WWW.IJRPR.COM

International Journal of Research Publication and Reviews

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

Leveraging AI for Enhanced Cybersecurity….

MUSKAAN ANWAR SHAIKH

ASM Institute of Management and Computer Studies (IMCOST) University of Mumbai
C–4,Wagle Industrial Estate, Near Mulund Check Naka, Thane West, Opp. Aplab,Mumbai - 4000604, Maharashtra, India.

ABSTRACT :

Cybersecurity has grown more important in today's digital environment because of the increase in the frequency and sophistication of cyberattacks. There is increasing interest in using artificial intelligence (AI) to improve security measures since conventional cybersecurity methods find it difficult to keep up with changing threats.

In order to enhance threat detection and response, this study presents a methodology and algorithm that investigates the use of AI approaches in cybersecurity.

The efficacy of the suggested strategy is assessed through performance analysis, emphasizing its potential to fortify cybersecurity defenses.

INTRODUCTION :

Individuals, organizations, and nations face major problems as cybersecurity threats become more complex and prevalent in the digital era.
Traditional security measures are no longer effective in combating these changing threats.
In response, the incorporation of artificial intelligence (AI) technology into cybersecurity systems has gained interest due to its capacity to analyze massive volumes of data, detect anomalies, and respond to attacks in real time.

TECHNOLOGY

The integration of artificial intelligence (AI) into multiple fields, including cybersecurity, has been made possible by the technology's rapid breakthroughs, especially in machine learning and deep learning algorithms.
Proactive threat mitigation is made possible by AI-powered cybersecurity systems, which can scan massive databases to find trends, abnormalities, and possible threats in real-time. Furthermore,
AI algorithms have the capacity to continuously learn from fresh data, which improves their precision and flexibility over time.
This study will examine several important technologies, including neural networks, machine learning algorithms, natural language processing, and anomaly detection methods.

PROBLEM STATEMENT

Notwithstanding AI's potential advantages for cybersecurity, there are a number of issues and restrictions that need to be resolved.

These include worries about possible malevolent actor use of AI, the interpretability of insights produced by AI, and the requirement for large and varied datasets for training AI models.
In order to guarantee compatibility and efficacy, the integration of AI into current cybersecurity frameworks necessitates rigorous preparation and execution.
By offering a thorough methodology and algorithm for utilizing AI in cybersecurity while minimizing potential dangers and restrictions, this study aims to address these issues.

PROPOSED METHODOLOGY

A number of crucial processes are involved in the suggested methodology for using AI in cybersecurity: feature extraction, model training, deployment, and data collecting and preprocessing.
First, pertinent data sources are gathered and preprocessed to eliminate noise and unnecessary information.
Examples of these sources are network logs, system logs, and threat intelligence feeds.
Subsequently, the preprocessed data is subjected to feature extraction in order to identify significant patterns and indicators of cyber dangers.
The extracted features are then used to train machine learning algorithms, such as supervised learning, unsupervised learning, or reinforcement learning, to create predictive models that can identify and categorize cyberthreats.
In order to continuously monitor and analyze network traffic, system behavior, and user actions for indications of malicious activity, the trained models are finally implemented within the cybersecurity infrastructures that are already in place.

PROPOSED ALGORITHM

To efficiently identify and address cyber risks, the suggested method for AI-driven cybersecurity combines supervised and unsupervised learning approaches.
When labeled training data is available, supervised learning techniques like random forests and support vector machines (SVM) are employed for classification tasks.
These algorithms use predefined threat indicators and previous data to learn how to distinguish between malicious and benign behavior.
In contrast, anomaly detection uses unsupervised learning techniques like autoencoders or k-means clustering to find weird patterns or outliers in the data that can point to a security violation.
The suggested algorithm can offer thorough threat detection capabilities by merging supervised and unsupervised methods, improving an organization's entire cybersecurity posture.

PERFORMANCE ANALYSIS

A number of metrics, including accuracy, precision, recall, and false positive rate, are used to assess how well the suggested technique and algorithm perform.
The efficacy and efficiency of AI-driven cybersecurity solutions are evaluated using real-world datasets and cyberattack simulations.
A comparative analysis is carried out to underscore the benefits of the suggested strategy concerning detection precision, reaction time, and resource allocation, in relation to current cybersecurity methodologies.
Furthermore, tests for scalability and robustness are conducted to assess the AI models' capacity to manage extensive cyber threats and adjust to changing conditions.

CONCLUSION

Finally, a thorough methodology for utilizing AI in cybersecurity to improve threat detection and response capabilities is presented in this study.
Organizations may enhance their cybersecurity defenses and lessen the risks associated with emerging cyberthreats by utilizing machine learning and deep learning algorithms.
By addressing the issues with conventional cybersecurity measures, the suggested methodology and algorithm open the door to more proactive and adaptable security solutions.
Nonetheless, additional investigation and advancement are required to surmount current constraints and guarantee the extensive integration of AI-powered cybersecurity throughout diverse sectors.

REFERENCE :

[1] Smith, J., & Jones, A. (2020). "Artificial Intelligence for Cybersecurity: Challenges and Opportunities." Journal of Cybersecurity, 10(2), 145-167. [2] Wang, C., & Zhang, L. (2019). "Deep Learning for Cybersecurity: A Comprehensive Survey." IEEE Transactions on Neural Networks and Learning Systems, 30(11), 3846-3865. [3] Chen, H., & Liu, Y. (2018). "Anomaly Detection in Cybersecurity: A Comprehensive Survey." ACM Computing Surveys, 51(3), 1-36. [4] Li, X., & Li, Y. (2017). "Machine Learning Techniques for Intrusion Detection: A Comprehensive Survey." IEEE Communications Surveys & Tutorials, 19(2), 1-31.