PHD ASSISTANCE
YOUR TRUSTED MENTOR SINCE 2001

An Overview of Cyber Security Data Science from a Perspective of Machine Learning

Today Discussion

Introduction

Machine learning tasks in cyber security

Supervised learning

Unsupervised learning

Neural networks and deep learning

Conclusion and future work

Introduction

- The information and communication technology (ICT) sector has advanced significantly over the past fifty years and is now pervasive and tightly intertwined with our contemporary society.
- As a result, the security policymakers have recently shown a great deal of worry over the protection of ICT applications and systems from cyber-attacks.
- Cyber security is currently a term used to describe the process of defending ICT systems from multiple cyber threats or attacks.
- The analysis of various cyber-attacks and the development of defense techniques that preserve several qualities described as below are the main issues with cyber security (Alhayani et al., 2021).

01.

Information access and disclosure to unauthorized parties, systems, or entities are prevented by the confidentiality attribute.

02.

Integrity is a quality that helps to stop any unauthorized changes to or deletions of data.

03.

A property called availability is used to guarantee prompt and dependable access to data assets and systems for a designated entity.

- The word "cyber security" refers to a range of situations, including commercial and mobile computers, and can be broken down into a number of standard categories.

- These include information security, which primarily focuses on the security and privacy of pertinent data, application security, which considers keeping software and devices free of risks or cyber-threats, network security, which primarily focuses on protecting a computer system from cyber attackers or intruders, and operational security, which also includes the procedures for handling and protecting data assets.

- Network security devices and computer security systems with a firewall, antivirus programme, or intrusion detection system make up typical cyber security systems.

Machine learning tasks in cyber security

- Machine learning (ML) is sometimes regarded as a subset of "Artificial Intelligence," and it is strongly related to data science, data mining, and computational statistics.

- It focuses on teaching computers to recognize patterns from data. Machine learning models, which could be crucial in the field of cyber security, often consist of a collection of rules, techniques, or intricate "transfer functions" that can be used to uncover interesting data patterns or to recognize or anticipate behavior.

- Here, we'll go through various approaches for handling machine learning problems and how they relate to cyber security issues (Assistance, 2022).

Supervised learning

- When specified goals are established to achieve from a particular set of inputs, or when using a task-driven approach, supervised learning is carried out.

- Regression and classification methods are the most widely used supervised learning techniques in the field of machine learning. These methods are frequently used to categorize or forecast the future of a specific security issue.

- For instance, classification methods can be utilized in the cyber security field to forecast denial-of-service attacks (yes, no), or to recognize various classes of malicious activities like scanning and spoofing.

- The well-known classification methods are ZeroR, OneR, Navies Bayes, Decision Tree, K-nearest neighbors, Support Vector Machines, Adaptive Boosting, and Logistic Regression.

Unsupervised learning

- Finding patterns, frameworks, or knowledge in unlabeled data, or using a data-driven strategy, are the main objective in unsupervised learning problems.
- Malware, a form of cyber-attack, hides itself in some ways, changing its behavior constantly and autonomously to evade detection.
- Unsupervised learning methods like clustering can be used to extract hidden structures and patterns from datasets to find clues to such complex attacks.
- Similar to this, clustering approaches can be helpful in locating anomalies, finding and removing rules breaches, and noisy examples in data. The well-liked hierarchical clustering techniques employed in numerous application domains include single linkage or complete linkages, K-means, and K-medoids.

Neural networks and deep learning

- Deep learning is a type of machine learning, a subset of artificial intelligence that takes cues from biological neural networks seen in the human brain.

- The most widely used neural network algorithm is back propagation, and artificial neural networks (ANN) are extensively employed in deep learning (Aversano et al., 2021).

- It executes learning on an input layer, one or more hidden layers, and an output layer of a multi-layer feed-forward neural network. Deep learning performs better as the volume of security data increases, which is the primary distinction between it and traditional machine learning.

- Typically, deep learning algorithms work best with vast amounts of data, whereas machine learning techniques work well with smaller datasets.

Conclusion and future work

- The implementation of a strong framework that allows data-driven decision making is the most crucial task for a smart cyber security system (Assistance, 2021).
- To make such a framework capable of minimizing these problems and offering automated and intelligent security services, enhanced data analytics based on machine learning approaches must be taken into account.
- As a result, developing a data-driven security model for a specific security issue as well as related empirical evaluation to gauge the model's efficacy and efficiency and determine its suitability for use in actual application domains may be future works.
- Further in order to develop a professional research proposal or dissertation in cyber security applications kindly get in touch with PhD assistance for a best and standard service.

References

- Alhayani, B., Jasim Mohammed, H., Zeghaiton Chaloob, I. & Saleh Ahmed, J. 2021. WITHDRAWN: Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry. Materials Today: Proceedings.

- Assistance, P. 2021. Scope And Significance Of Data Science In Cybersecurity.

- Assistance, P. 2022. The Contribution of Machine Learning in Cyber security.

- Aversano, L., Bernardi, M.L., Cimitile, M. & Pecori, R. 2021. A systematic review on Deep Learning approaches for IoT security. Computer Science Review. (40). pp. 100389.

Contact Us

UK: +44 7537144372

INDIA: +91-9176966446

info@phdassistance.com