IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 6, April 2024

Artificial Intelligence in Cybersecurity

Abhishek Gautam, Aditya Prakash, Gariyas Kaushal
Department of Computer Science Engineering
Dronacharya College of Engineering, Gurugram, India

Abstract: *The usage of Internet as increased with time ,but with the increase in usage of internet ,the cases of Cybercrime has also gone up. However, with increase of artificial intelligence ,the companies and business are starting to look for AI tools to help against cybercrime .AI is becoming an essential component of every business. Cybercrime is one of the important sectors where AI has begun demonstrating valuable inputs. It is due to the fact that AI is faster than humans to take action and make an alternate plan of action to protect business and send warning against cybercrime. We will discuss recent cyber crime and how AI is used in the industry to defend itself in the long run.*

Keywords: AI, Cybercrime, Cybersecurity, classification

I. INTRODUCTION

The Cybersecurity industry is undergoing a significant transformation due to artificial intelligence ,as the market for AI-driven cybersecurity. Products are increasing day by day.The various applications of AI have enabled it to be applied in different industries today.The idea of AI being in cybersecurity has also been applied through very effective systems [1].The systems that use AI have a recorded increased effectiveness and benefits.

1.1 Background In Cybercrime

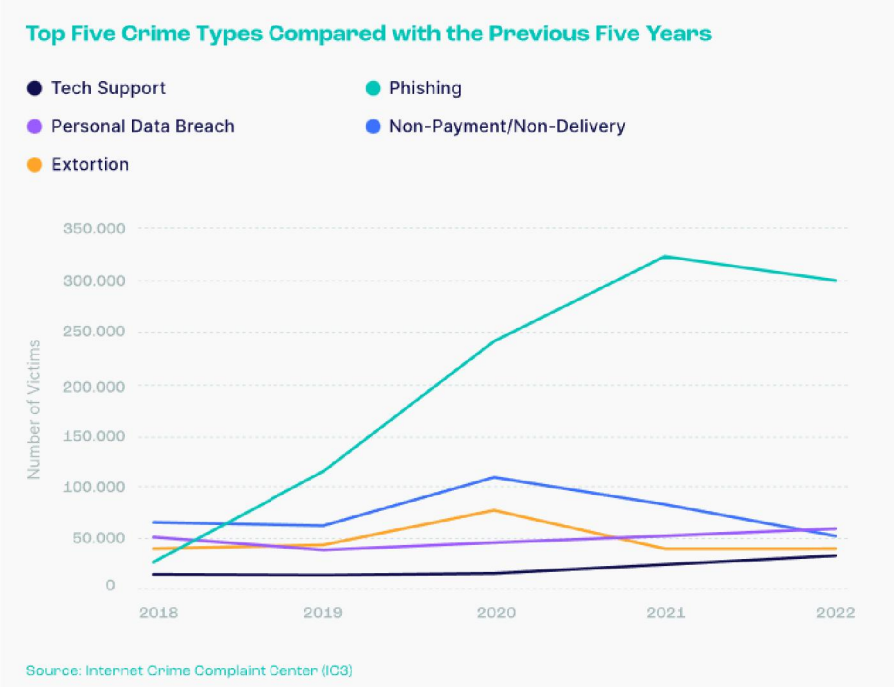
Cybercrime means committing any kind of crime or identity theft Through online means such as computers. There are several ways through which attackers engage in cybercrime [1].Despite making the tools for learning and entertainment ,many hackers use it to commit crime.Criminal activity across the internet increases with the development of every technology [2].

The increasing rates of cybercrime have created the need for most governments to include a cybercrime unit [2] [3]. These units ensure that cybersecurity has been increased across the country [3].Different countries have made specialized units for dealing with cybercrime.The main motive of cybercriminals for committing the crime is money and fame.Cybercriminals always focus on making a profit by using a defined attack on a company or another individual [3].The cybercriminals uses different methods for cybercrime like phishing ,DDoS attack ,ransomware ,identity theft ,software privacy,and more.Each of the above cybercrime includes different steps that can be included in achieving protection against it. A good example is a ransomware attack which ensures that the victim has paid a defined amount of money as directed by the criminal [4].There are times when different businesses get involved in cybercrime to keep their competitors in check .

Cybercrime was divided into three main types. The first type focuses on the device itself, the second type attacks are those used as a weapon against an organization, and the third is those attacks where a computer is an accessory to the crime .The major focus of cybercriminals are on the above three types.

Cybercrime has embraced AI technology to accomplish its critical attacks . Nowadays ,due to the advancements of AI you can see phishing attacks that are made to be social engineering through sophisticated AI tools ,like changing the voice on call to whom the victim recognizes. Cybercriminals utilize AI to optimize their password-cracking algorithms, resulting in swifter and more accurate password decryption. This heightened capability not only boosts hackers' efficiency and gains but also underscores the necessity for robust security protocols to counter such threats effectively. Moreover, it underscores the efficacy of anti-phishing algorithms in thwarting cyber threats.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 6, April 2024



Cybercrime has several effects on businesses in general. The below figure.1[13] depicts the impact of the $600 billion loss experienced in 2018 due to global cybercrimes [5]. These numbers indicate that cybercrimes are a growing menace to the community in general. Therefore, finding an effective solution to this issue is essential . Companies and businesses suffer greatly due to cybercriminals and cybercrimes due to which there is a need to update their security protocols. Finding security against cyberattack is therefore, it attracts attention from both corporations and countries.

1.2 AI in Cybersecurity

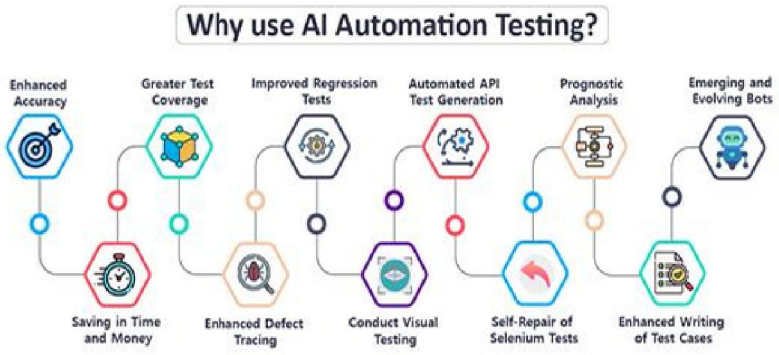
There is a growth in the cybersecurity industry due to application of AI. AI has increasingly been integrated in businesses by endorsing automation. Automation is primarily focused on increasing productivity and limiting human influence [3].AI is considered more applicable in data security because of the possibility of automation [7]. Automation is the machine-based execution of security actions, which can detect, investigate and remediate cyber threats with or without human intervention . Several factors are associated with AI being an essential part of cybersecurity . Most of these characteristics are related to the features of AI technology in the community today .

The primary attribute of AI technology integrated into cybersecurity lies in its prowess for detection. AI automation makes it an effective technology in

detection [8]. AI systems have the capability to be programmed to identify particular behaviors and trigger an alert if necessary. Given their ability to operate continuously, AI systems are perceived as highly efficient detection mechanisms. This attribute explains why the majority of organizations have adopted security protocols based on AI , as illustrated in Figure 2. Additionally, various network firewalls integrate AI algorithms as protective measures against cyber threats.

Intrusion Detection Systems (IDS) are essential components of modern network security infrastructure, designed to detect and prevent unauthorized access, misuse, and attacks on computer systems and networks [10]. Artificial Intelligence (AI)-based IDS, which leverage machine learning and other AI techniques, have emerged as a promising solution to address these challenges, offering significant advantages over traditional methods in terms of adaptability, pattern recognition, and real time detection and response capabilities [10].

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 6, April 2024



II. CHALLENGES OF AI IN CYBER SECURITY

There are several challenges and issues which affect AI development. The shortcomings and constraints of AI technology have been the primary obstacle to its wider adoption in cybersecurity.

2.1. AI Adaptability

AI can be considered a very new technology [6].Most of the people working do not have general awareness about AI. AI also requires significant investments from these organizations [3]. This challenge needs to be resolved by making people more aware about AI ,how it works, what its functions are and how it can be beneficial for them.

Despite the outlined limitations and challenges, AI remains a significant technology in the realm of cybersecurity defense systems. The technology has reportedly prevented attacks from different attackers [1]. The technology can be programmed into a cybersecurity system and be able to fend off different types of seizures [1]. This factor has made them cheaper to hire specialists [6].

2.2 IMPERSONATION

Impersonation is a tricky strategy utilized by cybercriminals to masquerade as somebody else, ordinarily a trusted person or substance, with the point of deceiving people into performing noxious activities or divulging sensitive information.Now due to headway in AI ,it has ended up very easy to mimic an individual voice ,deliver a confrontational call by utilizing their pictures that are accessible on distinctive stages. With the right footage,Anyone can make profound fake films by utilizing free apps. Individuals can also use free AI-powered devices to make strikingly practical fake voices trained on simple seconds of audio.AI is moreover being utilized in cybercrimes like virtual kidnapping tricks where the aggressor segregates the casualty whereas having access to their frameworks and requests a few emancipate. Law enforcement believes that in expansion to virtual capturing plans, AI may help criminals with other sorts of pantomime extortion in the future, including grandfather scams.

III. FUTURE OF CYBERSECURITY WITH AI

The future of cybersecurity with AI is poised for significant transformation, marked by innovative approaches to threat detection, response, and mitigation. As artificial intelligence continues to evolve and mature, its integration into cybersecurity practices holds immense potential to revolutionize the way organizations defend against cyber threats. Here are several key aspects shaping the future of cybersecurity with AI. More schools have been seen to include AI training across their institutions. Cybersecurity specialists are also urged to engage in skills in AI [12]. Each of these factors indicates the future of AI in cybersecurity is growing [3].Increased awareness promotes the development of AI defenses across cybersecurity [12].

The future of cybersecurity with AI promises to usher in a new era of proactive, adaptive, and resilient defenses against cyber threats. By harnessing the capabilities of AI for threat detection, predictive analytics, automated incident response, and adaptive security controls, organizations can strengthen their cyber resilience and effectively safeguard their digital assets in an increasingly interconnected and dynamic threat landscape.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 6, April 2024

IV. CONCLUSION

This paper the makes us understand a little better about the Artificial Intelligence ,its uses and its threats .How does Artificial Intelligence intrusion detection is better as it uses automation for 24*7 real-time threat analysis and faster than conventional intrusion detection systems.Companies ought to subsequently proceed to utilize AI calculations to adopt cybersecurity shields. Artificial intelligence should be taught to people and children in schools to make them more aware about it and make them less of a target for cybercrimes related to AI.

REFERENCES

[1] Bruschi, D., & Diomede, N. (2022). A framework for assessing AI ethics with applications to cybersecurity. AI and Ethics, 1-8.
[2] Papp, D., Krausz, B., & Gyuranecz, F. (2022). The AI is now in session – The impact of digitalisation on courts. Cybersecurity and Law, 7(1), 272–296.
[3] S. Lee, (2021). AI-based Cybersecurity: Benefits and Limitations. Robotics & AI Ethics, 6(1), 18-28.
[4] Kim, J., & Park, N. (2020). Blockchain-based data-preserving ai learning environment model for ai cybersecurity systems in IoT service environments. Applied Sciences, 10(14), 4718.
[5] Mengidis, N., Tsikrika, T., Vrochidis, S., & Kompatsiaris, I. (2019). Blockchain and AI for the next generation energy grids: cybersecurity challenges and opportunities. Information & Security, 43(1), 21-33.
[6] Sharma, P., Dash, B., & Ansari, M. F. (2022). Anti-phishing techniques – a review of Cyber Defense Mechanisms. IJARCCE, 11(7). https://doi.org/10.17148/ijarcce.2022.11728
[7] Dymicka, A. (2022). Cybersecurity from the perspective of a new technology user. Cybersecurity and Law, 7(1), 27–36. https://doi.org/10.35467/cal/151810
[8] Tagarev, T., Stoianov, N., Sharkov, G., & Yanakiev, Y. (2021). AI-driven Cybersecurity Solutions, Cyber Ranges for Education & Training, and ICT Applications for Military Purposes. Information & Security, 50(1), 5-8. https://doi.org/10.11610/isij.5000.
[9] Senouci, S. M., Sedjelmaci, H., Liu, J., Rehmani, M. H., & Bou-Harb, E. (2020). Ai-driven cybersecurity threats to future networks [from the guest editors]. IEEE Vehicular Technology Magazine, 15(3), 5-6.
[10] Drewek-Ossowicka A., Pietrołaj M., Rumiński J. A survey of neural networks usage for intrusion detection systems. Journal of Ambient Intelligence and Humanized Computing. 2020 May 12;12(1):497–514.
[11] Laghrissi F., Douzi S., Douzi K., Hssina B. IDS-attention: an efficient algorithm for intrusion detection systems using attention mechanism. Journal of Big Data. 2021 Nov 29;8(1).
[12] Tsvilii, O. (2021). Cyber Security Regulation: Cyber Security Certification of Operational Technologies. Technology audit and production reserves, 1(2), 57.
[13] Internet crime compliance center data graph