Online at: https://researchtrendsjournal.com **ISSN No:** 2584-282X

INTERNATIONAL JOURNAL OF TRENDS IN EMERGING RESEARCH AND DEVELOPMENT

Volume 2; Issue 4; 2024; Page No. 120-126

Received: 05-05-2024
Accepted: 13-06-2024

AI-driven cybersecurity solutions for real-time threat detection

[1]Aman Shrivastava and [2]Pooja Upadhyay

[1]Masters of Technology, 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.14716004

Corresponding Author: Aman Shrivastava

Abstract

To learn how AI-driven cybersecurity risks affect businesses, this project employed a case study research approach. So, here are the study questions: In order to better protect themselves against cybersecurity assaults powered by artificial intelligence, what steps should various sorts of companies take? In the second question, how and which AI tools will future hackers likely obtain? Question 3: How can businesses strengthen their defenses against phishing emails? To address these three research objectives, we relied on an analysis of three case studies. What we found is Question 1: While AI-powered assaults are a serious concern, networking companies and IT sectors may beef up their defenses with the help of AI solutions like Vectra Cognito and Amazon Web Services integration, which allow for real-time threat monitoring and response. Question 2: Hackers of the future will most certainly use generative AI technologies such as HackerGPT to launch complex assaults, such as creating botnets and sending convincing phishing emails. One shortcoming of these technologies is that they may misdiagnose vulnerabilities, which might lead to a streamlined onslaught. Thirdly, email security solutions powered by artificial intelligence (AI) such as Sentinel and Barracuda Essentials successfully counter phishing attacks by utilizing predictive analytics and multi-layered protection to thwart assaults. These solutions employ three layers of security to block and scan all incoming messages, thereby eliminating any potentially harmful threats.

Keywords: Cybersecurity, Threat Detection; cyberattacks, machine learning, AI

Introduction

The use of AI has altered the nature and frequency of cyberattacks across several sectors. Successfully launching a small number of assaults, including malware, botnet, and phishing email attacks (Das & Sandhane, 2021) [2]. Organizations need to figure out how to protect themselves from these assaults since they are happening more often. Malware assaults are on the rise, demonstrating the need for sophisticated technologies to safeguard systems (Das & Sandhane, 2021) [2]. A growing problem is that AI is outperforming humans in carrying out various assaults, and the problem is becoming worse as a result (Guembe *et al*., 2022) [3]. Traditional techniques of cyber threat detection are ineffective in the face of the urgency required to mitigate the potential damage and consequences of cyber assaults (Rajendran & Vyas, 2023) [8]. Organizations must use the AI defense approach to safeguard themselves against new assaults that are driven by AI. These days, companies may be better protected by using AI against AI (Rajendran & Vyas, 2023) [8].

According to the statistics

Cyberattacks cost approximately $400 billion a year, or almost $1,200 for every American. Data breaches in the United States cost an average of 8.19 million to 3.9 million dollars, and they are affecting people there.

Recent research from Statista (2023) indicates that data breaches in the US may cost organizations up to 1% of GDP every year on average. Cybercriminals pose a danger to individuals, businesses, and whole sectors. Organizations are attempting to protect themselves from AI-driven assaults by using AI technologies with other conventional cybersecurity measures (Truong *et al*., 2020) [5]. To lessen the impact of these assaults, more artificial intelligence technologies or tools should be used by businesses. Since phishing is the most basic kind of artificial intelligence

attack, it is where the majority of attackers' attention is concentrated (ChatGPT 3.5, September 2022).

There is a paradoxical result of using AI in cybersecurity. Although AI enhances productivity and data security for organizations, it also opens the door to more complex AI-driven cyberattacks, which increases the overall danger landscape. This paradox highlights an important problem: securing large data sets in the face of ever-increasing threats. The year (2018) by Fionta. A fine line between ethics and pragmatism must be drawn in the regulation of AI-driven attacks. To reduce cyber hazards without restricting innovation, it is vital to provide appropriate regulation of AI technologies (Zhao & Fariñas, 2023) [7]. Consequently, businesses may be able to fortify their defenses with an advanced AI deployment strategy, making sure that crucial data is secure from more sophisticated cyberattacks and that AI fulfills its cybersecurity promise. In order to successfully navigate the future of cybersecurity driven by AI, it is crucial to address ethical concerns and establish strategic regulatory frameworks (Zhao Fariñas, 2023) [7].

"AI can never be ethical because it is just a tool, and any tool can be used for good or evil." (Humans in World E can't make AI moral or ethical, but we must realize that stopping the use of AI to avoid cyberattacks may be the only way to eradicate these dangers.) Research by Mertz (2019) [16].

There are a lot of complicated ethical questions raised by the rapid expansion of artificial intelligence (AI) across many domains, given the technology's potential for both beneficial and harmful uses. This challenge is highlighted by the World Economic Forum (2021), which states that AI cannot have inherent moral or ethical attributes as a tool. In fields like cybersecurity, where AI has the potential to both strengthen protections and introduce new, more complex dangers, this begs the issue of whether or not it is compatible with human ethical standards. Researchers like Kim (2015) [17] are putting a lot of emphasis on how AI complies with ethical norms; they stress the need for responsible implementation and strong frameworks to make sure AI benefits are maximized and risks are avoided. Companies may improve their defensive strategy's accuracy and efficiency by using AI (Kim, 2015) [17].

Artificial intelligence cybersecurity measures are now at a highly developed level. Even if more and more businesses are moving to cloud storage and other safer online settings, hackers may still get into their systems (Bocetta & Soroter, 2020) [18]. The data security and integrity of organizations are jeopardized by these AI-driven attack strategies, which may have serious and even fatal effects. In extreme cases, they may bring about systemic failures, which in turn can cause consumers to lose faith in the impacted businesses (Hamadah & Aqel, 2020; Cabaj *et al*., 2018) [19, 20]. According to Hamadah and Aqel (2020) [19], systemic failures that might result from AI-driven attacks include data breaches, fraud, privacy infringement, brand harm, financial loss, compliance challenges, organizations malfunctioning, and a lack of knowledge and readiness. Detecting, preventing, and controlling such assaults is made much easier with the use of AI approaches and improved systems. (According to Truong and Zelinka, 2020) [5].

Literature Review

In 2021, Moualla, 2021 [1] *et al*. This paper presents a novel intrusion detection system (IDS) for networks using the UNSW-NB15 benchmark dataset. It makes a substantial contribution to network security and protects networks against current attacks. After utilizing the Synthetic Minority Oversampling Technique to address imbalanced datasets, the Extremely Randomized Trees Classifier is brought into play to select the crucial features for each class in accordance with the "Gini Impurity" standard. This process follows the use of the Extra Trees Classifier. A logistic regression layer applies gentle evaluations across all classes after receiving the ELM classifier O/Ps as inputs; a fully connected layer learns from all possible combinations of these inputs. The results show that when compared to similar works, our suggested strategy performs better in terms of accuracy, precision rate, and ROC curve.

"Feature Selection Techniques for Large-Scale Network Intrusion Detection Based on Machine Learning," etc. Despite the prevalence of this dangerous picture processing environment, few research have assessed the threat it poses to NIDS and proposed countermeasures. To fill this need, we offer Def-IDS, an ensemble defensive system tailored to NIDS that is effective against both known and unknown hostile attacks. In order to determine how well the mechanism works, we compare it to the other three defensive mechanisms and use the CIC-IDS2018 evaluation tool. When it comes to recognizing various adversarial assaults, the results demonstrate that Def-IDS has enhanced accuracy, F1 score, recall, and precision.

In 2023, Bajaj and Arora published a paper. The data size has been reduced by the use of feature selection. We improved the detection process and developed an intrusion detection model that uses feature reduction and machine learning to spot systematic intrusions. The effectiveness of the model is dependent on the accuracy of intrusion detection in the absence of level 21 attacks, the most obvious ones, and on the attacks that are harder to detect.

In Abuzneid 2019 [4] *et al*. Features dimensionality reduction strategies for ML-based NID. Two techniques for dimensionality reduction of features are used in this study: Two DL approaches are available for dimensionality reduction: Several classifiers, including as Linear Discriminant Analysis, Random Forest, and Quadratic Discriminant Analysis, are built using the low-dimensional features given by two techniques-AE (Auto-Encoder) and P (Component Analysis)-to develop an IDS. In both multiple and binary classifications, experimental findings using low-dimensional features perform better in terms of F-Measure, Accuracy, False Alarm Rate, and Detection Rate, respectively. In binary and multi-label classification, this study has the potential to reduce the CICIDS2017 feature dimensions to a level of 99.6 percent accuracy. Another feature that we give in this study is Multi-Class Combined Performance Metrics.

The existing machine learning-based intrusion detection systems are not suitable for analyzing traffic from the Internet of Things (IoT). In order to classify network traffic and differentiate between known and unknown anomalous behaviors in an IoT context, this paper proposes an IDS system that uses a mix of supervised and semi-supervised

deep learning. Furthermore, a new dataset tailored to the Internet of Things (IoT) called IoTR-DS was developed using the RPL protocol. Three known security attacks-DIS, Rank, and Wormhole-are used to categorize this dataset. Results from evaluating and comparing the proposed Hybrid Deep Learning-Based IDS to several current methods show promise.

Research Methods

How the research questions were answered is detailed in Chapter 3. The study's primary goals were to(1) strengthen defenses against AI-based threats;(2) describe future AI tools that cybercriminals may employ; and(3) develop methods to make systems more resistant to phishing attacks. In order to get this data, we searched Google for case studies that were published between 2020 and 2024. Because it allows for an in-depth analysis of complicated situations within their original context, the case study technique was selected for our research. This methodology enables a comprehensive examination of real-life events by capturing subtleties and dynamics that other methods could overlook (Yin, 2017) [21]. Concentrating on a single or small set of instances allows us to better comprehend the issue by revealing crucial processes, relationships, and causal mechanisms. Yin (2017) [21] argues that case studies, which allow us to collect qualitative data, provide a rich and complete viewpoint that may inform theory, practice, and future study.

The project will seek to answer the following research questions

1. How can different types of organizations improve their defenses against AI-driven attacks from those trying to harm them?
2. How will future hackers most likely access AI tools, and what AI tools will they use?
3. What strategies can organizations implement to enhance resilience against phishing emails?

"Safeguarding Against Phishing Attacks": A Case Study on Implementing an Effective Cybersecurity Information System" by Schonewille as well as "AI-driven Approach for Advanced Email Protection" by the author. Organizations and institutions who have taken proactive steps to combat phishing may find more details in this search, which helps to answer the research question.

Table 1: Case Study Analysis Criteria

1	Questions	How can different types of organizations improve their defenses against AI- driven attacks from those trying to harm them?	How will future hackers most likely access AI tools, and what AI tools will they use?	What strategies can organizations implement to enhance resilience against phishing emails?
2	Research propositions or justification for using an exploratory study	Case 1: The integration of Vectra's AI-powered Cognito platform with AWS improves cyber threat identification and prevention in global telecom organizations.	Cyberattack complexity and frequency have increased dramatically with the availability and usage of AI technologies such as Hacker GPT.	Case 1: By putting AI-based email security products like Barracuda Sentinel and Essentials into use, a business may drastically lower the frequency and impact of email-related risks
3	Units of analysis	Case 1: The unit of analysis for this case study in multinational telecommunication company.	The unit of analysis for this case study is the use of AI tools like Hacker GPT in cybersecurity.	Case 1: The unit of analysis for this case study is Avalon Biomedical which isa life science organization.
4	Logic linking the data to the research questions	Case 1: Data on the Vectra's Cognito platform with AWS will help to analyze the effective way of defense against AI driven attacks.	Analyzing the qualitative data on the use of Hacker GPT, including studies of cyber-attacks and how hackers can use it for performing attacks faster.	Case1: Gather data on email threat incidents. The implementation process and the outcomes observed to decide what defense mechanism is better to protect from the attacks.
5	criteria for interpreting the findings	Case 1: The criteria for interpreting outcomes include evaluating the improvement in threat detection and prevention capabilities because of Vectra's AI-based Cognito platform being integrated with AW Synthetize coms company's cybersecurity infrastructure.	The criterion for interpretation is the assessing Hacker GPT's influence on the complexity and frequency of cyberattacks, as well as the efficacy of existing cybersecurity solutions against these AI-driven threats, are among the criteria for interpretation and conclusions.	Case 1: The criteria for interpreting efficacy of Barracuda Essentials and Barracuda Sentinel in reducing email-related risks and enhancing cybersecurity resilience at Avalon Biomedical are among the criteria for evaluating the results.
6		OpenAI impact the company's capacity to successfully manage organizational governance and protect against cybersecurity risks caused by artificial intelligence (AI). This is one of the criteria for interpreting the case study's conclusions.		as staff knowledge and overall organizational resilience to cyber threats, are among the criteria used to evaluate the case study's conclusions.

Analysis and Findings

How can different types of organizations improve their defenses against AI-driven attacks from those trying to harm them?

Research Proposition: Integrating Vectra's AI-powered Cognito platform with AWS improves cyber threat identification and prevention in global telecom organizations.

Case Study

Telecom Provider Relies on Vectra and AWS to Stop Hidden Cyberthreats.

Theoretical Propositions
To improve the telecom provider's ability to detect and prevent cyberattacks, the theoretical proposal is based on the premise of integrating AWS with Vectra's Cognito platform. Threat detection, incident response time, and overall improvements in security post-integration were the chosen metrics after the establishment of data collection plan goals. Using this theoretical framework helped highlight the benefits of collecting information from cloud and network traffic, as well as the possibility of real-time threat detection.

Explanations
Because competing hypotheses were readily available, it was both encouraged and required to investigate the other side's reasoning and verify the validity of their findings. These were efficiency gains made later on, but brought about by heightened security awareness throughout the organization's structures, improvements made to the IT infrastructure as a whole, and the results of external security audits. All the evidence pointed to the combination of Vectra's AI technology and the AWS environment as the cause of the dramatic improvements in threat detection and reaction times. The findings demonstrated that these enhancements were linked only to the integration of Vectra and AWS, and not to any other variables, when a study was conducted to statistically measure factors connected with various cybersecurity methods.

Case Description
A global telecommunications firm was the unit of analysis. Particular metrics, such as the ability to identify threats in real-time and manage incident response times, were used to evaluate the performance of the integration. Among the most notable changes brought about by the integration is an increase in the degree of security for the firm. For instance, the integration was already having a good effect on cybersecurity due to some minor compatibility with hundredths-of-a-second timing, which was handled with agility throughout the integration's deployment.

Key Findings: The telecom provider's capacity to tackle and neutralize cyber attacks was amplified when Vectra's Cognito technology was connected with AWS. Because of this connection, monitoring cloud and network traffic and correlating metadata became more faster and easier. Response times were reduced as a consequence of integration, on the other hand. Accumulated and evaluated empirical evidence lends strong credence to the study premise, which states that improving AI is crucial to bolstering cybersecurity.

Case Study: OpenAI as A Case Study of Power Dynamics (Mukunda. G, 2024) [6].

Research Proposition
When the power dynamics of organizational structures are understood and managed, defending against cyber threats powered by artificial intelligence is far more effective.

Theoretical Propositions
This proposition underscores the importance of operational power relations in an organization to contain AI-powered cyber threats. The data collection was majorly based on knowledge and perceptions of leadership transitions, decision-making, and governance structures at OpenAI. A theoretical proposition was offered to focus attention on internal dynamics and their impact on cybersecurity and Organizations' AI threat-readiness.

Rival Explanations
Validity of the study proposition and satisfaction of competing explanations were both within reach. Technology improvements, cybersecurity advancements across businesses, and increased funding for cybersecurity initiatives are some of the other characteristics that have been studied. The data showed that OpenAI's cybersecurity policies were more affected by changes in leadership and regulations governing power relations than by technological or environmental considerations. Sound governance, strategic choices, and optimal usage of threat management strategies were shown to be substantially associated out of the total data set.

Case Description
Here, OpenAI served as the analytical unit, and the usage of the idea of power and authority inside the organization was the focus of the applicability's complicated pattern. The anticipated success criteria for enhancing the organization's cybersecurity architecture were synchronization in governance structures, swiftness in decision-making stages, and harmony in leadership. The case study has focused on how better performance in the fight against cyber threats was enabled by being aware of and managing these power relations.

Key Findings
An examination of the OpenAI case study revealed that effective strategies for distributing authority within an organization lead to more robust defenses against cyberattacks including artificial intelligence. To enhance OpenAI's performance, it is crucial to implement new leadership strategies and realign the organizational management structures. The findings provide strong support for the study hypothesis, which posits that power dynamics inside organizations significantly impact the efficacy of cybersecurity governance and threat management initiatives.

How will future hackers most likely access AI tools, and what AI tools will they use?
Case Study: Rise In Malicious AI Tools With HackerGPT (SOCRadar)

Research Proposition
Understanding the accessibility, capabilities, and ethical implications of AI-driven tools, such as HackerGPT, in cybersecurity is crucial for developing effective defence strategies and regulatory frameworks.

Theoretical Propositions
This case study builds on an existing theoretical approach that examines the setting of cybercrime via the lens of the availability and usage of tools, such as Hacker GPT AI. To carry out a wide range of cybercrimes, including phishing,

malware development, and botnet construction, these tools use cutting-edge artificial intelligence algorithms. Theoretical presumptions center on the idea that more people have access to these kinds of technologies due to the democratization of AI, particularly its open-source development. The data collecting strategy is informed by this concept, which highlights the tools' accessibility, usage, and responsibilities in characterizing cybersecurity risks.

Rival Explanations

Paying close attention to the competing explanations is necessary for proving the theoretical assertion. Ethical considerations that may play a role in the creation of AI to combat cyber threats, strict legal enforcement in response to cyber-attacks utilizing AI, and the use of alternative, more conventional methods to secure businesses' systems and structures are all potential competing explanations. But this data shows that Hacker GPT and comparable harmful AI tools, including Worm GPT, Fraud GPT, and Poison GPT, are very problematic since they are openly available and modular. There is a dramatic increase in cybersecurity risk due to the benefits these technologies provide threat actors, which enable them to evade traditional defenses.

Case Description

The case study's integrated unit of analysis includes HackerGPT and comparable advanced AI applications. It lays out the problems with combating cyber dangers caused by these technologies, but it also raises hopes for AI's resilience in the face of challenges. The article focuses on the ethical concerns surrounding the development and use of AI. The biggest issue is that these technologies are always evolving, which opens the door to new possibilities and dangers and necessitates rethinking cybersecurity measures and enforcing rigorous ethical standards.

Key Findings

As a result, the case study results back up the research claims by showing how AI technologies like HackerGPT greatly impact cybersecurity. The first takeaway from the case study is that there is mounting evidence that AI is constantly getting better and that more and more people are turning to open-source innovation to power their hacking tools. These tools are accessible to anyone with an internet connection, which means that bad actors have more leverage to accomplish their complicated goals. Additionally, the fact that thieves can use AI to craft convincing phishing emails and launch sophisticated assaults like botnet distributed denial of service attacks demonstrates the inadequacy of current security measures in the face of AI-assisted threats. Lastly, it stresses the need of thinking about the ethical concerns surrounding the development and use of AI systems. It demands better ethics and regulation in the cybersecurity industry and beyond. These findings provide light on how best to use new technology and make use of AI. All of the research hypotheses are backed by the case study's findings, which emphasize the importance of AI in shaping cybersecurity settings and the need of properly regulating risks associated with AI.

Table 2: AI Tools

Name of the Tool	Use of Tool	Year Published
WormGPT	Assists hackers with hacking and programming tasks, capable of unrestricted hacking.	2023
FraudGPT	Specialized in cybercrime, creates fake messages, viruses, and phishing content.	2023
PoisonGPT	Generates fake news and harmful information, capable of spreading viruses and malware.	2023

The case study further develops the relationship between AI and cybersecurity, highlighting the prospects and risks of using AI as an attacker, such as HackerGPT. Although these tools demonstrate the possibility of AI in cyber security, they also indicate the need for effective countermeasures, increased ethical standards, and constant monitoring of new threats in cyberspace.

What strategies can organizations implement to enhance resilience against phishing emails?

Case Study: AI-Driven Approach for Advanced Email Protection (Lee, 2021)

Research Proposition

Integrating AI technologies like Barracuda Essentials and Barracuda Sentinel enhances resilience against phishing through multi-layered protection and real-time threat detection.

Theoretical Propositions

This case study is based on the theoretical assumption that organizations may improve their defenses against phishing emails by using advanced artificial intelligence solutions such as Barracuda Essentials and Barracuda Sentinel. Understanding how AI algorithms and real-time threat detection decrease the influx of email-associated dangers improves the data gathering strategy. The case study is on the successful deployment of a solution to eliminate phishing attacks, which focuses attention on how the employment of AI-sponsored technology affects the organization's security measures.

Rival Explanations

Possible reasons were compared to several characteristics, such as the efficacy of staff education and standard IT safety procedures. Unfortunately, the study shows that Barracuda's AI solutions can protect users against upcoming phishing assaults. The enterprise's robust anti-phishing defenses are shown by the staff's training and the features provided by Barracuda Essentials and Sentinel. Because of the revolutionary nature of AL-led technologies in the field of information security, this research disregards rival hypotheses that suggest more conventional methods may provide the same level of protection.

Case Description

To emphasize how difficult it is to apply AI to the email security scenario, the case description incorporates Avalon Biomedical as an integrated analytical unit. The article goes on to say that additional aspects that were considered and

were successful in lowering phishing risks included educating staff and using AI. How these integrated methods dealt with new forms of phishing captures this pattern of complexity, which helps to explain why the organization's cybersecurity was better after the adoption.

Key Findings

The case study lays forth the evidence that backs up the research premise that companies may strengthen their defenses against phishing emails by using the AI technologies that were studied. Avalon Biomedical saw a significant decrease in phishing threats when Barracuda implemented AI technologies and provided comprehensive staff training services. This lends credence to the latter's theory of AI's ability to augment the current conventional defenses against complex email risk.

Case Study: Implementing An Effective Cybersecurity Information System Against Phishing Email Attacks (Schonewille, 2024) [10].

Research Proposition

Implementing a comprehensive Cybersecurity Information System, including advanced filters, secure authentication, and employee training, reduces susceptibility to phishing and enhances cybersecurity resilience.

Theoretical Propositions

Regarding the theoretical proposition, adopting complete IS cybersecurity decreases the organization's vulnerability to phishing attacks. This informs the data collection plan concerning understanding the parts of the IS, such as sophisticated filters in emails, secure methods of authentication, and training programs for employees. It directs attention towards assessing how these components enhance organizational safeguards against potential phishing threats.

Rival Explanations

Organizational culture, changes in the threat landscape, and the efficacy of training programs were additional factors that may impact results, making it necessary to evaluate alternative hypotheses. Despite the fact that IS negatively impacted employment, IS significantly reduced phishing risks. Directed email filters in conjunction with top-priority training successfully decreased phishing threats, disproving only competing approaches that assume the importance of other variables. This helps to explain why the organization's filters and employees rejected the identified threats. Phishing assaults are just as sneaky, and this study shows how important IS technologies are for fortifying organizational defenses against them.

Case Description

Use of the embedded unit of analysis-a global financial services organization-in this case study reveals difficulties in implementing CSIS. As a result, it stresses the need of educating staff and implementing sophisticated email security measures to prevent phishing. Organizational cybersecurity was enhanced by the application because of the general trends of complexity in how these coordinated approaches protected them from phishing attempts.

Key Findings

The study's evidence directly affirms the research proposition that enhancing the framework of a CIS helps lower organizations' vulnerability to phishing attacks. The IS, which included spear phishing email security, attempted email extinction and targeted training, improved the audience's phishing familiarity in the financial services organization. This substantiates the hypothesis that IS technologies are critical in managing phishing threats and enhancing the organization's security status.

Conclusion

With that being said, the study provides solid evidence that modern cybersecurity frameworks cannot function without integrating AI technologies into cloud services. The instance demonstrated the promise of AI technologies via their advantages in self-monitoring and danger detection, functioning in real-time, and rapid reaction time. OpenAI's leadership and governance have come together to tackle the complex issues caused by AI and associated dangers. Organizations that prioritize managing internal power relations are more likely to establish strong defenses against cyber attacks and successfully address their deficiencies. Taken together, the study's findings back up the idea that AI cybersecurity frameworks must include critical ethical and legal considerations. The case studies demonstrated that, in order to properly use AI technology, all relevant regulations must be followed and the fundamental standards of AI management must be met. Hence, companies and lawmakers should step up their efforts to set guidelines for cybersecurity AI. Following this path would guarantee that these technologies have beneficial effects.

References

1. Moualla S, Khorzom K, Jafar A. Improving the performance of machine learning-based network intrusion detection systems on the UNSW-NB15 dataset. Comput Intell Neurosci. 2021;2021:1-13.
2. Das R, Sandhane R. Artificial intelligence in cyber security. In Journal of Physics: Conference Series 2021;(4):042072. IOP Publishing.
3. Guembe B, Azeta A, Misra S, Osamor VC, Fernandez-Sanz L, Pospelova V. The emerging threat of ai-driven cyber attacks: A review. Applied Artificial Intelligence. 2022;36(1):2037254.
4. Abdulhammed R, Musafer H, Alessa A, Faezipour M, Abuzneid A. Features dimensionality reduction approaches for machine learning based network intrusion detection. Electronics. 2019;8(3):322.
5. Truong C, Oudre L, Vayatis N. Selective review of offline change point detection methods. Signal Processing. 2020;167:107299.
6. Mukunda G. Defense against the dark arts 101: OpenAI as a case study of power dynamics. Forbes [Internet]. 2024 Feb 6 [cited 2024 May 31]. Available from: https://www.forbes.com/sites/gautammukunda/2024/02/06/defense-against-the-dark-arts-101-openai-as-a-case-study-of-power-dynamics/?sh=7ff4b0f47bd7.
7. Zhao J, Gómez Fariñas B. Artificial intelligence and sustainable decisions. European Business Organization Law Review. 2023;24(1):1-39.
8. Rajendran R, Vyas B. Cyber security threat and its

prevention through artificial intelligence technology. Int J Multidiscip Res. 2023;5:1-18.
9. Rise of malicious AI tools: A case study with HackerGPT. SOCRadar® Cyber Intelligence Inc. [Internet]. 2024 [cited 2024 Jul 1]. Available from: https://socradar.io/rise-of-malicious-ai-tools-a-case-study-with-hackergpt/.
10. Schonewille M. Mini case - safeguarding against phishing attacks: A case study on implementing an effective cybersecurity information system. LinkedIn [Internet]. 2024 [cited 2024 May 31]. Available from: https://www.linkedin.com/pulse/safeguarding-against-phishing-attacks-case-study-matthew-schonewille-yv46c/.
11. Shaukat K, Luo S, Chen S, Liu D. Cyber threat detection using machine learning techniques: A performance evaluation perspective. In: 2020 International Conference on Cyber Warfare and Security (ICCWS); c2020. p. 1-6.
12. Vectra. Telecom provider relies on Vectra and AWS to stop hidden cyberthreats. Vectra [Internet]. 2021 [cited 2024 May 30]. Available from: https://content.vectra.ai/hubfs/downloadable-assets/ITCentral-CaseStudy-Manufacturing.pdf.
13. Willie MM. The role of organizational culture in cybersecurity: Building a security-first culture. J Res Innov Technol. 2023;2(2(4)):179-198.
14. Luckett J. Phishing resistant systems: A literature review. J Comput Sci Coll. 2023;39(3):347-347.
15. Meyer LA, Romero S, Bertoli G, Burt T, Weinert A, Ferres JL. How effective is multifactor authentication at deterring cyberattacks? arXiv preprint arXiv:2305.00945. 2023.
16. Mertz J. Introduction to optical microscopy. Cambridge University Press; c2019.
17. Kim JH. Understanding narrative inquiry: The crafting and analysis of stories as research. Sage publications; c2015.
18. Sorot R, Goel A, Rewari S. Phase Transition Material Modulated Hyper FET for Digital Applications. In2023 IEEE Devices for Integrated Circuit (DevIC); c2023. p. 261-265. IEEE.
19. Hamadah S, Aqel D. Cybersecurity becomes smart using artificial intelligent and machine learning approaches: An overview. ICIC Express Letters, Part B: Applications. 2020;11(12):1115-1123.
20. Cabaj K, Gregorczyk M, Mazurczyk W. Software-defined networking-based crypto ransomware detection using HTTP traffic characteristics. Computers & Electrical Engineering. 2018;66:353-368.
21. Yin J, Cao Y, Li YH, Liao SK, Zhang L, Ren JG, *et al*. Satellite-based entanglement distribution over 1200 kilometers. Science. 2017;356(6343):1140-1144.