by Deep Instincts highlights the impact of generative AI in the cybersecurity industry, analyzing the technology's positive and negative effect on organizations' security preparedness. The report reveals 75% of security professionals witnessed an increase in attacks over the past 12 months, with 85% attributing this rise to bad actors using generative AI[4].

[2] https://aag-it.com/the-latest-phishing-statistics/
[3] Beware of fake delivery scam! What to do if victim of cybercrime | Mint (livemint.com)
[4] https://www.securitymagazine.com/articles/99832-study-finds-increase-in-cybersecurity-attacks-fueled-by-generative-ai

A recent global study found that out of 7,000 people surveyed, one in four said that they had experienced an AI voice cloning scam or knew someone who had[5]. In addition, the study reveals that nearly half (47%) of Indian adults have either been a victim of or know someone who has fallen prey to some form of AI voice scam. This percentage is almost twice the global average (25%).



Source: MIT Technology Review Insights

AI-powered cyber-attacks are becoming more common. Incidents such as 2017 WannaCry ransomware attack[6], which affected over 200,000 computers in 150 countries, carried out using an AI-powered worm that was able to spread rapidly and infect vulnerable systems shows how vulnerable our systems are compared to AI.

[5] https://www.mcafee.com/blogs/privacy-identity-protection/artificial-imposters-cybercriminals-turn-to-ai-voice-cloning-for-a-new-breed-of-scam/
[6] WannaCry explained: A perfect ransomware storm | CSO Online

Case Study: AI Voice scams

The widespread adoption of AI tools has facilitated the ease of cloning or altering images, videos, and sounds, a phenomenon commonly referred to as Deepfake. Deepfake, a fusion of "deep learning" and "fake media," involves the use of AI to generate or modify multimedia content to appear genuine. This technology is increasingly being exploited by scammers, who manipulate the voices of targeted individuals to make fraudulent calls to their family or friends. Through these deceptive calls, scammers coerce unwitting recipients into divulging money or sensitive information. A recent study indicates that India is the country with highest number of such victims, with 83% Indians losing their money in such scams[7].

According to a recent news[8] published in the Times of India, a woman lost 1.4 Lakh Rupees to AI voice scam. The caller, skillfully emulating her nephew based in Canada, made up a distressing story, asserting an urgent need for immediate financial aid. The woman thought it was her nephew calling for help, but it was an AI generated voice. As voice is distinct and acts as a digital biometric, the woman did not find it suspicious as the voice sounded just like her nephew and lost the money while trying to help. Scammers use AI generated voice and call posing as family members or even customer service representative, to trick the victim to give their information, or money, or whatever it is that the scammer wants.

This case paints a clear picture of how fraudulent activities are becoming easier to carry out, and more difficult to suspect. AI has made cloning and manipulation of multimedia very easy, which has led to increasing concerns for our digital security. Artificial intelligence has spiked up the need to be more cautious while engaging with anything or anyone online. Any kind of information can easily be manipulated to something entirely different, and this raises concern for our digital wellbeing.

[7] https://economictimes.indiatimes.com/tech/technology/almost-half-of-indians-experience-ai-enabled-fake-voice-scams-83-victims-lost-money-mcafee-survey/articleshow/99915954.cms
[8] https://timesofindia.indiatimes.com/gadgets-news/woman-loses-rs-1-4-lakh-to-ai-voice-scam-what-is-it-and-how-not-to-become-a-victim/articleshow/105298323.cms

Challenges on Digital security due to AI

With society becoming more dependent on technology, information security has become increasingly critical. Rise of the digital age has led to a rise in the number and complexity of cyber threats, making it challenging for organizations to detect and respond to them effectively.[9]

Nowadays, researchers are working on the possibilities of AI to cope with varying issues of systems security across diverse sectors. AI is commonly considered an interdisciplinary research area that attracts considerable attention both in economics and social domains as it offers a range of technological breakthroughs regarding systems security[10]. The active use of artificial intelligence leads to the need to resolve several ethical and legal problems. The ethical framework for the application and use of data today is highly blurred, which poses great risks in ensuring data confidentiality.[11]

The ever-evolving nature of cyber threats poses significant challenges for organizations working to maintain robust security. With the advent of AI models, the threat landscape has become difficult to identify, demanding adaptive strategies to safeguard sensitive data and protect against potential breaches. Due to AI, IT teams are tasked with navigating an extremely agile business landscape, oftentimes creating environments that are very complex as IT practices, systems, and infrastructure are being radically transformed with new waves of technology, further leading to vulnerabilities that may be exploited by cybercriminals. Furthermore, issues like Deepfake, which spreads misinformation and even manipulates information to mislead people is a big challenge.

Best practices to combat security threats due to AI.

With the rapid advancement of technology, the integration of artificial intelligence (AI) presents unprecedented opportunities alongside complex security challenges. As organizations increasingly rely on AI for diverse applications, safeguarding against potential threats becomes paramount.

[9] https://journals.sagescience.org/index.php/jamm/article/view/51
[10] https://acisinternational.org/conferences/snpd-2021-winter/

[11] International Journal of Cyber Criminology . Jul-Dec2019, Vol. 13 Issue 2, p564-577. 14p.

Implementing comprehensive security measures, enhancing transparency in decision-making, fostering a culture of continuous monitoring and adaptation, and collaborating within the industry are foundational practices for effectively navigating the intricate landscape of AI security. While AI-driven cyberattacks may seem unstoppable, they are not insurmountable.

Implement Comprehensive Security Measures: Enforcing strong authentication and access controls, regularly updating software, and utilizing encryption for data transmission and storage are essential to address vulnerabilities promptly and safeguard against unauthorized access.

Enhance Transparency and Explainability: Striving for transparency in AI decision-making processes, especially in complex models, helps address biases proactively and prevent breaches in digital wellbeing.

Proactive Security Measures: Conducting regular security audits and assessments, embracing ethical AI practices, and addressing issues such as bias, fairness, and accountability are crucial for responsible AI use.

Incident Response and Employee Training: Developing an incident response plan for AI-related security threats, providing employee training on AI security best practices, and raising awareness about potential threats strengthen digital security.

Collaborate and Stay Informed: Participating in collaborative efforts within the industry to share threat intelligence and complying with relevant data protection and privacy regulations are vital for combating digital security threats due to AI.

Secure AI Development Lifecycle: Integrating security measures throughout the AI development lifecycle and conducting thorough security assessments of third-party AI vendors ensure alignment with security standards.

Continuous Monitoring and Adaptation: Implementing continuous monitoring of AI systems and adapting security measures based on evolving threats and technological advancements are essential for staying ahead of security threats.

Numerous companies worldwide are working to combat the challenges of digital security brought about by the widespread use of AI. Some notable examples include:

Crowdstrike: Provides cloud-native endpoint protection software, offering prevention and visibility across endpoints and proactive threat hunting to customers in various industries.

Vectra: Uses AI to detect cyber-attacks in real-time, automating tasks typically performed by security analysts and reducing the workload required for threat investigations.

Check Point: Offers computer and network security solutions to governments and enterprises globally, providing customizable threat intelligence to meet organizations' real-time needs.

DataDome: Utilizes artificial intelligence and machine learning to develop solutions protecting mobile apps, websites, and APIs against bot attacks. The company's threat analytics and notifications enhance security while optimizing user experiences.

While AI is making it easier for cybercriminals to launch attacks, it is also being used to prevent them. As AI technology becomes more advanced, we can see both sides of the story with more sophisticated cyber-attacks and more powerful cybersecurity solutions. To stay ahead of the curve, organizations need to take cybersecurity seriously with reference to AI.

Conclusion

The rapid integration of artificial intelligence (AI) into our digital landscape presents both unparalleled opportunities and formidable challenges for digital security. This article has illuminated the multifaceted impact of AI on digital security, encompassing issues such as phishing attacks, deepfakes, and various other AI-driven scams.

The case study on AI voice scams vividly illustrates how cybercriminals exploit AI technologies to deceive individuals, underscoring the urgent necessity for heightened awareness and protective measures. The complexities posed by AI to data privacy, ethical considerations, and the dynamic nature of cyber threats necessitate adaptive strategies and interdisciplinary research efforts.

While AI exacerbates the complexity of digital security challenges, it also serves as a potent tool for combating cyber threats. Leading companies like CrowdStrike, Vectra, Check Point, and DataDome are pioneering the use of AI to develop innovative solutions that detect, prevent, and mitigate cyber-attacks.

Amidst these challenges, public awareness emerges as paramount. Educating and communicating the implications of AI on digital security can empower individuals and organizations to adopt best practices and remain vigilant against emerging threats. Moving forward, the convergence of AI and cybersecurity will continue to shape the future, highlighting the imperative for collaboration, ethical considerations, and proactive adoption of cybersecurity measures to safeguard our increasingly interconnected digital world.