

Detection of attacks by artificial intelligence

Artificial intelligence (AI) enables machines to perform tasks that typically require human intelligence, including making decisions, recognizing human speech, perceiving visual elements, and translating languages.

in cybersecurity is increasingly critical to protecting online systems from attacks by cyber criminals and unauthorized access attempts. If used correctly, AI systems can be trained to enable automatic cyber threat detection, generate alerts, identify new strands of malware, and protect businesses' sensitive data, include leveraging AI techniques.

So, we will explain numerous studies

Study	Authors	Year	Research Design	Methodology	Limitation
Study1	Jian-hua LI	2018	Cyber security meets artificial intelligence: a survey	Traditional ML and DL schemes against cyberspace attacks Combating cyber-attacks using AI with machine learning and deep learning.	Lack of detailed discussion on specific cyber threats. Limited focus on the implementation process and experimental results.
Study2	Xin Y Kong L Liu Z et al.	2018	Machine Learning and Deep Learning Methods for Cybersecurity	Machine learning and deep learning methods for network intrusion detection. Recursive neural network (RNN) for processing sequence data.	Challenges in using ML/DL for cybersecurity are discussed. No specific limitations are explicitly mentioned in the contexts provided.
Study3	Liu H, Lang B	2019	Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey	Machine learning and deep learning methods for intrusion detection systems. Domain knowledge, deep learning models, machine learning algorithms, and benchmark datasets. DARPA1998 dataset, metrics for evaluation, and multiple metrics for detection	Lack of available datasets is a major challenge
Study4	Handa A	2019	Machine learning in		

	Sharma A Shukla S		cybersecurity: A review	Machine learning techniques for cybersecurity applications. Adversarial attacks on machine learning algorithms	Protective systems for one ML model may not work for others. Privacy compromise due to data exchange in collaborative learning
Study5	Alrajhi A		A Survey of Artificial Intelligence Techniques for Cybersecurity Improvement	Introduces AI techniques for cybersecurity improvement and intrusion detection systems. Proposes a new detector generation algorithm for AIS-based intrusion detection.	AI techniques have limitations affecting intrusion detection performance. Existing AI tools may not fit specific security needs.
Study6	2022	Halboun i et al.	Machine Learning and Deep Learning Approaches for Cybersecurity : A Review	Anomaly Detection Methods and Misuse Detection Methods are utilized	Dataset impact on research. Feature processing complexity in machine learning versus deep learning

Study 1

Cyber security meets artificial intelligence: a survey

Abstract

show the intersection between cyber security and artificial intelligence and the use of AI technologies in building smart models for malware classification, intrusion detection, and threat intelligence sensing. It also explores the challenges and defense methods for AI models in the face of cyber threats. And other topics such as secure federated deep learning, encrypted neural networks.Li (2018)

Introduction:

This survey shows the connection between cyber security and artificial intelligence (AI). It shows how AI technologies, such as deep learning, can be utilized in cyber security to develop AI models for tasks like malware classification and intrusion detection. The goal of survey is to Concentrate the intersection of AI and cyber security.

Key search:

Cyber security; (AI); Attack detection; Defensive techniques

Advantage

Give an overview of the intersection between cyber security and artificial intelligence. research gaps and opportunities This can guide future research efforts and help researchers identify areas where additional work is needed.

analyzes the attacks that AI models may face and arranges them corresponding defense methods. By understanding the potential vulnerabilities and defense strategies, organizations and researchers can protect AI systems against cyber threats better.

Disadvantage

It may not cover all relevant subtopics or emerging areas within this broad field

Limited focus on the implementation process and experimental results.

How is ai effect on cybersecurity?

By deep learning techniques, can be employed to improve threat detection capabilities leveraging deep learning algorithms, AI can learn from vast amounts of data to accurately classify and categorize malware

continuously analyzing network traffic and user behavior, AI algorithms can identify suspicious activities and potential intrusions

Why is ai sufficient in cybersecurity?

AI is considered sufficient in cybersecurity because its advanced threat detection capabilities, adaptability to evolving threats, efficient malware classification, countermeasures against adversarial machine learning, automation and scalability, and the ability to preserve privacy and facilitate secure collaboration.

Study 2

Machine Learning and Deep Learning Methods for Cybersecurity

Abstract

The use of machine learning and deep-learning techniques for network analysis and intrusion detection in cybersecurity.

also shows types of network analysis for intrusion detection. It describes advantages and disadvantages of these methods and emphasizes the importance of data in ML/DL approaches. It shows suggestions for future research directions in network intrusion detection. Xin et al. (2018)

Introduction

It focuses on the increasing integration of the Internet with various aspects of our lives and the subsequent rise in security threats. Also defines cybersecurity as a group of technologies and processes made to protect computers, networks, programs, and data from unauthorized.

discusses several types of security breaches, including external and internal intrusions, and introduces three main types of network analysis for IDS: misuse-based, anomaly-based, and hybrid techniques. And the importance of machine learning (ML) and deep learning (DL) methods.

Key search

Deep learning, machine learning, cybersecurity, network

Advantages

This paper offers a thorough literature review of machine learning (ML) and deep learning (DL) methods for cybersecurity applications.

and focuses on the application of ML/DL methods in network intrusion detection. It provides insights into the techniques used for detecting and mitigating network attacks.

Disadvantage

Lack of Experimental Validation does not explicitly mention any experimental validation or results to support the effectiveness of the ML/DL methods discussed. It does not address the ethical and privacy considerations associated with the use of ML/DL methods in cybersecurity.

And does not provide a comparative analysis of different ML/DL methods or evaluate their relative strengths and weaknesses. (2)

What are the key advantages of using deep learning techniques for network intrusion detection?

Deep learning techniques offer several advantages for network intrusion detection. Deep learning models can automatically learn representations of complex features from raw network data. This allows for the detection of subtle and previously unseen patterns associated with network attacks. Deep learning models can handle large-scale datasets and process and analyze vast amounts of network traffic in real-time. This enables timely detection and response to network intrusions. Additionally, deep learning models can adapt and learn from new attack patterns, making them more resilient to evolving threats.

What are the challenges associated with using machine learning techniques for cybersecurity?

There are several challenges that need to be addressed. One challenge is the availability and quality of labeled training data.

Machine learning models require substantial amounts of labeled data to learn effectively, but obtaining accurately labeled cybersecurity datasets can be difficult and time-consuming.

Another challenge is the high dimensionality and complexity of network data, which can make feature extraction and selection challenging. Additionally, machine learning models may struggle with detecting unknown or zero-day attacks that have no previous training examples.

Study 3

Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey

Abstract

Networks play an important part in new life, and cybersecurity has become a research area. Intrusion Detection Systems (IDSs) are essential cybersecurity techniques that monitor the state of software and hardware in a network. existing and still face challenges in improving detection accuracy, reducing false alarm rates, and detecting unknown attacks. Machine learning algorithms can automatically identify the differences between normal and abnormal data with high accuracy and can detect unknown attacks due to their generalizability. clarifies the concept and taxonomy of IDSs, introduces frequently used machine learning algorithms, metrics, and shows how to solve key IDS issues ML and DL techniques. Also discusses challenges and future developments in IDSs. Liu & Lang (2019)

Introduction

A Survey" focuses on the application of machine learning and deep learning techniques in Intrusion Detection Systems (IDSs).

Despite advancements in IDS technology, challenges such as improving detection accuracy, reducing false alarm rates, and detecting unknown attacks persist. Deep learning, a subset of machine learning, has gained significant attention for its exceptional performance. And show taxonomy of IDSs that classifies and summarizes machine learning-based and deep learning-based approaches, with a focus on data objects, also discusses challenges and future developments in the field of machine learning-based IDSs.

Key search

machine learning, deep learning, intrusion detection system, cybersecurity.

Advantage

provides a comprehensive overview of the application of machine learning and deep learning methods in Intrusion Detection Systems (IDSs).

Taxonomy framework offers a structured approach to categorize and summarize the existing research on machine learning-based and deep learning-based IDSs. Challenges faced by existing IDSs highlight potential future developments in machine learning based IDSs.

Disadvantage

The paper focuses on representative papers published from 2015 to 2019, which may result in a limited scope and overlook recent advancements in the field.

ack of Practical Implementation Details

Study 4

Machine learning in cybersecurity: A review

Abstract

Machine learning has become an integral part of various domains, including cybersecurity. This review shows the applications of machine learning techniques in cybersecurity and discusses the challenges posed by adversarial attacks on these methods. the need for machine learning algorithms to adapt to dynamic and evolving cyber threats. cybersecurity and discusses the challenges posed by adversarial attacks on these methods. The authors highlight several areas where machine learning is being used, such as malware analysis, threat analysis, and anomaly-based intrusion detection. Handa et al. (2019)

Introduction

Machine learning in cybersecurity applications for threat detection and analysis. aims to provide insights into the applications of machine learning in cybersecurity while also discussing the adversarial threats posed to these methods. Review discusses adversarial attacks on machine learning algorithms in cybersecurity. The paper focuses on specific applications of machine learning in cybersecurity and the potential adversarial attacks that can compromise the security of these systems.

Key search

cybersecurity, algorithms, Machine learning, Malware analysis

Advantage

The review provides a comprehensive overview of the applications of machine learning in cybersecurity.

Show highlights the challenges posed by adversarial attacks on machine learning algorithms in cybersecurity and examples of the application of machine learning in cybersecurity.

Disadvantage

Lack of Specificity

Incomplete Coverage of Adversarial Attacks:

Lack of Recent Developments

Protective systems for one ML model may not work for others.

Privacy compromise due to data exchange in collaborative learning.

What are some examples of cybersecurity applications where machine learning techniques are being used?

There are many examples of cybersecurity applications where machine learning techniques are employed. Some of these examples include malware analysis, especially for zero-day malware detection, threat analysis, and anomaly-based intrusion detection of prevalent attacks on critical infrastructures. These applications demonstrate the effectiveness of machine learning in addressing the limitations of signature-based methods and detecting new or variant attacks in cybersecurity.

Study 5

A Survey of Artificial Intelligence Techniques for Cybersecurity Improvement

Abstract

discusses the need for innovative cybersecurity approaches and the role of artificial intelligence (AI) in enhancing security systems, particularly intrusion detection systems. The paper highlights the advantages of AI in improving cybersecurity, such as its ability to handle large volumes of data and quickly identify and recover from threats. It also acknowledges the potential risks associated with AI, including the manipulation of AI methods for malicious purposes. Alrajhi (n.d.)

Introduction

Shows the concept of artificial intelligence (AI) and its significance in performing tasks associated with intelligent beings. The growth of AI over the past two decades is acknowledged, and it is categorized into weak AI and strong AI. Weak AI refers to systems that perform intelligent tasks without true understanding, while strong AI possesses human-like intelligence and self-awareness. highlights that integrating AI into security systems can significantly reduce cybersecurity. Explore how AI can enhance cybersecurity, specifically focusing on intrusion detection systems. It discusses the limitations of traditional fixed techniques in defending against dynamically evolving security attacks. The detection and prevention of intelligent attacks require an intelligent tool, and AI techniques can play a crucial role in this regard. The paper mentions various AI methods that can be employed for cybercrime detection and prevention, such as neural networks, deep learning, intelligent agents, and pattern recognition.

Advantage

provides a comprehensive overview of artificial intelligence techniques for cybersecurity improvement. It covers various AI methods, such as neural networks, deep learning, and pattern recognition. provides up-to-date information on the subject matter. It discusses the growing importance of cybersecurity and the need for innovative approaches, highlighting the role of AI in addressing these challenges. How AI techniques can enhance cybersecurity by handling large volumes of data and aiding in the recovery process. It emphasizes the practical implications of integrating AI into security systems and how it can improve the performance and effectiveness of defense mechanisms.

Disadvantage

aims to provide a survey of AI techniques for cybersecurity improvement, it may lack in-depth analysis and detailed explanations of specific AI algorithms or methodologies. The paper does not mention any specific experiments or case studies to support the effectiveness of the discussed AI techniques. This does not explicitly discuss any potential biases or limitations in its approach. As with any research, the authors' perspectives and biases may influence the presentation and interpretation of the information.

Key search

AI methods, pattern recognition, cybersecurity

What are the potential risks associated with artificial intelligence in cybersecurity?

The paper acknowledges that while artificial intelligence (AI) techniques can enhance cybersecurity, there are potential risks involved. One of the risks is the possibility of AI methods being manipulated to perform malicious activities and steal classified information. Attackers can exploit vulnerabilities in AI systems, resulting in biased or inaccurate outcomes. Adversarial attacks, where attackers intentionally manipulate AI models to evade detection or cause false positives, are also a concern. Therefore, it is crucial to ensure the robustness and security of AI systems to mitigate these risks and protect against potential threats.

Study 6

Machine Learning and Deep Learning Approaches for Cybersecurity: A Review

abstract

explores the use of machine learning and deep learning algorithms in intrusion detection systems. Artificial intelligence subfields such as machine learning and deep learning have emerged as successful approaches to address this problem. reviews various intrusion detection systems and discusses the learning algorithms employed by machine learning and deep learning to protect data from malicious behavior.

Introduction

Cybersecurity, defined as the implementation of measures and policies to protect data, programs, servers, and network infrastructures from unauthorized access or modification, has become crucial. Intrusion detection is a subset of network security that aims to safeguard networked computers and ensure data security, integrity, and accessibility. AI, ML, and DL are terms often used interchangeably to describe machines programmed to learn and find optimal solutions to problems. DL is a subfield of ML, which, in turn, is a subfield of AI. Deep learning, a subfield of machine learning, is introduced as a powerful approach that can learn from unstructured or unlabeled data.

Advantages

provides a comprehensive review of machine learning and deep learning approaches for cybersecurity, including network implementations, algorithms, specifically focusing on intrusion detection systems. Integration of AI Subfields. integrates the concepts of artificial intelligence (AI), machine learning (ML), and deep learning (DL). It clarifies the relationship between these subfields and their application in addressing cybersecurity challenges. discusses recent machine learning and deep learning work with real-world network

implementations, applications, and datasets. insights into the operational aspects of building intrusion detection systems.

Disadvantages

The paper does not provide specific examples or case studies to illustrate the application of machine learning and deep learning techniques in intrusion detection systems. This absence of concrete examples may limit the readers' understanding of how these techniques are employed in real-world scenarios.

How does the paper address the evolving nature of cyber-attacks and the need for adaptive intrusion detection systems?

by focusing on machine learning and deep learning approaches. These approaches can learn from new and unknown attack patterns, allowing intrusion detection systems to adapt and detect emerging threats.

Reference:

- Alrajhi, A. M. (n.d.). *A Survey of Artificial Intelligence Techniques for Cybersecurity Improvement*.
- Halbouni, A., Gunawan, T. S., Habaebi, M. H., Halbouni, M., Kartiwi, M., & Ahmad, R. (2022). Machine Learning and Deep Learning Approaches for CyberSecurity: A Review. In *IEEE Access* (Vol. 10, pp. 19572–19585). Institute of Electrical and Electronics Engineers Inc. <https://doi.org/10.1109/ACCESS.2022.3151248>
- Handa, A., Sharma, A., & Shukla, S. K. (2019). Machine learning in cybersecurity: A review. In *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery* (Vol. 9, Issue 4). Wiley-Blackwell. <https://doi.org/10.1002/widm.1306>
- Li, J. hua. (2018). Cyber security meets artificial intelligence: a survey. In *Frontiers of Information Technology and Electronic Engineering* (Vol. 19, Issue 12, pp. 1462–1474). Zhejiang University. <https://doi.org/10.1631/FITEE.1800573>
- Liu, H., & Lang, B. (2019). Machine learning and deep learning methods for intrusion detection systems: A survey. In *Applied Sciences (Switzerland)* (Vol. 9, Issue 20). MDPI AG. <https://doi.org/10.3390/app9204396>
- Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., Gao, M., Hou, H., & Wang, C. (2018). Machine Learning and Deep Learning Methods for Cybersecurity. *IEEE Access*, 6, 35365–35381. <https://doi.org/10.1109/ACCESS.2018.2836950>