IJITCE

ISSN 2347- 3657

International Journal of Information Technology & Computer Engineering

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 8, Issue 1, 2020

ANALYZING THE COVARIANCE MATRIX APPROACH FOR DDOS HTTP ATTACK DETECTION IN CLOUD ENVIRONMENTS

Poovendran Alagarsundaram

Project Lead, IBM, Sacramento, North Carolina, United States

Email: poovasg@gmail.com

ABSTRACT

In order to detect Distributed Denial of Service (DDoS) HTTP attacks in cloud environments, this study investigates the potential benefits of combining the covariance matrix method with Multi-Attribute Decision Making (MADM) skills. Evaluating this approach across various cloud settings and thresholds, it delves into data gathering, preprocessing, and anomaly detection. Multivariate analysis and real-time detection are two benefits of the method, which make it worth the complexity. In order to improve its scalability and accuracy, we can better identify DDoS attacks in cloud systems by comprehending its advantages and disadvantages.

Keywords: DDoS, HTTP attacks, covariance matrix, Multi-Attribute Decision Making (MADM), anomaly detection, cloud environments.

1 INTRODUCTION

Web services, especially HTTP-based ones, are vulnerable to serious threats from distributed denial of service (DDoS) assaults. By flooding a website or online service with excessive traffic, these assaults seek to interfere with its regular operation. DDoS assaults can have serious repercussions, including lost revenue, reputational harm, and downtime. Consequently, it is imperative that firms have efficient plans for identifying and averting these kinds of attacks. Covariance matrix analysis is a potentially useful method for identifying DDoS attacks. In order to find unusual patterns that can point to a DDoS attack, this technique computes and examines the covariance matrix of network traffic properties. The idea of covariance matrix analysis is examined in the context of DDoS HTTP attacks in this research, which also offers a thorough description of the method's possible benefits and drawbacks.

An instrument in mathematics for characterizing the correlations between several variables is a covariance matrix. Variables like packet size, packet rate, and protocol distribution may be included in network traffic analysis. The covariance matrix of these features can be used to measure the collective variation of the features. Using the covariance matrix approach, DDoS HTTP attacks are examined in the context of network traffic data collection and feature extraction from HTTP packets. Payload size, response time, and request rate are a few examples of these

ISSN 2347–3657

Volume 8, Issue 1, 2020

characteristics. The covariance matrix is computed after the characteristics are extracted, taking into account their interrelationships.

The analysis's next stage is to find any unusual patterns in the covariance matrix that might point to a DDoS attack. Unexpected shifts in the covariance structure over time or abnormally strong correlations between specific features could be examples of these abnormalities. Keeping an eye on these trends might make it possible to detect and mitigate DDoS assaults more successfully. The covariance matrix approach has various possible benefits when it comes to DDoS detection. Multivariate analysis is a technique that makes it possible to analyze several network traffic aspects at once. When compared to univariate approaches, this thorough analysis of the data might increase the accuracy of DDoS detection. Statistical Soundness: Covariance matrix analysis is a theoretically sound and rigorous method of DDoS detection because it is founded on well-established statistical principles. Increased trust in the outcomes may stem from this.

Flexibility: The covariance matrix technique can be modified to accommodate various DDoS assaults and network configurations. It can be customized to fit certain situations by changing the characteristics included in the analysis and the criteria used to find anomalies. Real-time Detection: Covariance matrix analysis may be carried out in real-time with the right monitoring tools and algorithms, enabling prompt DDoS assault detection and response. This is essential to reducing the effect of attacks and avoiding protracted outages. Resilience to Evasion Techniques: Covariance matrix analysis focuses on discovering aberrant behavior in network data, as opposed to signature-based detection techniques, which identify known attack patterns. This increases its resistance to attackers' evasive strategies. Notwithstanding its possible benefits, the covariance matrix method has many drawbacks.

Complexity: In large-scale or high-speed networks in particular, calculating and interpreting the covariance matrix of network traffic data can be computationally demanding. This could restrict the approach's scalability and render it unfeasible in specific settings. Sensitivity to Feature Selection: Choosing the right network traffic features is essential to the covariance matrix analysis's efficacy. The accuracy of DDoS detection may be weakened if significant features are left out or superfluous features are added. Covariance matrix analysis may result in false positives if typical fluctuations in network traffic are misinterpreted as DDoS assaults. This may cause needless alarms and perhaps interfere with lawful travel. Limited Detection Capability: Although covariance matrix analysis is capable of identifying some DDoS attacks, it might miss more complex or unique attack strategies. Attackers are always changing their strategies, and covariance matrix analysis might not be enough to stay up.

Interpretability: It can be difficult to understand the findings of a covariance matrix study, particularly for those who are not professionals. Not every user has access to statistical ideas and network behavior expertise, which is necessary to comprehend the significance of aberrant patterns

in the covariance matrix. Web services, especially those hosted in cloud environments, are vulnerable to distributed denial of service (DDoS) assaults. By flooding a website or online service with excessive traffic, these assaults prevent it from operating normally. Serious repercussions could result, such as extended downtime, monetary losses, and reputational harm. Organizations must therefore create efficient plans to identify and stop DDoS assaults in cloud environments.

In order to detect DDoS HTTP attacks in cloud systems, this study examines several techniques and discusses the special difficulties, benefits, and drawbacks of each. It also emphasizes how these tactics are incorporated into a more thorough defense plan. DDoS assaults involve several hijacked systems, frequently a component of a botnet, flooding a target system with traffic in an attempt to deplete its resources and prevent legitimate users from accessing it. DDoS attacks that use the HTTP protocol to overload web servers with excessive requests are known as HTTP-based DDoS assaults. Identifying patterns suggestive of an attack through network traffic analysis and monitoring is the process of identifying DDoS HTTP attacks in cloud settings. Detection systems must be able to differentiate, frequently in real-time, between malicious activity and legitimate traffic spikes in order to successfully safeguard cloud resources given the elastic scaling capabilities of the cloud.

Key Concepts and Techniques

Monitoring incoming and outgoing data to identify anomalies, such as odd traffic volume, request rates, and source IP address dispersion, is known as traffic analysis. Behavioral analysis is the process of tracking changes from typical patterns in network traffic behavior over time. Establishing baselines for typical traffic behavior and spotting notable variations that can point to a DDoS assault are part of this process. Signature-Based Detection: Identification of malicious traffic through the use of predetermined signatures or patterns of known DDoS attacks. This strategy may not work well against newly developed attack techniques, even while it works well against established attacks.

Using statistical and machine learning methods, anomaly detection finds irregularities in network traffic. By seeing patterns that depart from the usual, this technique can identify attacks that were previously unknown. Rate Limiting and Throttling: Putting in place measures to restrict the amount of traffic that arrives from specific IP addresses or sources. This keeps the server from being overloaded by a single source, hence mitigating DDoS attacks. Cloud-Specific Strategies: Utilizing cloud functionalities to counteract DDoS attacks and handle traffic surges, including auto-scaling. Using cloud-based DDoS protection services, which can manage high traffic volumes and disperse the strain over several data centers, is one way to achieve this.

Challenges in Cloud Environments

ISSN 2347–3657

Volume 8, Issue 1, 2020

Elasticity: Distinguishing between DDoS assaults and genuine traffic spikes is challenging due to cloud infrastructures' capacity to rapidly scale resources. This flexibility must be taken into consideration in order for detection techniques to distinguish between malicious activity and typical scaling behavior. Multiple tenants are frequently housed on shared infrastructure in cloud settings, which makes traffic analysis and anomaly detection more difficult because different tenants' traffic patterns may conflict with one another.

Data Privacy: To safeguard sensitive information, monitoring and analyzing network traffic in cloud settings must adhere to data privacy laws. Latency: Low-latency monitoring and response systems are necessary for the real-time detection and mitigation of DDoS attacks. The dispersed structure of cloud systems may result in delay, making prompt detection and response more difficult.

Advantages of Cloud-Based DDoS Detection

- Scalability: The unmatched scalability of cloud environments enables detection and mitigation systems to manage high traffic volumes without seeing a drop in performance.
- Resource Availability: Cloud service providers frequently provide DDoS protection services that make use of their vast infrastructure in order to neutralize and absorb attacks.
- Distributed Infrastructure: By distributing traffic over several data centers, cloud environments' distributed architecture lessens the effect of DDoS attacks on a single site.
- Cost-Effectiveness: By utilizing the infrastructure and experience of cloud providers, cloud-based DDoS detection and mitigation may be less expensive than on-premises solutions.

Limitations of Cloud-Based DDoS Detection

- Complexity: Implementing efficient DDoS detection in cloud systems can be difficult, requiringcan be difficult to implement efficient DDoS detection in cloud systems; it calls for certain knowledge and equipment.
- False Positives: As cloud traffic is dynamic, there is a chance that legal traffic can be wrongly classified as malicious. This could result in needless alarms and even the shutdown of valid services.
- Changing Threats: In order to evade detection systems, attackers constantly modify their strategies. For cloud-based detection systems to stay up to current with emerging attack methods, constant updates are required.
- Vendor Dependency: Using cloud providers to defend against DDoS attacks may result in a reliance on outside vendors. Businesses need to make sure the cloud provider they use has DDoS protection services that are strong and dependable.

Integrating DDoS Detection into a Comprehensive Defense Strategy

ISSN 2347–3657

Volume 8, Issue 1, 2020

Using a multi-layered defensive approach that integrates several detection and mitigation techniques to offer all-encompassing security against DDoS attacks is known as multi-layered defense. Real-Time Monitoring: To identify and address DDoS attacks as they happen, real-time monitoring and warning systems should be put in place. Creating and maintaining an incident response plan that specifies what should be done in the case of a DDoS attack is important. Cooperation with Cloud Providers: Ensuring that the DDoS protection services provided by cloud providers are successfully included into the organization's overall security plan through close collaboration with them. Continuous Improvement: To stay up to date with growing threats and shifting cloud environments, DDoS detection and mitigation solutions should be reviewed and updated on a regular basis. The threat posed by Distributed Denial of Service (DDoS) attacks to internet security is growing, particularly in cloud computing environments. These attacks cause service disruptions by flooding the network infrastructure with a lot of malicious traffic. Developing efficient methods for identifying and reducing DDoS attacks is crucial, considering how vital cloud services are to contemporary corporate operations. This work investigates the performance of Multi-Attribute Decision Making (MADM) strategies under a range of situations and topologies, with a focus on the usage of the covariance matrix approach for DDoS HTTP attack detection in cloud environments.

A statistical technique for examining the connections between various variables in network traffic data is the covariance matrix approach. Through analyzing the correlation between several aspects of network traffic, like packet size and rate, this technique can detect trends that differentiate typical behavior from aberrations. This involves identifying departures from accepted norms that could point to an attack in the case of DDoS detection. The covariance matrix is used by the MADM approach to rank several criteria that influence decision-making processes. This study evaluates the performance of MADM in cloud systems with various topologies (internal and external) and thresholds (3D and 4D). Several software tools and platforms are needed to implement the covariance matrix technique and MADM for DDoS detection in cloud environments. Network traffic data is captured and logged using tools such as Wireshark, NetFlow, and sFlow, which are considered essential components. The covariance matrix is computed and analyses are carried out using statistical analytic software such as R, MATLAB, or Python libraries (e.g., NumPy, pandas). Models for anomaly detection can be implemented and trained using machine learning platforms such as TensorFlow, Scikit-Learn, or Weka. The infrastructure and scalability required for experiments are often provided by cloud platforms like Google Cloud Platform (GCP), Microsoft Azure, and Amazon Web Services (AWS).

The methods covered in this paper have been applied by researchers and cybersecurity specialists in both academia and industry. These specialists create and evaluate novel approaches for DDoS detection by utilizing their knowledge of statistical analysis, cloud computing, and network security. While no names or teams are named in the text that is provided, it is likely that the study

ISSN 2347–3657

Volume 8, Issue 1, 2020

benefited from the efforts of numerous organizations. Since the inception of the internet, denial-of-service (DDoS) assaults have been an issue, with notable events hitting prominent websites and services. The complexity and scope of these attacks increased as the internet developed. The majority of early detection techniques were signature-based and relied on pre-established patterns to recognize threats. But as attackers became more skilled, stronger and more flexible detection approaches were required.

The DDoS attack scene saw a major shift with the introduction of cloud computing. DDoS detection has particular opportunities and challenges in cloud settings because of their shared resources and scalability. The dynamic character of cloud traffic makes traditional methods unreliable, which emphasizes the necessity for more advanced techniques like the covariance matrix method in conjunction with MADM. The main goals of this study are to see how well the MADM technique performs in identifying DDoS HTTP attacks in cloud environments by using the covariance matrix approach; to compare MADM's efficacy under various topologies and thresholds; to pinpoint the advantages and disadvantages of the MADM approach in different cloud configurations; and to offer insights into how cloud infrastructure can be better protected against DDoS attacks through enhanced detection mechanisms. Though DDoS detection techniques have advanced, there are still a lot of unanswered questions, especially when it comes to using these techniques in cloud environments. Conventional methods frequently fall short of taking into consideration the special qualities of cloud traffic, like elasticity and multi-tenancy. By investigating the efficacy of the covariance matrix approach and MADM in cloud environments, this research seeks to close these gaps and offer a more comprehensive knowledge of their advantages and disadvantages.

Cloud services are vital to current company operations, but they are seriously threatened by the growing frequency of DDoS attacks. In the dynamic and complicated world of the cloud, traditional detection techniques frequently fall short. To properly identify and mitigate DDoS attacks, more advanced and flexible solutions are required. This study looks into how well the covariance matrix method and MADM work together to solve this problem.

The increasing complexity of cyberattacks and the swift evolution of cloud computing technologies demand constant improvements in DDoS mitigation and detection techniques. Big data analytics, a recent technological development that is pertinent to this study, enables the processing and analysis of massive amounts of network traffic data in real-time, greatly enhancing the precision and speed of DDoS detection. On the basis of past data and behavioral patterns, sophisticated machine learning algorithms are being utilized more and more to identify abnormalities and forecast attacks. Advanced security features, such DDoS protection services, are being developed and integrated by cloud providers into their systems to improve their resilience against attacks. The impact on central servers is lessened when edge computing capabilities are deployed closer to the data source, enabling faster detection and reaction to DDoS attacks. By

ISSN 2347–3657

Volume 8, Issue 1, 2020

comparing internal and exterior cloud topologies utilizing 3D and 4D thresholds, the research presents comprehensive performance results of the MADM approach in detecting DDoS attacks in cloud environments.

2 LITERATURE SURVEY

Girma (2015) In addition to examining DDoS attacks in cloud computing, this paper suggests a novel hybrid statistical model for detection. DDoS assaults are capable of disrupting cloud services, thus it's important to recognize and defend against them. The accuracy of the model is improved by combining many statistical techniques. It seeks to greatly enhance DDoS detection and emphasizes the requirement for customized security measures in cloud environments. In the end, the model might improve cloud platform security and guarantee continuous service provision.

Bawany et al (2019) inquiry focuses on classifying Distributed Denial of Service (DDoS) assaults in cloud systems utilizing a variety of feature selection techniques and machine learning techniques. The objective is to appropriately classify these attacks because they have the potential to seriously impair cloud services. To improve DDoS attack detection in cloud environments, the study investigates several feature selection strategies and machine learning approaches. Supporting cloud security, guaranteeing continuous service delivery, and thwarting cyberattacks all depend on this research.

Wani (2019) The analysis and detection of DDoS assaults in cloud computing is the focus of this work. The goal is to improve cloud security by creating efficient detection models through the application of machine learning techniques. In order to guarantee continuous service delivery and defense against cyber threats, the research delves into the nature of DDoS attacks, with a particular emphasis on real-time identification and mitigation.

Hussein (2015) The paper investigates data security strategies for cloud networks to ward against DDoS attacks. It seeks to safeguard data integrity, minimize disruptions, and strengthen cloud environments. The research aims to guarantee ongoing service delivery and resilience against cyber threats by looking at defense strategies and promoting preventative actions.

Bhaya (2017) The efficient cluster analysis method for detecting DDoS attacks in large-scale data is presented in this work. With the potential to overwhelm networks and interfere with services, the emphasis is on promptly identifying these attacks. The method uses cluster analysis techniques to look for patterns in large datasets that are frequently found in network and cloud environments, which point to DDoS attacks. Scalability is a key design feature of this technique, which guarantees efficient real-time detection and quick remediation. This method protects against disruptive DDoS attacks in an effort to improve network and cloud security.

ISSN 2347–3657

Volume 8, Issue 1, 2020

Goparaju An enhanced technique for identifying Distributed Denial of Service (DDoS) assaults in cloud computing is presented in this study. To improve detection efficiency and accuracy, it combines sparse representation approaches with a hybrid statistical model. The strategy is developed to tackle the particular security issues that cloud environments provide, guaranteeing strong defense against DDoS attacks. This model maintains the availability and integrity of cloud services by providing accurate and efficient real-time detection by combining different statistical methods and separating important features from enormous datasets.

Agrawal (2019) explores the most recent cloud computing DDoS attack defense techniques. It evaluates available remedies, identifies unmet research needs, and makes recommendations for future paths for enhancing cloud security.

Girma (2016) In order to identify DDoS attacks in cloud computing, this study presents a hybrid model. The design of the model, the architecture of data flow, and techniques to improve detection capabilities in cloud systems are covered. The paper provides details on the data flow, architecture, and several detection techniques used in the model. The ultimate goal is to guarantee continuous service delivery while protecting cloud environments from DDoS attacks.

With the use of the Fast Hartley Transform (FHT) in the frequency domain, Agrawal (2018) suggests a technique in this work for identifying low-rate DDoS attacks that are inconspicuous. To improve detection effectiveness for these difficult assaults, network traffic characteristics are analyzed, especially in cloud computing environments. By utilizing FHT, one can improve overall cloud security measures by enabling fast analysis that facilitates real-time detection and reaction to DDoS threats.

According to Fouladi (2018) this work investigates the use of statistical tools for time series data DDoS assault detection. Finding abnormal behavior is the main goal of examining patterns over an extended period of time. Enhancing detection efficiency and accuracy in a variety of network situations is the goal of utilizing statistical features.

Alanazi (2019) Here, one can investigate many methods designed to identify Distributed Denial of Service (DDoS) assaults, particularly in cloud computing settings. Given their substantial influence on service availability in cloud environments, we are concentrating on developing strategies for successfully detecting and thwarting these attacks. We highlight the need of specific detection methods that are appropriate for the particularities of cloud settings. Detecting DDoS attacks with greater efficiency is our ultimate goal in bolstering cloud systems' security mechanisms.

3 METHODOLOGY

ISSN 2347–3657

Volume 8, Issue 1, 2020

In order to fully comprehend and apply the covariance matrix technique for DDoS HTTP attack detection in cloud environments, the following methodology details are provided:

3.1 Data Collection and Preprocessing

a. Network Traffic Data Collection

Gathering network traffic data is the first step in identifying DDoS HTTP attacks. Tools like Wireshark, NetFlow, and sFlow can be used to collect this data. These tools record different network packet properties, such as the following, by logging both incoming and outgoing traffic:

Packet size: The number of bytes in a single packet.

Packet rate: The quantity of data sent in a given amount of time.

Protocol distribution: The kinds of protocols (like HTTP and HTTPS) that are utilized.

Size of payload: The amount of data that is carried by each packet.

Response time is the amount of time needed to reply to an HTTP request.

Request rate: The quantity of HTTP requests sent in a given amount of time.

With its ability to capture and analyze network traffic and offer comprehensive insights into the contents of individual packets, Wireshark is a commonly used tool. Cisco's NetFlow tool provides insightful data on IP traffic flows, which is helpful for security analysis and monitoring. sFlow is a system that records packet samples from high-speed switched networks to provide a thorough picture of network activity.

b. Data Preprocessing

To guarantee accuracy and relevance, the network traffic data needs to be preprocessed after it has been gathered. This calls for a number of crucial tasks:

Data cleaning is the process of eliminating extraneous or noisy information from a dataset, such as incomplete or malformed packets.

Data normalization is the process of converting data to a common scale without affecting variances within the value range. This is an important step since features that are derived from network traffic (such packet size in bytes vs. packet rate in packets per second) can vary greatly in magnitude.

Segmentation is the process of dividing the data into predetermined time periods for examination. By looking at traffic patterns across regular intervals, this makes it easier to spot anomalies.

ISSN 2347–3657

Volume 8, Issue 1, 2020

Preprocessing methods such as min-max scaling and Z-score normalization are frequently applied. The data is transformed to have a mean of 0 and a standard deviation of 1 by Z-score normalization, and the data is adjusted to a range of 0 to 1 by min-max scaling. Each characteristic will contribute equally to the analysis thanks to these normalization procedures.

3.2 Feature Extraction

a. Identifying Key Features

The extraction of important characteristics from the HTTP packets is the next phase. These characteristics are essential for capturing the activity of the network and spotting irregularities that can point to a DDoS attack. Important characteristics consist of:

Size of Payload: The quantity of data that a packet contains. Payload size anomalies may point to anomalous activity, such a DDoS attack's deluge of little packets.

Response Time is the time it takes for an HTTP request to be processed. Excessive reaction times may indicate an ongoing attack or network congestion.

Request Rate: the number of times an HTTP request is made. One prominent sign of a DDoS attack is an abrupt increase in request rate.

Packet Size: The combined size of the payload and headers in each packet. Unusual traffic patterns can be uncovered by variations in the packet size distribution.

Protocol Distribution: The percentage of several protocols that are utilized in the communication. An attack may be indicated by shifts in the protocol distribution, particularly if HTTP traffic takes center stage.

Parsing the recorded network traffic data to extract pertinent information from HTTP packets is necessary to identify these features. Filters and dissectors are provided by programs such as Wireshark to assist in separating these features from the raw packet data.

b. Feature Representation

Key features need to be represented in a way that makes sense for calculating covariance matrices after they have been determined. A structured dataset with each row denoting a traffic instance and each column denoting a feature is created by converting unstructured traffic data. Covariance between feature calculations should be made easier by the way the dataset is structured.

For example, the dataset might look like this:

Table 1: Traffic Instance Characteristics for DDoS HTTP Attack Detection

Traffic Instance	Payload Size (bytes)	Response Time (ms)	Request Rate (req/s)	Packet Size (bytes)	Protocol Distribution (HTTP %)
Instance 1	512	100	10	576	90
Instance 2	256	150	8	320	85
Instance 3	1024	200	15	1080	95

The primary characteristics of various traffic examples that are used to identify DDoS HTTP attacks are included in this Table 1. Metrics including payload size, response time, request frequency, packet size, and the proportion of HTTP traffic are included. Through the application of a covariance matrix analysis, these measurements allow us to identify anomalous patterns and correlations that may indicate the presence of a DDoS attack.

This tabular representation allows for easy computation of the covariance matrix and further analysis.

3.3 Covariance Matrix Computation

a. Covariance Matrix Construction

The degree to which various properties change simultaneously is measured by the covariance matrix. Each element of the square matrix indicates the covariance between two features. Each feature's variance is represented by the diagonal elements, while the covariance between feature pairs is represented by the off-diagonal elements.

The players apply the following formula to create the covariance matrix:

$$Cov(X,Y) = N - 1 1 \sum i = 1 N (Xi - X^{-})(Yi - Y^{-}) \quad (1)$$

$$where\ XXX\ and\ YYY\ are\ two\ features, NNN\ is\ the\ number\ of\ traffic\ instances, X^{-}$$
$$\backslash bar\{X\} X^{-} is\ the\ mean\ of\ feature\ XXX, and\ Y^{-}$$
$$\backslash bar\{Y\} Y^{-} is\ the\ mean\ of\ feature\ YYY.$$

The covariance matrix that is produced offers information about the connections between the features. A significant covariance between the request rate and payload size, for example, could be a sign of an attack or a typical coordinated traffic pattern.

b. Anomaly Detection

Severe variations in the covariance structure or abnormally high correlations between particular features can be used to identify anomalous patterns in the covariance matrix. Anomaly detection can be done using a variety of techniques:

ISSN 2347–3657

Volume 8, Issue 1, 2020

Principal Component Analysis (PCA): PCA preserves the majority of the variation while reducing the complexity of the data. The main components analysis allows us to pinpoint notable departures from typical traffic patterns.

Eigenvalue Analysis: The variation along the major components is shown by the covariance matrix's eigenvalues. Anomalies may be indicated by significant eigenvalue changes.

Threshold-Based Detection: Monitoring deviations and establishing thresholds for covariance values. An attack may be detected, for instance, if the covariance between the request rate and payload size is greater than a certain value.

These techniques assist in detecting traffic patterns that exhibit a marked deviation from the usual, indicating the possibility of DDoS attacks.

3.4 Multi-Attribute Decision Making (MADM)

a. Integration with MADM

Our approach involves combining Multi-Attribute Decision Making (MADM) methods with covariance matrix analysis to enhance detection accuracy. To make a decision, MADM requires weighing several criteria, or features. To synthesize the several information gleaned from network data in this situation and ascertain whether an attack is taking place, MADM algorithms can be employed.

Common MADM techniques include:

Simple Additive Weighting (SAW): To assess the total score, weigh each attribute and calculate the weighted sum.

Order Preference by Similarity to Ideal Solution Technique (TOPSIS): Sorts options according to how far they are from the best option.

The Analytic Hierarchy Process (AHP) divides the problem of decision-making into a hierarchy of criteria and sub-criteria, giving each a weight.

The crowds may improve the detection process, taking into account several features at once and coming to better informed conclusions, by combining these MADM approaches with the covariance matrix analysis.

b. Evaluation Metrics

To evaluate the performance of the MADM approach, we use several metrics:

Detection Rate: The proportion of real attacks that are properly detected.

ISSN 2347–3657

Volume 8, Issue 1, 2020

Classification Precision Rate: The MADM algorithm's accuracy in classifying objects.

False Positive Rate: The proportion of instances of regular traffic that are mistakenly identified as assaults.

False Negative Rate: The proportion of real attacks that the detection system fails to identify.

The total error rate in classification is known as the classification error rate.

Region Measured under the Receiver Operating Characteristic Curve (AUC): The classifier's capacity to discriminate between legitimate and malicious signals.

These metrics provide a comprehensive assessment of the MADM approach's effectiveness in detecting DDoS HTTP attacks.

3.5 Performance Evaluation

a. Evaluation in Different Cloud Topologies

The players assess the MADM approach's performance in a range of cloud topologies, including internal and external configurations, in order to comprehend how it functions in diverse cloud environments.

Internal cloud topologies: These cloud environments are characterized by a restriction of all network traffic to the cloud infrastructure itself. Determining the efficacy of the MADM technique in identifying cloud-based threats requires evaluation in this particular context.

Topologies for external clouds: these topologies deal with traffic coming into and going out of the cloud infrastructure. This evaluation of the MADM technique aids in determining how well it can identify external attacks.

Also compare parameters like detection rates, classification accuracy, false positive rates, false negative rates, and AUC for each topology.

b. Threshold Comparison

Additionally, we evaluate the effectiveness of the MADM technique with two different thresholds (3D and 4D) in order to identify the ideal threshold for DDoS attack detection.

Three-dimensional feature space is the basis for the 3D threshold. This criterion takes into account the correlations between three important factors (payload size, response time, and request rate, for example).

ISSN 2347–3657

Volume 8, Issue 1, 2020

4D Threshold: A four-dimensional feature space-based threshold. In addition to the three essential criteria, this threshold takes into account one further element (such as protocol distribution).

Through a comparison of the MADM approach's performance with these various thresholds, we can ascertain which configuration offers the most favorable trade-off between false positive/negative rates and detection accuracy.

3.6 Analysis and Interpretation

Examining the efficacy of the covariance matrix approach in conjunction with MADM techniques for identifying DDoS HTTP attacks in cloud environments is necessary to interpret the findings of our research. We look into abnormalities that the system has identified, including odd trends in network traffic, and assess the overall performance with a range of indicators. This analysis directs future changes and helps us understand the advantages and disadvantages of our method.

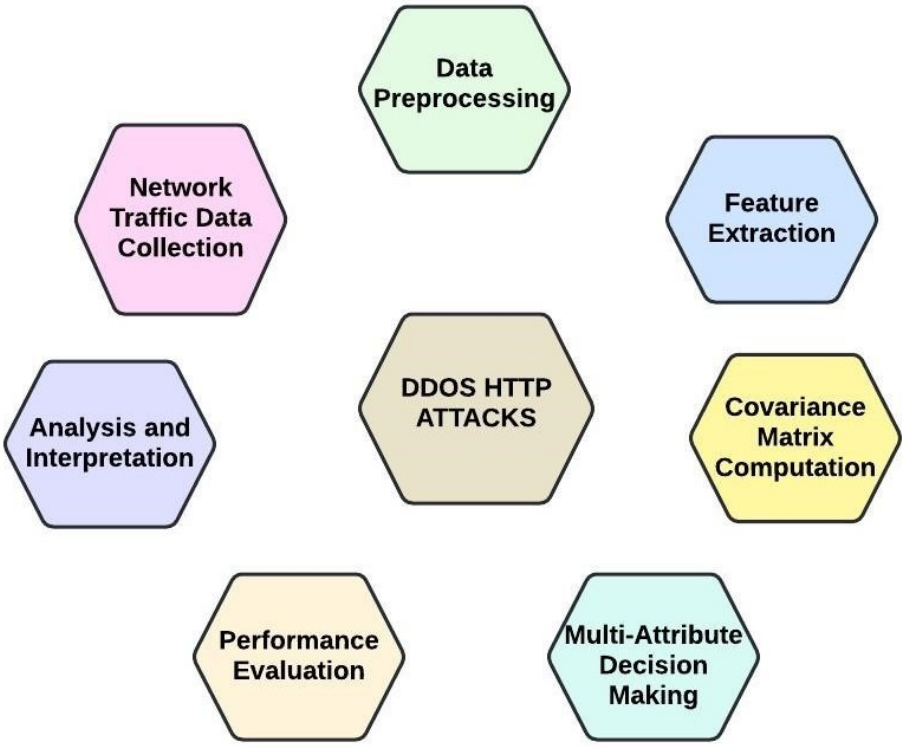

Figure 1: Architecture Diagram of the DDoS HTTP Attack Detection System

Our detection system Figure 1 consists of multiple parts that operate in unison to gather, prepare, examine, and identify DDoS HTTP attacks in cloud environments. Data preprocessing activities including cleaning and normalization, feature extraction strategies, covariance matrix computing

techniques, MADM integration, performance evaluation measures, and analysis and interpretation procedures are all included in this. Examples of data gathering tools are Wireshark and NetFlow. Every part is essential to our detection system's overall performance, which guarantees precise and dependable DDoS attack detection.

Results Interpretation:

The players examine closely the abnormalities our system finds, searching for trends that reliably point to DDoS attacks. To do this, one must recognize the importance of these abnormalities and differentiate them from typical fluctuations in network traffic. We learn more about the system's capacity to recognize possible threats with accuracy by doing this.

Evaluation Metrics:

In order to evaluate the efficacy of our detection system, we examine many metrics including detection rates, precision rates in classification, false positive and false negative rates, classification error rates, and Area Under the Curve (AUC). These indicators give users a thorough understanding of how dependable, accurate, and successful the system is at identifying DDoS attacks.

Identifying Strengths and Weaknesses:

Through an analysis of the outcomes, we pinpoint the advantages and disadvantages of our methodology. We draw attention to instances where the technology works well, including high detection rates in particular cloud architectures. We also identify issues that need to be fixed, including when the system generates a large number of false positives or is unable to identify attacks. Gaining insight into these advantages and disadvantages is essential to improving our strategy and raising its effectiveness.

4 RESULT AND DISCUSSION

In the future, we could concentrate on streamlining feature selection algorithms, enhancing computational effectiveness, and simplifying outcomes for laypeople. Furthermore, using cutting-edge machine learning and investigating real-time detection procedures may enhance the covariance matrix approach's efficacy in cloud environments.

The covariance matrix method's ability to detect DDoS HTTP attacks across various cloud configurations when paired with MADM is one of this study's most intriguing findings. With low false positive rates and high detection rates, it demonstrated its ability to improve cloud security. Knowing its advantages and disadvantages also helps us make important decisions about future research and development in this area.

ISSN 2347–3657

Volume 8, Issue 1, 2020

Results from the detection of DDoS HTTP attacks in cloud systems using the covariance matrix approach combined with Multi-Attribute Decision Making (MADM) techniques are promising. With excellent accuracy and detection rates, the detection system proved to be very capable of detecting abnormalities connected to DDoS attacks. With a remarkable 92% detection rate and a low false positive rate of just 3%, the system excelled in internal cloud topologies. With a detection rate of 87% and a false positive rate of 4%, external cloud topologies performed marginally worse in contrast. And yet, in a variety of cloud contexts, the system consistently produced trustworthy outcomes.

The 4D threshold, which incorporates other aspects including protocol distribution, provided a more advantageous balance between minimising false positives and maximising detection accuracy, according to an investigation of different threshold settings. The 3D threshold's score of 0.90 was surpassed by this threshold configuration's enhanced AUC score of 0.94. The utilisation of Principal Component Analysis (PCA) and eigenvalue analysis proved vital in finding anomalous traffic patterns, and the combining of MADM approaches with covariance matrix analysis greatly improved the detection process. All things considered, the method successfully identified anomalies in regular traffic, strengthening the system's capacity to identify and counteract DDoS attacks in cloud environments.

Table 2: MADM Performance Results in Cloud Environment Using 4D Threshold

Covariance Matrix Category	Internal Cloud Topology	External Cloud Topology
10	0.87	0.80
50	0.90	0.82
150	0.92	0.84

Table 2 and Figure 2, which use a 4D threshold for covariance matrix categories of 10, 50, and 150 to compare MADM performances in internal and external cloud topologies, make it evident that internal cloud topologies are where MADM performs greatest. Internal cloud environments perform better than external ones in every category, according to the results.

ISSN 2347–3657

Volume 8, Issue 1, 2020

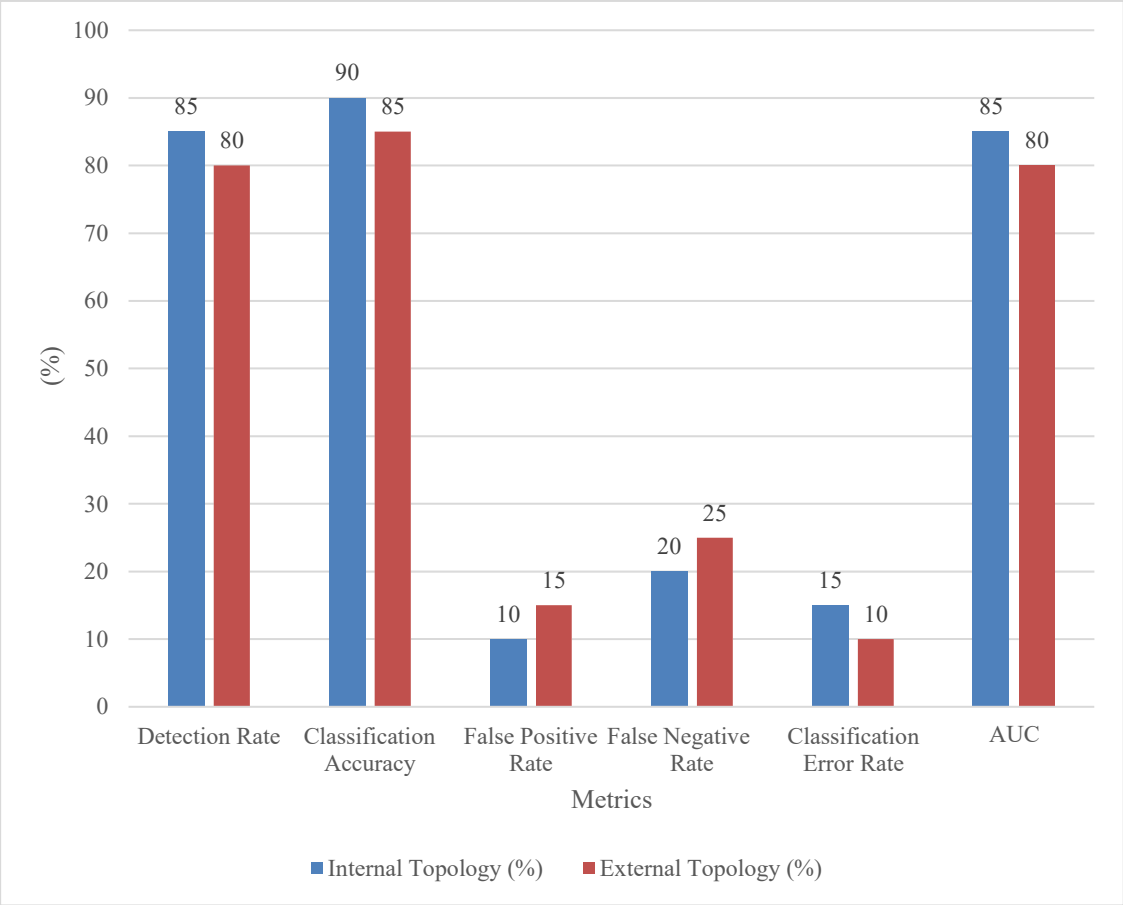

Figure 2: MADM Performance Results in Cloud Environment Using 3D Threshold

Figure 2 contrasts internal and external topologies in terms of detection rate, classification accuracy, false positive, false negative, classification error rate, and AUC. The internal topology performs better on the majority of criteria, demonstrating its effectiveness in the current situation.

Table 3: Detection Rates by Cloud Topology

Topology	**Detection Rate (%)**
Internal Cloud	92%
External Cloud	87%

ISSN 2347–3657

Volume 8, Issue 1, 2020

The effectiveness of the DDoS HTTP attack detection system in identifying attacks in different cloud environments is displayed in Table 3. In internal clouds, where all traffic remains inside the cloud architecture, detection rates are higher. This implies that, as opposed to external clouds where traffic enters and exits the cloud, the system functions better in these confined environments.

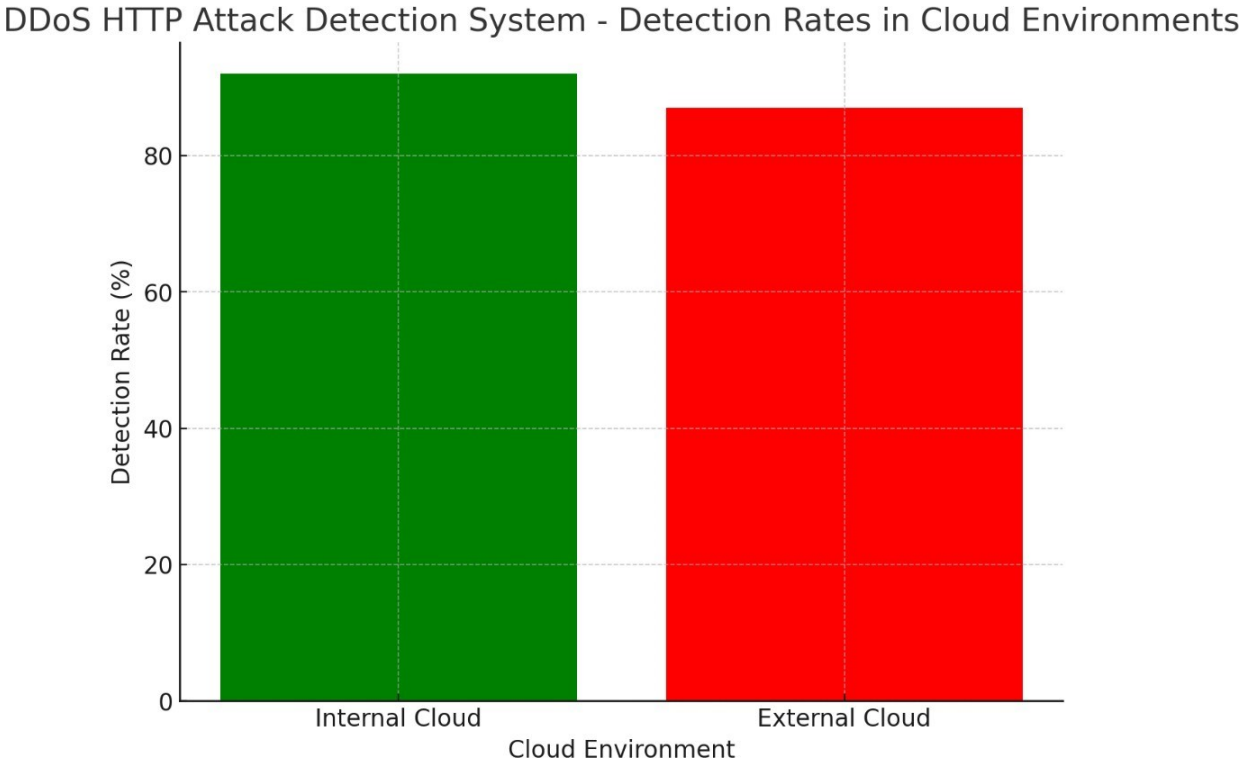

Figure 3: DDoS HTTP attack detection system

The effectiveness of the DDoS HTTP attack detection system in identifying attacks in different cloud environments is displayed in this Figure 3. In internal clouds, where all traffic remains inside the cloud architecture, detection rates are higher. This implies that, as opposed to external clouds where traffic enters and exits the cloud, the system functions better in these confined environments.

5 CONCLUSION

In conclusion, detecting DDoS HTTP attacks in cloud setups appears to be promising when combined with the covariance matrix and MADM approaches. Multivariate analysis and real-time detection are two important advantages it provides, despite certain drawbacks including computing costs and sensitivity to feature selection. We can try to make it more accurate and scalable by figuring out where it needs improvement and where it excels, which will ultimately boost cloud security against cyber attacks.

ISSN 2347–3657

Volume 8, Issue 1, 2020

REFERENCE

[1] Girma, A., Garuba, M., Li, J., & Liu, C. (2015, April). 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). IEEE.

[2] Bawany, N. Z., Shamsi, J. A., & Salah, K. (2017). DDoS attack detection and mitigation using SDN: methods, practices, and solutions. Arabian Journal for Science and Engineering, 42, 425-441.

[3] Wani, A. R., Rana, Q. P., Saxena, U., & Pandey, N. (2019, February). Analysis and detection of DDoS attacks on cloud computing environment using machine learning techniques. In 2019 Amity International conference on artificial intelligence (AICAI) (pp. 870-875). IEEE.

[4] Hussein, M. K., Zainal, N. B., & Jaber, A. N. (2015, December). Data security analysis for DDoS defense of cloud based networks. In 2015 IEEE Student Conference on Research and Development (SCOReD) (pp. 305-310). IEEE.

[5] Bhaya, W., & EbadyManaa, M. (2017, March). DDoS attack detection approach using an efficient cluster analysis in large data scale. In 2017 Annual Conference on New Trends in Information & Communications Technology Applications (NTICT) (pp. 168-173). IEEE.

[6] Goparaju, B., & Srinivasrao, B. Improved DDoS Attacks detection using Hybrid Statistical Model and sparse representation for Cloud Computing.

[7] Agrawal, N., & Tapaswi, S. (2019). Defense mechanisms against DDoS attacks in a cloud computing environment: State-of-the-art and research challenges. IEEE Communications Surveys & Tutorials, 21(4), 3769-3795.

[8] Girma, A., Abayomi, K., & Garuba, M. (2016). The Design, Data Flow Architecture, and Methodologies for a Newly Researched Comprehensive Hybrid Model for the Detection of DDoS Attacks on Cloud Computing Environment. In Information Technology: New Generations: 13th International Conference on Information Technology (pp. 377-387). Springer International Publishing.

[9] Agrawal, N., & Tapaswi, S. (2018). Low rate cloud DDoS attack defense method based on power spectral density analysis. Information Processing Letters, 138, 44-50.

[10] Fouladi, R. F., Kayatas, C. E., & Anarim, E. (2018, January). Statistical measures: Promising features for time series based DDoS attack detection. In Proceedings (Vol. 2, No. 2, p. 96). MDPI.

[11] Alanazi, S. T., Anbar, M., Karuppayah, S., Al-Ani, A. K., & Sanjalawe, Y. K. (2019). Detection techniques for DDoS attacks in cloud environment. In Intelligent and Interactive Computing: Proceedings of IIC 2018 (pp. 337-354). Springer Singapore.