

NEW IDENTIFICATION OF SECURITY CYBER METHODS USING ARTIFICIAL INTELLIGENCE

¹G. Ravi Chandra ²Dr. A. Tirupataiah ³T Seshasai

¹M. Tech Scholar, Dept.of CSE, St. Ann's College of Engineering & Technology, Chirala.

²Associate Professor, Dept.of CSE, St. Ann's College of Engineering & Technology, Chirala.

³Assistant Professor, Dept.of CSE, St. Ann's College of Engineering & Technology, Chirala.

e-mail: atp.tiru@gmail.com

ABSTRACT: Without substantial automation, individuals cannot manage the complexity of operations and the scale of information to be utilized to secure cyberspace. Artificial intelligence (AI) is a powerful technology that helps cyber security teams automate repetitive tasks, accelerate threat detection and response, and improve the accuracy of their actions to strengthen the security posture against various security issues and cyber-attacks. Machine learning is a powerful tool for investigating complex financial security threats that constantly evolve and can be difficult to predict. The findings contribute to a deeper understanding of AI's capabilities and limitations, providing insights that can guide the development and deployment of AI driven security systems. The surging menace of cyber-attacks got a jolt from the recent advancements in Artificial Intelligence. AI is being applied in almost every field of different sciences and engineering. The intervention of AI not only automates a particular task but also improves efficiency by many folds. Cybercriminals may now reach their targets from anywhere in the globe and at any time. In strategic decision making, for example, comprehensive information is important, and logical decision assistance is one of the still unanswered cyber security issues. Machine learning algorithms are constantly being improved to identify anomalies in the data that might indicate a security threats. We look at real examples of AI success and consider ethics and teamwork with human experts. The findings show AI's promise in making cyber security stronger against changing cyber threats. Artificial intelligence is increasingly critical to information security since these technologies are capable of rapidly evaluating millions of data sets and identifying a broad range of cyber risks, ranging from malware attacks to suspicious behavior that may result in a phishing assault.

Index Terms: Artificial Intelligence, Intelligent Agents, Neural networks, Smart Cyber Security methods, Cyber-attacks, AI, Cyber threats, Vulnerability, Response, Detection.

1. INTRODUCTION

This is clear that only smart technologies can help defend against sophisticated cyber devices, with the sophistication of malware and cyber-arms increasing exponentially in the past two years. The following case of "On 15 January 2009, Conficker corrupted "Ultramar" the French Navy computer network [1]. Advisory organizations, such as the National Institute of Standards and Technologies (NIST) are also encouraging the use of more proactive and adaptive approaches by shifting towards real-time assessments, continuous monitoring and data-driven analysis to identify, protect against, detect, respond to, and catalogue cyber attacks to prevent future security incidents [2]. Financial statements can be used to indicate the performance of a company.

Investors, market analysts, and creditors exploit financial reports to investigate and assess the financial health and earnings potentials of a business [3]. National Institute of Standards and Technologies (NIST) are also encouraging the use of more proactive and adaptive approaches by shifting towards real-time assessments, continuous monitoring, and data-driven analysis to identify, protect against, detect, respond to, and catalogue cyber-attacks to prevent future security incidents [4]. Cyber-crime is a type of crime that uses digital media to commit fraud, steal data, or cause damage. Cyber-crime is an umbrella term that encompasses all forms of cyber-related crimes [5]. Even when the most robust preventive measures are in place, hackers will attempt to circumvent them. It is doubtful that cyber dangers will ever be fully eradicated since hackers are clever and persistent, always looking for new methods to penetrate a company's defenses [6]. This presents a new issue for businesses whose information systems are mostly accessible by humans rather than other machines. It took years and a slew of high-profile cyber attacks, government laws, and fines for businesses to develop effective information technology security defenses [7].



Figure 1. AI in Cyber Security

2. RELATED WORKS

The search results which we got were limited only to the papers published in the last four years, as the determination of this paper is to bring out the newest trends of AI in cyber security. Last, the findings were categorized by the number of certifications [8]. A well-known cyber security framework proposed by NIST was used to understand the solution categories needed to protect, detect, react and defend against cyber attacks [9]. The NIST cyber security framework's core describes the practices to improve the cyber security of any organization [10]. Prior research in the fields of accounting and information systems has shed some light on the significant effects of financial reporting fraud on multiple levels of the economy. AI-based cyber security tools have emerged to help security teams efficiently mitigate risks and improve security. Given the heterogeneity of AI and cyber security, a uniformly accepted and consolidated taxonomy is needed to examine the literature on applying AI for cyber security [11]. Cyber security is a broad term encompassing all measures taken in an effort to safeguard an entity from cyber threats,

including securing data and mitigating damage from a cyber security incident [12]. The cyber security landscape should include measures to protect the organization from crypto-jacking, data leaks, data phishing, and Internet of Things threats (IoT). One should use experienced IT professionals and ethical hackers to guarantee that your AI security solution is impenetrable [12]. One of the main game changers in the area of cyber security is the development of tools and methods that are supplemented as a sub-group by artificial intelligence (AI) [13]. Artificial Intelligence (AI) is no longer simply a trendy term; it is now being utilized widely across a wide range of sectors.

3. SYSTEM MODELS

As an area of study journal, artificial intelligence (AI) is about as ancient as computer systems . From the yesteryears of AI, it was "on the horizon" that devices/software/structures could be built cleverer than humans [13]. The functions provide a comprehensive view of the lifecycle for managing cyber security over time. The solution categories listed under each function offer a good starting point to identify the AI use cases to improve the cyber security [14]. The proposed botnet detection model based on machine learning using DNS query data. The model is built on the analysis that Threats of CS Threats routinely send lookup queries to the DNS system to find IP addresses of servers using automatically generated domain names [15]. In practical terms, AI refers to a number of different technologies and ap- plications that are used in a variety of ways. There are many tools that can be used to launch a DDoS attack, and the most common is the use of a botnet. The attacker does not need to control the botnet, as they may simply rent it from an online service or purchase [16].

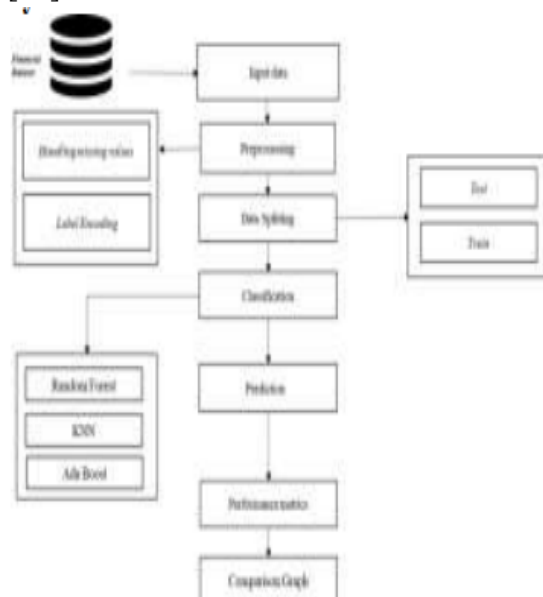


Figure 2. System Architecture

4. PROPOSED SYSTEM

In our proposed system, we detect the fraud in financial statements by using the machine learning algorithm. We select and view the imported dataset for future purpose and we get missing values and fill the default values to the dataset. We encode the label in the dataset. And we split the

dataset to the Train and Test data for predict the fraud or non-fraud [17]. There are Random forest algorithm, KNN classifiers and Ada-Boost Algorithm. Now, we fit the training data from the dataset.

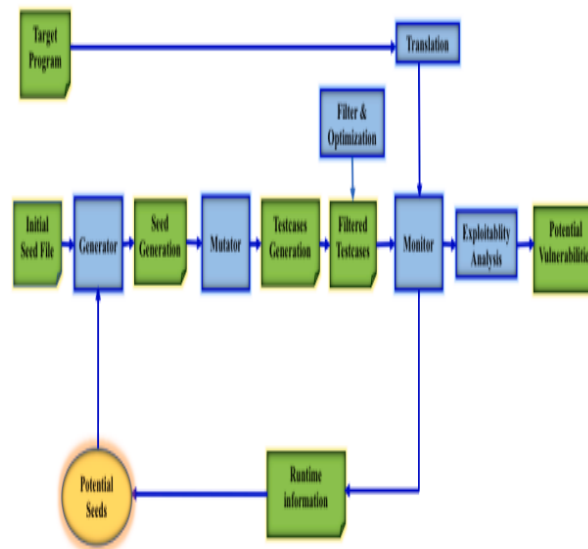


Figure 3. Smart fuzzing process for vulnerability detection.

5. ADABOOST ALGORITHM

Adaboost is one of the earliest implementations of the boosting algorithm. It forms the base of other boosting algorithms, like gradient boosting and xgboost [18]. We first build a weak model and then build a second model based on the errors from the first model. This process is repeated over and over again until we build a classifier that can make predictions accurately and the error is mini missed [19].

Algorithm behind Adaboost It works in the following

Steps: 1. Initially Adaboost selects a training subset randomly

Step: 2. it iteratively trains the AdaBoost machine learning model by selecting the training set based on the accurate prediction of the last training

Step: 3. it assigns the higher weight to wrong classified observations so that in the next iteration these observations will get the high probability for classification

Step: 4. Also, It assigns the weight to the trained classifier in each iteration according to the accuracy of the classifier. The more accurate classifier will get high weight

Step: 5. This process iterates until the complete training data fits without any error or until reached to the specified maximum number of estimators

Cyber Security

Cyber security is the practice of protecting critical systems and sensitive information from digital attacks. There are many ways to safeguard data and organizational infrastructure, including intrusion detection, malware protection strict adherence to sound security practices [20]. A cyber security threat can be a cyber-attack using malware to gain access to data, disrupt digital operations, or damage information

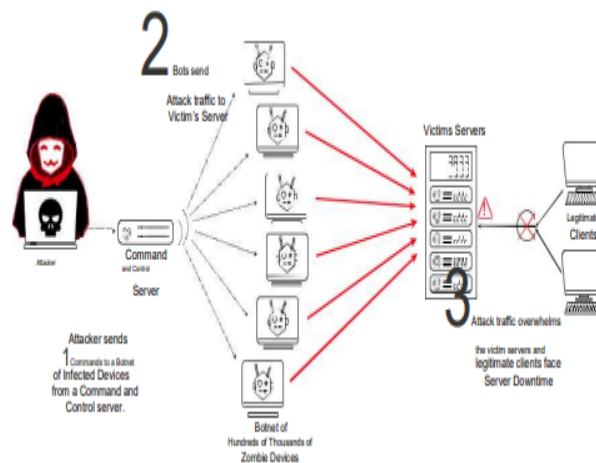


Figure.4. Distributed Denial of Services Attack scenario.

6. INTERVENTION OF AI

The use of AI in cyber-attacks is a new and emerging trend. It is not yet clear how this will affect the future of cybercrime. There are several different AI and machine learning techniques used in cyber security. The most common ones include strategies that use AI to identify and monitor malicious activities, detect cyber threats, and protect an organization's networks [21].

Recent Trends

Along with this trend, cyber security is also increasingly adopting cognitive technologies. AI-powered cognitive technologies are an essential part of a holistic approach to cyber security in which the human element guides the process and plays a pivotal role. In general, cyber defense is a constantly shifting space where the nature of security threats changes with each new development. Cyber security professionals who can adopt successful cognitive technologies and guide their human element on a holistic approach will be more successful in defending against cyber-attacks [22].

AI based mitigation of Cyber threats

Malware detection and identification: Artificial intelligence being used for malware detection and identification is still in its infancy, but it has the potential to revolutionize the way we deal with cyber crime. AI can help identify malicious files before they reach the end-user and, by doing so, can provide significant security benefits. Many different AI/ML approaches have been used to detect malware, some more successful than others [23].

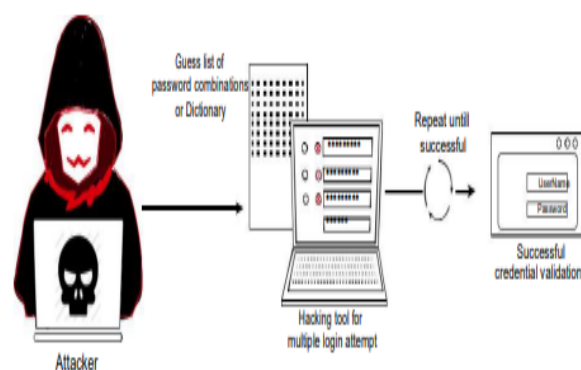


Figure.5. Depiction of generalized principle of a Password Attack

7. PERFORMANCE METRICS

The Final Result will get generated based on the overall classification and prediction. The performance of this proposed approach is evaluated using some measures like, Accuracy: Accuracy of classifier refers to the ability of classifier. It predicts the class label correctly and the accuracy of the predictor refers to how well a given predictor can guess the value of predicted attribute for a new data. Even though the organization's information is essential to any organization, the cost of implementing AI technology is much higher, limiting the number of individuals who will use the technology for the safety of their data and information.

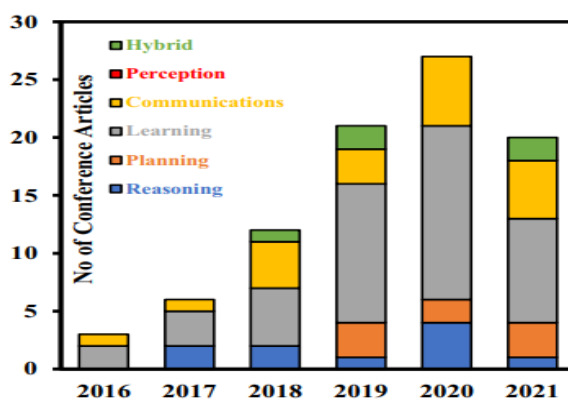


Figure.6. Distribution of use of AI domain during

8. CONCLUSIONS AND FUTURE OPPORTUNITIES

In a scenario where malicious intelligence and cyber threats are rising exponentially, sophisticated cyber security strategies cannot be ignored. Also security against large-scale threats, with very minimal resources, has been demonstrated from experience in DDoS prevention if smart approaches are used. The evolution of AI in cyber security was studied with respect to different functions, solution categories, specific use cases, and the type of AI technique used. The results of the analysis revealed that the number of publications is increasing, but more attention must be paid to the acquisition and representation of historical data related to different cyber security functions to implement practical AI-based cyber security solutions. The Classifications classifier gives high accuracy results that are comparable or superior to other fraud detection techniques in spite of working with reduced data and also compared with graph. Research shows that artificial intelligence has seemingly positively affected cyber security and risks. Hence the continuation of AI and machine learning will take the cyber security field to a new level of

intelligence. In future, discovery of additional information based on cause-event Fraud detection well as prediction of detection based on cause events, etc. The working of the proposed approach in a web application

9. REFERENCES

- [1] Bhardwaj, M.D. Alshehri, K. Kaushik, H.J. Alyamani, M. Kumar, Secure framework against cyber-attacks on cyber-physical robotic systems, *J. Electron. Imaging* 31 (6) (2022), 061802-061802.
- [2] P. Chithaluru, A.T. Fadi, M. Kumar, T. Stephan, Computational intelligence inspired adaptive opportunistic clustering approach for industrial IoT networks, *IEEE Internet Things J* (2023), <https://doi.org/10.1109/JIOT.2022.3231605>.
- [3] M. Barrett, Technical Report, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2018.
- [4] I. Wiafe, F.N. Koranteng, E.N. Obeng, N. Assyne, A. Wiafe, S.R. Gulliver, Artificial intelligence for cybersecurity: a systematic mapping of literature, *IEEE Access* 8 (2020) 146598–146612.
- [5] Z. Zhang, H. Ning, F. Shi, F. Farha, Y. Xu, J. Xu, F. Zhang, K.K.R. Choo, Artificial intelligence in cyber security: research advances, challenges, and opportunities, *Artif. Intell. Rev.* 55 (2022) 1029–1053.
- [6] Dr. Ratna Raju Mukiri, Dr. Prasuna Grandhi, Dr. Hari Kishan Chapala, “NEW SECURITY MODELS IN CLOUD IOT SYSTEM USING HASH MACHINE LEARNING,” *Industrial Engineering Journal* ISSN: 0970-2555 Volume : 52, Issue 8, August : 2023.
- [7] T.C. Truong, I. Zelinka, J. Plucar, M. Candík, ˇ V. Sulc, ˇ Artificial intelligence and cybersecurity: past, presence, and future, in: *Artificial intelligence and evolutionary computations in engineering systems*, 2020, pp. 351–363.
- [8] S. Samoli, M.L. Cobo, E. Gomez, G. De Prato, F. Martinez-Plumed, B. Delipetrev, A.I. Watch, Technical report, Joint Research Center (Seville site), 2020.
- [9] High-Level Expert Group on Artificial Intelligence. (HLEG AI), A definition of AI: main capabilities and disciplines, (2019). Retrieved from Brussels https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=56341.
- [10] D. Zhao, A. Strotmann, Analysis and visualization of citation networks, *Synthesis lectures on information concepts, retrieval, and services*, 7 1 (2015) 1–207.
- [11] M. Zajko, "Canada's cyber security and the changing threat landscape", *Critical Studies on Security*, vol. 3, no. 2, pp. 147-161, 2015.
- [12] R. Winkels, Eleventh International Conference on Artificial Intelligence and Law: proceedings: June 4-8, 2007, Stanford Law School, Stanford, California. Place of publication not identified: ACM, 2007.
- [13] H. Bidgoli, *Handbook of information security*. Hoboken, NJ: John Wiley, 2006.
- [14] H. Zhuge, "Semantic linking through spaces for cyber-physical-socio intelligence: A methodology", *Artificial Intelligence*, vol. 175, no. 5- 6, pp. 988-1019, 2011.
- [15] C. Blackwell and H. Zhu, *Cyberpatterns: Unifying Design Patterns with Security and Attack Patterns*, 2nd ed. Cham : Springer International Publishing, 2014.
- [16] A. R. Dengel, K. Berns, T. M. Breuel, F. Bomarius, and T. R. RothBerghofer, *KI* 2008:

advances in artificial intelligence 31st Annual

- [17] D. Feng, D. Lin, and M. Yung, Information Security and Cryptology First SKLOIS Conference, CISC 2005, Beijing, China, December 15- 17, 2005, Proceedings. Berlin: Springer, 2005.
- [18] J. G. Siegel, The artificial intelligence handbook: business applications in accounting, banking, finance, management, marketing. Mason, OH: Thomson/South-Western, 2003.
- [19] H. Zhuge, "Semantic linking through spaces for cyber-physical-socio intelligence: A methodology," Artificial Intelligence, vol. 175, no. 5- 6, pp. 988–1019, 2011.
- [20] J. R. Vacca, Computer and information security handbook. Waltham, MA, USA: Morgan Kaufmann Publishers, 2013
- [21] Rajani, P., Adike, S., & Abhishek, S. G. K. (2020). ARTIFICIAL INTELLIGENCE : THE NEW AGE. 8(2), 1398–1403.
- [22] Rosenblatt, F. (1957). The Perceptron - A Perceiving and Recognizing Automaton. In Report 85, Cornell Aeronautical Laboratory (pp. 460–461).
- [23] Sadiku, M. N. O., Fagbohunge, O. I., & Musa, S. M. (2020). Artificial Intelligence in Cyber Security. International Journal of Engineering Research and Advanced Technology,
- [24] Shankarapani, M. K., Ramamoorthy, S., Movva, R. S., & Mukkamala, S. (2011). Malware detection using assembly and API call sequences. Journal in Computer Virology, 7(2), 107– 119.
- [25] Tyugu, E. (2011). Artificial intelligence in cyber defense. 2011 3rd International Conference on Cyber Conflict, ICC3 2011 - Proceedings, 95–105.