INFORMATICS INSTITUTE OF TECHNOLOGY

INFORMATICS INSTITUTE OF TECHNOLOGY

In Collaboration with

UNIVERSITY OF WESTMINSTER

DDoS Attack Mitigation in Content Delivery Networks using Blockchain and Machine Learning

Dissertation by

Mr. A. Panitha Dineth Bimsara.

UoW student ID: w1869953

IIT Student ID: 20210995

Supervised by

Mr. Sithira Hewaarachchi

Submitted in partial fulfilment of the requirements for the MSc in Cyber Security and Forensics degree at the University of Westminster.

September 2023

Abstract

Distributer Denial of Services attacks remain a persistent and severe threats to internet and internet infrastructure and services, causing significant financial losses and disrupting critical online operations. This these address the escalating challenges of combating DDoS attacks that against the content delivery networks by proposing and innovative conceptual framework that integrates with serval technologies like Machine learning, blockchain.

The first part of the research focuses on developing a framework for ML-based DDoS detection system capable of identifying and mitigating attack traffic in real-time. Using machine learning built in solution analysis and dataset analysis, a feature-rich model is proposed to recognize attack patterns, thereby enabling early identification and timely response to evolve attack techniques. The second part of the thesis introduces a novel Blockchain-based reputation system, which use for a secure and decentralized environment for communication and cooperation between CDN nodes. By leveraging the transparency and immutability of Blockchain, the proposed reputation system ensures the trustworthiness and accountability of CDN nodes, promoting collaboration to handle DDoS attacks more effectively.

The final segment explores the integration of Content Delivery Networks with the ML-based detection and the Blockchain reputation system. This integration empowers CDNs to distribute network traffic efficiently, optimize resource allocation, and proactively defend against DDoS attacks across distributed server locations. Therefore, the proposed conceptual framework not only bolsters network performance but also enhances DDoS resilience by quickly diverting and filtering malicious traffic at the network's edge.

To evaluate the effectiveness of the proposed conceptual framework, Self-evaluation and expert evaluation has done. The results demonstrate significant improvements in attack detection effectiveness, architecture and overall network robustness.

In conclusion, this thesis contributes to the ongoing efforts to combat DDoS attacks by providing an innovative approach that leverages the potential of Machine Learning, Blockchain technology, and Content Delivery Networks. The integrated framework offers a comprehensive and powerful solution to mitigate DDoS attacks, safeguard network infrastructure, and preserve the uninterrupted functionality of critical online services.