VOLUME - 14, ISSUE - 12, DECEMBER - 2025 • PRINT ISSN No. 2277 - 8160 • DOI : 10.36106/gjra

Original Research Paper | Information Technology

AI AND CYBERSECURITY: A STUDY OF AWARENESS, ACCEPTANCE AND APPREHENSION

Vaishali Fating — Associate Professor, Department of Commerce, Dr.Ambedkar College, Nagpur, Maharashtra,(India).

Sheetal Jaikar* — Assistant Professor, GHRCE, Nagpur, Maharashtra, (India). *Corresponding Author

ABSTRACT Artificial intelligence (AI) is swiftly transforming the cybersecurity perspective techniques like machine learning, can assess vast amount of data to recognize styles of spiteful activities.AI has enormous and constantly expanding promise in cybersecurity. We may anticipate ever more advanced threat detection, prevention, and response capabilities as AI develops. But it's crucial to keep in mind that AI is a tool, and that means that its efficacy depends on how well it's implemented and integrated with current security procedures. For example, it is present in language processing, gaming, expert systems, financial transactions, expert systems and many more areas. Despite its many benefits, artificial intelligence (AI) has the potential to end human life, which is why human oversight of its operations is necessary . Cybercrimes are now often reported about in the media on a daily basis. It is a global issue, not one that only affects a single nation. Artificial Intelligence is useless without robust security measures as anybody may readily access it. Because of cyber attacks online, governments, banks and global corporations are now seriously threatened. This research paper studies to explore the plausible of AI to boost defenses against cyber threats. Finding the best possible AI techniques of defense in every aspect of human existence and digital environment also.

KEYWORDS : cyberattacks, virtual world, techniques , measures , risks, cyber security.

INTRODUCTION:

AI-driven cyber security makes it feasible for all these--real-time detection ,analysis and action in response to cyber threats .The AI algorithms are able to identify vulnerabilities throughout the entire network and halt common modes of cyber attacks by examining large quantities of data that exhibit a pattern indicative of a threat.In essence ,with AI-powered cyber security, you can proactively address any potential cyber risks identified by AI in real time---- an essential part of managing cyber security. Cyberattacks have grown dramatically in complexity, quantity, and impact ,when the first denial-of-service(DoS) assault was conducted since 1988. Cybersecurity countermeasures have evolved along with the sophistication and targeting of cyberattacks. Although the initial security tool was restricted to identifying viral signatures and stopping their execution ,modern solutions are made to offer comprehensive defense against a wide range of target systems and attack methods, protecting information assets in the virtual world has grown more difficult.Cyber crimes are on the rise even with the rise with adequate security measures in hand. This can be accomplished by malicious software, phishing, password attacks, drive-by downloads through hyperlinks, virus attacks, and other methods.[1]

According to the SSL Store's most recent estimate, cybercrimes will bring in 1.5 trillion dollars in revenue in 2018.There's a good likelihood the real numbers are higher.

Cybercrimes' Diverse Revenue Sources

Crime	Annual Crime revenue in US dollar
Data Exchange	$160,000,000,000
Theft of Trade Secrets and Intellectual Property	$5,000,000,000
Illegal Internet Markets	$860000000000
Crime Ware / CaaS	$16000000000
ransomware	$10000000000
Total Income by Cybercrime	$150,000,000,000

*Source: Re-Hashed: Cybercrime Data for 2018.

The data presented in the table above indicates that more than half of the revenue from cybercrime originates from online marketplaces. It is astonishing that ransom ware generated $10,000,000,000 in just three years, from 2013 to 2016. The challenges posed by cybercrime are becoming increasingly critical and alarming, necessitating robust security measures for organizations to protect against these threats. Therefore, vigilant cybersecurity is essential. Cybersecurity is also necessary for emerging digital platform technologies like cloud computing, internet banking, mobile and electronic commerce, and mobile computing. This should include a variety of strategies to guard against hackers' damage and illegal access to networks, programs, and stored data.[2]

Literature Review:

- According to the study conducted by Sarker, Furhad, & Nowrozy (2021) , the stusy laid stress on various cyber attacks in IT fields and various other sectors where data vulnerability is highly at risk and hackers are easily hacking the system through malicious ways .In their research they have discussed about AI-based security intelligence modelling to detect the online cybercrime and take more actionable and intelligent measures to solve the problem. Using AIbased methods such as machine learningbased, modeling, natural language processing, knowledge representation, and concept modeling, we have enabled intelligent cybersecurity systems to use this information to solve complex safety issues such as people.
- Another study by Hassan & Ibrahim (2023), emphasizes that a significant role that AI plays in protecting today's business enterprises statistical records, properties and services costs are on rise in case of online data or even money transferring is at high risk. AI is increasingly a way to solve this problem. This issue already exists in the field of cybersecurity in literature and security products. A methodological approach to assess and assess vulnerabilities in an organization's IT infrastructure, applications, and systems. This includes aggressive scans, testing and analysis of potential weaknesses that malicious people can exploit.
- According to Jakka ,Yathiraju& Ansari (2022) ,the study says that in today's world of Information technology there is a huge amount of malicious software virus spotting like malware and delivering cyberriskmanagement.There is a wide range of AI technologies that are intensively used to recognize malware within a system that is classified by several sections such as authentication, security, and

confidentiality. Malware recognition processes are classified after several sections such as authentication, security, and confidentiality.All three aspects are managed by a variety of AIbased solutions to recognize malware and protect your computer system from despiteful attacks. In the modern world, individuals who are directly or indirectly connected to the internet are strongly exposed to cyber attacks. In organizations, AIbased systems can help detect threats and response capabilities related to advanced assault It also helps in hyper responsive to data escape, malware, conscript attacks, and ransomware.

- According to Chinenye Cordelia Nnamani (2024),laid stress on AItechnologies,AI practices and emphasizes the need for careful and ethical inclusion of AI cybersecurity. The spread of AI with threat intelligence flows enables a constantly updated knowledge base, enabling businesses to respond effectively to new threats. The author describes the key cooperatives between human experts and AI technology. This is highlighted in advance in this paper The essay highlights for value of ongoing funding for cybersecurity experts' AI training programs, recognizing that AI works best When combined with human insights.

Research Methodology:

We have studied few literature reviews and found the gaps to tackle the problem study.Both primary and secondary methods of data collection have been used to study this problem statement.

There are several AI tools that are utilized for cybersecurity purposes. Here are some of the commonly used ones: **1. Aidriven Threat Detection:** Large data sets can be analyzed by AI systems, which can then spot trends that point to possible dangers or attacks. Artificial intelligence is used by programs like Darkrace and Cylance to identify and react to online threats instantly.

2. Natural Language processing (NLP) for security monitoring: NLP algorithms help identify and understand security scripts, allowing for threat detection and faster response. Tools like Exabeam use NLP capabilities to improve security monitoring.

3.Analytics for risk assessment: AI algorithms can predict security risks by analyzing historical data and identifying vulnerabilities. Tools like Rapid7 and Splunk use predictive analytics for risk assessment

4.Behavior analysis for anomaly detection: AIbased behavior analysis tools monitor user action and behavior to detect differences in patterns; This may indicate that there is security protection. User and Site Behavior Analysis (UEBA) tools such as Securonix and Varonis use this method to detect vulnerabilities.

5.Automated incident response: AIpowered tools can help organizations respond to threats more effectively by automating the incident response process. Security orchestration platforms such as Demisto and Phantom can be integrated with various security systems in the network for efficient operation.

6.Machine learning for fraud detection: Unauthorized access attempts and fraudulent activities can be identified by training machine learning models. Tools like Fortscale and ThreatMetrix use machine learning for fraud detection and user identification.

There are many such online fraudulent cases taking place daily in some or other cities not only in India but across the world .Many of the innocent people are duped of lakhs and crores of rupees in lieu of job placement in domestic and international level as well.Very few culprits are punished under the cyber laws.Many incidents are such which are not even registered with the official cyber office.

Important Cyber Law Case Studies:

1.Fraud at the Pune Citibank MphasiS Call Center: Some former employers of Mphasis Ltd , Msource's BPO ARM, are Citibank who was deceived for 1.5 crore. It was one of these cases of cybercrime that raised many types of concern, including the role of "data protection."The crime was clearly committed to the "e-account room" of customers with "unauthorized access."

Therefore, it is firmly in the field of "cybercrime."ITA20000 is so versatile that it is not covered by ITA20000, but is covered by the crime aspects covered by other laws. This is because each IPC crime using an "electronic document" can be considered a crime that can be initiated using a "written document." Therefore, "fraud", "conspiracy", "broken trust" etc. can be applied in the above cases, in addition to the ITA-20000 section.

2.Sony.Sambandh.ComCase:

He was first found guilty of cybercrime in India in 2013. It all began with a complaint filed by Sony India Private Ltd, the company that created www.sonysambandh.com. This website allows NRIs to send Sony products to friends and family in India after paying for them.

The organization guarantees that everyone involved will receive the product. According to a Cyber Crime case study, someone using Barbara Campa's identity registered on the website in May 2002 and placed an order for a Sony color TV and wireless headphones. She asked Arif Azim in Noida for the merchandise and provided her credit card number to make the payment. The credit card agent executed the transaction after correctly removing the payments.

3. The Financial institution NSP Case: One of the biggest examples of cybercrime is the case of a married bank management trainer. The two sent and received numerous emails on company computers. Following their eventual breakup, the girl created fake email addresses, such as "Indian Bar Association," and sent them to the boy's clients abroad. She used a bank computer for this. The boy's company lost many customers after suing the bank. The bank had authority over emails sent through its system.

Later, it was discovered that the accused ran five businesses under false pretenses and employed computer-aided and fictitious vouchers to save money and show taxes.[6]

Key terms	Description
Malware	Malware violates the network due to its security sensitivity. Usually, users will click on a dangerous link or e-mail attachment to install risky software.
Phishing	Sending phony messages that appear to be from reliable sources, primarily through email, is known as phishing.
Ransomeware	The other party will encrypt the victim's data in the case of a ransomware attack and offer to supply a decryption key in return for money.
File less Malware	A form of malicious activity known as fileless malware uses legitimate, native tools built into the system to carry out cyberattacks. Compared to ordinary malware, files that require less malware to install code on the target system are more difficult to detect.

Spyware	Spyware is undesired malicious software that infiltrates computers or other devices and gathers data about a user's online activities without the user's consent or knowledge.
Trojan	Trojans are malware and appear to be disguised as legal software as harmless files such as native operating system programs and free downloads. Social engineering techniques, like fishing and bait websites, are used to install Trojan horses.
Worms	A self-replicating program that spreads copies to other computers is called a worm. Worms can be distributed phishing-style or seamlessly, or they might infect targets through software sensitivity to security.

Major Cyber Attacks And Data Breaches In 2025:

1.	**Star Health Insurance Data Leak (October 2025):**	Sensitive data of over 31 million policyholders was leaked online, with a hacker claiming responsibility.
2.	**Angel One Potential Data Leak (February 2025):**	An unsecured cloud storage bucket may have exposed data for 7.9 million users.
3.	**Aditya Birla Capital Digital App Hack (2025):**	An API vulnerability exposed customers' loan and PAN details.
4.	**AI-Generated Phishing Attacks (2025):**	Banks and fintech platforms reported an increase in sophisticated, AI-generated phishing to steal credentials and financial information.
5.	**Dellhi Hospitals Ransomware Attack (June 2025):**	Hospitals were hit by ransomware that compromised patient and billing data.
6.	**Hospitals were hit by ransomware that compromised patient and billing data.**	Pakistan-backed hacking groups used malware-infected PDFs to target researchers at DRDO.
7.	**Attack on Small Cooperative Banks**	A ransomware attack on an IT service provider affected the digital payment services of around 300 small banks.
18.	**Star Health Insurance Data Leak (October 2025):**	Sensitive data of over 31 million policyholders was leaked online, with a hacker claiming responsibility.

CONCLUSION:

Cybercrime are now becoming the menace in today's world that are hampering the growth of any industry including IT ,Banking ,Education ,Business ,Armed forces etc..AI has come to the rescue in this regard having its own constraints .The AI tools are so very diligently applied that the hackers are also now become more vigilant and escape the trial if found guilty .Both the pros and cons of AI tools have helped to overcome the problem that is generated through unethical increase in cybercrime since a decade that has harmed and damaged vital information in many fields. With its rigorous detection, prevention and response capabilities of threats, AI has great potential to improve cybersecurity However, how well it is incorporated into current security frameworks will determine how effective it is. Despite the fact that artificial intelligence (AI) could strengthen defenses against cyberattacks,

REFERENCES:

1) Wirkuttis, N., & Klein, H. (2017). Artificial intelligence in cybersecurity. *Cyber, Intelligence, and Security*, *1*(1), 103-119.
2) Camacho, N. G. (2024). The Role of AI in Cybersecurity: Addressing Threats in the Digital Age. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *3*(1), 143-154.
3) Patil, P. (2016). Artificial intelligence in cybersecurity. *International journal of research in computer applications and robotics*, *4*(5), 1-5.
4) Sarker, I. H., Furhad, M. H., &Nowrozy, R. (2021). Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. *SN Computer Science*, *2*(3), 173.
5) https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/
6) LAZIĆ, L. (2019, October). Benefit from Ai in cybersecurity. In *The 11th International Conference on Business Information Security (BISEC-2019), 18th October*.
7) Hassan, S. K., & Ibrahim, A. (2023). The role of artificial intelligence in cyber security and incident response. *International Journal for Electronic Crime Investigation*, *7*(2).
8) Jakka, G., Yathiraju, N., & Ansari, M. F. (2022). Artificial Intelligence in Terms of Spotting Malware and Delivering Cyber Risk Management. *Journal of Positive School Psychology*, *6*(3), 6156-6165.