iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 13 **Issue:** I **Month of publication:** January 2025

**DOI:** https://doi.org/10.22214/ijraset.2025.66649

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 13 Issue I Jan 2025- Available at www.ijraset.com*

# A Review on: DDoS Detection in Cloud-Based Website Hosting Using Covariance Matrix Approach

Anjali Saxena[1], Unmukh Datta[2]
[1]*M.E Scholar,* [2]*Associate Professor, Department of Computer Science and Engineering, Maharana Pratap College of Technology, Gwalior, MP*

***Abstract:*** ***Particularly in cloud and IoT systems, this work investigates how the covariance matrix might improve Distributed Denial of Service (DDoS) detection in challenging network situations. Still a constant difficulty, DDoS attacks take advantage of the linked character of contemporary networks. Improving detection accuracy, reducing false positives, and allowing real-time harmful traffic identification is the aim. The suggested approach analyses interactions between several network traffic characteristics using the covariance matrix, therefore spotting abnormalities suggestive of DDoS activity. This method captures subtle, multi-dimensional patterns usually missed by volume-based or signature-based techniques, therefore transcending conventional approaches. In cloud and IoT environments, comprehensive datasets encompassing both valid & hostile traffic assist the models to be trained. Dynamic adaptation to shifting assault pathways and advanced machine learning methods serve to enhance the detection process. Comparative analysis reveals that by basically achieving superior accuracy and resilience, the covariance matrix-based approach overcomes low-rate and zero-day threats. Strong network security is thus guaranteed even in multi-tenant, high-traffic environments since the results demonstrate a clear decrease in false positives and improved detection rates. This work offers a foundation for sophisticated, customizable anomaly detection techniques, therefore offering a possible way to guard critical infrastructure from sophisticated DDoS attacks.***

***Keywords: Covariance Matrix, DDoS Detection, Anomaly Detection, Cloud Security, IoT Networks, Machine Learning, Multi-Tenant Environments.***

## I. INTRODUCTION

By offering organisations and people scalable, dependable, and reasonably priced options, cloud-based website hosting has transformed the digital scene. It provides flawless access to resources, deployment flexibility, and improved management of online services' efficiency. Growing use of cloud hosting has made it a top target for cyberattacks, especially Distributed Denial of Service (DDoS) attacks. DDoS attacks are designed to drain the resources of a target, therefore depriving services from permitted users. These attacks not only impair operations but also create significant financial and reputational damage, hence they critically endanger businesses largely depending on cloud-based infrastructure[1]–[3].

Finding DDoS attacks in cloud systems is challenging work. Unlike traditional hosting setups, cloud infrastructues are dynamic, involving many nodes and regions, distributed and dynamic. This makes it challenging to distinguish true traffic surges—those resulting from marketing campaigns or viral content—from detrimental behaviour. Since they usually rely on predefined thresholds or signature-based techniques, conventional detection systems cannot manage the intricate and changing character of modern DDoS attacks.

These methods find it challenging to meet the scale and complexity of cloud systems; so, imaginative and flexible solutions that can investigate traffic patterns and identify anomalies suggestive of assaults are significantly needed. One hopeful solution to this challenge is the covariance matrix approach, a statistical method based on mathematical tools to find variances in network data[4]–[8]. Examining relationships among multiple traffic parameters—such as packet size, flow rate, or connection duration—the covariance matrix approach searches for trends and correlations pointing to hostile activity. By stressing the interconnectedness of these features, the method helps to identify small variations that could otherwise go unnoticed with traditional methods. This ability makes the covariance matrix particularly suitable demand cloud systems, where the volume or complexities of traffic demand for advanced analytical methods[9]–[11].

©IJRASET: All Rights are Reserved 

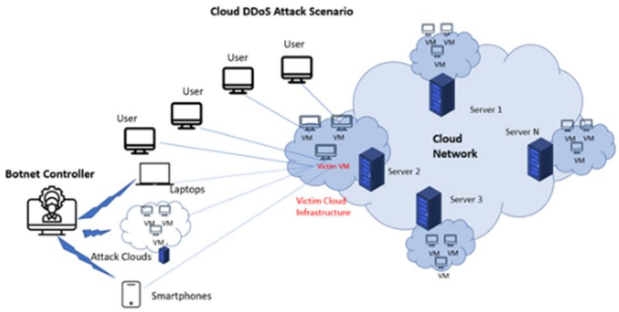



Fig: 1 DDoS Detection in Cloud-Based Website [12]

The covariance matrix approach's benefits come from its flexibility and precision. It detects statistical outliers to identify fresh and changing attack patterns unlike rigid signature-based systems. Moreover, its real-time operation enables the prompt prevention of DDoS attacks, so reducing their effect on services housed on clouds. Implementing such sophisticated detection systems becomes crucial to guarantee the security and resilience of cloud systems as they keep expanding in scope and relevance. The use of the covariance matrix technique to DDoS detection in cloud-based website hosting is investigated in this work. It emphasises the need of using statistical approaches for anomaly detection in cloud systems and tackles the limits of current detection methods. The paper offers a thorough analysis of the technique, stressing how to efficiently use the covariance matrix to spot and stop DDoS attacks. Furthermore, it assesses the efficacy of this method using simulations and case studies, thereby highlighting its ability to improve the security architecture of systems housed on clouds. In the domain of DDoS detection, the covariance matrix technique marks a notable development. Using statistical analysis to find anomalies provides a strong and scalable answer to the problems presented by contemporary cyberattacks. Securing these infrastructures against DDoS threats becomes a significant concern since cloud-based hosting underpins important internet services. By proving the effectiveness of the covariance matrix technique and offering a route for next advancements in cloud security technology, this study hopes to support this endeavor.

## II. RELATED WORK

Shafi 2024 et al. examines sixteen publicly accessible datasets and finds fifteen major flaws to satisfy demand for better DDoS datasets within cloud systems. Then displayed with seventeen DDoS assault scenarios and over eight benign user actions in response is the Bicut-cPacket-Cloud-DDoS-2024 dataset. Designed to replicate benign user traffic, a Benign User Profiler (BUP) program was created; NTLFlowLyzer was used to hand label the dataset with over 300 features retrieved. Three algorithms—ANOVA, information gain, and additional tree—are used in the paper to find the best feature set. Finally, attempting to surpass the constraints of conventional detection techniques, a multi-layered DDoS detection model is suggested and assessed using the new dataset[13].

Nagah 2024 et al. Denial of Service (DoS) attacks in cybersecurity seek to overload systems with too many requests therefore compromising their availability. More complicated and using several hacked sources are distributed denial of service (DDoS) assaults. Protection of online platforms depends on fast identification and classification of these assaults. This work focusses on DDoS detection by means of Machine Learning (ML) methods to distinguish between benign and hostile network behaviour. The method is meant to let systems independently identify and react to DDoS threats using the apaDDoS-dataset, therefore increasing digital security[14].

Ashraf 2024 et al. Internet's widespread use and the rapid growth of IoT devices relying on cloud services have increased the vulnerability of these devices to threats, particularly DDoS and DoS attacks. DDoS attacks are challenging to detect with traditional intrusion detection methods. a machine learning-based model for detecting DDoS attacks, using the CICDDoS2019 dataset. Various machine learning techniques were explored, with AdaBoost and XGBoost delivering exceptional performance in identifying attack characteristics. Future work will involve a hybrid approach to enhance the model's capabilities. The model will also be updated continuously with new DDoS attack data to ensure its effectiveness against evolving threats. By leveraging machine learning, this model aims to improve the detection of DDoS attacks in IoT networks, enhancing the security and integrity of connected devices[15].

Pawar 2024 et al. Fast IoT development has transformed modern life but also made people more vulnerable to hackers since portable and insecure devices change everything. Notwithstanding several studies to pinpoint security risks, problems such limited storage, high processing costs, and system failures still exist.

By simplifying network management and handling some of these problems, Software Defined Networking (SDN) presents a solution. A key hazard still present in IoT devices is security, particularly DDoS attacks. Looks at DDoS threats in IoT and SDN systems and investigates Blockchain (BC) integration to improve security. Further used to increase detection accuracy is an Attention-based Convolutional Long Short-Term Memory (At-C-L) model. Tested on the InSDN database, the suggested model effectively separated regular traffic from DDoS attacks and attained an amazing detection accuracy of 98.3%[16].

TABLE 1 LITERATURE SUMMARY

| Authors/year | Model/method | Research gap | Findings |
|---|---|---|---|
| Saiyedand/2024 [17] | DEEPShield detects DDoS using ensemble learning. | Lack of efficient DDoS detection in resource-constrained IoT environments. | DEEPShield detects DDoS with over 90% accuracy in constrained environments. |
| Ahmed/2024 [18] | Ensemble online ML model enhances DDoS detection in SDN environments. | Limited feature scope and adaptability in current DDoS detection models. | Ensemble online ML model achieves 99.2% detection rate for DDoS. |
| Naqvi/2024 [19] | Reconstructive deep learning detects DDoS attacks with minimal disruptions. | Need for adaptive DDoS detection without retraining in smart grids. | Proposed method improves DDoS detection without requiring full retraining. |
| Pakmehr/2024 [20] | DDoS attacks in IoT require effective detection and prevention solutions. | Lack of effective DDoS detection solutions for resource-constrained IoT networks. | DDoS attacks disrupt IoT systems; solutions for detection remain evolving. |
| Alamer/2023 [21] | BCO-LSTM optimizes DDoS detection, outperforming traditional LSTM models effectively. | LSTM parameter optimization for DDoS detection lacks efficiency and accuracy. | BCO-LSTM outperforms traditional models in DDoS detection accuracy. |

## III. THE RISING THREAT OF DDOS ATTACKS

Since distributed denial of service (DDoS) attacks have grown to be one of the most often occurring and destructive kinds of cyberattack, their increasing threat becomes a major issue in the digital age. DDoS assaults seek to flood the targeted servers, networks, or systems with so much traffic that they are inaccessible to authorised users. Organisations and people who depend on consistent and safe internet services are seriously at risk from these increasingly complex and challenging attacks. Fundamentally, DDoS assaults use many hijacked devices—often part of a botnet—to send an excessive volume of traffic towards a target, therefore causing disturbance or total denial of access to vital services by exploiting the spread character of the internet. The risk of such assaults has been heightened by the growing number of Internet of Things (IoT) linked devices, particularly their general acceptance. From home appliances to industrial systems, IoT devices—often susceptible due to inadequate security—are perfect targets for fraudsters hoping to take over equipment and create vast botnets. Among the most well-known examples of this is the Mirai botnet attack in 2016, which broke into IoT devices and launched one of the greatest DDoS attacks in history, so seriously compromising major websites and infrastructure all throughout the United States. The fast development of IoT and the expanding network of devices worsen the problem even more since many of these devices lack strong security features, therefore offering simple access points for cybercrime. Moreover significantly changed is the extent of DDoS attacks. Though early attacks were often limited to bandwidth levels of 10–15 gigabytes per second (Gbps), the size of these attacks has expanded to the point where they now reach several terabytes per second (Tbps), as witnessed by the major strikes of recent years. Such high-volume attacks can surpass even the most robust systems and cause extended outages, therefore compromising services and resulting in significant financial losses. Apart from their vast reach, DDoS attacks have developed to be ever more complicated. Attackers use a variety of tactics, including amplification attacks—which double the attack flow using publicly accessible servers—and evasion techniques to avoid traditional security measures. Modern DDoS attacks may also be associated with other types of cyberattacks, such as information breaches and ransomware, to create varied threats that are significantly more difficult to find and eradicate.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

These shifting tactics make it harder for businesses to defend against DDoS attacks using traditional methods, which are usually insufficient for controlling dynamic, high-scale, well-hidden threats. Another emerging issue is the financial effect of DDoS attacks. For companies, particularly those mostly dependent on online services for income creation or consumer contact, the downtime resulting from a DDoS attack can have major consequences. Should their systems be hacked, for example, e-commerce sites, online banking systems, and cloud-based businesses would experience significant income losses[22], [23]. Such incidents could lead to long-lasting harm to reputation when customers start to doubt the company's capacity to safeguard their products and data. Another element raising the financial load of these attacks is the expense of DDoS mitigating solutions. If companies want to properly identify and counter these assaults, they must make investments in specialist security infrastructure like traffic monitoring tools, firewalls, and anti-DDoS systems. Moreover, as they depend more on cloud computing and digital transformation, businesses are more susceptible to DDoS attacks as the digital landscape grows and more important services are housed online. Reacting to the increasing risk, businesses have to change their proactive, multi-layered cybersecurity strategy. This covers not only protecting IoT devices and networks but also deploying sophisticated threat detection systems grounded on artificial intelligence and machine learning to instantly spot odd traffic patterns and possible attacks. Moreover crucial are cloud-based DDoS prevention systems since they provide scalable and adaptable ways to stop attacks before they may affect the business infrastructure[24]. Dealing with major DDoS attacks also depends much on threat intelligence sharing and cooperation with Internet Service Providers (ISPs), which helps to enable faster reactions and more successful defences. The growing DDoS attack danger basically compromises the dependability and security of the digital infrastructure. Advanced, adaptive, and cooperative security solutions will become increasingly crucial as the internet grows and new vulnerabilities cropping up with IoT and cloud computing persist. Organisations can reduce DDoS attack risks and safeguard their digital assets and services against interruption by means of preemptive measures, ongoing innovation, and defensive development focus.

## IV. CHALLENGES IN DETECTING DDOS IN CLOUD ENVIRONMENTS

### A. *Scale and Complexity of Cloud Infrastructure:*

Cloud environments are inherently vast and dynamic, which complicates the task of monitoring and detecting Distributed Denial of Service (DDoS) attacks. The infrastructure in a cloud environment can span multiple geographic locations, with varying levels of virtualized resources like servers, storage, and networks that scale automatically based on demand. As resources are dynamically allocated and deallocated, tracking the vast number of interconnected components becomes difficult. When a DDoS attack occurs, it may target multiple cloud-based services simultaneously or even exploit weaknesses in a specific resource.

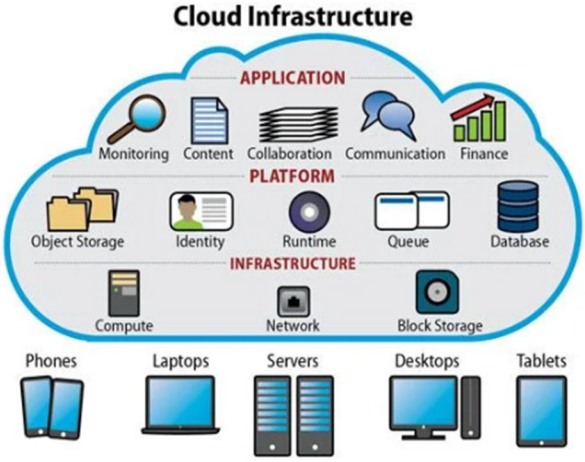



Fig: 2 Cloud Infrastructure

Quick changes in resource allocation mean that models of attack detection depending on fixed infrastructure configurations cannot be able to provide accurate real-time evaluations. Moreover, the way resources are scattered among several data centres or regions compromises centralised monitoring and may complicate the identification of the attack's source and scope. Since this complex structure requires adaptive detection systems able of scaling with the dynamic character of the cloud, it offers a constant challenge for both cloud providers and companies[25].

### B. Diverse Attack Vectors

Targeting several tiers of the cloud infrastructure—including the network, application, and service levels—DDoS assaults in cloud systems are more complicated. The breadth of attack vectors that spans from volumetric attacks overwhelming network capacity to application-layer attacks aimed to deplete certain resources presents enormous challenges for detection systems. Conventional DDoS mitigating strategies including traffic rate-limiting and network filtering may not be enough against multi-layered attacks. attackers could utilise amplification techniques to increase the volume of dangerous traffic, therefore complicating identification. A multi-vector DDoS assault can have a cascading impact, concurrently upsetting numerous linked cloud services. Effective detection and mitigation of DDoS assaults depend on cloud systems able to simultaneously recognise and classify several kinds of attacks. This calls for the creation of sophisticated, multifarious detection techniques that may dynamically change to fit the type, strength, and approach of assault. Creating such systems involves for advanced anomaly detection algorithms and the capacity to monitor attack behaviour in real-time across several cloud levels[26].

### C. Resource Sharing in Cloud Systems

DDoS detection is confused by resource sharing among several tenants in cloud systems. Unlike traditional networks, where hostile traffic is easier to identify, the shared infrastructure in cloud systems makes it difficult to separate real traffic from attacks, especially during traffic surges. DDoS attackers mix routine activity with damaging traffic to hide abnormal patterns. Resources are shared, so the consequences of an assault can affect numerous customers, so generating additional disturbance. Effective DDoS detection in the cloud depends on thorough traffic analysis and closer access into each tenant's usage patterns to distinguish between benign fluctuations and hostile surges[27].

### D. High Volumes of Traffic

DDoS detection is challenging in large quantities of data and bandwidth handled by cloud systems. The scope and global distribution of services make it challenging to differentiate regular from attack traffic. DDoS assaults especially at access points like load balancers try to overwhelm networks by combining illegal material with lawful information. Small-scale assaults can seriously disrupt cloud services, thereby affecting large user numbers. Real-time traffic analysis is required to identify odd trends among regular traffic surges even if conventional signature-based methods cannot keep up. Though sophisticated anomaly detection systems are needed, their high processing requirements cannot be feasible in every cloud environment[28].

### E. Evasion Techniques

Sophisticated attackers use advanced evasion techniques to escape traditional DDoS detection systems. Since they mirror actual user behaviour, slow-rate attacks and other techniques make identification difficult. By spreading damaging requests over hijacked IoT devices, traffic masking covers the attack's source. IP spoofing and changed attack paths add still another level of complication to identification.

Sophisticated detection techniques—such as behavior-based analysis or machine learning—that can identify hostile patterns even in circumstances when attacks resemble normal traffic must be present in cloud systems to guarantee more effective detection and response to address these challenges[29].

## V. THE ROLE OF COVARIANCE MATRIX IN ANOMALY DETECTION

By recording correlations between variables in multivariate datasets, the covariance matrix is absolutely important in anomaly identification. Using methods such Mahalanobis distance and PCA, feature co-variance analysis finds unusual data points, hence increasing the accuracy and durability of anomaly identification in demanding data environments.

### A. Understanding Covariance Matrix in Statistical Analysis

Within statistics, a matrix for covariance offers a fundamental idea with a metric for the interaction among many variables in a dataset. When one represents the covariance between pairs of factors across the diagonal or the variance for each variable along the diagonal, one is describing a square matrix. Understanding how variables co-vary in one another using the covariance matrix enables one to identify trends departing from normal behaviour. Applied one anomaly detection, the covariance matrix helps to uncover correlations between numerous features thereby enabling the identification of unexpected data points showing aberrant interactions between several features[30].

### B. Covariance Matrix for Multivariate Data Analysis

Many times including many factors, anomaly detection requires multivariate analysis. A clean and efficient method to capture the interactions among numerous dimensions is provided by the covariance matrix. By means of feature analysis, one can identify outliers or anomalies deviating from the expected relationship structure in a dataset. An anomaly can be identified, for instance, if one variable deviates significantly from its normal pattern in respect to the other variables. Thus, covariance matrices offer the basis of numerous multivariate anomaly detection techniques such Mahalanobis distance and Principal Component Analysis (PCA), depending on the covariance structure of the data.

### C. Role of Covariance in Mahalanobis Distance-Based Anomaly Detection

One well-known anomaly detection method based on the covariance matrix is the Mahalanobis distance. Given feature correlation, it determines a data point's distance from the mean of a distribution. Unlike the Euclidean distance, which assumes all features as independent and hence provides a more accurate estimate of how far a point is from the centre of the data distribution, Mahalanobis distance considers the covariance structure. Since they differ significantly from the expected patterns of the data, points with high Mahalanobis distance are considered anomalies in anomaly identification. The covariance matrix allows one to find multivariate outliers and computes this distance[31].

### D. Improving Anomaly Detection with Covariance Matrix Regularization

Since covariance matrices can become unstable especially with small sample numbers or high-dimensional data, anomaly detection using them offers a challenge. Many times used to solve this are covariance matrix regularisation techniques. Regularisation techniques including shrinkage enable to stabilise the covariance estimations by reducing the effect of noise in the data. This ensures that, in circumstances of sparse or extremely dimensionally distributed data, the covariance matrix remains robust. By improving the dependability within the covariance matrix, regularisation techniques raise the accuracy and efficiency of anomaly detection, hence strengthening the resilience against outliers and noise.

### E. Applications of Covariance Matrix in Real-World Anomaly Detection

In the actual world, covariance matrices find extensive use in anomaly detection. For fraud detection, for example, bank transactions are routinely checked to identify unusual expenditure patterns. Finding anomalies suggesting fraudulent behaviour requires the computation of the covariance between many transaction properties. In network security, too, the covariance matrix can be used to track the relationships between numerous network traffic variables (e.g., packet size, transfer rate) and find abnormal activity suggestive of a cyberattack. Other applications include predictive maintenance, medical diagnostics, and industrial defect detection in which the covariance matrix communicates prospective system faults or risks by enabling the identification of deviations from expected trends[32].

## VI. Advantages of Covariance Matrix for DDoS Detection

### A. Captures Relationships Between Variables

The covariance matrix provides interesting study of the connections among different network traffic properties, hence supporting DDoS detection. Finding unusual traffic patterns requires an analysis of various elements, including packet size, frequency, or source, which changes concurrently. Common in DDoS attacks are unusual combinations of these components; the covariance matrix helps stress this. This helps one to recognise destructive behaviour that could be invisible with individual feature focus. Therefore, the covariance matrix helps to precisely and comprehensively analyse traffic, so enabling the discovery of attack patterns dependent on inter-feature correlations[33].

### B. Dimensionality Reduction

The covariance matrix helps to lower dimensionality by means of the identification of the most crucial components in network traffic. High-dimensional datasets with many variables could be challenging computationally and taxing. Covariance analysis reduces the number of features by focussing on those that capture the basic relationships between traffic components, therefore enabling the data to be more manageable. Focussing on the most relevant traffic patterns helps this simplicity to speed DDoS detection and improve real-time performance. Reducing dimensionality also decreases the computing load on detection systems so that they may examine larger datasets more effectively without reducing attack identification accuracy[34].

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

### C. Noise Reduction

Accurate DDoS detection depends on noise in network traffic data being reduced, which is achieved in part by covariance matrix algorithms. Variations in legal activity or other outside elements that hide attack patterns can cause noise in network traffic. The covariance matrix separates meaningless fluctuations from which features are most crucial for attack detection. Focusing on important relationships helps to enhance the signal-to---- Noise by lowering the effect of noise. This helps one to better understand traffic behaviour, so enabling the identification of DDoS attacks and helping to lower false positives resulting from unrelated traffic oscillations[35].

### D. Anomaly Detection

Anomaly detection is a basic application for the covariance matrix in DDoS protection. By replicating the normal interactions among different traffic variables, the covariance matrix helps to detect deviations from predicted patterns. Usually bringing unusual behaviour, DDoS attacks produce unanticipated packet size changes or traffic surges. The covariance matrix stresses these anomalies by correlating known typical correlations with present traffic patterns. Early detection of DDoS assaults made possible by this capacity to identify anomalies in complicated traffic behaviour promises fast mitigating steps before the attack can cause major disturbance or system damage[36].

### E. Improved Detection Accuracy

Using the covariance matrix and providing a comprehensive DDoS detecting accuracy can be raised by means of network data analysis. Unlike conventional approaches depending on single traffic characteristics, covariance-based analysis evaluates concurrently the interactions among several parameters. This all-encompassing approach reveals attack patterns that, if one focusses only on specific areas, might be overlooked. For instance, the covariance matrix shows that the mix of traffic volume and packet size distribution is rare and indicates a continuous attack even if an increase in traffic volume should not be alarming. From this comes lesser false positives and more reliable DDoS attack detection[37].

## VII. CONCLUSION

At last, particularly in contexts such as cloud computing and IoT, the use of the covariance matrix for DDoS detection offers a significant advantage in improving the accuracy and efficiency of recognising damaging traffic inside complex networks. By recording the interactions between many traffic parameters, the covariance matrix helps one to have a more full knowledge of network activity and hence helps to identify tiny anomalies that could otherwise be missed. Common difficulties in large-scale network research include dimensionality and noise, hence this method not only helps in spotting aberrant patterns but also helps to reduce these factors[38], [39]. Recognizing these connections helps one especially distinguish between real DDoS assaults and reasonable traffic variations. Moreover, the decrease of false positives and the improvement of detection accuracy lead to more dependable and prompt identification of threats. Particularly in contexts with high traffic volumes and different traffic patterns, the ability of the covariance matrix to manage complicated, multi-dimensional data makes it a necessary instrument for modern network security systems. Using cutting-edge methods like covariance matrix-based anomaly detection will be crucial to maintain the security and stability of digital infrastructures as cyber-attacks becoming more complex. Thus, including this approach into DDoS detection systems will help to significantly increase response times, reduce the effect of attacks, and guarantee greater security of important systems and services over several sectors[40], [41].

## REFERENCES

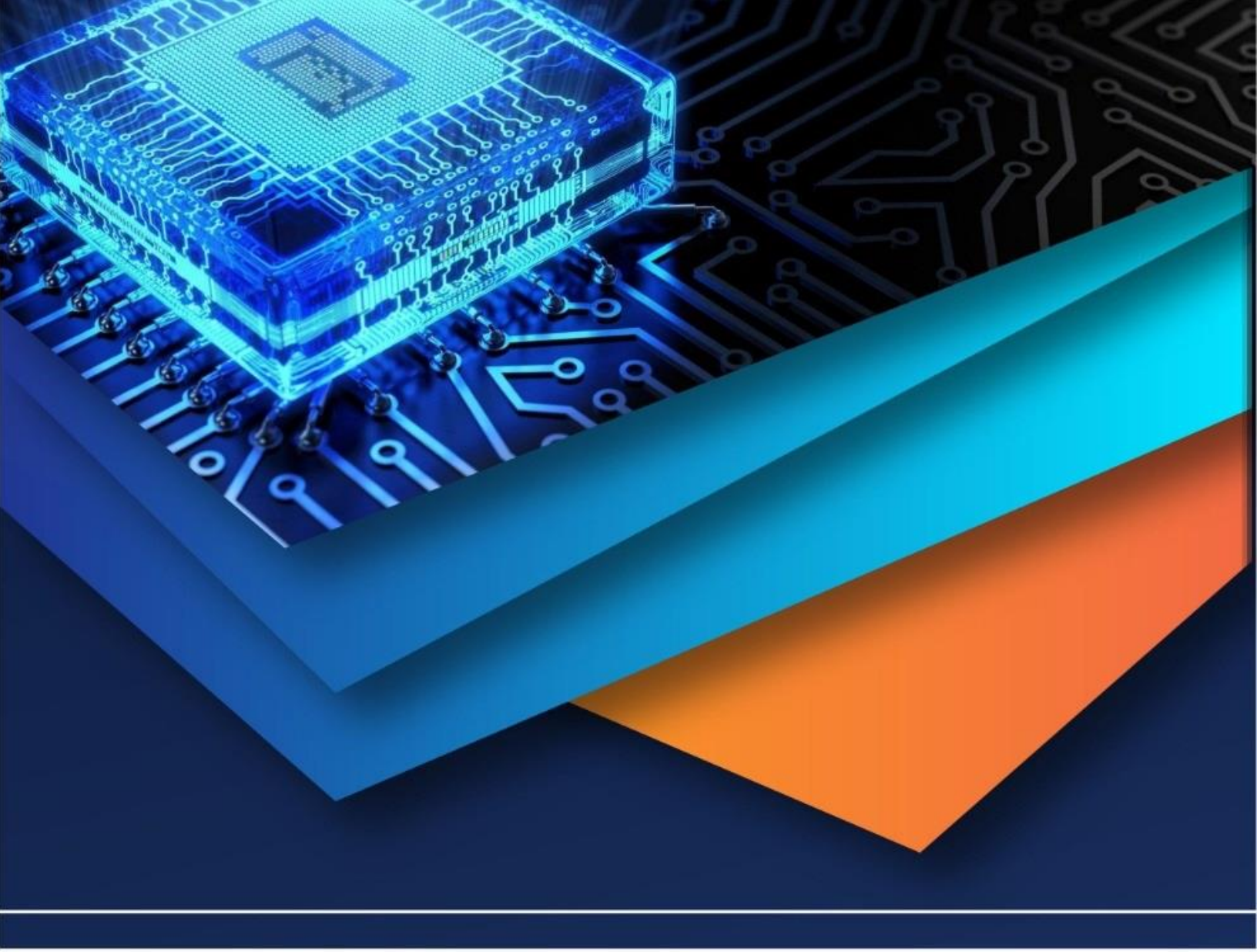
[1] R. Chaganti, B. Bhushan, and V. Ravi, “A survey on Blockchain solutions in DDoS attacks mitigation: Techniques, open challenges and future directions,” Comput. Commun., vol. 197, pp. 96–112, 2023, doi: 10.1016/j.comcom.2022.10.026.
[2] C. M. Nalayini and J. Katiravan, “A New IDS for Detecting DDoS Attacks in Wireless Networks using Spotted Hyena Optimization and Fuzzy Temporal CNN,” J. Internet Technol., vol. 24, no. 1, pp. 23–34, 2023, doi: 10.53106/160792642023012401003.
[3] A. Khatri and R. Khatri, “DDoS Attack Detection Using Artificial Neural Network on IoT Devices in a Simulated Environment,” Lect. Notes Electr. Eng., vol. 982, pp. 221–233, 2023, doi: 10.1007/978-981-19-8136-4_19.
[4] A. Jaber, “Model for Preventing DDoS Attacks Using a Hypervisor,” Lect. Notes Networks Syst., vol. 571 LNNS, pp. 62–85, 2023, doi: 10.1007/978-3-031-19945-5_7.
[5] A. W. Kazaure, “D ETECTION AND C LASSIFICATION OF DD O S FLOODING A TTACKS IN S MART H OME N ETWORKS U SING M ACHINE L EARNING T ECHNIQUES AND R ULE - BASED A LGORITHM .,” pp. 1–153, 2023.
[6] S. Aktar and A. Yasin Nur, “Towards DDoS attack detection using deep learning approach,” Comput. Secur., vol. 129, no. May, 2023, doi: 10.1016/j.cose.2023.103251.

[7] B. Hashim Mohammed, U. Kebangsaan Malaysia Hasimi Sallehudin, N. Sae, M. Satar, and S. Abdelghany Mohamed, "Anomaly Detection of Distributed Denial of Service (DDoS) in IoT Network Using Machine Learning," pp. 1–27, 2023.
[8] M. W. Nadeem, H. G. Goh, Y. Aun, and V. Ponnusamy, "Detecting and Mitigating Botnet Attacks in Software-Defined Networks Using Deep Learning Techniques," IEEE Access, vol. 11, no. May, pp. 49153–49171, 2023, doi: 10.1109/ACCESS.2023.3277397.
[9] S. V. J. Rani et al., "Detection of DDoS attacks in D2D communications using machine learning approach," Comput. Commun., vol. 198, no. June 2023, pp. 32–51, 2023, doi: 10.1016/j.comcom.2022.11.013.
[10] W. I. Khedr, A. E. Gouda, and E. R. Mohamed, "FMDADM: A Multi-Layer DDoS Attack Detection and Mitigation Framework Using Machine Learning for Stateful SDN-Based IoT Networks," IEEE Access, vol. 11, no. March, pp. 28934–28954, 2023, doi: 10.1109/ACCESS.2023.3260256.
[11] F. Suthar and N. Patel, "A Survey on DDoS Detection and Prevention Mechanism," J. Adv. Inf. Technol., vol. 14, no. 3, pp. 444–453, 2023, doi: 10.12720/jait.14.3.444-453.
[12] "DDoS Detection in Cloud-Based Website Hosting - - Image Search results." https://in.images.search.yahoo.com/yhs/search;_ylt=AwrPrjb8Y01na_M0tu_nHgx.;_ylu=Y29sbwMEcG9zAzEEdnRpZAMEc2VjA3BpdnM-?p=DDoS+Detection+in+Cloud-Based+Website+Hosting&type=fc_AC934C13286_s58_g_e_d022424_n9998_c999&param1=7&param2=eJwtj0tugzAQhq%2FiZSIFGI%2BNsc0ugR6g6qpRFo5xiMVTQEXV09dOq9l8%2F2OkmdY31%2FL2XlEAlCCup9sYtFJKBowRIHLkQdg%2FP5CfAyIHqrkC0FIi1U7dpc6tpbqh0mljMUhxN6Heuin0%2FRjwywQaph%2Ff9ybLUyCH3Y%2FNtK9k3AiFFEoSDMFL8i34kZh57t3u7p3fspwVKRPk0D23oT%2BR3neOtM5205HY5zINLqOMphCHrOZhFv%2B%2FEg9eX1%2FGA1a3vPgisGDnCpJKAEsorevkzGUk%2BnYRIVWqjn0bywjIE8AE5QcIzYTOVYpF8fkLURJaXg%3D%3D&hsimp=yhs-2461&hspart=fc&ei=UTF-8&fr=yhs-fc-2461#id=1&iurl=https%3A%2F%2Fwww.indusface.com%2Fwp-content%2Fuploads%2F2020%2F11%2FCloud-DDoS-attacks.png&action=click (accessed Dec. 02, 2024).
[13] M. M. Shafi, A. H. Lashkari, V. Rodriguez, and R. Nevo, "Toward Generating a New Cloud-Based Distributed Denial of Service (DDoS) Dataset and Cloud Intrusion Traffic Characterization," Inf., vol. 15, no. 4, 2024, doi: 10.3390/info15040195.
[14] N. A. Nagah, M. Bahaa, and W. F. Elsersy, DDoS Detection using Machine Learning. Springer Singapore, 2024. doi: 10.1109/ICMISI61517.2024.10580319.
[15] U. Ashraf, H. Sharif, S. Usman, and M. Hasnain, "A Machine Learning Based Approach for the Detection of DDoS Attacks on Internet of Things Using CICDDoS2019 Dataset - PortMap," Lahore Garrison Univ. Res. J. Comput. Sci. Inf. Technol., vol. 8, no. 2, 2024, doi: 10.54692/lgurjcsit.2024.082569.
[16] P. P. Pawar, D. Kumar, B. Ananthan, A. S. Pradeepa, and A. S. Selvi, "An Efficient DDoS Attack Detection using Attention based Hybrid Model in Blockchain based SDN-IoT," 2024 3rd Int. Conf. Artif. Intell. Internet Things, AIIoT 2024, no. August, 2024, doi: 10.1109/AIIoT58432.2024.10574596.
[17] M. F. Saiyedand and I. Al-Anbagi, "Deep Ensemble Learning With Pruning for DDoS Attack Detection in IoT Networks," IEEE Trans. Mach. Learn. Commun. Netw., vol. 2, no. April, pp. 596–616, 2024, doi: 10.1109/tmlcn.2024.3395419.
[18] A. A. Alashhab et al., "Enhancing DDoS Attack Detection and Mitigation in SDN Using an Ensemble Online Machine Learning Model," IEEE Access, vol. 12, no. April, pp. 51630–51649, 2024, doi: 10.1109/ACCESS.2024.3384398.
[19] S. S. A. Naqvi, Y. Li, and M. Uzair, "DDoS attack detection in smart grid network using reconstructive machine learning models," PeerJ Comput. Sci., vol. 10, pp. 1–23, 2024, doi: 10.7717/peerj-cs.1784.
[20] A. Pakmehr, A. Aßmuth, N. Taheri, and A. Ghaffari, DDoS attack detection techniques in IoT networks: a survey, vol. 27, no. 10. Springer US, 2024. doi: 10.1007/s10586-024-04662-6.
[21] L. Alamer and E. Shadadi, "DDoS Attack Detection using Long-short Term Memory with Bacterial Colony Optimization on IoT Environment," J. Internet Serv. Inf. Secur., vol. 13, no. 1, pp. 44–53, 2023, doi: 10.58346/JISIS.2023.I1.005.
[22] P. Kumari and A. K. Jain, "A comprehensive study of DDoS attacks over IoT network and their countermeasures," Comput. Secur., vol. 127, 2023, doi: 10.1016/j.cose.2023.103096.
[23] A. K. Silivery, K. R. M. Rao, and L. K. Suresh Kumar, "An Effective Deep Learning Based Multi-Class Classification of DoS and DDoS Attack Detection," Int. J. Electr. Comput. Eng. Syst., vol. 14, no. 4, pp. 421–431, 2023, doi: 10.32985/ijeces.14.4.6.
[24] J. Bhayo, S. A. Shah, S. Hameed, A. Ahmed, J. Nasir, and D. Draheim, "Towards a machine learning-based framework for DDOS attack detection in software-defined IoT (SD-IoT) networks," Eng. Appl. Artif. Intell., vol. 123, no. July 2022, p. 106432, 2023, doi: 10.1016/j.engappai.2023.106432.
[25] A. Odeh, A. Aboshgifa, and N. Belhaj, "Mitigating DDoS Attacks in Cloud Computing Environments: Challenges and Strategies," Int. Conf. Electr. Comput. Energy Technol. ICECET 2023, no. January, pp. 1–4, 2023, doi: 10.1109/ICECET58911.2023.10389269.
[26] C. Boin, T. Groleat, X. Guillaume, G. Grimaud, and M. Hauspie, "Scale matters: a Comparative Study of Datasets for DDoS Attack Detection in CSP Infrastructure," 2023 IEEE 12th Int. Conf. Cloud Networking, CloudNet 2023, pp. 27–35, 2023, doi: 10.1109/CloudNet59005.2023.10490030.
[27] S. Sureshkumar, G. K. D. P. Venkatesan, and R. Santhosh, "Detection of DDOS Attacks on Cloud Computing Environment Using Altered Convolutional Deep Belief Networks," Int. J. Comput. Netw. Inf. Secur., vol. 15, no. 5, pp. 63–72, 2023, doi: 10.5815/IJCNIS.2023.05.06.
[28] "International Journal of Intelligent Systems - 2023 - Balasubramaniam - Optimization Enabled Deep Learning□Based DDoS.pdf."
[29] R. R. Papalkar, A. S. Alvi, S. Ali, M. Awasthy, and R. Kanse, "An optimized feature selection guided light-weight machine learning models for DDoS attacks detection in cloud computing," Artif. Intell. Blockchain, Comput. Secur. - Proc. Int. Conf. Artif. Intell. Blockchain, Comput. Secur. ICABCS 2023, vol. 1, no. November, pp. 975–982, 2024, doi: 10.1201/9781003393580-146.
[30] Y. Zheng et al., "Correlation-Aware Spatial–Temporal Graph Learning for Multivariate Time-Series Anomaly Detection," IEEE Trans. Neural Networks Learn. Syst., vol. X, no. X, pp. 1–17, 2023, doi: 10.1109/TNNLS.2023.3325667.
[31] H. Zhang, B. Xu, and M. Müller, "A Distance-based Anomaly Detection Framework for Deep Reinforcement Learning," pp. 1–38, 2024.
[32] Y. Ma, X. Zhu, J. Lu, P. Yang, and J. Sun, "Construction of Data-Driven Performance Digital Twin for a Real-World Gas Turbine Anomaly Detection Considering Uncertainty," Sensors, vol. 23, no. 15, 2023, doi: 10.3390/s23156660.
[33] S. U. Otor, B. O. Akumba, A. A. Adeyelu, and I. T. Adom, "A Hybrid Intrusion Detection Model to Alleviate Denial of Service and Distributed Denial of Service Attacks in Internet of Things," Int. J. Adv. Trends Comput. Sci. Eng., vol. 12, no. 6, pp. 277–283, 2023, doi: 10.30534/ijatcse/2023/031262023.
[34] Hayder Jalo and Mohsen Heydarian, "A Hybrid Technique Based on RF-PCA and ANN for Detecting DDoS Attacks IoT," InfoTech Spectr. Iraqi J. Data Sci., vol. 1, no. 1, pp. 27–41, 2024, doi: 10.51173/ijds.v1i1.9.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

[35] Z. Majidian, S. TaghipourEivazi, B. Arasteh, and S. Babai, "An intrusion detection method to detect denial of service attacks using error-correcting output codes and adaptive neuro-fuzzy inference," Comput. Electr. Eng., vol. 106, no. November 2022, p. 108600, 2023, doi: 10.1016/j.compeleceng.2023.108600.
[36] J. P. A. Maranhão, J. P. C. L. da Costa, E. P. de Freitas, E. Javidi, and R. T. de Sousa Júnior, "Error-robust distributed denial of service attack detection based on an average common feature extraction technique," Sensors (Switzerland), vol. 20, no. 20, pp. 1–21, 2020, doi: 10.3390/s20205845.
[37] A. R. Tapsoba, T. Frédéric Ouédraogo, and A. E. Ouédraogo, "Relevance of the Gaussian classification on the Detection of DDoS Attacks," Proc. - 2022 Int. Conf. Cyber-Enabled Distrib. Comput. Knowl. Discov. CyberC 2022, no. October 2022, pp. 42–49, 2022, doi: 10.1109/CyberC55534.2022.00018.
[38] S. Sokkalingam and R. Ramakrishnan, "An intelligent intrusion detection system for distributed denial of service attacks: A support vector machine with hybrid optimization algorithm based approach," Concurr. Comput. Pract. Exp., vol. 34, no. 27, pp. 1–18, 2022, doi: 10.1002/cpe.7334.
[39] M. M. Cherian and S. L. Varma, "Mitigation of DDOS and MiTM Attacks using Belief Based Secure Correlation Approach in SDN-Based IoT Networks," Int. J. Comput. Netw. Inf. Secur., vol. 14, no. 1, pp. 52–68, 2022, doi: 10.5815/ijcnis.2022.01.05.
[40] G. S. Kushwah and V. Ranga, "Distributed denial of service attack detection in cloud computing using hybrid extreme learning machine," Turkish J. Electr. Eng. Comput. Sci., vol. 29, no. 4, pp. 1852–1870, 2021, doi: 10.3906/ELK-1908-87.
[41] J. K. Seth and S. Chandra, "An Effective DOS Attack Detection Model in Cloud Using Artificial Bee Colony Optimization," 3D Res., vol. 9, no. 3, 2018, doi: 10.1007/s13319-018-0195-6.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)