EMBRACING ARTIFICIAL INTELLIGENCE FOR SUSTAINABILITY & LIFE SKILLS

An International Bhutan Conference Proceedings

IJISEM INTERNATIONAL JOURNAL OF INNOVATIONS IN SCIENCE ENGINEERING AND MANAGEMENT

International Journal of Innovations In Science Engineering And Management

Redefining Cybercrimes in light of Artificial Intelligence: Emerging threats and Challenges

Dr. Amit Singh[1], Nidhi Shanker[2]

[1]*Head of Law, Dept. in MJPRU, Bareilly*
[2]*Research Scholar of law, Dept. in MJPRU, Bareilly*

OPEN ACCESS

Volume: 3

Issue: Special issue 2

Month: December

Year: 2024

ISSN: 2583-7117

Citation:

Amit Singh and Nidhi Shanker, "Redefining Cybercrimes in light of Artificial Intelligence: Emerging threats and Challenges" International Journal of Innovations In Science Engineering And Management, vol. 3, no. Special Issue 2, 2024, pp.192-201.

DOI:

10.69968/ijisem.2024v3si2192-201

This work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

Abstract

In the contemporary developing world, artificial intelligence (AI) is one of the key forces behind technological growth. Artificial intelligence refers to something that is not natural, whereas intelligence is the ability to learn and use new skills and information. Various definitions of artificial intelligence have been repeatedly put forth. The ability of a machine to mimic intelligent behaviour is known as artificial intelligence. An American computer scientist known as the "father of artificial intelligence," John McCarthy, first used the term "artificial intelligence" in 1956. During the Dartmouth Conference at the Massachusetts Institute of Technology, he coined the term and explained its meaning. It was during the Massachusetts Institute of Technology's Dartmouth Conference when the term artificial intelligence (AI) was first used. According to him, artificial intelligence (AI) creates intelligent machines, especially intelligent computer programs, using science and engineering. Improvements in artificial intelligence could significantly benefit humanity by boosting output, efficiency, and cost savings.

Keyword: Artificial Intelligence, Redefining Cybercrimes, Emerging threats

INTRODUCTION

In the contemporary developing world, artificial intelligence (AI) is one of the key forces behind technological growth. Artificial intelligence refers to something that is not natural, whereas intelligence is the ability to learn and use new skills and information. Various definitions of artificial intelligence have been repeatedly put forth. The ability of a machine to mimic intelligent behaviour is known as artificial intelligence. An American computer scientist known as the "father of artificial intelligence," John McCarthy, first used the term "artificial intelligence" in 1956. During the Dartmouth Conference at the Massachusetts Institute of Technology, he coined the term and explained its meaning. It was during the Massachusetts Institute of Technology's Dartmouth Conference when the term artificial intelligence (AI) was first used. According to him, artificial intelligence (AI) creates intelligent machines, especially intelligent computer programs, using science and engineering. Improvements in artificial intelligence could significantly benefit humanity by boosting output, efficiency, and cost savings. As a result, reliance on AI will unavoidably lead to greater production, trade, transportation, healthcare, rescue operations, education, and farming, as well as a significant increase in the capacity and level of social governance. During the early days of computer and computing system use, a human programmer had to instruct the machine on how to carry out a task or resolve an issue. But because it cannot accomplish some tasks that are essential to human life, that approach has serious drawbacks. As artificial intelligence (AI) has advanced, machines can now perform these tasks through a "machine learning process." is created or programmed in this manner. By turning the preceding premise on its head, the machine learning process has barely begun to make AI operate. Instead, then instructing a machine on how to perform a task, a vast amount of input and output data is supplied to it. For instance, if the task is to determine how many photographs contain dogs, 1 billion photos with dogs and 1 billion without are provided and set in the machine as data. Then a learning algorithm is given to the computer or machine, assisting it in learning and completing the assignment by recognizing patterns of similarity between the two types of photographs. Therefore, the only things that humans can provide the computer are "data" and "learning algorithms," which tell it how to learn something. The machine programs itself when it comes to determining how to solve the given task. We are not always able to comprehend the actions of a computer in machine learning. There are just three things we know:

- The goal for which the machine was taught;
- The learning algorithm used; and
- The kinds of data the machine received

MEANING OF AI

It is not a simple process to define artificial intelligence. It cannot be limited to a single topic of study because its scope is so wide. AI presently touches upon every aspect of life. Every researcher has defined AI differently as per its applicability in their own field. The question that encounters researcher in this field are question such as ‘what is intelligence?’, ‘how can intelligence be measured?’, ‘how does the brain work?’

All this question is necessary to be answered while trying to understand AI. Thus, AI has been considered to be more of an ambition now that seeks to understand how a human brain works and its cognitive capacity by creating some cognitive process that function similarly as human brain.

A number of disciplines, including computer science, cognitive science, and mathematics (which includes analysis, logic, probability, and linear algebra), are at the intersection of AI research. Once again, this scientific discipline needs to be paired with specific knowledge of the industries it is being applied in. Furthermore, a wide range of techniques, such as deep learning, machine learning, artificial neural networks, semantic analysis, symbolic computing, and more, underpin each algorithm that AI employs.

Definition of Artificial Intelligence

The study of creating robots that can carry out tasks that normally require human intelligence is known as artificial intelligence (AI), according to its creator. Marvin Lee Minsky. For a computer like this to work, it needs sophisticated mental processes like critical reasoning, memory, and perceptual learning.[3]

In simple words AI can be said to be as the art of building computer programs that are made with the aim of performing certain task which otherwise require human intelligence to perform.

One of AI's pioneers, John McCarthy, defined artificial intelligence in general terms in 1955, stating that the field's objective is to create robots that exhibit intelligent behavior. 15 robotic cars, for instance, are designed to travel in an enclosed box using various behavioral patterns. A small group of automobiles moves more slowly than others. Within that area, some people are moving with grace and without running into each other. Some are aggressive, while others have a tendency to follow a leader. Whether or not what we are witnessing is an intelligent activity is the question that now emerges.

The robots mentioned above are considered intelligent by McCarthy's definition. Valentin Braitenberg, a psychologist, has stated that basic electric circuits may readily manufacture this apparently sophisticated behavior.

Artificial Intelligence (AI) is defined by Encyclopedia Britannica as "the ability of digital computers or computer-controlled robots to solve problems normally associated with higher intellectual processing capability of humans." Additionally, there are certain shortcomings in this definition. An clever aspect of a computer is its huge memory, which allows it to store and retrieve lengthy texts or data when needed. In accordance with the concept given above, all computers must be regarded as AI systems.

Types of AI

A. Based on Capabilities

- **Narrow AI (Weak AI:): AI of this kind** is designed to do particular activities, like driving, facial recognition, and internet searches. They operate under a limited, preset range of circumstances.

- **General AI (Strong AI):** A type of AI endowed with broad human-like cognitive capabilities, enabling it to tackle new and unfamiliar tasks autonomously. Such a robust AI framework possesses the capacity to discern, assimilate, and utilize its intelligence to resolve any challenge without needing human guidance.

- **Superintelligent AI:** Here's an example of a future artificial intelligence system where machines might surpass people in all areas, such as creativity, general knowledge, and problem-solving. Superintelligence is a theory that has not been validated.

B. Based on Functionalities

- **Reactive Machines:** These artificial intelligence systems don't keep track of memories or past experiences for use in the future. They analyze and respond to different situations. For example, Garry Kasparov lost against IBM's Deep Blue in a chess match.
- **Limited Memory:** These artificial intelligence (AI) systems can make smarter, more informed decisions by evaluating the past data they have collected. The vast majority of contemporary AI applications, including chatbots, virtual assistants, and self-driving cars, fall under this category.
- **Theory of Mind:** Researchers are continuing working on this more complex form of AI. It would require recognizing and retaining feelings, needs, and beliefs in order to make judgments based on them. This kind necessitates that the machine fully comprehend people.
- **Self-aware AI:** In the future, AI will be represented by machines that are sentient, conscious, and self-aware. This kind of artificial intelligence is still in the theoretical stage, but it could develop opinions and desires if it could comprehend and feel emotions**.**

CHALLENGES IN INCORPORATION OF ARTIFICIAL INGTELLIGENCE IN INDIA

India's socioeconomic, technological, and regulatory realities present particular challenges that must be acknowledged and taken into account when creating policy and implementing the technology, Although there is a lot of room for the country to develop artificial intelligence in the governance sector.

Improved capacity and enhanced understanding of emerging technologies- To effectively adopt AI-driven solutions, the government must increase its capabilities. This would also require more openness to, knowledge of, and skill with information technologies—qualities that the people in charge of putting the solution into action, such as teachers, police officers, or government officialsperhaps not have Given that partnerships with the business sector are the primary means of pursuing the development of AI-driven governance solutions, the corporate sector may need to provide a sizable amount of this capacity building. Open communication between the private sector developer, the government official or individual putting the solution into practice locally, and the government agency deploying the technology is necessary to build capacity.

Infrastructure-According to our research, the necessary infrastructure has not yet been created for the efficient and well-coordinated implementation of AI-driven solutions. To develop algorithmic models that faithfully capture the diverse array of socioeconomic realities in India that must be included into models for predictive policing, the inputs that can be used as training data in the law enforcement sector are not sufficiently comprehensive or cohesive. Lack of internet access and the availability of IoT devices are two infrastructure issues in the sphere of education.

. In India as a whole, 31% of people have access to the internet as of 2016. Out of 444 million people, 269 million in urban India utilise the internet (or 60% of the population), whereas just 163 million in rural India use the service (17% of the population, according to the 2011 census). The defence minister Nirmala Sitharaman has identified the absence of a sufficient technology infrastructure as a major barrier to the deployment of AI in the sector

Trust- Genuine worries about potential cultural ambiguity arise from each society that has grown accustomed to employing conventional tools rather than algorithmic models, especially intelligent models, across sectors. Locally employed police officers and educators have obtained training and practical experience utilizing methods unrelated to the usage of AI or knowledge derived from it. In many instances, their training and experience don't even involve the usage of ICTs Despite being enthusiastic about the strategic advantages of building autonomous solutions, the operational units of the defence forces do not entirely trust the CAIR-developed solutions

Funding-Funding AI-driven solutions is becoming a problem for all growing economies. The Rs. 3,037 crores included in the 2022 budget for the "Digital India Programme" further demonstrates the government's commitment for the advancement of AI-based solutions. This is being carried out in an attempt to expand resources and expertise in the domains of robots, artificial intelligence, and the Internet of Things (IoT). There has been some emphasis on developing a National Artificial Intelligence Program under NITI Aayog's leadership. According to an NITI AAYOG report, International Centers for the Transformation of Artificial Intelligence (ICTAI) should be established. The research recommends that seed money (between INR 200 crore and INR 500 crore per ICTAI) funded by grants from the public and private sectors should cover the ICTAI's operating expenses for the first five years in addition to the costs of the physical infrastructure and technological/computing infrastructure. The distribution of funds among the several subsectors remains uncertain, notwithstanding these positive advances. Given the ambiguity surrounding this matter, the government probably allocates the majority of cash to particular subsectors that it deems essential at the expense of others.

USES OF AI IN SECTORS INCORPORATING IN INDIA

Law enforcement around the world is researching and, in certain cases, using key AI technologies, such as drones, robocops, autonomous police cars, speech recognition, facial recognition, and predictive analytics. Our research in this area revealed that India's technical development is still in its infancy. Many initiatives are still in the ideation stage and lack the proficiency to completely integrate AI solutions for law enforcement. Additionally. India is working on projects that will supply the infrastructure and data needed to support AI solutions in the field of law enforcement. The following are some notable applications of AI in Indian law enforcement and other domains:

Speech and Facial recognition

In order to evaluate the gigabytes of data streaming from CCTV cameras placed in public areas, Best Group recently partnered with the Israeli security and artificial intelligence research company Cortica. One of the main objectives of this project is to make public areas like streets, bus stops, and train stations safer. The Punjab Artificial Intelligence System (PAIS), which uses facial recognition and other characteristics to automate research and digitize criminal records, was developed by the Punjab Officers in collaboration with Staqu. By using facial recognition, police may get information about the offender. If a police officer finds a suspect, he snaps a photo of him. The photo is next entered into the phone app, which compares the digital image with the previously stored photo. Additionally, the app will quickly convey the individual's criminal history to the concerned officer's phone.

H-Bots Robotics, a Hyderabad-based technological start-up, has created a smart policing robot that has not yet been used in the field The "robocop" can help maintain law and order and improve traffic control. If it were to be deployed autonomously, In places like malls and airports, it may carry out a variety of vital security-related duties, like maintaining security at key intersections.

Education

- Our research indicates that the most prevalent uses of AI in education are in progress tracking, student services, decision-making, and tailored instruction. It appears that few of the solutions being developed in this field have a linguistic focus, despite the fact that India is home to a large number of different languages. Machine learning seems to be the most popular approach among the solutions.

- Decision making- HTC Global Services, a US-based service provider, is concentrating on introducing products in the Indian education sector. Thanks to this web-based technology, college students will be able to choose courses and electives more wisely.This application will effectively employ the same algorithms that let users choose products on e-commerce sites by using AI and machine learning to analyze historical data

- Student Service- From both the viewpoints of students and instructors, this would include responses to challenges such as admissions questions, which are mostly manual and time-consuming. They are preparing to introduce an algorithm that can accurately interpret students' facial expressions to determine their comprehension level, as stated by Global Practice Head for AI & Data Science Vishal Sethi.

- Student Progress Monitoring-In order to enable tailored child monitoring and offer them with individualized attention regarding their progress, Microsoft's Machine Learning Platform is being used by the Chandrababu Naidu-led government of Andhra Pradesh to collect data from many databases. As a result, there will be fewer school dropouts.

- Personalized Learning- An open-source learning tool called Ek-step makes use of APIs (API). The platform makes use of gamified apps that may be found on Google Play As of 2016, it was purportedly used in more than 10,000 government schools in Karnataka. Additionally, the platform is accessible in 18 states and 5 languages. Co-Impact, a grouping of the world's top philanthropists that includes the Rockefeller Foundation and the Bill and Melinda Gates Foundation, recently announced that it will soon begin working with the Ek-Step Foundation. To spread the platform across the nation, the government also intends to collaborate with Ek-Step. According to CEO Shankar Maruwada, this project can be scaled up in the future even if for now, only teachers will need a mobile phone or IoT device to access the content. Using artificial intelligence to organise and filter pertinent content for each individual learner would undoubtedly be advantageous for such a project. It might either develop into a smart content platform that serves as a teaching tool or be employed to create an ITS model using the current platform.

DEFENCE

- Our research indicates that the defence industry primarily uses artificial intelligence (AI) for cyber security, robot soldiers, intelligence, surveillance, and reconnaissance, as well as intelligent weapons systems and risk terrain assessments. Defence is the only industry we examined where the use of autonomous systems is being expressly researched. It's unclear how much the various parts of government genuinely trust and support these efforts, though, as many are still in the planning and trial stages.

- **Intelligence, Surveillance, and Reconnaissance**: In order to keep an eye out for invasions and identify naval mines in coastal regions, the Indian army has started using unmanned autonomous vehicles. To conduct airborne surveillance and reconnaissance, a range of unmanned aerial vehicles have also been developed, including the recently tested Rustom-248, which can function in both robotic and manual modes. The robot Daksh, created by the DRDO, can be controlled remotely from 500 meters away. Similar to PackBot, which is used by the US army, its main function is to spread explosives. Working together with the private sector has also helped to improve this technology. As an illustration, the AI business Crone Systems, based in New Delhi, has analyzed seasonal data to look for indications of border infiltration and is able to estimate the probability of border crossings at particular times using an algorithm. In order to anticipate the place and timing of unrest and send the appropriate personnel, Innefu Labs is working with the Central Reserve Police Force and Border Security Force to monitor social media posts.

- **Robot Soldiers**- The Centre for Artificial Intelligence and Robotics (CAIR), a facility connected to DRDO, has been working on a project to develop a Multi Agent Robotics Framework (MARF). By using a multilayered AI-powered architecture, this aims to promote the development of a range of robots that can collaborate and work as a team, similar to human trops.A Wheeled Robot with Passive Suspension, a Snake Robot, and a Robot Sentry are some of the 407 robots that have previously been built. By 2025, the US hopes to develop both manned and unmanned intelligent teaming for autonomous convoy operations and combat missions, suggesting the direction of technology and the potential for a greater number of "robot warriors" than humans.

- **Cyber Defence**-The use of AI by the government is enhancing and expanding cyber security capabilities. For instance, CDAC and IIT Patna are working together on a project to create artificial intelligence (AI)-powered cyber forensic tools that law enforcement, the government, and intelligence services may use. In their latest product, Prophecy, Innefu has been commissioned by the Indian government to analyze intelligence agency data in order to evaluate threat patterns and predict future events.

- **Risk Analysis-** The following are some ways that AI is being applied to risk terrain analysis, per an article from the Defence Research and Development Organization (DRDO):

1. ***Military Geospatial Information System:*** This facilitates the creation of terrain traffic ability maps, sometimes referred to as Going Maps or GMs, with respect to the Soil, slope, moisture, land usage, and landform are the five thematic layers. The maps are then produced in a three-level hierarchical manner once they have been combined.
2. ***Terrain Feature Extraction System:*** This technique trains a multilayer perceptron, which produces a variety of themes, allowing land use classification.
3. ***Terrain Reasoner System:*** provides decision-makers with the flexibility to create various routes to achieve a target,
4. ***Terrain-Matching Systems:*** These clever tools combine complex case-based reasoning to create a logical whole.

- **Intelligent weapon System•** In February 2018, after a number of successful testing cycles, DRDO confirmed that a modified Pilotless Target Aircraft (PTA) Lakshya-II was India's first "armed drone." According to the DRDO, nine flights with an accuracy level of 20 meters have been successfully completed.

Artificial intelligence-based cybercrimes

Artificial intelligence - Controlled Cyberattacks

- **Deepfakes**

Deepfake, which combines the terms "profound learning" and "fake media," describes how computers with artificial intelligence are used to alter and make conventional media seem real. Currently, cybercriminals utilize this technology to create non-consensual pornography of celebrities or other well-known individuals or to spread political misinformation. Notably, they deceived an energy firm in the UK into sending €220,000 to a bank account in Hungary in 2019.

Types of deepfakes and their uses

AI is used in deepfakes to create or modify audio and video content. They are employed for a variety of objectives, both good and bad, including the following:

Pornography: Deepfakes are most frequently used for non-consensual pornographic content. Without permission, the faces of regular people or female celebrities are switched onto the bodies of porn actors. Both, privacy is violated and reputation is harmed by this. For example, in 2019 an Indian guy was arrested for deepfake pornography of his girlfriend.

Politics: While worries about artificial intelligence (AI) in politics have existed since the late 2010s, their relevance to democracies and the electoral process in particular has increased with AI's recent development. This new technology puts democracies at danger in a number of ways. First, it can spread misinformation and disinformation, which can inflame emotions and lead to violence or conflict over elections. For instance, AI has the ability to produce misleading information, propagate bias, or hold views that are not representative of the general public. In summary, even with its advantages, artificial intelligence (AI) has the potential to negatively impact the democratic process. A BJP leader's authentic video was edited to depict him disparaging rivals during the Delhi polls. Campaign sabotage and candidate maligning can occur from such fakes. Unchecked, political deepfakes have the potential to sabotage impartial and free elections.

Legal Framework for Deepfakes in India

In its most recent suggestion, dated November 07, 2023, the Ministry of Electronics and Information Technology instructed the primary social media intermediaries to undertake the following:

- Ensure that due diligence is carried out and that the proper steps are taken to identify deepfakes and misleading information, particularly anything that violates user agreements, laws, and/or regulations.
- To ensure that situations of this kind are handled as soon as possible while meeting the timelines specified in the IT Rules 2021.
- the hosting of such Deep Fakes, information, or content is discouraged.
- If such material is brought to light it must be taken down within 36 hours.
- Ensure that access to the material and information is disabled and that prompt action is done, well within the timeframe specified in the IT Rules 2021.

Humor/Parody: Parody AI is the result of artificial intelligence becoming a part of the creative process. This is a cutting-edge approach to creating content that parodies or imitates current literary, musical, or artistic masterpieces. Parody AI is capable of examining patterns in the source material by utilizing machine learning methods. After then, it generates fresh works that keep the spirit of the original while adding a lighthearted or insightful twist. The technology pushes the limits of artificial intelligence's application in creative processes while also offering a fresh method to interact with content.

However, it raises certain serious concerns as politicians or celebrities are frequently included in satirical deepfake videos. They use their voice or face in absurdist or humorous contexts. Although it is common to parody public personalities, consent concerns arise when private individuals are involved as their rights become vulnerable. Funny fakes can also blind viewers to the riskier applications of this technology.

Fraud: AI speech cloning can mimic government officials or CEOs in order to get private information. This strategy stole €200,000 from a UK energy company in 2022. By presenting bogus business statements, deepfakes can potentially be used to affect stock values. The financial system can become unstable as a result of such fraud. Therefore, it is always suggested to be mindful that erroneous or incorrect information can be produced and disseminated by AI. Before making an investment, verify the reliability of the underlying sources and consult a variety of information sources.

Disinformation: Deepfakes can be weaponized by state and non-state actors to disseminate false information on an unprecedented scale. For example, a fake film that purported to show a Bahraini opposition leader plotting with Qatar intensified tensions in the Middle East in 2018. In unstable environments, viral deepfakes have the potential to spark violence, public panic, and civil unrest.

INFORMATION TECHNOLOGY ACT, 2000

- **The Information Technology Act of 2000, Section 66D**: Section 66D of the IT Act of 2000 addresses impersonation cheating using computer resources or communication devices. Violations of Section 66D can result in a fine of ₹1 lakh or up to three years in jail.

- **Section 66E of Information Technology Act, 2000**: This section specifically targets privacy violations related to the creation, publication, or transmission of a person's images through deepfake means. Section 66E offenses carry a maximum sentence of three years in jail or a fine of ₹2 lakh.

When someone is used to create convincing images, audio and video hoaxes or any related cybercrimes like deepfake is punished under the section 66D and section 66E of the IT Act,2000.

In a recent legal development, Bollywood actor **Anil Kapoor** initiated legal proceedings after discovering AI-generated deepfake content that exploited his likeness and voice. The content ranged from innocuous GIFs and emojis to sexually explicit material. This lawsuit, titled **"Anil Kapoor v. Simply Life India and Others"**, appeared in the **Delhi High Court**. The importance of protecting a person's identity and personal characteristics from abuse was acknowledged by the court, especially when deepfakes are produced using AI methods. The Delhi High Court thereupon ordered an ex-parte injunction, essentially prohibiting sixteen (16) businesses from using Anil Kapoor's name, picture, or image for profit or business.

Amitabh Bachchan, the renowned actor, also pursued legal action in the matter of **"Amitabh Bachchan v. Rajat Negi and Others**." In order to prevent the unapproved use of his personality rights, such as his voice, name, image, and likeness, for commercial reasons, the court issued him an ad interim in rem injunction.

Artificial intelligence - Controlled Password Cracking and Helped Hacking:

Cybercriminals are developing algorithms for guessing customers' passwords by using artificial intelligence (AI) and computer-based intelligence. Although there are currently some secret key breaking algorithms available, cybercriminals will really want to analyze large secret key datasets and generate many secret word variants.

In addition to unlocking secret keys, cybercriminals are also employing artificial intelligence to automate and improve a variety of hacking techniques. Automated vulnerability screening, system defect identification and manipulation, flexible malware building, and more are made possible by artificial intelligence computations.

LEGAL FRAMEWORK IN INDIA

- **Section 66 of the IT Act, 2000:** The Section states that hacking is a crime that carries a maximum three-year jail sentence, a fine of five lakh rupees, or both.

- **Section 66B of the IT Act, 2000:** It penalizes someone who obtains a stolen computer system or other communication device dishonestly. A fine of up to one lakh rupees, three years in prison, or both are the possible punishments.

When someone used to unauthorized login to others' computer resources with fraudulent and dishonest intention or any related cybercrimes is punished under the section 66 and section 66B of the IT Act, 2000.

Supply Chain Attacks

When dangerous code or components are added to genuine goods or services, artificial intelligence can also be utilized to force a corporation to reevaluate its programming or equipment inventory network.

Potential artificial intelligence- Helped Attacks Targeting Organizations

Not surprisingly, scammers are increasingly taking advantage of artificial intelligence. These cyberattacks, which are managed by computer-based intelligence, have the potential to impact businesses.

Business Email Compromise (BEC)

Corporate email breaches are one kind of phishing assault that targets businesses in an attempt to steal funds or personal data. Artificial intelligence algorithms have the ability to decipher correspondence designs and produce convincing phishing messages that pose as high-level executives or associates in an attempt to trick representatives into carrying out prohibited actions such as initiating dishonest conversations or discovering sensitive information.

- **Advanced Persistent Threats (APTs)**

APTs break into company networks, avoid detection, and steal confidential data over time by using complex protocols. Aggressors can alter their strategies, circumvent security measures, and take advantage of weaknesses in company systems by using simulated intelligence computations.

- **Ransomware Attacks**

Business-critical data is corrupted by ransomware, which also demands payment to unlock the codes. The potential payoff for thieves can be increased by using computer-based intelligence calculations to target specific resources and mechanize the spread of ransomware.

- **Fraudulent Transactions**

Cybercriminals can use advanced man-made intelligence calculations to automate fake discussions focused on enterprises. Artificial intelligence-driven extortion may mimic real transactions to circumvent common fraud detection systems and take advantage of weaknesses in payment processes.

- **Installment Passage Extortion**

Cybercriminals may employ artificial intelligence advancements to automate and impact several aspects of installment door extortion, hence enhancing its sophistication and difficulty of detection. In order to evade detection systems, fraudsters may employ techniques such as creating plausible fake personas, breaking down samples, or directing targeted phishing attacks with content generated by artificial intelligence.

- **Distributed Denial of Service (DDoS) Attacks**

Computer-based intelligence can be used to boost the effectiveness of DDoS assaults against for-profit websites and online services. Computer-intelligence-powered botnets may coordinate massive volumes of malicious traffic, overloading servers and disrupting business operations.

- **Intellectual Property Theft**

Cybercriminals can computerize the process of focusing on firms to take substantial licensed innovation with the aid of man-made intelligence. Massive volumes of data can be decoded by artificial intelligence systems, which can then detect sensitive information or valuable proprietary breakthroughs., which they can then use to gain an advantage or profit.

EFFECT OF ARTIFICIAL INTELLIGENCE ON DATA PRIVACY

Because AI is so complex, the privacy of both individuals and organizations is at risk .People might not even be aware that their personal data is being used to make judgments that impact them as AI advances since it may be able to make decisions based on small patterns in data that are difficult for humans to discover. AI systems require enormous amounts of (personal) data, which can be misused for malicious purposes like identity theft or cyberbullying.

Most information privacy regulations in Victoria are based on the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Privacy laws around the world continue to uphold eight core principles stated in these guidelines. One benefit of principle-based law is that, in line with shifting social norms and technological developments, it recognizes the nuanced and complicated nature of privacy and allows for some flexibility in how it can be protected in various contexts. Although the OECD Guidelines have been incredibly successful in expanding information privacy regulations around the world, the core principles that the Guidelines are based on are threatened by artificial intelligence (AI).

The most comprehensive privacy law in the world is the General Data Protection Regulation ("GDPR") of the European Union. All people living in the EU and the EEA are subject to its privacy and data protection regulations, which also give data subjects a number of rights. Additionally, the GDPR places severe requirements on data controllers and processors, forcing them to handle personal data according to exacting standards and by putting data protection principles into practice. In the United States, privacy laws are governed by both federal and state laws. Sector-specific laws, such the Health Insurance Portability and Accountability Act ("HIPAA") and the Children's Online Privacy Protection Act ("COPPA"), safeguard particular kinds of data and apply to certain companies.

. However, AI-driven data processing is not particularly covered by any federal privacy laws. The strongest state privacy law in the union is the California Consumer Privacy Act ("CCPA"). It gives Californians broad control over their personal information and places requirements on companies that gather, use, or sell personal data.

CONCLUSION AND SUGGESTIONS

The concept of imitating human intelligence in computers with the aim of making them think and behave like humans is known as artificial intelligence (AI). This would enable AI computers to carry out jobs that were previously limited to human performance. AI might even be more efficient than humans at some tasks. AI is reshaping nearly every industry – and cybersecurity is no exception. In addition to more conventional technologies like antivirus protection, fraud detection. AI is becoming increasingly important to cybersecurity firms in areas such as risk management, intrusion detection, identity and access management, data loss prevention, and other critical security domains. Having this intelligence would provide cybersecurity companies a big advantage in thwarting assaults in the future. Preventing breaches would help save organizations' IT expenses while also protecting the data of both individuals and corporations.

However, there is also the other side of the coin i.e., Concerns about risk management and data protection for both individuals and businesses will grow as artificial intelligence advances. Regulators are considering ways to maximize the benefits of AI and progress its development while reducing the likelihood of negative consequences on society. But as of right now, India lacks comprehensive AI legislation.

Artificial Intelligence (AI) tools are creating new opportunities for society in almost every industry. To keep the AI threat under control, the industry will need to keep up with hackers' increasing use of massive language model technology. . The majority of the conversation centers on artificial intelligence and how it affects cybersecurity and crimes. The paper has attempted to discuss the challenges in incorporating AI in India, effect of AI on data privacy and cyber security. In order to effectively regulate deepfakes in India, methodical reforms must be implemented in order to manage this potent and dangerous technology. It is critically necessary to pass a strong, comprehensive deepfake law that addresses consent, privacy, redress, and criminal ramifications.

Important measures include mandatory labeling, restrictions, and fines for malevolent deepfakes. Guidelines for verifying video evidence are necessary for law enforcement, courts, and the media to prevent injustices from occurring. Social media companies should be required to quickly identify and eliminate dangerous deepfakes. To confirm the legitimacy of material, they can use digital fingerprinting based on blockchain. On the other hand, high liabilities can encourage over-censorship, necessitating safety measures. Government and media public awareness initiatives are essential for educating the public about the dangers of deepfake information. Education in media literacy, particularly for young people, can produce critical, informed digital citizens. To combat misinformation risks, fact-checking networks and cybersecurity need to be improved. A flexible and dynamic regulatory strategy is essential for this intricate problem combining technology, ethics, and law. With thoughtful planning and cooperation from all stakeholders, India can set the standard for ethically maximizing deepfakes while mitigating their perils.

Following are the suggestions put forth by the author-

- Since there are no foolproof methods for dealing with cybercrimes, it is reasonable to assume that every instance will need to be examined based on its unique set of circumstances, especially considering the proliferation of computer resources, gadgets, communication devices and advanced technology. Laws must evolve in a more effective manner to stop cybercrimes especially in this growing age of artificial intelligence.

- A comprehensive law must be brought to regulate the activities concerned with using AI in different fields specially when it is being used in upgrading or modernizing the cybercrimes.

- The Information Technology Act, 2000, the Indian cyber law, has a chapter on offenses; however, it only addresses a small number of cybercrimes, whereas cybercrimes such as cyberterrorism, cyber nuisance, cyberstalking, and cyber harassment, are not specifically covered by the IPC or the I.T. Act. This is a problem for the judiciary as well because it makes it difficult to slot these offenses into the pre-drawn, generic categories without discussing particular cybercrimes. Therefore, a thorough legal and regulatory framework is required to regulate cybercrimes of all kinds.

- In order to modernize the systems and functions, substantial resource mobilization is required for computer literacy among judges, prosecutors, and police personnel. Additionally, because cybercrimes are high tech and require some degree of technology skill, specific courts handling cybercrimes are necessary for the prompt administration of justice in this area specially when technology is becoming even faster and more advanced due to advent of AI.

- To help protect victims of deepfakes, regulators are updating the laws. However, the current legal framework is a little disjointed because different jurisdictions have different strategies and regulate deepfakes in different ways to different extents. Therefore, steps must be taken globally to bring a uniform set of rules to tackle these emerging issues and challenges.

- With AI technologies and chatbots becoming more and more popular, it's critical to take the appropriate safety measures to protect against fraud. Vigilance and proactive steps are crucial. Individuals and companies may strengthen their defenses against these new threats by remaining aware and putting strong cybersecurity procedures into place, guaranteeing a safer online environment for everybody.

REFERENCE

[1] Agnieszka Jabłonowska, Maciej Kuziemski, Anna Maria Nowak, Hans W. Micklitz, PrzemysławPałka & Giovanni Sartor, “Consumer Law and Artificial Intelligence: challenges to the EU consumer law and policy stemming from the business' use of artificial intelligence” 2 ARSTY project report 26-38

[2] Wolfgang Ertel, Introduction to Artificial intelligence (2017).Govt working report on applications of Artificial Intelligence for military use, Nirmala Sitharaman” available at<http://www.dnaindia.com/india/report-govt-working-on-applicationsofartificial- intelligence- for-military-use-nirmala-sitharaman-2617429>

[3] R. Sane, “Budgeting for the police” Live Mint.

[4] S. Goudarzi and N. Khaniejo, “The Centre for Internet and Society” (2018, March 18). AI and S. Janyala, “Hyderabad-based startup launches smart ‘robocop’, named after 26/11 martyr Hemant Karkare”, Indian Express

[5] S. Moorthy, “HTC Global sets sights on education space” Hindu Businessline

[6] S. Lakshmi, “EkStep takes a giant step to empower government school children through technology”India Times.

[7] Anil Kapoor v. Simply Life India & Others., CS(COMM) 652/2023, Delhi High Court (Sept. 20, 2023)