Digital Receipt

This receipt acknowledges that Turnitin received your paper. Below you will find the receipt information regarding your submission.

The first page of your submissions is displayed below.

Submission author:	Araharan Loganayagam
Assignment title:	E1: Literature Review
Submission title:	21524785_2_new.pdf
File name:	21524785_2_new.pdf
File size:	142.69K
Page count:	20
Word count:	7,642
Character count:	45,528
Submission date:	30-Apr-2023 10:11PM (UTC+0100)
Submission ID:	204050196

An Analysis of Blockchain-and ML based Malware Detection and Integrity Checking Systems

Name: Araharan Loganayagam
Student Id: 21524785
School of Computing and Engineering
University of West London
21524785@student.uwl.ac.uk

Supervisor: Dr Waqar Asif
Senior Lecturer in Computing Science and Cyber Security
School of Computing and Engineering
waqar.asif@uwl.ac.uk

Abstract—This review paper provides an overview of the current state of malware detection and integrity checking techniques, highlighting their limitations and challenges. The review then focuses on the use of blockchain technology and machine learning algorithms for malware detection and integrity checking. First, the paper provides a review of the use of blockchain technology for security purposes, highlighting its potential benefits in providing a secure and decentralized platform for malware detection and integrity checking. The paper then discusses the use of machine learning algorithms for malware detection, analysing the different approaches proposed in existing literature. The paper also discusses the limitations and challenges of these approaches, including the need for large datasets and the risk of false positives. The integration of machine learning algorithms enables the system to learn and adapt to new threats, improving its effectiveness over time. The review concludes with a discussion of future directions and emerging trends in blockchain-and ML based malware detection and integrity checking.

Keywords— NLP, Malware, Blockchain, CNN, Cloud, Integrity, Cryptography, RAID

Introduction

In recent years, malware attacks have become increasingly prevalent, sophisticated and pose a significant threat to the security of computer systems and networks. To address this challenge, researchers have developed various malware detection and integrity checking techniques, ranging from traditional signature-based methods to more advanced machine learning and blockchain-based approaches. While these techniques have been successful in detecting and preventing malware attacks, the ever-evolving nature of malware requires continued research and innovation to stay ahead of threats. This literature review will focus on the current state of malware detection and integrity checking techniques, specifically exploring the potential of a decentralized approach

Copyright 2023 Turnitin. All rights reserved.