ABSTRACT

The proliferation of malware poses a significant threat to the security and privacy of computer systems and networks. This abstract provides an overview of the current state of research in malware detection and classification, a critical area in cybersecurity. Malware refers to a broad range of malicious software, including viruses, worms, trojans, ransomware, and spyware, designed to compromise the integrity of systems and steal sensitive information.

This review highlights the importance of developing robust and efficient techniques for the detection and classification of malware. Traditional signature-based methods are no longer sufficient to combat the evolving landscape of malware, leading to the emergence of more advanced approaches. These modern techniques include behavior analysis, machine learning, deep learning, and artificial intelligence. They focus on identifying malware based on its behavior, characteristics, or structure, providing enhanced detection capabilities.

The abstract discusses the challenges in the field, such as the emergence of polymorphic and metamorphic malware that can change their signatures to evade detection. It also addresses the need for large and diverse datasets to train and evaluate malware detection models effectively. Furthermore, the abstract explores the trade-offs between accuracy, speed, and resource consumption in malware detection systems.

In summary, the research in malware detection and classification continues to evolve to meet the dynamic threat landscape. New techniques and models are being developed to enhance detection accuracy while minimizing false positives and negatives. This abstract serves as an introduction to the complex and critical field of malware analysis, which is crucial for safeguarding digital assets and ensuring the security of information systems.