WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Evaluating the Effectiveness of AI-Driven Frameworks in Predicting and Preventing Cyber Attacks

Karthik Meduri [a], Hari Gonaygunta [b], Geeta Sandeep Nadella [c]

[a,b,c] University of the Cumberlands, KY, USA
DOI: https://doi.org/10.55248/gengpi.5.0324.0875

A B S T R A C T

With the escalating use of technology and major computer systems, cyberattack threats loom larger than ever. These attacks, categorized as any malicious attempt to gain unauthorized access to a computer system or network that intends to cause damage, necessitate the development of new security approaches. AI has emerged as a practical solution, enabling early identification and mitigation of various attack vectors. This research delves into AI frameworks for predicting and preventing cyberattacks in diverse organizational contexts. The data collected from qualitative sources, including secondary data and literature, as well as primary sources like case studies, was analyzed using content analysis. The evaluation criteria focused on the framework's applicability in different environmental settings. The key AI frameworks considered are spam detection, fraud detection, breach risk prediction, and behavioral analysis. These frameworks have proven instrumental in enhancing cybersecurity and ensuring operational effectiveness. The research underscores the importance of organizations fully automating AI processes to bolster security.

Keywords: AI-driven cybersecurity, AI Frameworks, Cyberattack Prediction, Fraud Detection, Cyberattack prevention, machine learning

1. Introduction

In a business context or any environmental setting today, it is notable that different technologies are being implemented to ensure the organization can meet its operational demands. As companies are known for focusing on the implementation and the use of technology to meet different business needs, it is notable that these increase the chances and risk of being attacked and hacked by other attackers and hackers (Kaushik & Dahiya, 2022). A cyber-attack is categorized as any malicious attempt to gain unauthorized access to any given computer system or computer network with the intent of causing any damage. These attacks aim to disable, destroy, disrupt, and control computer systems or alter, block, manipulate, delete, or steal data within the compromised systems (Kaur et al., 2023).

For any organization to operate effectively, it is notable that using different AI frameworks can be vital for helping predict and prevent cyberattacks. Artificial Intelligence (AI) simulates human intelligence processes through machines such as computer science (Basit et al., 2021). Some of the significant applications of AI include natural language processing, expert systems, machine vision, and speech recognition. Hence, these approaches are essential as they can be vital in predicting, understanding, and preventing cyberattacks in any given environmental setting (Zeadally et al., 2020). These approaches are necessary for understanding the different threats that can lead to cyberattacks and vulnerabilities and mitigating them to operate computer systems effectively.

1.1 Aims and Scope of the Paper

Cyberattacks are categorized to be expected in the current organizational setting for different reasons. Some of the significant reasons why cyberattacks are common include improper securing of computer systems, increased use of computer systems and other major technologies in the organization, and lack of appropriate measures to identify and mitigate the different threats and vulnerabilities in the computer systems and other machines (Zhu et al., 2021). Hence, the main objective of the paper includes:

- To understand the different AI frameworks that can be used to predict and prevent cyberattacks.
- To recommend the best AI framework and how it can be implemented in an organization to predict and prevent cyberattacks.

2. Literature Review

Cyberattacks are becoming increasingly common in today's business world. According to the Cisco Annual Cybersecurity Report, some companies have been hacked, while others are unaware that they have been hacked. Between 2016 and 2017, cyberattacks significantly increased (Kaushik & Dahiya,

2022). Cybercriminals and cybercrimes have grown as people and businesses take advantage of the various vulnerable systems. Attackers often seek to extort money by hacking and attacking business systems. Additionally, attackers may aim to destroy systems and data within an organization as a form of hacktivism.

Different AI approaches have been developed and applied to mitigate various cyberattack issues. These systems analyze large amounts of data to identify and detect risks like malware and phishing attacks. Cybercriminals modify and change malware code to evade detection, but AI is ideal for anti-malware protection. AI uses data from previously detected malware to detect new variants (Al-Hashedi & Magalingam, 2021). Some AI frameworks for predicting and preventing malware include spam filtering, bot identification, behavioral analysis, breach risk prediction, and fraud detection.

3. Methodology

3.1 Framework Selection

Different frameworks have been mentioned as crucial and are used to predict and prevent cyberattacks. Some significant frameworks include breach risk prediction, phishing detection, user authentication, spam filtering, bot identification, behavioral analysis, fraud detection, and threat intelligence. These frameworks have been selected according to their importance and application in different organizational settings to provide the required cybersecurity and demanded security (Kaushik & Dahiya, 2022). Hence, their importance and usage in various corporate settings are essential for predicting and preventing cyberattacks.

AI frameworks and technologies predict and prevent cyberattacks in different organizations. These frameworks leverage machine learning, deep learning, and other AI techniques to analyze vast amounts of data and identify potential threats (Truong et al., 2020). When implementing AI frameworks for cybersecurity, it is essential to consider the specific needs and characteristics of the organization. Continuous monitoring, updating models, and adapting to new threats are crucial for an effective cybersecurity strategy.

3.2 Data Collection

There are various sources and data types to construct such an understanding of the different frameworks and how they can be used in any organizational setting. The research highlights that the data were captured from various secondary sources, such as archival material and other vital information retrieved from literature. The secondary data sources cite the standard information typically collected by one person outside the primary source party occupant as users on a particular dataset (Rao et al., 2021). Some of the sources that are generally familiar with this data also come from the information obtained by various Departments concerned and a second sample collected for other research.

It also includes the case studies among the primary data sources essential for the research. Here, we mean a deep dive into a subject, for example, the detailed analysis of how an AI framework operates in that specific environment. However, this critical approach gives a clear understanding of how any AI framework is necessary for use in the atmosphere to fulfill the need by satisfying predicting and avoiding cyberattacks, particular or comprehensive (Alowaidi et al., 2023). Case studies are important data sources in this research because they allow a vivid understanding of nature and how these frameworks have been used to respond by predicting and preventing different forms.

3.3 AI Models and Techniques

Various AI techniques and many methods can be applied to comprehend the workings of these frameworks and their applicability in a specific environment. In this case, the primary process used is the content analysis. This is a very relevant method, which has the purpose of helping to evaluate and understand different concepts and bits of information found in specific sources. Emphasizing the other use cases, it becomes evident that content analysis plays a significant role in extracting relevant information and understanding various AI frameworks (Rao et al., 2021). Primary uses of the content analysis that could help quantify and analyze the presence, relationship, and meanings of these different frameworks, together with how each organization is used, were facilitated. The method was significantly instrumental in understanding how the working accuracy operates among other frameworks, which could also be applied for cyberattack prediction and prevention in any surrounding environment.

However, content analysis is critical because it has frequently revealed many diverse aspects concerning the frameworks and their variants in applied situations (John et al., 2023). Evaluation is done to show an accurate conception of how the framework could be used in a specified position and accommodate different requirements associated with cyberattack prediction and prevention. Implementing the method demonstrates how the framework can be used, what points are crucial for using protection systems to provide security, and that it is possible to use adaptable tools appropriately when identifying or mitigating cyber threats at different locations. It is also straightforward to understand all the necessary frameworks using this approach (Floridi et al., 2018).

3.4 Evaluation Criteria

The parameters of evaluation for the various frameworks concentrated on the use of the framework and ways in which they could be utilized under different environmental settings. These aspects are critical because they ensure that the structures can serve the need to predict and prevent cyberattacks in various settings. Such measures are very important because they provide that the models can be utilized effectively when and where it is necessary, as

stated by Alowaidi et al. (2023), to satisfy specific purposes and needs for enabling cybersecurity. This evaluation also used the negative impacts of these frameworks as an indication to get a clear image of how the phenomenon can be utilized. These criteria determined them essential in ensuring sustainability so that all framework elements were available. It then becomes straightforward to comprehend the use and application of any AI framework in a given environmental scenario that will help combat cyberattacks by providing users with detailed information on how the technology functions (Kaloudi & Li, 2021).

4. Results and Discussions

4.1 Analysis of AI-driven Frameworks

However, the most essential method used in AI for predicting and averting cyberattacks depends on breach risk prediction. It is classified as a method to account for an organization's multiple IT asset inventories, threat exposure levels, and control effectiveness of the different control approaches (Zhu et al., 2021). Based on their fundamental strategies about how and where the various IT components will likely be breached, AI-based systems can predict which inputs and allocation of resources they need in an organization. Descriptive insights are necessary to improve the configurational aspects and improve the controls and processes in the organization. Lastly, spam filtering must be addressed as an essential tool for foreseeing and preventing cyberattacks (Nallamothu & Khan, 2023). The program is necessary to identify unwanted, virus-infected emails that can keep the mains off limits in any organization. Using Bayesian and heuristic filters is essential, as they help detect suspicious spam messages because of their observation approach towards multiple suspect information.

However, fraud detection is another crucial approach that has always been identified as playing a vital role in predicting and preventing cyberattacks by trying to avoid attacks from cancer. This is regarded as a method based on observing various transactions and customer behaviors to detect fraudulent activities. It is an inevitable approach that should be used as a preventive measure in the organization. It assists in understanding the various aspects of machine learning used for identifying transactions and determining if they are reliable or fraudulent (Alowaidi et al., 2023). Finally, behavioral analysis is also an essential method by which AI predicts and prevents a few cyberattacks in any organization. It operates by adopting big data analytics and AI on user behavioral data in an organization to detect many patterns, trends, and anomaly-labeled vulnerabilities. It is also mandatory because it helps in understanding various behaviors that are found within the organization and detecting any abnormalities that may result in cyber-attacks.

4.2 Comparative Evaluation

The types of AI frameworks, breach risk production, spam filtering, fraud detection, and behavioral analysis are paramount for predicting cyberattacks. Such frameworks are vital and serve a significant function in various contexts to find the multiple vulnerabilities and threats (Himeur et al., 2024). The risk in breach prediction is critical since it helps businesses develop and enhance the processes and controls that ensure acceptable requirements for cyber resilience. It relies on AI to predict the attack surface and what must be done to strengthen cyber security.

Spam filtering is a critical AI framework that plays a significant role in identifying various illegal, unnecessary, and virus-infected traffic to email and making sure such emails are secured from the reach of users about their presence at the Inbox level (Al-Hashedi& Magalingamp2021). A critical approach to using the Bayesian and heuristic filters is identifying all the vulnerabilities and risks in emails to prevent cyberattacks by diverting these attacks before they infect emails. SpamRip space further works by learning the users' preferences based on various spam-marked emails, according to Nallamothu and Khan (2023). That is an integral strategy to ensure that cyberattacks employ these measures, for instance, phishing attacks, so as not to get into the organization.

Fraud detection uses different approaches to identify fraudulent activities directed towards a given organization and transactions that can cause the system to be attacked. For instance, it uses statistical parameter calculations, regression analysis, probability distribution and models, and data matching techniques. These approaches are fundamental as they help understand and monitor the transactions according to the previous transactions to identify different fraudulent activities. Machine learning has been categorized as the most essential approach to detecting fraud and identifying fraudulent activities (Akinyelu, 2021). Behavioral analytics is known for working through the use of different AI and also big data analytics on the various user behavioral data for identifying the patterns and anomalies in the data. By identifying the other abnormalities, it is notable that behavioral analysis understands various aspects and anomalies noted in the data. It provides a clear understanding of cyberattack threats and vulnerabilities in the organization's computer system.

4.3 Case studies

Breach risk prediction is featured as one of the leading AI frameworks used in different organizations. Breach risk prediction is commonly used in an organization to identify the areas likely to be breached through human errors. Hence, it eliminates the chances of human errors being noted in the organizations. Spam filtering is known for ensuring that the emails in an organization cannot be compromised (Himeur et al., 2024). This is achieved through the user marking emails from a given sender as spam. Using Bayesian filters, it recognizes the patterns and automatically moves future emails from the particular sender to the spam folder. This is key for helping to predict and prevent cyberattacks. Fraud detection is commonly applied in organizations to check for fraudulent activities and ensure that the organization does not suffer from cyberattacks. Behavioral analysis has been used in organizations to achieve corporate hardware use (Al-Hashedi & Magalingam, 2021). This is achieved through tracking the behavioral analytics on how the employees use different company hardware such as printers and computers.

4.4 Interpretation of the Results

These results are crucial and provide a clear understanding of the different AI frameworks for predicting and preventing cyberattacks in organizations implementing other technologies. The result explains and applies different AI frameworks to provide cybersecurity in any organizational setting (Zhu et al., 2021). These frameworks are known for working through machine learning to understand what is happening and how organizations can get the best out of the framework. For instance, breach risk prediction is an important aspect that works through monitoring tools to ensure that it can understand the different areas where cyberattacks can occur in the organization (Zeadally et al., 2020). These frameworks apply different AI approaches such as pattern recognition, machine learning, data mining, and neural networks to ensure they can understand the data and predict anomalies in organizational activities and processes.

4.5 Implication of Cybersecurity

Different AI frameworks will be critical in the organization's cybersecurity posture. Significantly, it is noteworthy that it led to faster threat detection and response in organizations (Himeur et al., 2024). Leveraging the different AI frameworks will help better comprehend the network systems and identify potential threats faster. AI can automate the various security processes, making the organization stay on top of the cybersecurity needs much simpler and more manageable. AI frameworks are also important as they improve efficiency and accuracy in organizational cybersecurity approaches (Al-Hashedi & Magalingam, 2021). AI-based security systems are known for providing improved accuracy and efficiency compared to traditional solutions that can be implemented in any setting. For instance, spam filtering is critical for ensuring that only the required emails are accessed by users in the organization.

Additionally, the AI framework will be vital for greater scalability and cost savings in the organization. The frameworks are also known for handling massive amounts of data with high accuracy and speed, which enables them to note several threats and weaknesses in the organization (Zhu et al.,2021). This is a key due to the gaining of understanding that this hinders response time to numerous security breaches, and fewer costs are needed for defense after diverse cyber campaigns and menaces in an institution.

4.6 Limitation of AI in Cybersecurity

However, the challenge of bias and discrimination in decision-making is classified as a form of AI that bears risk for cybersecurity. These biases arise from a variety of sources, including the data sets. It is also essential to note that if biases are not controlled well in an organization, the behavior can prompt many discriminatory judgment calls on various persons and interfere with decisions within such a unit (Bao et al., 2022). The abuse of AI is also a possibility in the firm. AI algorithms can also be misused in a way that they are used by attackers for different reasons rather than improving the working of the organization. AI frameworks should not be considered and used in other settings as they can lead to various challenges. AI frameworks are also challenged to achieve explainability and transparency in organizations (Zhu et al., 2021). The different algorithms used in these frameworks to make decisions about the other security threats are not always transparent, making them more vulnerable to manipulation or potential bias in the results.

4.7 Recommendations for Future Research

With the need for improving and achieving cybersecurity approaches in any given organization, future research must focus on incorporating AI in the current working process of the organization from the start to the end to ensure that all the activities are automated (Al-Hashedi & Magalingam, 2021). This is key as it will help understand and reach a more automated environment that does not give any security challenges.

5. Conclusion

In conclusion, cybersecurity is one of the critical aspects that should be considered for any given organization to ensure that the organization can operate most effectively to meet the different demands of the consumers. AI frameworks are essential for ensuring that cybersecurity in the organization is achieved and that all the services can be accomplished without any vulnerabilities or threats. Artificial Intelligence (AI) simulates human intelligence processes through machines such as computer science. Using different approaches, such as natural language processing, machine vision, and expert systems, AI can predict and help prevent cyberattacks in organizations. It provides straightforward approaches that can be used, such as spam detection, fraud detection, breach risk prediction, and behavioral analysis, as major AI frameworks for understanding data in the organization and providing recommendations on how to secure systems in the organization.

With the different benefits noted with AI in various settings, it is notable that AI is the future of cybersecurity for any given organization that has implemented the use of other technologies and computer systems to meet the needs of the consumers. AI continues to provide solutions for predicting and preventing various cybersecurity threats and vulnerabilities that can disrupt the organization's regular operation. Hence, AI will be vital for improving and developing new frameworks to enhance cybersecurity and ensure that organizations can easily predict and prevent attacks that differ from their operations. For the future operation of the organization, it will be vital to focus on implementing different AI frameworks, such as spam detection and fraud detection, to ensure that the systems are protected and can be reliable for accomplishing diverse business needs. These frameworks are essential as they help comprehend and provide security to the required and sensitive data in the organization.

6. Illustrations

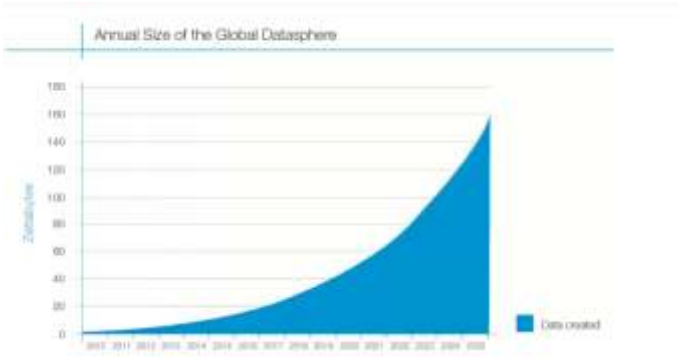

Fig 1: Data creation across different organizations.

References

Akinyelu, A. A. (2021). Advances in spam detection for email spam, web spam, Social Network Spam, and review spam: ML-based and nature-inspired-based techniques. Journal of Computer Security, 1–57. https://doi.org/10.3233/jcs-210022

Al-Hashedi, K. G., & Magalingam, P. (2021). Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019. Computer Science Review, 40, 100402. https://doi.org/10.1016/j.cosrev.2021.100402

Alowaidi, M., Sharma, S. K., AlEnizi, A., & Bhardwaj, S. (2023). Integrating Artificial Intelligence in cyber security for cyber-physical systems. Electronic Research Archive, 31(4), 1876–1896. https://doi.org/10.3934/era.2023097

Bao, Y., Hilary, G., & Ke, B. (2022). Artificial Intelligence and Fraud Detection. Innovative Technology at the Interface of Finance and Operations, pp. 223–247. https://doi.org/10.1007/978-3-030-75729-8_8

Basit, A., Zafar, M., Liu, X., Javed, A. R., Jalil, Z., & Kifayat, K. (2021). A comprehensive survey of AI-enabled phishing attack detection techniques. Telecommunication Systems, 76(1), 139–154. https://doi.org/10.1007/s11235-020-00733-2

Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P., & Vayena, E. (2018). AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations. Minds and Machines, 28(4), 689–707. https://doi.org/10.1007/s11023-018-9482-5

Himeur, Y., Sayed, A. N., Alsalemi, A., Bensaali, F., & Amira, A. (2024). Edge AI for the Internet of Energy: Challenges and perspectives. Internet of Things, 25, 101035. https://doi.org/10.1016/j.iot.2023.101035

John, M. M., Olsson, H. H., & Bosch, J. (2023). Towards an AI-driven business development framework: A multi-case study. Journal of Software : Evolution and Process, 35(6). https://doi.org/10.1002/smr.2432

Kaloudi, N., & Li, J. (2021). The AI-Based Cyber Threat Landscape: A Survey. ACM Computing Surveys, 53(1), 1–34. https://doi.org/10.1145/3372823

Kaushik, K., & Dahiya, S. (2022). An artificial intelligence-assisted defensive framework for Securing Cyberspace. Algorithms for Intelligent Systems, 323–333. https://doi.org/10.1007/978-981-19-1657-1_28

Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial Intelligence for cybersecurity: Literature review and future research directions. Information Fusion, 97, 101804. https://doi.org/10.1016/j.inffus.2023.101804

Rao, S., Verma, A. K., & Bhatia, T. (2021). A review on Social Spam Detection: Challenges, open issues, and future directions. Expert Systems with Applications, 186, 115742. https://doi.org/10.1016/j.eswa.2021.115742

Nallamothu, P. T., & Khan, M. S. (2023). Machine Learning for SPAM Detection. Asian Journal of Advances in Research, 6(1), 167–179. Retrieved from https://www.mbimph.com/index.php/AJOAIR/article/view/3417

Truong, T. C., Diep, Q. B., & Zelinka, I. (2020). Artificial Intelligence in the cyber domain: Offense and Defense. Symmetry, 12(3), 410. https://doi.org/10.3390/sym12030410

Zeadally, S., Adi, E., Baig, Z., & Khan, I. A. (2020). Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity. IEEE Access, p. 8, 23817–23837. https://doi.org/10.1109/ACCESS.2020.2968045

Zhu, X., Ao, X., Qin, Z., Chang, Y., Liu, Y., He, Q., & Li, J. (2021). Intelligent Financial Fraud Detection Practices in the Post-Pandemic Era. The Innovation, 2(4), 100176. https://doi.org/10.1016/j.xinn.2021.100176