Smart Internz

Project Name

MALWARE DETECTION AND CLASSIFICATION

ANMOL KANT
MILAN RATH
BHUPESH

PROJECT DESCRIPTION

In today's digital landscape, malware is a significant threat to the security of organizations' digital assets. The "Malware Detection and Classification the development of an advanced system that harnesses the power of artificial intelligence to identify and categorize different types of malware accurately. Organizations can bolster their cybersecurity defenses by leveraging cutting-edge AI techniques, proactively detecting malicious software, and enhancing their incident response capabilities.

PROJECT PROBLEM STATEMENT:

Malware is a malicious program that causes damage to files and information systems. cyber attackers have been using different techniques to spread malware for monetary and other reasons. Attackers have economic benefits in making such attacks. Artificial Intelligence techniques have evolved rapidly in recent years, revolutionizing the approaches used to fight against cybercriminals. But as the cyber security field has progressed, so has malware development, making it an economic imperative to strengthen businesses' defensive capability against malware attacks. Here we see AI techniques used in malware detection and prevention, providing an in-depth analysis of the latest studies in this field. The problem at hand is the need to develop effective strategies and solutions to mitigate malware attacks in systems. Existing security measures often fall short of protecting devices and networks from sophisticated malware attacks.

ABSTRACT:

In today's era, Malware is continuously growing in sophistication and numbers. Over the last decade, remarkable progress has been achieved in anti-malware mechanisms. There is fast development in the field of Information Technology. It is a matter of great concern for cyber professionals to maintain security and privacy. Studies revealed that the number of new malware is increasing tremendously. It is a never-ending cycle between the world of attack and the defense of malicious software. Antivirus companies are always putting their efforts into developing signatures of malicious software and attackers are always trying to overcome those signatures. For the detection of malware, we use an AI-based system to identify targets. The process of

detection of malware is split into two categories first is feature extraction and the second is malware classification. In this paper, firstly an in-depth study of the features is provided that can be used to differentiate malware. Artificial Intelligence techniques have evolved rapidly in recent years, revolutionizing the approaches used to fight against cybercriminals. But as the cyber security field has progressed, so has malware development, making it an economic imperative to strengthen businesses' defensive capability against malware attacks. This review outlines the state-of-the-art AI techniques used in malware detection and prevention, providing an in-depth analysis of the latest studies in this field. This work also touches on the rapid adoption of AI by cybercriminals as a means to create ever more advanced malware and exploit the AI algorithms designed to defend against them.

OBJECTIVES:

AI models for malware classification and Detection are a powerful tool for detecting and identifying malicious software. By using AI models, organizations can improve their security posture and protect themselves from a wide range of malware threats.

#) Malware Detection Approaches:

1. **Dynamic Deep Learning-Based Methods: A new systematic approach to identifying modern malware uses dynamic deep learning-based methods combined with heuristic approaches. This method can classify and detect five modern malware families: adware, Radware, rootkit, SMS malware, and ransomware1.**

2. **Shallow Learning, Deep Learning, and Bio-Inspired Computing: These AI techniques are used in malware detection and prevention. They provide an in-depth analysis of the latest studies in this field.**

#)Malware Classification Approaches:

- **MalwareNet: MalwareNet is a deep learning model that was developed by researchers at the University of California, Berkeley. MalwareNet is a convolutional neural network that is trained to classify malware samples based on their images.**
- **DeepGuard: DeepGuard is a deep learning model that was developed by researchers at the University of Texas at Austin. DeepGuard is a recurrent neural network that is trained to classify malware samples based on their opcodes.**
- **CylancePROTECT: CylancePROTECT is a cloud-based endpoint security solution that uses AI to detect and block malware infections. CylancePROTECT uses a variety of AI models, including MalwareNet and DeepGuard, to classify malware samples.**

Current Trends:

Google AI is using deep learning to detect malware in Android apps: Google AI has developed a deep learning model called Neural Networks for Malware Detection (NeuralNetMD) that can detect malware in Android apps with high

accuracy. NeuralNetMD is used to scan all Android apps submitted to the Google Play Store.

Microsoft is using AI to improve Windows Defender Antivirus: Microsoft is using AI to improve the detection and classification of malware in Windows Defender Antivirus. Microsoft is also using AI to develop new features for Windows Defender Antivirus, such as the ability to detect malware in real-time.

Cisco is using AI to develop a new generation of security products: Cisco is using AI to develop a new generation of security products that can detect and block a wide range of malware threats. Cisco's AI-powered security products can be deployed on endpoints, networks, and in the cloud.

These are just a few examples of how AI is being used to improve malware detection and classification. As AI technology continues to develop, we can expect to see even more innovative and effective ways to use AI to combat malware threats.

REFERENCES:

[1] M. Fichtenkamm, G. Burch, J. Burch, “Cybersecurity in a COVID-19 World: Insights on How Decisions Are Made.” libraryguides.vu.edu.au. https://www.isaca.org/resources/isacajournal/issues/2022/volume-2/cybersecurity-in-a-covid-19-world (accessed September 12, 2022).

[2] S. Morgan, “Cybercrime to Cost the World $10.5 Trillion Annually by 2025.” cybersecurityventures.com https://cybersecurityventures.com/hackerpocalypse-cybercrimereport-2016/ (accessed September 12, 2022).

[3] Deloitte, “Cybercrime – the risks of working from home.” deloitte.com https://www2.deloitte.com/ch/en/pages/risk/articles/covid-19-cyber-crime-working-fromhome.html (accessed September 13, 2022). [4] C. Nabe, “Impact of COVID-19 on Cybersecurity.” deloitte.com https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html (accessed September 14, 2022).

[4] C. Nabe, “Impact of COVID-19 on Cybersecurity.” deloitte.com https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html (accessed September 14, 2022).