A STUDY TO INVESTIGATE THE ROLE OF MACHINE LEARNING IN CYBERSECURITY AND IDENTIFY THE CAPABILITIES OF MACHINE LEARNING IN CYBERSECURITY BEYOND THREAT DETECTION.

Li Qinying[1], Divya Midhunchakkaravarthy[1]

[1]Lincoln University College, Petaling Jaya, Malaysia.

ABSTRACT

This research explores the revolutionary effects of ML on cybersecurity, particularly as it pertains to its function beyond the conventional detection of threats. Traditional approaches often fail to counteract increasingly complex cyberattacks. Machine learning has the potential to greatly improve cybersecurity techniques by analyzing large datasets and identifying trends. Threat prediction, anomaly detection, or automated response are just a few areas that can benefit from using ML approaches, which are the focus of this study. It delves into how ML models can look at past assault patterns and find small signs humans would miss to foresee new attacks. The research also delves into the function of ML in real-time reaction systems, which can learn from fresh data in real time and adapt to changing threats. The report emphasizes that ML can improve threat intelligence, automate regular security chores, and optimize resource allocation, in addition to detection and response. Organizations may achieve more proactive and adaptable security postures by incorporating ML into cybersecurity frameworks. Among these methods is the use of ML for behavioral analysis, which sheds light on user actions and highlights any discrepancies that can indicate security holes. The study concludes with a thorough examination of how machine learning may reshape cybersecurity procedures. It highlights how technology can provide unique solutions for prediction, reaction, and total security management, going beyond just threat detection. The results could help direct ML studies and applications in the future, to develop cybersecurity systems that are more robust and flexible.

Keywords: Machine Learning, Cybersecurity, Capabilities, Threat Detection.

INTRODUCTION

Cybersecurity is still a major issue for people and businesses in today's ever-changing digital world. The need for cutting-edge innovation to fortify security measures is at an all-time high because cyber threats are becoming smarter by the day. In particular, machine learning (ML) has been a game-changer among these technologies, providing vast improvements over more conventional forms of threat identification (Shah, 2021). Machine learning has several uses in cybersecurity, and this research will explore those

uses as well as its more famous use in threat detection. Machine learning is a subfield of AI that focuses on creating algorithms that let computers learn from their experiences and become better over time without human intervention. Machine learning has completely changed the game when it comes to cybersecurity threat detection. It allows computers to see trends and abnormalities that might indicate an assault is on the horizon. Nevertheless, its usefulness goes much beyond this crucial use case (Apruzzese et al., 2023).

Automated incident response, vulnerability management, or behavioral analytics are additional vital parts of cybersecurity that this inquiry aims to examine. Better attack prediction and mitigation, more accurate threat information, and easier administration of security operations are all possible thanks to cybersecurity systems that use ML approaches (Nassar & Kamal, 2021). To top it all off, the research will look at how ML might help with security measure adaptation to new threats and attack vectors. This study shed light on the present capabilities of machine learning in cybersecurity via a thorough investigation, offering insights into how these technologies are transforming the industry. The research aspires to provide a better understanding of ML's potential and aid in the creation of more resilient and adaptable cybersecurity tactics by identifying and assessing its expanding responsibilities (Dasgupta et al., 2022).

BACKGROUND OF THE STUDY

The area of information security has seen a remarkable transformation due to the convergence of machine studying and cybersecurity. The significance of signature-based threat detection approaches in cybersecurity has been emphasized in the past. In this approach, computers would identify harmful actions by comparing them to previously recognized threat signatures (Ahsan et al., 2022). Although it worked well back then, this strategy hasn't been able to adapt to the ever-evolving cyber threat scenario. Cybersecurity tactics underwent a sea change with the introduction of machine learning, a kind of AI that allows computers to discover new patterns in data and become better with time. As computing power and data availability improved, the late 20th-century uses of early machine-learning models grew beyond their initial simplicity. The possibility that machine learning may improve threat detection skills by seeing trends and outliers that conventional approaches missed was first considered in the early 2000s (Bouchama & Kamal, 2021).

As computing power and algorithmic sophistication increased in the 2010s, machine learning's use in cybersecurity became more prominent. Pattern recognition or predictive analytics made possible by techniques like supervised and unsupervised learning as well as neural networks allowed for the detection of both known and new dangers (Manoharan & Sarker, 2023). Researchers and practitioners in the field of

cybersecurity began to investigate new uses of machine learning beyond threat detection. Security solutions like behavioral analytics, vulnerability management tools, or automated incident response systems started using ML to make them more responsive and dynamic. These developments demonstrated the promise of machine learning for handling threat identification, prevention, response, and management in general. The importance of machine learning in creating proactive and adaptive security measures is being acknowledged more and more as cybersecurity evolves. The purpose of this research is to add to that body of knowledge by exploring the wider uses of machine learning in cybersecurity beyond threat detection and its increased capabilities in this area (Mijwil et al., 2023).

PURPOSE OF THE STUDY

The study's overarching goal is to uncover how machine learning is changing the face of cybersecurity by delving deeper beyond its typical use case of threat detection. The goal of this study is to find and explain the wider uses of machine learning in cybersecurity by looking at how it might improve things like automated incident response, exposure management, or behavioral analytics. In the end, the research aims to shed light on how machine learning may be used to create cybersecurity measures that are more proactive, adaptable, and comprehensive. This will help strengthen and fortify cybersecurity methods.

LITERATURE REVIEW

The revolutionary potential of machine learning (ML) has made its incorporation into cybersecurity a hot topic. The ever-changing nature of cyber threats has proven too much for traditional cybersecurity tactics, which mostly use signature-based detection methods. Machine learning has become an invaluable resource in this regard due to its capacity to sift through mountains of data in search of patterns (Sarker et al., 2020). Several studies have shown that ML may improve threat detection skills. By examining trends in user activity and network traffic, methods like supervised studying and anomaly detection were used to spot both old and new dangers. In tests, these techniques were able to detect zero-day threats and complex malware that were previously undetected (Martínez Torres et al., 2019).

New research has shifted the emphasis to other critical elements of cybersecurity in addition to threat detection. Rapid analysis of security events and execution of pre-defined steps to mitigate risks may be achieved by automated incident response systems driven by ML. Instead of relying on human procedures, these solutions use ML algorithms to prioritize and react to events more effectively (Berghout et al., 2022). Applying ML approaches to historical data and attack patterns allows vulnerability

managers to anticipate possible vulnerabilities. Organizations may now fix security flaws before they are exploited thanks to these predictive capabilities. One such area where ML shows promise in cybersecurity is behavioral analytics. A possible insider threat or hacked account may be detected by ML algorithms by examining user behavior patterns. This method improves the capacity to identify and react to internal dangers instantly (Sewak et al., 2021).

In conclusion, machine learning has greatly improved threat detection, but it also can automate responses, manage vulnerabilities, and analyze behavior. The need to take a comprehensive strategy to use ML's capabilities in cybersecurity is highlighted by the continuing research.

RESEARCH QUESTION

What specific machine learning techniques are currently being utilized in cybersecurity beyond threat detection?

RESEARCH METHODOLOGY

The researcher used a convenient sampling technique in this research.

RESEARCH DESIGN

Quantitative data analysis was conducted using SPSS version 25. The combination of the odds ratio and the 95% confidence interval provided information about the nature and trajectory of this statistical association. The p-value was set at less than 0.05 as the statistical significance level. The data was analyzed descriptively to provide a comprehensive understanding of its core characteristics. Quantitative approaches are characterized by their dependence on computing tools for data processing and their use of mathematical, arithmetic, or statistical analyses to objectively assess replies to surveys, polls, or questionnaires.

SAMPLING

A convenient sampling technique was applied for the study. The research relied on questionnaires to gather its data. The Rao-soft program determined a sample size of 1463. A total of 1600 questionnaires were distributed; 1557 were returned, and 57 were excluded due to incompleteness. In the end, 1500 questionnaires were used for the research.

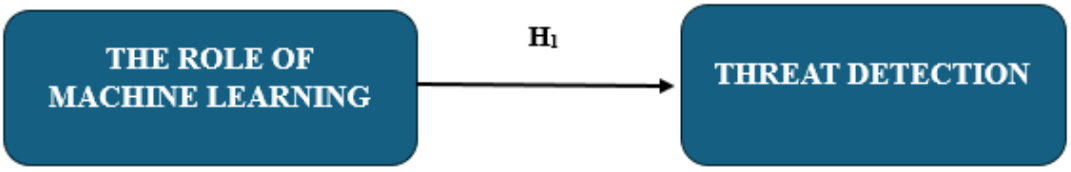
DATA & MEASUREMENT

A questionnaire survey served as the main data collector for the study. There were two sections to the survey: (A) General demographic information and (B) Online & non-online channel factor replies on a 5-point Likert scale. Secondary data was gathered from a variety of sources, with an emphasis on online databases.

STATISTICAL TOOLS

Descriptive analysis was used to grasp the fundamental character of the data. The researcher applied ANOVA for the analysis of the data.

CONCEPTUAL FRAMEWORK



RESULTS

Factor Analysis: Factor Analysis (FA) is often used to validate the underlying component structure of a collection of measurement items. The scores of the observed variables are thought to be impacted by latent factors that are not readily observable. The methodology of accuracy analysis (FA) is a method that relies on models. This research primarily focuses on constructing causal pathways that link observable events, underlying causes, and measurement errors.

The suitability of the data for factor analysis may be evaluated using the Kaiser-Meyer-Olkin (KMO) Method. The sufficiency of the sample for each variable in the model, as well as for the model as a whole, is evaluated. The statistics measure the magnitude of potential shared variation among many variables. Data that has smaller percentages is often more appropriate for factor analysis.

KMO generates random integers within the range of zero to one. A sample is considered sufficient if the Kaiser-Meyer-Olkin (KMO) value is between 0.8 and 1.

It is necessary to take remedial action if the KMO is less than 0.6, which indicates that the sampling is inadequate. Use your best discretion; some authors use 0.5 as this, therefore the range is 0.5 to 0.6.

• If the KMO is close to 0, it means that the partial correlations are large compared to the overall correlations. Component analysis is severely hindered by large correlations, to restate.

Kaiser's cutoffs for acceptability are as follows:

A dismal 0.050 to 0.059.

• 0.60 - 0.69 below-average

Typical range for a middle grade: 0.70–0.79.

Having a quality point value between 0.80 and 0.89.

The range from 0.90 to 1.00 is stunning.

Table 1: KMO and Bartlett's Test.

KMO and Bartlett's Test[a]		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.984
Bartlett's Test of Sphericity	Approx. Chi-Square	6850.175
	df	190
	Sig.	.000
a. Based on correlations		

The overall significance of the correlation matrices was further confirmed by using Bartlett's Test of Sphericity. A value of 0.984 is the Kaiser-Meyer-Olkin sampling adequacy. By using Bartlett's sphericity test, researchers found a p-value of 0.00. A significant test result from Bartlett's sphericity test demonstrated that the correlation matrix is not a correlation matrix.

TEST FOR HYPOTHESIS

DEPENDENT VARIABLE

Threat Detection: When it comes to cybersecurity, threat detection is all about finding and detecting possible security risks or harmful behaviors in a system or network. To detect any suspicious patterns, behaviors, or abnormalities that may point to an ongoing or attempted cyber-attack, it is necessary to monitor, analyze, and review data from several sources. To prevent risks from wreaking havoc, effective threat detection seeks to swiftly identify weak spots and possible dangers. Timely warnings and rapid actions are enabled to preserve digital assets and information via the use of numerous tools and methodologies, such as signature-based, behavior-based, or machine-learning approaches (Dini et al., 2023).

INDEPENDENT VARIABLE

The Role of Machine Learning: Machine learning (ML) is an area of AI that allows computers to automatically improve their performance as time passes by learning from data, without being specifically programmed to do so. Machine learning algorithms can forecast outcomes, determine courses of action, or spot trends by examining data for patterns and correlations. These models improve their precision and effectiveness in managing jobs or addressing issues by adapting as additional data becomes available. They are trained on enormous datasets (Karn et al., 2021).

Relationship Between the Role of Machine Learning and Threat Detection: Through the analysis of massive volumes of data, artificial intelligence improves threat detection by spotting trends and outliers that might suggest possible dangers. Machine learning algorithms can learn from fresh data and adapt and improve over time, in contrast to conventional approaches that depend on predetermined rules (Gupta & Sheng, 2019). Because of their adaptability, they can identify new dangers and change assault tactics with more precision. Machine learning aids early detection and response by constantly improving models in response to new threats, which lessens the likelihood and severity of security breaches. It is an essential tool in contemporary cybersecurity due to its capacity to analyze and understand intricate data patterns (Alloghani et al., 2020).

Based on the above discussion, the researcher formulated the following hypothesis, which was to analyze the relationship between the role of machine learning and threat detection.

H_{01}: There is no significant relationship between the role of machine learning and threat detection.

H_1: There is a significant relationship between the role of machine learning and threat detection.

Table 2: H_1 ANOVA Test.

ANOVA					
Sum					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	65692.704	496	5474.392	2829.974	.000
Within Groups	168.296	1003	1.934		
Total	65861.000	1499			

In this study, the result is significant. The value of F is 2829.974, which reaches significance with a p-value of .000 (which is less than the .05 alpha level). This means the **"H_1: There is a significant relationship between the role of machine learning and threat detection."** is accepted and the null hypothesis is rejected.

DISCUSSION

Machine learning's (ML) revolutionary promise in cybersecurity goes much beyond its conventional use in threat identification. With ML, automated incident response is improved since security events are analyzed and mitigated faster, which reduces reaction times and human error. Machine learning (ML) is used in vulnerability management to analyze previous data and identify possible flaws. This enables proactive steps to be taken. By identifying anomalies in user behavior, behavioral analytics enabled by ML enhance the identification of insider threats. Even with all the improvements, there are still problems with things like data quality, algorithmic bias, or connecting to other systems. To maximize the influence of ML on comprehensive cybersecurity policies, it is essential to address these concerns.

CONCLUSION

Ultimately, machine learning takes cybersecurity to the next level by enhancing automated incident response, strengthening vulnerability management, and honing behavioral analytics, going beyond only conventional threat detection. These capabilities allow for a wider spectrum of cyber threats to be addressed by more proactive and adaptable security methods. To effectively use the promise of ML, however, issues like data quality or system integration need to be resolved. To maximize machine learning's contribution to the creation of more robust and efficient cybersecurity measures, ongoing studies and developments are required.

REFERENCES

1. Ahsan, M., Nygard, K. E., Gomes, R., Chowdhury, M. M., Rifat, N., & Connolly, J. F. (2022). Cybersecurity threats and their mitigation approaches using Machine Learning—A Review. Journal of Cybersecurity and Privacy, 2(3), 527-555.
2. Alloghani, M., Al-Jumeily, D., Hussain, A., Mustafina, J., Baker, T., & Aljaaf, A. J. (2020). Implementation of machine learning and data mining to improve cybersecurity and limit vulnerabilities to cyber-attacks. Nature-inspired computation in data mining and machine learning, 47-76.
3. Apruzzese, G., Laskov, P., Montes de Oca, E., Mallouli, W., Brdalo Rapa, L., Grammatopoulos, A. V., & Di Franco, F. (2023). The role of machine learning in cybersecurity. Digital Threats: Research and Practice, 4(1), 1-38.

4. Berghout, T., Benbouzid, M., & Muyeen, S. M. (2022). Machine learning for cybersecurity in smart grids: A comprehensive review-based study on methods, solutions, and prospects. International Journal of Critical Infrastructure Protection, 38, 100547.
5. Bouchama, F., & Kamal, M. (2021). Enhancing cyber threat detection through machine learning-based behavioural modelling of network traffic patterns. International Journal of Business Intelligence and Big Data Analytics, 4(9), 1-9.
6. Dasgupta, D., Akhtar, Z., & Sen, S. (2022). Machine learning in cybersecurity: a comprehensive survey. The Journal of Defense Modeling and Simulation, 19(1), 57-106.
7. Dini, P., Elhanashi, A., Begni, A., Saponara, S., Zheng, Q., & Gasmi, K. (2023). Overview of intrusion detection systems design exploiting machine learning for networking cybersecurity. Applied Sciences, 13(13), 7507.
8. Gupta, B. B., & Sheng, M. (2019). Machine Learning for Computer and Cyber Security. ed: CRC Press. Preface.
9. Karn, R. R., Kudva, P., & Elfadel, I. M. (2021). Learning without forgetting: A new framework for network cyber security threat detection. IEEE Access, 9, 137042-137062.
10. Manoharan, A., & Sarker, M. (2023). Revolutionizing Cybersecurity: Unleashing the Power of Artificial Intelligence and Machine Learning for Next-Generation Threat Detection. DOI: https://www. doi. org/10.56726/IRJMETS32644, 1.
11. Martínez Torres, J., Iglesias Comesaña, C., & García-Nieto, P. J. (2019). Machine learning techniques applied to cybersecurity. International Journal of Machine Learning and Cybernetics, 10(10), 2823-2836.
12. Mijwil, M., Salem, I. E., & Ismaeel, M. M. (2023). The significance of machine learning and deep learning techniques in cybersecurity: A comprehensive review. Iraqi Journal for Computer Science and Mathematics, 4(1), 87-101.
13. Nassar, A., & Kamal, M. (2021). Machine Learning and Big Data analytics for Cybersecurity Threat Detection: A Holistic review of techniques and case studies. Journal of Artificial Intelligence and Machine Learning in Management, 5(1), 51-63.
14. Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: an overview from a machine learning perspective. Journal of Big Data, 7, 1-29.
15. Sewak, M., Sahay, S. K., & Rathore, H. (2021, October). Deep reinforcement learning for cybersecurity threat detection and protection: A review. In International Conference on Secure Knowledge Management in Artificial Intelligence Era (pp. 51-72). Cham: Springer International Publishing.
16. Shah, V. (2021). Machine Learning Algorithms for Cybersecurity: Detecting and Preventing Threats. Revista Espanola de Documentacion Cientifica, 15(4), 42-66.