International Journal of Multidisciplinary Research and Growth Evaluation.

AI-Driven cyber security: Security intelligence modelling

Guru Prasad BS [1*], Dr. Kiran GM [2], Dr. Dinesha HA [3]

[1] Student, Shridevi Institute of Engineering and Technology, Tumakuru, Karnataka, India

[2] Associate Professor, Department of CSE, Shridevi Institute of Engineering and Technology ,Tumakuru, Karnataka, India

[3] Professor, Dept. of CSE, Shridevi Institute of Engineering and Technology, Tumakuru, Karnataka, India

* Corresponding Author: **Guru Prasad BS**

Article Info

ISSN (online): 2582-7138
Volume: 04
Issue: 06
November-December 2023
Received: 05-10-2023;
Accepted: 07-11-2023
Page No: 961-965

Abstract

The process of defending computer networks from cyber-attacks or unintended, unauthorized access is known as cyber security. Organizations, businesses, and governments need cyber security solutions because cyber criminals pose a threat to everyone. Artificial intelligence promises to be a great solution for this. Security experts are better able to defend vulnerable networks and data from cyber attackers by combining the strengths of artificial intelligence and cyber security. This paper provides an introduction to the use of artificial intelligence in cyber security. AI-driven cyber security refers to the use of artificial intelligence and machine learning technologies to enhance the protection of computer systems and networks from cyber threats such as hacking, malware, phishing, and other forms of cyberattacks. AI-powered security solutions are designed to automate the process of detecting, analyzing, and responding to security incidents in real-time, thereby improving the efficiency and effectiveness of cyber defense. These solutions can analyze large amounts of data, identify patterns and anomalies, and make decisions faster and more accurately than humans alone, enabling organizations to stay ahead of evolving cyber threats.

DOI: https://doi.org/10.54660/.IJMRGE.2023.4.6.961-965

Keywords: Cyber security, cyber-attacks, artificial intelligence

Introduction

Cybercriminals pose a significant threat to the online world, and it is essential to take necessary precautions to protect sensitive information. It is crucial for organizations, businesses, governments, and individuals to understand the risks associated with online activities and to implement measures to reduce these risks. This includes using strong passwords, regularly updating software and hardware, keeping software up-to-date, and backing up important data. Additionally, it is recommended to educate employees and family members about safe online practices and to be aware of common scams and phishing attempts. By being proactive in protecting personal and sensitive information, the risk of cyber-attacks can be minimized and individuals and organizations can secure their online presence. Cyber security refers to technology and practices designed to protect networks and information from damage or unauthorized access [5]. It is vital because governments, companies, and military organizations collect, process, and store a lot of data. Cyber security takes different forms, including military, law enforcement, judicial, commerce, infrastructure, and interior, intelligence, and information systems. Cyber security is a dynamic, interdisciplinary field involving information systems, computer science, and criminology. The security objectives have been availability, authentication, confidentiality, no-repudiation, and integrity [7].

The management of organizations should adopt a holistic approach to cyber security that covers people, processes, and technology. This includes regular security training for employees, risk assessments, and incident response planning. The use of encryption and multi-factor authentication can also help to secure sensitive information. In conclusion, managing cyber risks requires a comprehensive and proactive approach that involves the entire organization [8].

By adopting best practices and staying informed about the latest threats and trends, organizations can reduce the risk of cyber-attacks and ensure the safety of their data and systems.

Challenges

Although artificial intelligence tools could help fight cybercrime, the tools are not a silver bullet and could be exploited by malicious hackers. There are limitations that prevent AI from becoming a mainstream tool. The downsides of AI in cyber security include cost, intensive resources, and training. AI in cyber security necessitates more resources and funds than traditional, non-AI cyber security solutions, and it may be impractical in some cases. Cyber security is a domain where absolute security is impossible. If a machine learning-based security tool misses a particular kind of cyber-attack because it is not coded into it that may lead to problems [4]. Hackers themselves can use AI to test and develop their malware and make it potentially AI-proof. Some critics have warned that AI could make cyber-attacks more dangerous and difficult to spot than ever before [1]. Some regard AI in cyber security as posing both a blessing and a curse, although the good outweighs the bad. Just as AI technologies can be used to identify and stop cyber-attacks, cybercriminals can also use the AI systems to launch attacks. Besides, a shortage of cyber security experts is another problem. These challenges prevent AI from becoming the only cyber security solution.

AI for Cyber Security

The study concludes by emphasizing the importance of XAI in improving the transparency and accountability of AI models in the field of cyber security, thereby enabling organizations to better understand and manage the risks associated with AI-based cyber security solutions [2]. The authors hope that the review will provide a valuable resource for researchers, practitioners, and stakeholders in the field of XAI and cyber security, and will encourage further research and development in this area [3].

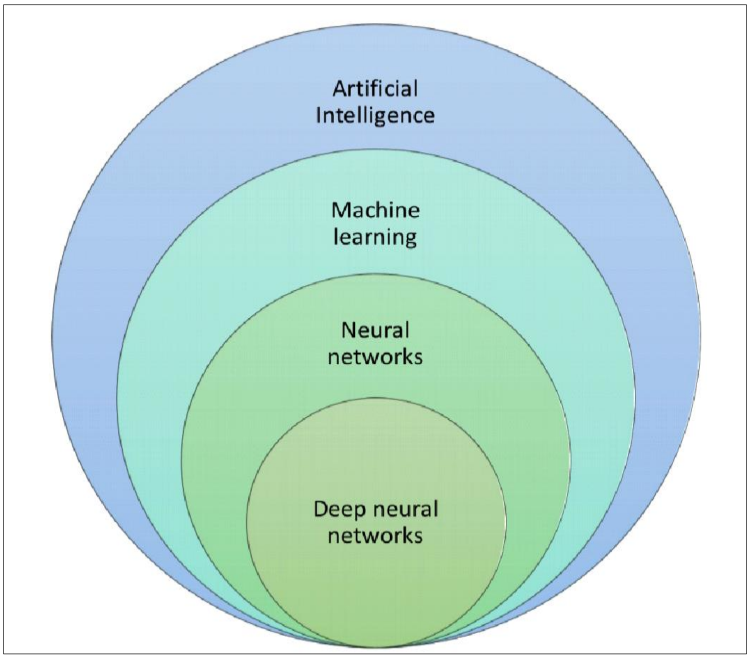

Fig 1: Relationship between AI and ML

AI limitations necessitate the use of XAI in cyber security

AI in cyber security has its own set of challenges and limitations. Evasion attacks are one of the major concerns where attackers can manipulate the malware in a way that it evades the AI-based detection framework. This highlights the need for continuous improvement and adaptation of AI models to stay ahead of attackers and provide effective cyber security solutions [10].

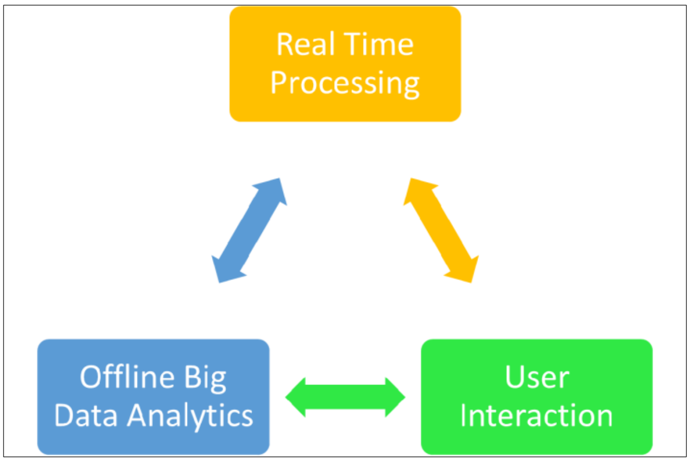

Fig 2: AI cyber incidents detection and response

AI-driven cyber security refers to the use of artificial intelligence and machine learning technologies to enhance the protection of computer systems and networks from cyber threats such as hacking, malware, phishing, and other forms of cyberattacks. AI-powered security solutions are designed to automate the process of detecting, analyzing, and responding to security incidents in real-time, thereby improving the efficiency and effectiveness of cyber defense. These solutions can analyze large amounts of data, identify patterns and anomalies, and make decisions faster and more accurately than humans alone, enabling organizations to stay ahead of evolving cyber threats [3].

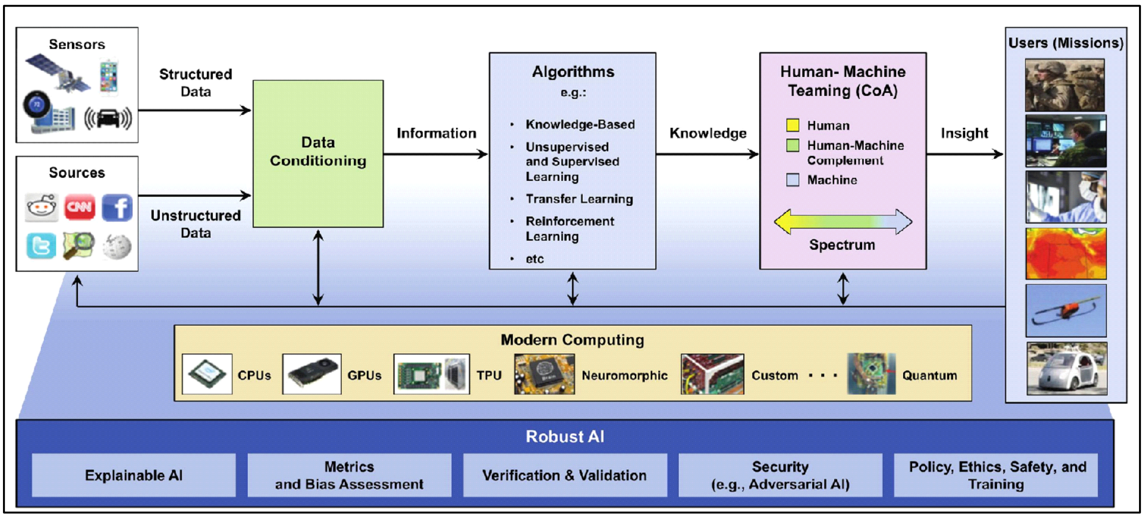

Fig 3: Schematic representation of the AI architecture and its attack surface

AI Cyber security Solutions

As cyberattacks grow in volume and complexity, artificial intelligence (AI) is helping under-resourced security operations analysts stay ahead of threats. Curating threat intelligence from millions of research papers, blogs and news stories, AI technologies like machine learning and natural language processing provide rapid insights to cut through the noise of daily alerts, drastically reducing response times. Watch the video to see how AI helps analysts connect the dots between threats [6].

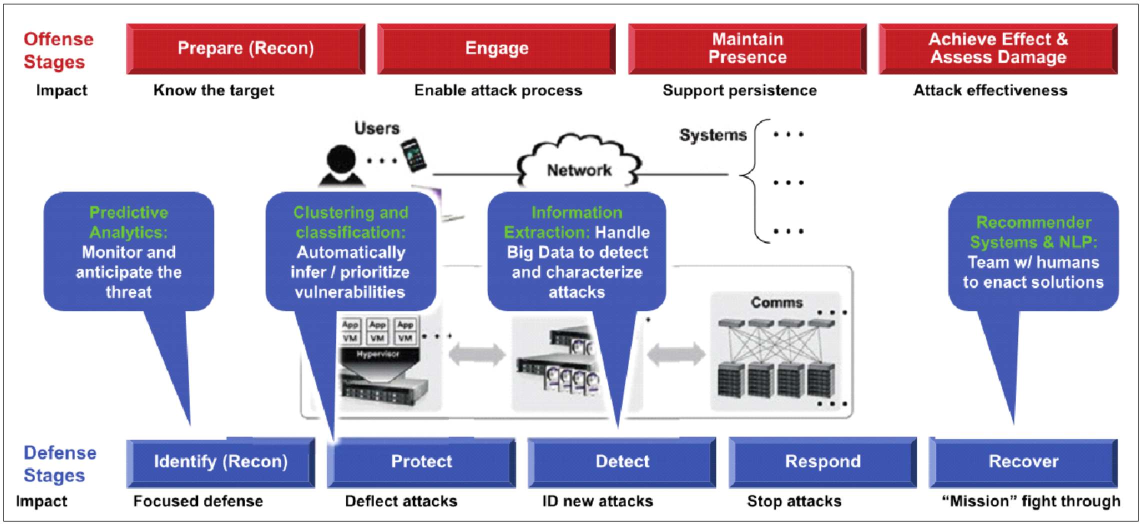

Fig 4: Application of AI across the cyber kill chain

Enabling AI-powered Smarter Cyber security Solutions Service offerings for Enabling AI-driven Cyber Security for Security Intelligence, Operations and Analytics, Malware Detection and Vulnerability management Solutions.

Table 1: Results of website legitimacy decision – Database 1

Decision	Database 1		
	Phishing	Non-phishing	Suspicious
Phishing	567	256	212
Non-Phishing	284	159	369
Suspicious	216	241	152

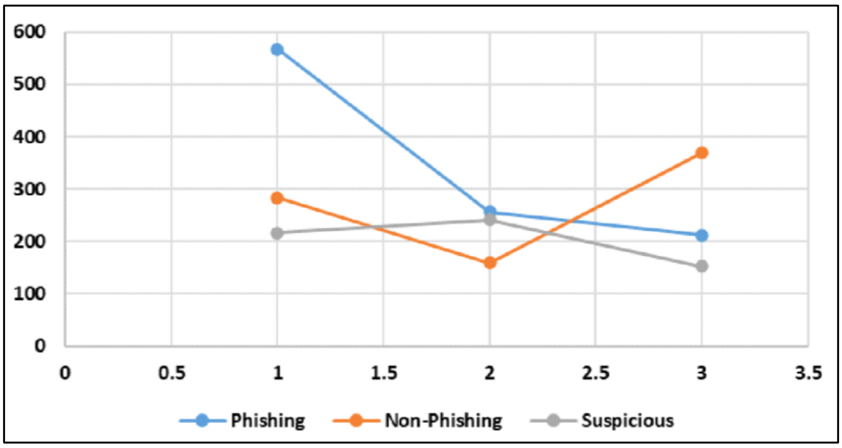

Fig 5: Website legitimacy decision-database 1

Table 2: Results of website legitimacy decision – Database 2

Decision	**Database 2**		
	Phishing	**Non-phishing**	**Suspicious**
Phishing	201	135	189
Non-Phishing	125	125	152
Suspicious	157	141	128

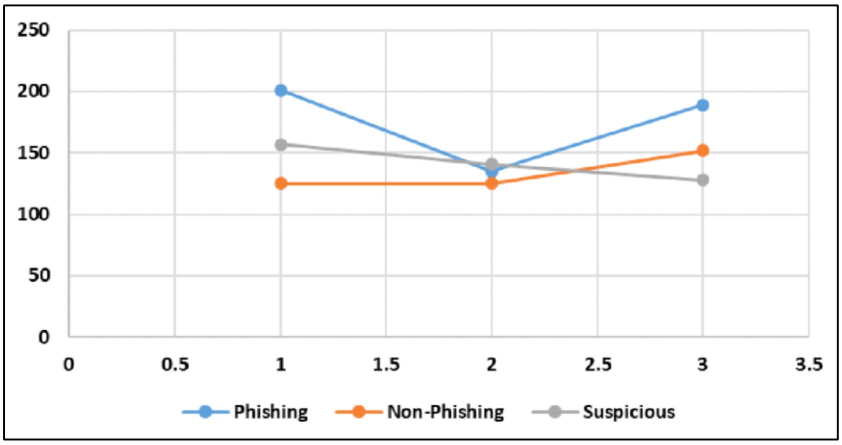

Fig 6: Website legitimacy decision-database 2

Conclusion

AI can detect and stop cyber threats in real-time with limited resources. The constantly evolving nature of cyber-attacks means that humans shall struggle to keep up with the intel. However, using machine learning, AI can chomp down data for quick analysis and provide excellent security coverage without taking much time or energy away from the existing tasks. Machine learning allows Human analysts to focus on interpreting the results from deep analysis and devising novel techniques for fighting cyber-crime.

References

1. Al-Yaseen W, Othman Z, Ahmad Nazri MZ. Multi-level hybrid support vector machine and extreme learning machine based on modified k-means for intrusion detection system. Expert Systems with Applications. 2017;67:1-10.
2. Banu R, MA, CA, SA, Ujwala H, NH. Detecting phishing attacks using natural language processing and machine learning. International Conference on Intelligent Computing and Control Systems; c2019. p. 1210-1214.
3. Baptista I, Shiaeles S, Kolokotronis N. A novel malware detection system based on machine learning and binary visualization; c2019. p. 1-6. Available from: https://doi.org/10.1109/ICCW.2019.8757060
4. Barbara D, Couto J, Jajodia S, Popyack L, Wu N. Adam: Detecting intrusions by data mining; c2001 .p. 5-6.
5. Bose S, Barao T, Liu X. Explaining AI for malware detection: Analysis of mechanisms of MalConv. In: 2020 International Joint Conference on Neural Networks (IJCNN); c2020 .p. 1-8.
6. Chowdhury M, Rahman A, Islam MR. Malware analysis and detection using data mining and machine learning classification; c2018. p. 266-274. Available from: https://doi.org/10.1007/978-3-319-67071-3_33
7. Coull SE, Gardner C. Activation analysis of a byte-based deep neural network for malware classification. In2019 IEEE Security and Privacy Workshops (SPW) IEEE; c2019. p. 21-27. Available from: https://doi.org/10.1109/SPW.2019.00017
8. Demetrio L, Biggio B, Lagorio G, Roli F, Armando A. Explaining vulnerabilities of deep learning to adversarial malware binaries. arXiv preprint arXiv; c2019.
9. Feng F, Zhou Q, Shen Z, Xuhui Y, Lihong H, Wang J. The application of a novel neural network in the

detection of phishing websites. Journal of Ambient Intelligence and Humanized Computing; c2018.

10. Feng W, Sun J, Zhang L, Cao C, Yang Q. A support vector machine based naive Bayes algorithm for spam filtering. In2016 IEEE 35th International Performance Computing and Communications Conference (IPCCC). IEEE.; c2016. p. 1-8.