**A Survey On Security Analysis Of Machine Learning- Oriented Hardware And Software Intellectual Property**

**Problem Statement**

According to the article “A survey on security analysis of machine learning-oriented hardware and software intellectual property” by Ashraful Tauhid, whatever the existing intellectual property (IP) protection mechanisms, such as patents, copyrights, etc., are insufficient in preventing unauthorized modifications and theft of IP entities. There is a need for strong and effective IP protection techniques, both in hardware and software domains.

**Summary**

The article discusses the vulnerabilities of intellectual property and the inadequacies of current IP protection regulations. It examines the domain of Intellectual Property Protection (IPP) and presents different approaches and techniques for protecting hardware IP and software IP. The article also points the applications of IP protection and identifies the challenges and future research towards hardware and software IP security. Machine Learning based approaches are discussed as a favorable solution for IP protection.

**Approach and Solution**

This article suggests that both hardware and software IP protection techniques are important to secure IP entities effectively. In the hardware domain, techniques such as hardware obfuscation, hardware metering, split manufacturing, logic locking, fingerprinting, watermarking and IC camouflaging are proposed as generic approaches. For software IP protection, fingerprinting, watermarking, stenographic techniques, code obfuscation and surprisal analysis are mentioned. Moreover, Machine Learning (ML) is presented as a recent alternative to protect both hardware and software IPs. Different ML techniques, along with Convolutional Neural Networks (CNN), Generative Adversarial Network (GAN), and Deep Neural Networks (DNN) are used to detect and defend against attacks on IP entities.

**Critical Points – Strong and Weak Points**

**Strong Points:**

1. The article provides a complete overview of IP protection, covering both hardware and software domains.
2. It discusses about various existing IP protection techniques and their applications.
3. It is concentrating on machine learning approaches for IP protection, giving future direction for research.
4. The introduction of specific examples and detection mechanisms for different IP attacks shows the article’s practicality.

**Weak Points:**

1. The article lacks specific details and technical depth in explaining the discussed IP protection techniques.
2. The limitations and inherent weakness of the proposed approaches are not extensively addressed.
3. The article does not provide equivalent or relevant analysis of different IP protection techniques or actual evidence of their effectiveness.

**Missing Technology**

The article would have mentioned about utilization of block chain technology in IP protection. Block chain has the ability to provide secure and immutable records of IP ownership, by preventing unauthorized modifications and ensuring trust in the IP registration process.

**Proposing a better solution**

Based on the findings from the article, I believe that in order to enhance IP protection, an extensive approach can be adopted by combining legal measures, technical solutions, and block chain technology. By developing strong algorithms and methodologies for IP protection and more in-depth research on machine learning techniques and their limitations can lead to more success in IP security. Additionally by considering block chain technology in IP protection system can provide a better tamper-proof platform for IP registration and enforcement. Then there is more chance of transparency, traceability, and trust in the IP ecosystem, reducing the risks of infringement and theft.

**References**

Tauhid, A., Xu, L., Rahman, M., & Tomai, E. (2023). A survey on security analysis of machine learning-oriented hardware and software intellectual property. High-Confidence Computing, 100114.