

Assignment 1

**Research Title: "Exploring the Impact of Machine Learning Algorithms on
Cybersecurity: A Comprehensive Review"**

ABDULAZIZ AWAD ALHOMIDI
[241000916](#)

Master of Science in Artificial Intelligence

1– Mishra, S. (2023):

Advantages:

- Strengthening the link between artificial intelligence (AI) and cybersecurity.
- It proposes a practical application of AI for cybersecurity in the financial sector.

Defects:

- It does not contain an in-depth analysis of potential biases and limitations associated with AI algorithms.

Style:

- It uses artificial intelligence algorithms such as K-Nearest Neighbor (KNN) algorithm and Enhanced Encryption (EES).

2– Al-Ruwaili, M. (2020):

Advantages:

- Researches the effectiveness of machine learning techniques for intrusion detection systems (IDS).
- It proposes a cooperative learning model and a hybrid feature selection approach.

Defects:

- It does not adequately discuss the potential weakness of machine learning algorithms.

Style:

- It uses machine learning techniques and feature selection approaches.

Data sources:

- Uses the latest public CICIDS2017 dataset.

3– Shah, V. (2021):

Advantages:

- Provides a comprehensive overview of machine learning algorithms in cybersecurity.

- It highlights the versatility and effectiveness of machine learning algorithms in detecting and preventing threats.

Defects:

- It would benefit from a deeper analysis of the limitations and challenges associated with machine learning.

Style:

- Analyzes various machine learning algorithms.

4– Abbruzzese, J., et al. (2023):

Advantages:

- Provides valuable insights into the role of machine learning in cybersecurity.
- Emphasizes the importance of understanding the positive and negative points of machine learning.

Defects:

- Lacks detailed analysis of specific machine learning techniques.

Style:

- Provides a comprehensive understanding of machine learning in cybersecurity.

Data sources:

Real case studies describing industrial applications.

5– Dasgupta, D., et al. (2022):

Advantages:

- Provides a comprehensive survey of recent work on machine learning in cybersecurity.
- Covers various machine learning algorithms and data mining schemes.

Defects:

- It could benefit from a deeper analysis of the effectiveness of specific algorithms.

Style:

- Conducts a comprehensive survey of recent research.

6– Geetha, R., and Thilagam, T. (2021):

Advantages:

- Provides a review of the effectiveness of machine learning and deep learning algorithms in cybersecurity.
- It classifies various algorithms and discusses their applications in detecting cyber attacks.

Defects:

- It can provide a deeper analysis of constraints and challenges.

Style:

- Reviews the effectiveness of machine learning and deep learning algorithms.

reference	Publication Year	Author(s)	Methodology Employed	Key Findings	Weaknesses/Limitations
Exploring the impact of AI-based cybersecurity on financial sector management.	2023	Mishra, S.	The study used an experimental methodology to evaluate the impact of artificial intelligence-based cybersecurity technologies on financial sector management.	AI-based Cybersecurity for Financial Sector Management (CS-FSM) technology is introduced. This technology contributes to enhancing the performance of cybersecurity systems by increasing their defense against cyberattacks. The main impact of this technology includes increased data privacy (18.3%), scalability (17.2%), risk reduction (13.2%), data protection (16.2%), and attack avoidance (11.2%).	The study may be limited to a specific environment or financial services sector only, and the proposed method may need further improvement and testing in different environments.

Investigation of Machine Learning Algorithms for Intrusion Detection System in Cybersecurity.	2020	Alrowaily, M	experimental study	Achieving three major contributions in the field of intrusion detection systems based on machine learning techniques. The first contribution suggests the effectiveness of using traditional machine learning techniques in intrusion detection systems. The second contribution proposes an ensemble learning algorithm to detect security threats. The third contribution proposes a hybrid feature selection approach to improve network attack detection.	Results may be dependent on a specific dataset and may need to be validated in other settings and datasets.
---	------	--------------	--------------------	---	---

Machine Learning Algorithms for Cybersecurity: Detecting and Preventing Threats	2021	Shah, V.	review	Highlight the role of machine learning algorithms in cybersecurity, with an emphasis on their ability to detect and prevent a wide range of threats. Machine learning algorithms analyze huge amounts of information to identify unusual patterns and changes that may indicate malicious activities. Leveraging technologies such as deep learning, these algorithms can analyze different types of unstructured data, making it easier to detect threats across various channels. In terms of threat prevention, machine learning algorithms play a crucial role in precautionary defense strategies, as these algorithms can predict potential threats and identify vulnerability in the system, allowing	There can be challenges in applying machine learning algorithms in real cybersecurity environments, including difficulty in handling large amounts of data and identifying positive and negative false positives.
---	------	----------	--------	---	--

				organizations to take preventive measures before an attack occurs.	
The role of machine learning in cybersecurity.	2023	Apruzzese, G., Laskov, P., Montes de Oca, E., Mallouli, W., Brdalo Rapa, L., Grammatopoulos, A. V., & Di Franco, F.	review	This article provides a comprehensive understanding of the role of machine learning in cybersecurity, highlighting its advantages compared to human-based detection methods, as well as the additional tasks that can be addressed by machine learning in this field. The article also outlines fundamental issues affecting actual machine learning applications in cybersecurity. Finally, the article presents how different stakeholders can contribute to developing the future of machine learning in cybersecurity, which is essential for progress in this field.	Another weakness is the absence of comparative analysis between different machine learning and deep learning algorithms in terms of their effectiveness in detecting different categories of cyber-attacks. Such comparative analysis can provide valuable insights into the strengths and weaknesses of different approaches. The problems resulting from the use of machine learning in cybersecurity are not mentioned in detail, nor are they sufficiently explained in the article.

Machine learning in cybersecurity: a comprehensive survey	2022	Dasgupta, D., Akhtar, Z., & Sen, S.	comprehensive review	This research provides a comprehensive review of recent work (from 2013 to 2018) on the use of machine learning in cybersecurity. The paper describes the fundamentals of cyberattacks and corresponding defenses, as well as the fundamentals of the most popular machine learning algorithms in use and proposed machine learning and data refinement schemes for the cybersecurity field in terms of features, dimensionality reduction, and classification/detection techniques. The research also provides an overview of adversarial machine learning, including security features of deep learning methods. Finally, it highlights outstanding issues and challenges in	The methodology used in the research was not precisely defined, making it difficult to assess the quality of evidence and results presented in the study. The study mainly focuses on presenting a different classification of machine learning and deep learning algorithms used in the field of information security. Although this classification is useful, the study may lack depth in analyzing the specific algorithms or their effectiveness in actual business scenarios.
---	------	-------------------------------------	----------------------	---	---

				cybersecurity and discusses potential future research directions.	
A Review on the Effectiveness of Machine Learning and Deep Learning Algorithms for Cyber Security	2021	Geetha, R., & Thilagam, T.	review and classification	This research provides a comprehensive review of the effectiveness of machine learning and deep learning methods in the field of cybersecurity. The research focuses on a detailed classification of different deep learning and machine learning algorithms, as well as a directed review of the use of different types of these methods to detect different classes of attacks. The platforms and tools used to implement deep learning and machine learning methods are also explored, and security solutions for different categories of attacks are summarized.	The study may generalize the effectiveness of machine learning and deep learning algorithms in the field of information security without considering the special contexts or challenges associated with different types of attacks or different data environments. This can lead to oversimplification or incorrect interpretation of the results.

Communications/conflicts:

- All studies emphasize the importance of using machine learning and artificial intelligence in enhancing cybersecurity.
- However, a diversity can be seen in the approaches proposed to achieve this goal, with some studies focusing on practical applications of AI in cybersecurity, while others focus on comprehensive surveys and evaluations.
- Conflicts can emerge in the specific methods proposed in each paper, suggesting differences in visions of how machine learning and artificial intelligence should be applied in cybersecurity.

Reference:

- Mishra, S. (2023). Exploring the impact of ai-based cyber security financial sector management. Applied Sciences, 13(10), 5875.
- Alrowaily, M. (2020). Investigation of Machine Learning Algorithms for Intrusion Detection System in Cybersecurity.
- Shah, V. (2021). Machine Learning Algorithms for Cybersecurity: Detecting and Preventing Threats. Revista Espanola de Documentacion Cientifica, 15(4), 42–66.

- 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.
- 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.
- Geetha, R., & Thilagam, T. (2021). A review on the effectiveness of machine learning and deep learning algorithms for cyber security. *Archives of Computational Methods in Engineering*, 28(4), 2861–2879.