E-ISSN: 2583-9667
Indexed Journal
Peer Reviewed Journal
https://multiresearchjournal.theviews.in

Received: 09-04-2024
Accepted: 20-06-2024

INTERNATIONAL JOURNAL OF ADVANCE RESEARCH IN MULTIDISCIPLINARY

Volume 2; Issue 3; 2024; Page No. 492-496

To identify the types of AI technologies being integrated into cyber security

[1]Siddharth, [2]Avinash Anand and [3]Pooja Upadhyay

[1, 2]M. Tech, Department of Computer Science, Mahakaushal University, Jabalpur, Madhya Pradesh, India
[2]Assistant Professor, Department of Computer Science, Mahakaushal University, Jabalpur, Madhya Pradesh, India

DOI: https://doi.org/10.5281/zenodo.15068997

Corresponding Author: Siddharth

Abstract

In light of the increasing cyber threats, this research seeks to examine how AI might improve cyber security systems by increasing the rates of threat detection and response. Data collected from cyber security specialists was analyzed using a quantitative technique. In order to gauge the efficacy of AI in preventing accidents, the difficulties encountered, and their actual use across different sectors, surveys are conducted. The results demonstrate that AI, like deep learning and machine learning, greatly enhances the capacity to identify and lessen the impact of possible dangers. it is now widely recognized that artificial intelligence (AI) technology may enhance cyber security measures by facilitating better detection and reaction to intrusions.

Keywords: Artificial intelligence, cyber security, threat detection, machine learning, data privacy

Introduction

In current age of cyberspace, artificial intelligence (AI) is a strong technology that greatly improves cyber security infrastructures' ability to identify threats and respond quickly. Artificial intelligence has changed cyberspace in a manner that has changed cyber security procedures. Thanks to AI, many leading companies can now spot risks with ease, allowing them to react quickly before they wreak havoc on the company. In the past, security systems that match incoming traffic to a database of known threats or malicious code signatures were used to stop threats. One example of this is signature-based detention systems. The system will immediately take action to block or isolate the danger when an alert is received, indicating a match. Even though it has been around for a while, this approach of threat management just can't keep up with the more sophisticated ways that threats are being detected.

The use of cutting-edge technologies to combat cyberattacks has been spurred by this development. The ability to quickly sift through massive amounts of data in search of patterns and abnormalities gives artificial intelligence a leg up when compared to more conventional forms of cyber defence. Through the application of AI, user authentication procedures have been enhanced, suspicious login attempts have been blocked, and unauthorized access has been prevented. With the use of AI, malware detection has been much improved, and suspicious cyber behaviours have been identified. The use of AI in cyber security risks and the rapid reaction solutions it provides have completely transformed cyber security.

Although governments and large companies were the first to use AI in the cyber security field, the technology has now made its way down to managed service providers (MSPs) and small and medium-sized firms. With the use of AI, hackers are becoming better at targeting organisations and enterprises, even tiny ones. Simply said, their use of AI in cyberattacks has made them a major concern. In order to protect themselves against cyberattacks, governments and organizations should use AI. There is a daily increase in the number of dangers that governments and organizations face from hackers and cyberattacks due to the huge advancement in technology.

Literature Review

Introduced by Botacin *et al.* (2022) [3], HEAVEN is a Hardware-Enhanced Antivirus Engine developed to

accelerate real-time malware detection using signature-based approaches. The core idea of HEAVEN is to use specialized hardware components, such HPC, to efficiently process and analyse malware signatures, which results in faster and more accurate detection. This article details the HEAVEN implementation and how it uses HPC to remove the main processor's workload from signature matching and analysis. HEAVEN is able to analyze a large number of signatures and identify malware in real-time or near real-time thanks to hardware-based acceleration, which significantly reduces the computational cost. Our detection system is now more effective and scalable, all thanks to the parallel processing made available by HPC.

A method for real-time app monitoring and evaluation is proposed by Patte *et al*. (2022) [4] using PMCs, which are specialized registers found in modern microprocessors. The technique uses PMCs and the different patterns shown by malicious software to analyse the dynamic behaviour of programs in an effort to detect and classify malware. This article discusses the design and implementation of an intelligent malware detection system to process and analyse the information obtained from PMCs. The system employs a number of models and approaches to analyze the performance counter data and distinguish between malicious and safe applications. By using PMCs to gather valuable data on program execution patterns and resource use, the system is able to detect suspicious activity linked to malware.

(Tirumala *et al*. 2020) [5], An approach of encoding raw input data, namely malware samples, into a lower-dimensional appearance or latent space using autoencoders is presented in. This allows autoencoders to recognise the most important characteristics and trends seen in malware data. characteristics, both static and dynamic, often used in malware analysis are used to train the autoencoder. These characteristics are collected from the malware samples. In contrast, the autoencoder is trained using the raw binary characters of the malware samples in the signature-based training approach.

(Yu *et al*. 2013) [2] pay attention to relieving growing worries over the need for trustworthy detection methods and the rapidly propagating Android malware. For this reason, the author zeroes focused on examining how Android apps change their behaviour while running. The writers compile a large database of Android apps, including both good and bad examples, to ensure they cover all the bases in terms of app types and features. During the execution of these samples, this study records and monitors a multitude of behavioural characteristics, such as system calls, API requests, network interactions, and file operations. Methods like sandboxing and dynamic analysis are used for this purpose. To distinguish between safe apps and harmful software, these dynamic properties are crucial indicators, and they also provide invaluable insights into the apps' real-time working.

Using a unique approach, a team of researchers from Obaidat *et al*. (2022) [1] examined both the static behaviour of Java programs and the dynamic visuals generated by Java bytecode. By converting Java bytecode into visual representations called images, they create a feature extraction technique that can detect unique patterns and structural aspects of the code. A deep learning model takes the pictures and other behavioural features, such as API calls, system events, and network activity, as input data. The sequential nature of behavioural data is handled by Recurrent Neural Networks (RNNs), while image-based properties are analysed and relevant patterns are captured by Convolutional Neural Networks (CNNs). To improve the accuracy of Java malware detection while decreasing false positive rates, the proposed Jadeite solution use deep learning techniques to merge data based on behaviour with data based on images.

Research Methodology

The requirement for systematic, reproducible, and scalable techniques to understand the dynamics of AI integration into cyber security practices justifies the use of survey design, notably structured questionnaires, as the key tool for gathering quantitative data on AI technology in cyber defence. the study demonstrates its dedication to gathering diverse perspectives on how AI may improve threat detection and response systems. Twenty people participated in the survey; they were chosen at random to ensure that the selection procedure was fair and that the results were representative of the population under investigation. Creating a structured questionnaire is an essential tool for gathering quantitative data for evaluating the efficacy of AI-based solutions in cyber security. We opted for this method to collect data methodically on the AI systems in use, how well they are doing, and the problems that arise when they are integrated into cyber security frameworks. The questionnaire was made up of closed-ended questions so that it could be easily analysed and compared across various demographics of the target audience. To understand how well AI-based systems handle cyber security, this study relies on SPSS for data analysis. This research used statistical methods to interpret quantitative data obtained from structured questionnaires in order to shed light on the complex interplay between AI technology and cyber security results.

Data Analysis

Descriptive Statistics of Respondents Demographic Data

Twenty people took part in the study, with the vast majority having worked for at least a year for companies that use ICT exclusively in the cloud or on-premises. Respondents came from a wide variety of backgrounds, including the information and communication technology (ICT), banking, healthcare, government, and others. While analyzing the data, descriptive statistics, frequency, and percentage were used.

Table 1: Demographic Data of Respondents

	Frequency	Percentage%	
Age range	(20–29)	5	25%
	(30-39)	15	70%
	(40-49)	1	5%
Years of experience	<1year	6	30%
	1-5years	11	55%
	6-10years	3	15%
Gender	Male	18	90%
	Female	2	10%
Type of organization	Financial	7	35%
	Government	1	5%
	Healthcare	2	10%
	Technology (ICT)	8	40%
	Others	2	10%
Type of AI technology used	Anomaly system	3	15%
	Automated security	1	5%
	Deep learning	2	10%
	Machine learning	11	55%
	Neural network	1	5%
	Threat intelligence	2	10%

Based on its capabilities, features, and technologies, Artificial Intelligence technology may be generally divided into numerous sorts, as shown in table 1. Threat intelligence (10%), neural networks (5%), deep learning (10%), automated security (5%), and anomaly systems (15%) are some of the topics covered in this research and the percentages and frequencies of replies provided. Machine learning is the most widely employed artificial intelligence technology in diverse organizations, accounting for 55% of all AI integrations in cyber security.

Test of Normality: Without a test of normalcy, we cannot say whether or not our distribution is normally distributed. The Shapiro-Wilk test and the Kolmogorov-Smirnov test are two popular normality tests that SPSS displayed. The previous test is better suited for smaller samples (<50 samples) and can manage sample sizes up to 2000. Therefore, we have chosen the Shapiro-Wilk test as our numerical method of establishing normality. The results, with numerical values of 0.212, 0.069, and 100%, are closer to the maximum validity of one and above the necessary validity average of 0.05.

Table 2: Tests of Normality

		Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	years of experience	Statistic	df	Sig.	Statistic	df	Sig.
AI rank	<1year	.254	6	.200*	.866	6	.212
	1-5years	.310	11	.004	.866	11	.069
	6-10years	.175	3	.	1.000	3	1.000

*. This is a lower bound of the true significance
a. Lilliefors Significance Correction

Evaluation of AI's Performance
All respondents' opinions, ranked from 1 (not effective at all) to 5 (very effective), were considered while making a determination in this research on the efficacy of AI technology. Therefore, this will be the deciding factor.

High Perception: If the average value is close to 5 scale or proportionally close to 100%.

Low Perception: Assuming the average value is around one scale or significantly lower than 100%.
The descriptive statistics show an average value of 3.75, or around 4, in Table 3a. This works out to 80%, which is the same as 4/5 times 100. The results show that AI significantly improves cyber security infrastructure's threat detection and response capabilities. The vast majority of people who took the survey had a positive impression about AI. It is vital for the organisation to have the right expertise and understanding about artificial intelligence. On the other hand, the average value for responders in the three categories-less than a year, one to five years, and six to ten years-can be seen in table 3b.

Table 3a: Descriptive Statistics

	N	Minimum	Maximum	Mean		Std. Deviation
	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic
AI Rank(effectiveness)	20	2.00	5.00	3.7500	.17584	.78640
Valid N (listwise)	20					

Table 3b: Mean value for respondents in each group

Descriptives

AI rank

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
<1year	6	3.8333	.75277	.30732	3.0433	4.6233	3.00	5.00
1-5years	11	3.6364	.80904	.24393	3.0928	4.1799	2.00	5.00
6-10years	3	4.0000	1.00000	.57735	1.5159	6.4841	3.00	5.00
Total	20	3.7500	.78640	.17584	3.3820	4.1180	2.00	5.00

4.2 Integration of AI has Reduce the Time taken to Detect and Respond to Threat
According to most people who took the survey, the time it

takes to identify and react to a cyber-attack has been significantly reduced since artificial intelligence technologies have been integrated into cyber security infrastructure. With the use of AI, the detection and reaction times for cyber threats have been significantly reduced, according to eighty-five percent of the twenty participants. Nevertheless, 15% were unsure.

Table 4: Reduction in Time Taken to Detect and Respond to Threat

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not sure	3	15.0	15.0	15.0
	yes	17	85.0	85.0	100.0
	Total	20	100.0	100.0	

Measuring AI performance in Cyber security Infrastructure

To establish and monitor performance indicators that represent the system's efficacy in carrying out its intended function, it is essential to conduct an evaluation of the AI system's effectiveness. Threat detection rate (at 90%) and response time (at 10%) are two of them that were brought up in this research. In addition to scanning threat detection when the host is doing a scan, threat detection rate provides the organisation with information about different risks. Threat reaction time, on the other hand, is the amount of time it takes for a team to identify, assess, and fix a problem or interruption.

Table 5: Metric for AI Performance

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Response time	2	10.0	10.0	10.0
	Threat rate	18	90.0	90.0	100.0
	Total	20	100.0	100.0	

How Organization Address Issue Related to Data Privacy When Using AI

Artificial intelligence design must prioritize data privacy. Addressing these concerns contextually is crucial, and for companies operating with consumer-facing artificial intelligence. There are several techniques, and some of them considered in this study include data anonymization, regular audit, training and awareness.

Table 6: Data Privacy

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Data anonymizattion	1	5.0	5.0	5.0
	Regular audits	13	65.0	65.0	70.0
	Training&awareness	6	30.0	30.0	100.0
	Total	20	100.0	100.0	

Significant Challenges Encountered as a Result of AI Integration

With the ability to automate repetitive work and enhance decision-making, artificial intelligence has the potential to revolutionize the way business's function. The report does acknowledge that there are obstacles to applying AI solutions and among them are concerns about data protection (15%), a shortage of trained individuals (30%), and a high cost (55%). Major challenges include data privacy concerns, a shortage of trained staff, and the high expense of incorporating AI.

Table 7: AI's Limitation

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Data privacy	3	15.0	15.0	15.0
	High cost	11	55.0	55.0	70.0
	Lack of skilled personnel	6	30.0	30.0	100.0
	Total	20	100.0	100.0	

Key Area for Improvement or Further Research in the Field of AI Powered by Cyber security

Businesses are incorporating AI into many aspects of their operations, either by acquiring pre-built solutions or creating their own. It is well-known that AI models age. No number of advanced algorithms will prevent a model from falling short of expectations if it is not regularly updated and retrained. Algorithms (70%), data privacy (20%), and user-friendliness (10%) are some of the related topics covered by our research.

Table 8: Improvement in Key Areas in the Field of AI-Powered by Cyber security

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	AI-algorithms	14	70.0	70.0	70.0
	Data privacy	4	20.0	20.0	90.0
	User-friendliness	2	10.0	10.0	100.0
	Total	20	100.0	100.0	

How AI lead to qualitative reduction in the time taken to detect and respond to threat?

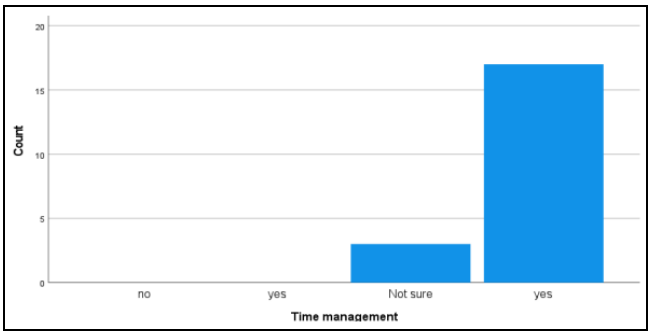

Fig 1: Graph showing Respondents' awareness of artificial intelligence efficiency

The effectiveness of artificial intelligence in cyber security infrastructure was recognized by 85% of respondents, the clear majority. Only 15% of respondents were ignorant of this efficiency.

How do organizations address issues related to data privacy when using AI?

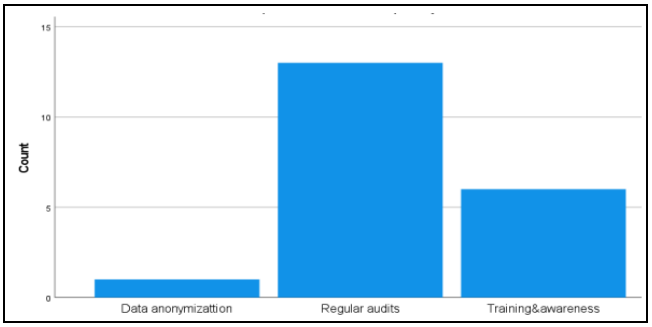

Fig 2: Graph showing data privacy policies adopted by organization when using artificial intelligence technology.

A majority of about 65% of respondents adopted the regular audits approach, 30%adoptedthe training and awareness approach and 5% used the data anonymization method.
What are the most significant challenges when integrating AI into cyber security?

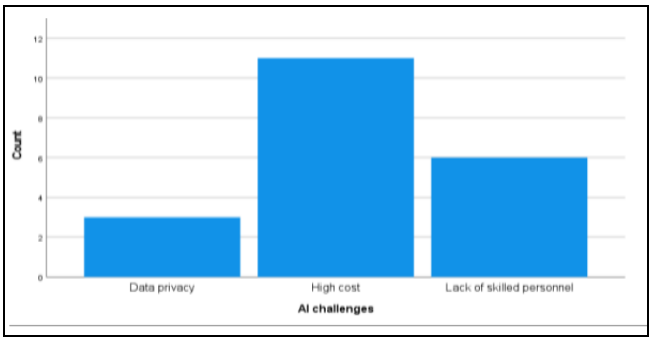

Fig 3: Graph showing challenges when integrating AI into cyber security

Some fundamental challenges in artificial intelligence mentioned in this study include high cost of implementation (55%), data privacy (15%) and lack of skilled personnel (30%).

Conclusion

The study's findings on the efficacy of AI technologies in improving cyber security infrastructures' threat detection and response capabilities are very important. These findings highlight the crucial role of AI in enhancing security procedures and have major ramifications for the area of cyber security. Nevertheless, the report emphasizes the need of continuous research and development to tackle the obstacles and constraints of AI integration. In order to monitor both host-and network-level activity, this study suggests a hybrid intrusion detection alert system that runs on a scalable architecture on commodity hardware servers. For real-time management and analysis of very large-scale data, the system used a distributed DL model with DNNs. A thorough evaluation of the DNN model's performance in contrast to traditional ML classifiers on several benchmark IDS data sets was conducted in order to choose it. This study has also used the suggested DNN model to identify intrusions and assaults by collecting characteristics based on hosts and networks in real-time.

Reference

1. Obaidat I, Sridhar M, Pham KM, Phung PH. Jadeite: A novel image behavior-based approach for java malware detection using deep learning. Computers and Security. 2022;113:102547.
2. Yu W, Zhang H, Ge L, Hardy R. On behavior-based detection of malware on android platform. In: 2013 IEEE Global Communications Conference (GLOBECOM); Atlanta, GA, USA. IEEE; c2013. p. 814–819.
3. Botacin M, Alves MZ, Oliveira D, Gregio A. Heaven: A hardware-enhanced antivirus engine to accelerate real-time, signature-based malware detection. Expert Systems with Applications. 2022;201:117083.
4. Pattee J, Anik SM, Lee BK. Performance monitoring counter based intelligent malware detection and design alternatives. IEEE Access. 2022;10:28685–28692.
5. Tirumala SS, Valluri MR, Nanadigam D. Evaluation of feature and signature-based training approaches for malware classification using autoencoders. In: 2020 International Conference on Communication Systems and Networks (COMSNETS); 2020; Bangalore, India. IEEE; c2020. p. 1–5.
6. Krishnamurthy P, Karri R, Khorrami F. Anomaly detection in real-time multi-threaded processes using hardware performance counters. IEEE Transactions on Information Forensics and Security. 2019;15:666–680.
7. Kuruvila AP, Kundu S, Basu K. Analyzing the efficiency of machine learning classifiers in hardware-based malware detectors. In: 2020 IEEE Computer Society Annual Symposium on VLSI (ISVLSI); 2020; Lyon, France. IEEE; c2020. p. 452–457.
8. Le HV, Ngo QD. V-sandbox for dynamic analysis IoT botnet. IEEE Access. 2020;8:145768–145786.
9. Aslan OA, Samet R. A comprehensive review on malware detection approaches. IEEE Access. 2020;8:6249–6271.
10. Kumar N, Sen AC. AI in Cyber security: Threat Detection and Response with Machine Learning. Journal of Propulsion Technology. 2023;44(3).
11. Barrett M. Technical Report. National Institute of Standards and Technology, Gaithersburg, MD, USA; c2018.
12. Xin Y, Kong L, Liu Z, Chen Y, Li Y, Zhu H, *et al.* Machine learning and deep learning methods for cybersecurity. IEEE Access. 2018;6:35365–35381.
13. Nguyen S, Marchal A, State R, Engel T. Autonomous and intelligent defense system using reinforcement learning. In: Proceedings of the 2018 IEEE International Conference on Communications (ICC); 2018; Kansas City, MO, USA. IEEE; c2018.
14. Sarker H, Furhad MH, Nowrozy R. AI-driven cybersecurity: An overview, security intelligence modeling, and research directions. SN Computer Science. 2021;2(3). DOI: https://doi.org/10.1007/s42979-021-00557-0.
15. Kaloudi N, Li J. The AI-based cyber threat landscape. ACM Computing Surveys (CSUR). 2020;53(1):1–34. DOI: https://doi.org/10.1145/3372823.