Mitigating Distributed Denial of Service Threats with Machine Learning-Powered Intrusion Detection System

Kalp Chiragkumar Gandhi

Department of Computer Science and Engineering
National Institute of Technology Rourkela

Mitigating Distributed Denial of Service Threats with Machine Learning-Powered Intrusion Detection System

A report submitted in partial fulfillment

of the requirements for the degree of

Bachelor of Technology

in

Computer Science and Engineering

by

Kalp Chiragkumar Gandhi

(Roll Number: 120CS0661)

based on research carried out

under the supervision of

Prof. Manmath Narayan Sahoo

Nov, 2023

Department of Computer Science and Engineering
National Institute of Technology Rourkela

Acknowledgment

First and foremost, I'd want to convey my heartfelt thanks to my supervisor, Dr. Manmath Narayan Sahoo, for his invaluable guidance during my research. He has consistently pushed me to stay focused on my objective. His observations and suggestions aided me in determining the research's broad direction and moving forward with in-depth inquiry. He has been a tremendous source of information and assistance to me. For his support and encouragement, I appreciate our department's HOD, Prof. Bibhudatta Sahoo, along with all the department's academicians and faculties.

I owe a debt of gratitude to my classmates who assisted me with course work and thesis writing. I am very grateful to everyone who has given me nice words, a sympathetic ear, fresh ideas, constructive criticism, or their important time.

I must thank NIT Rourkela for providing me with academic resources. I'd want to express my gratitude to the Department's administrative and technical staff members who have been willing to offer advice and assistance in their various jobs. Last but not least, I'd want to express my gratitude for my parents' love, support, and drive, and therefore I dedicate my thesis to them.

Nov 14, 2023
NIT Rourkela

Kalp Chiragkumar Gandhi
120CS0661

Abstract

Cloud computing has revolutionized the way we store, access, and manage data and services by offering unparalleled flexibility and scalability. However, in this digital era, ensuring the security of cloud-based systems is paramount. The importance of security in cloud computing cannot be overstated, as these platforms handle vast amounts of sensitive data and critical applications. One of the most persistent and damaging threats in the world of cloud security is Distributed Denial of Service (DDoS) attacks. DDoS attacks involve overwhelming a target system with a flood of traffic from multiple sources, rendering it inaccessible to legitimate users. These attacks can disrupt businesses, causing financial losses and tarnishing reputations. Many possible solutions are there to tackle DDoS threats, such as deploying content delivery networks (CDNs) to distribute traffic, employing traffic filtering and rate limiting techniques, leveraging load balancing systems, and utilizing specialized DDoS mitigation services provided by third-party vendors. While these methods have their merits, I will be utilising a machine learning-based Intrusion Detection System (IDS) because it offers the advantage of adaptability, making it well-suited to counter the evolving and complex nature of DDoS attacks. This IDS will swiftly identify and respond to DDoS attack patterns in real-time, fortifying the security of cloud-based systems and ensuring uninterrupted access for users.

Contents

List of Figures

Chapter 1

Introduction

1.1 Context

In the realm of computer science engineering, cloud computing has emerged as a transformative force, reshaping how organizations manage and deliver their services. Its promise of scalability, flexibility, and cost-efficiency has led to widespread adoption, becoming an indispensable element of modern IT infrastructure. However, this evolution has also exposed the cloud to security challenges, with Distributed Denial of Service (DDoS) attacks emerging as a persistent and escalating threat.

This research proposal resides at the intersection of cloud computing and cybersecurity, addressing the vital need to safeguard cloud environments from the disruptive impact of DDoS attacks. These attacks involve a network of compromised devices bombarding a target system with overwhelming traffic, rendering it inaccessible to legitimate users. Due to their distributed nature, they can paralyze cloud-based services, causing financial losses, damage to reputation, and compromised data integrity.

The significance of this research problem in computer science engineering is substantial. Cloud computing has revolutionized organizational operations, offering unprecedented efficiency and scalability. However, cloud service effectiveness relies on security. Ensuring cloud resource availability and resilience against DDoS attacks is crucial for business continuity and sustaining the growth of cloud-based solutions.

This research emphasizes the need for intelligent, adaptive, and context-aware intrusion detection mechanisms tailored to the cloud. By combining traditional DDoS mitigation and machine learning, we aim to create a comprehensive defense framework capable of identifying and mitigating DDoS threats at both the cloud application and control levels.

1.2 Research Problem:

The research problem at the heart of this study revolves around effectively mitigating Distributed Denial of Service (DDoS) threats within cloud computing environments. Specifically, we seek to address the challenge of enhancing cloud security by implementing a machine learning-powered Intrusion Detection System (IDS) capable of identifying and countering DDoS attacks at multiple levels within the cloud infrastructure.

The rationale for choosing this problem is deeply rooted in the transformative impact of cloud computing on contemporary information technology. Cloud environments have become the backbone of modern enterprises, offering unparalleled scalability and cost-efficiency. However, this evolution has simultaneously exposed cloud systems to an escalating threat landscape, with DDoS attacks emerging as a persistent and highly damaging menace.

The relevance of this research problem is evident in its implications for both cloud service providers and users. Cloud service providers rely on the trust and confidence of their clients, making the security and availability of cloud resources paramount. A successful DDoS attack not only disrupts services but also jeopardises an organisation's reputation, potentially leading to financial losses and legal liabilities. Users of cloud services, including businesses and individuals, entrust their critical data and applications to cloud providers, making them reliant on the security measures in place.

1.3 Motivation and Objective

The motivation behind this research stems from the escalating threat of Distributed Denial of Service (DDoS) attacks in cloud computing, which can disrupt services and incur substantial losses. As cloud adoption grows, there's a pressing need for a proactive Intrusion Detection System (IDS) powered by machine learning. This research aims to develop such an IDS to bolster cloud security, ensuring the uninterrupted functioning of essential online services.

1.3.1 Objective

The primary objectives of this research are:

- To design and implement an effective Intrusion Detection System (IDS) for cloud computing environments.
- To integrate machine learning techniques into the IDS to enhance its capability to detect and mitigate Distributed Denial of Service (DDoS) threats.
- To evaluate the performance and effectiveness of the proposed IDS through extensive experimentation and analysis.
- To contribute to the field of computer science engineering by providing a practical solution for mitigating DDoS threats in cloud computing, thereby enhancing the security of cloud-based services.

Chapter 2

Literature Review

[1] This research paper explores the critical issue of DDoS attacks in cloud computing, emphasizing their disruptive potential and the challenges associated with their detection. It presents a comprehensive literature review of existing DDoS detection techniques, discussing their advantages and limitations. The paper introduces a novel hybrid model that combines entropy-based and covariance matrix-based approaches to effectively detect DDoS attacks. It highlights the importance of addressing the evolving threat landscape in cloud environments and the potential of the proposed model to significantly enhance detection and mitigation capabilities.

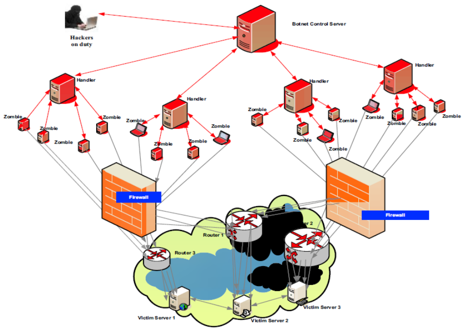

Figure 2.1: Typical DDoS attack organization [1]

[2] The research paper discusses the challenges posed by Distributed Denial of Service (DDoS) attacks in cloud computing. It emphasizes the need for robust detection and prevention mechanisms due to the dynamic nature of cloud environments. The paper reviews various DDoS attack prevention approaches, including machine learning, neural networks, deep learning, software-defined networks, genetic algorithms, blockchain, and Internet of Things (IoT). It also provides an overview of DDoS attack constituents and classifications. While presenting promising prevention methods, the paper acknowledges the ongoing research in this area and the need for efficient mechanisms to counter DDoS attacks in cloud computing environments.

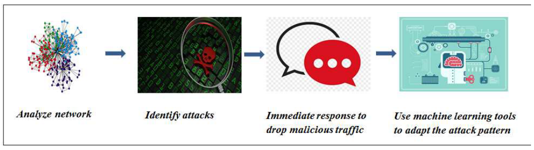
Analyze network
Identify attacks
Immediate response to drop malicious traffic
Use machine learning tools to adapt the attack pattern

Figure 2.2: DDoS prevention using machine learning [2]

[3] The research paper discusses the challenges and solutions related to security in cloud computing. The paper explores the rapid development of cloud computing and its importance in today's IT landscape, highlighting the critical issue of network reliability in cloud environments. It emphasizes the role of Intrusion Detection Systems (IDS) in mitigating security vulnerabilities in the cloud and provides an overview of various cloud-based IDS solutions. The paper proposes Network Intrusion Detection technology as a solution to enhance cloud-based system security. It categorizes security concerns in different cloud service models (SAAS, PAAS, IAAS) and discusses the need for advanced intrusion detection mechanisms to address cloud-specific threats. The research concludes with recommendations for future work, including the integration of AI and machine learning techniques to improve cloud security.

[4] This research paper addresses the critical issue of intrusion detection in cloud computing environments. With the increasing prevalence of security threats in the cloud, the paper highlights the importance of timely intrusion detection to safeguard a company's reputation and finances. The research proposes a solution that leverages machine learning techniques, focusing on the effectiveness and speed of detection. Various machine learning approaches, including statistical models, neural networks, and hybrid techniques, are explored to enhance intrusion detection accuracy. The study concludes with promising results, demonstrating high detection rates and accuracy, making it a valuable contribution to cloud security research.

[5] The research paper addresses the challenge of detecting distributed intrusion attacks in cloud computing environments. The paper introduces a distributed intrusion detection model consisting of two subsystems: the Intrusion Detection Agent subsystem and the Data Aggregation subsystem. The former includes data collection, cloud decision-making, and communication modules, employing an intrusion detection algorithm based on Cloud theory. This algorithm distinguishes normal and abnormal behaviors by computing feature values and degrees of difference. The Data Aggregation subsystem assesses intrusion behavior, warns ID Agents, and adjusts parameters dynamically. The paper also discusses a strategy for defending against DDoS attacks using the elasticity of cloud platforms. This research offers a promising approach to improving intrusion detection and network security in cloud computing environments.

[6] The research paper addresses the limitations of traditional intrusion detection systems (IDSs) in private cloud environments. The paper argues that these traditional IDSs are inadequate for private clouds, as they do not consider cloud-specific mechanisms and network traffic patterns, which can lead to delayed or unnoticed intrusions. To overcome these challenges, the authors propose a unified, multi-level IDS architecture that complements traditional approaches by leveraging knowledge of typical private cloud operations. They provide a case study involving an intruder attempting to manipulate VM-level scheduling in an OpenStack-based private cloud, demonstrating how their approach can significantly enhance security in private cloud deployments. The research highlights the need for cloud-specific intrusion detection mechanisms to protect against various types of attacks, ultimately contributing to the security and viability of private clouds.

[7] The research paper explores the challenges posed by Distributed Denial of Service (DDoS) attacks in cloud computing and investigates various Intrusion Detection Systems (IDS) as a means to mitigate these threats. Cloud computing has gained immense popularity as a business concept, but its security remains a significant concern. DDoS attacks, in particular, have emerged as a top security threat to cloud services, with potentially severe consequences for businesses dependent on the internet. The paper categorizes IDS into host-based, network-based, distributed, and hybrid systems, emphasizing their role in defending against DDoS attacks. It also discusses the benefits and challenges of cloud computing, highlighting the importance of security in its adoption. Overall, the paper underscores the critical role of IDS in safeguarding cloud environments from DDoS threats.

Chapter 3

Proposed Work

3.1 Proposed Approach

1. **Data Collection and Preprocessing:**

    - Gather real-world cloud network traffic data.
    - Clean, extract features, and normalize the data.

2. **Machine Learning Model Selection:**

    - Select effective machine learning models for intrusion detection.
    - Train models on diverse datasets.

3. **Evaluation:**

    - Rigorously test the IDS using simulated attacks and real data.
    - Assess performance using metrics like accuracy and resilience to evasion techniques.

3.2 Methodology

1. **Data Collection:**
   The first step involves acquiring the NSL-KDD dataset, a widely used dataset for intrusion detection system research. This dataset contains a mix of normal and various types of intrusive network activities. The dataset will be divided into training and testing sets to facilitate model training and evaluation.

2. **Data Preprocessing:**

   To enhance the performance of the decision tree classifier, data preprocessing steps will be implemented. This includes handling missing values, encoding categorical variables, and scaling numerical features. Additionally, exploratory data analysis will be conducted to gain insights into the distribution and characteristics of the data.

3. **Feature Selection:**
   Feature selection is crucial for optimizing the decision tree model. Techniques such as information gain and recursive feature elimination will be employed to identify the most relevant features that contribute to the classification accuracy. This step aims to reduce dimensionality and enhance model interpretability.

4. **Model Development:**
   The decision tree classifier will be implemented for intrusion detection. The model will be trained on the preprocessed training data, considering various hyperparameters to fine-tune its performance. The effectiveness of the decision tree model in capturing patterns associated with normal and intrusive network behaviors will be evaluated.

5. **Model Evaluation:**
   The trained model will be evaluated on the separate testing dataset using performance metrics such as accuracy, precision, recall, and F1 score. Receiver Operating Characteristic (ROC) analysis will also be conducted to assess the model's ability to distinguish between normal and intrusive activities.

3.3 Contributions

1. **Improved Cloud Security:** The study improves computer science by creating a Machine Learning-Powered Intrusion Detection System optimised for cloud computing. This improves cloud security, particularly in terms of minimising Distributed Denial of Service (DDoS) attacks.

2. **Improved Accuracy and Robustness:** The project intends to demonstrate improved IDS accuracy by minimising false positives and false negatives through testing and simulation. This helps to create a more precise and strong security system.

3. **Scalability:** The study investigates the scalability of the IDS inside cloud systems, taking into account different network conditions.

4. **Adjustable Security Measures:** The research adds to adaptive security by analysing various DDoS attack types and evasion tactics. The IDS can adapt to successfully address evolving threats.

5. **Future Research Foundation:** The methodology and tests laid the framework for future cloud security research, enabling continued advances in intrusion detection and prevention.

6. **Contribution to Computer Science:** This study adds to the body of knowledge in computer science by addressing the confluence of machine learning, cloud security, and cybersecurity. It helps to guide future study in this area.

Chapter 4

Timeline

1. **Till 1st September 2023 (Completed)**
   Abstract Submission for the research project

2. **Till 5th October 2023 (Completed)**
   Report Submission for the research project consisting sections like

   (a) Research Problem/Hyphthesis

   (b) Research Objectives

   (c) Literature Review

3. **Till November 2023 (Completed)**

   (a) Design and implement the algorithm

   (b) Begin initial testing and simulations to validate the protocol's functionality

   (c) Gather baseline data for evaluation

Chapter 5

Conclusion

Finally, our study aims to address the important issue of mitigating Distributed Denial of Service (DDoS) attacks in cloud computing systems. Recognising the serious implications of these threats for modern IT infrastructure and cloud service reliability, our primary goal is to create a machine learning-powered Intrusion Detection System (IDS) tailored for cloud environments, capable of effectively detecting and mitigating DDoS attacks. Our extensive literature study emphasises the need of effective DDoS detection and prevention technologies in the ever-changing cloud ecosystem. To accomplish our objectives, we developed a methodology that prioritises flexibility, scalability, and energy efficiency in algorithm implementation, which is supplemented by rigorous data collecting, modelling, and simulation. Improved cloud security, effective DDoS mitigation, increased intrusion detection accuracy, scalability, flexibility to evolving threats, practical real-world application, and a solid platform for future cloud security research are all expected contributions. Our dedication remains steadfast as we proceed along our research timetable, driven by the ambition to improve cloud service dependability and advance the area of computer science at the convergence of machine learning, cloud security, and cybersecurity.

References

[1] Girma, A., Garuba, M., Li, J., and Liu, C., 2015. “Analysis of ddos attacks and an introduction of a hybrid statistical model to detect ddos attacks on cloud computing environment”. In 2015 12th International Conference on Information Technology - New Generations, pp. 212–217.

[2] Potluri, S., Mangla, M., Satpathy, S., and Mohanty, S. N., 2020. “Detection and prevention mechanisms for ddos attack in cloud computing environment”. In 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), pp. 1–6.

[3] Snehi, J., Snehi, M., Bhandari, A., Baggan, V., and Ahuja, R., 2021. “Introspecting intrusion detection systems in dealing with security concerns in cloud environment”. In 2021 10th International Conference on System Modeling Advancement in Research Trends (SMART), pp. 345–349.

[4] G, G. R., Santhoshkumar, R., Venkatesan, D., S, K., and Santosh Kumar Patra, P., 2022. “Intrusion detection in cloud architecture using machine learning”. In 2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), pp. 483–487.

[5] Li, H., and Wu, Q., 2012. “A distributed intrusion detection model based on cloud theory”. In 2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems, pp. 435–439.

[6] Humphrey, M., Emerson, R., and Beekwilder, N., 2016. “Unified, multi-level intrusion detection in private cloud infrastructures”. In 2016 IEEE International Conference on Smart Cloud (SmartCloud), pp. 11–15.

[7] Kumar, N., and Sharma, S., 2013. “Study of intrusion detection system for ddos attacks in cloud computing”. In 2013 Tenth International Conference on Wireless and Optical Communications Networks (WOCN), pp. 1–5.

[0] This reference format follows ASME style. You are advised to follow one reference format of any dominant journal of your field.