

Research problem

1.

Problem domain

The need for specific defense and protection techniques in cybersecurity to address the challenges faced by artificial intelligence models in the face of cyber threats. Emphasizing the necessity of combating adversarial and preserving privacy in machine learning.

Problem description

It is a weakness in artificial intelligence models facing cyber threats, which can lead to disruption of their learning and decision-making processes. Artificial intelligence models need effective and effective defense methods to confront these threats and to ensure the safety and security of the artificial intelligence system.

Highlighting the importance

considered in the increasing integration of artificial intelligence technologies in various fields, including cybersecurity. It is important to address security concerns related to AI (Artificial Intelligence) models to ensure trust and credibility of AI systems. By exploring the intersection between artificial intelligence and cybersecurity, researchers can develop innovative defensive methods and techniques to protect artificial intelligence models from cyber threats.

Existing solutions

Adopting usual machine learning methods and deep learning solutions to combat cyber-attacks using artificial intelligence. It discusses methods of defending against hostile attacks, such as modifying the network structure, using external models as additions to the network, and modifying the training process or input samples. He focused on the emergence of distributed learning patterns such as federated learning and the need to protect privacy in building a secure AI system.

The objective of this problem

- To develop robust defensive methods and techniques to protect AI models from malicious attacks and ensure the security and integrity of AI systems.
 - By addressing challenges at the intersection of cybersecurity and artificial intelligence, researchers can help develop safe and reliable AI applications.
- To review the intersection between AI and cybersecurity, summarize and analyze current research efforts in combating cyberattacks using AI and counterattacks to which AI models may be exposed, and identify corresponding defense methods.
- To explore how to build encrypted neural networks and achieve secure deep learning to build a secure artificial intelligence system.
- The need for continuous research is justified by the continuous and increasing reliance on artificial intelligence technologies and the sophistication of cyber threats.

2.

Problem domain

There is a need to improve intrusion detection systems (IDSs) in cybersecurity. Current IDS systems face difficulties in detection accuracy and the ability to identify unknown attacks. These challenges arise due to the constantly evolving nature of network environments and the emergence of new, evolving attacks.

The significance of addressing

This problem lies in the importance of cybersecurity in today's evolving life and the constant influence of networks. IDS systems play a critical role in protecting networks from internal and external attacks by monitoring the states of software and hardware in the network. By improving detection accuracy and reducing false alarms, IDS can provide better security and reduce the burden on security analysts. Plus, the ability to detect previously unknown attacks is vital to staying ahead of emerging threats.

Existing solutions

This problem involves applying machine learning methods in IDS systems. Machine learning techniques can automatically detect differences between normal and abnormal data with high accuracy. They have strong generalization ability, which makes them able to detect unknown attacks. Deep learning, which is a branch of machine learning, has been able to show remarkable performance and has become a vital research point in this field.

The objective of this research

- To classify the machine learning-based IDS proposed to date, and analyze the steps to address basic IDS problems,
- To discuss the difficulties and future developments in this field. The research aims.
- To provide a classification scope for cybersecurity researchers, enabling them to understand the application of machine learning and deep learning techniques in information detection systems (IDS) and identify study ideas for problems.
- There is a need for research in this field into the limitations imposed on current IDS systems and deep learning methods to overcome these limitations.
- By conducting a comprehensive survey and analysis of the literature, researchers can identify the most effective techniques and methods for improving IDS performance.
- This research can contribute to the development of more robust and efficient IDS systems, enhancing cybersecurity in various network environments.