وزارة التعليم العالي والبحث العلمي
جامعة ميسان
كلية التربية الاساسية

Ministry of Higher Education and Scientific Research
University of Misan
College of Basic Education

Misan Journal for Academic Studies
Humanities, social and applied sciences

مجلة ميسان للدراسات الاكاديمية

العلوم الانسانية والاجتماعية والتطبيقية

ISSN (Print) 1994-697X
(Online)- 2706-722X

المجلد 23 العدد 52 كانون الاول 2024

Dec 2024 Issue 52 Vol 23

مجلة ميسان للدراسات الاكاديمية

العلوم الإنسانية والاجتماعية والتطبيقية

كلية التربية الأساسية/ جامعة ميسان/العراق

Misan Journal for Academic Studies

Humanities, social and applied sciences

College of Basic Education/University of Misan/Iraq

ISSN (Print) 1994-697X (Online) 2706-722X

المجلد (23) العدد (52) كانون الاول (2024)

VOL 23 ISSUE52 DEC 2024

www.misan-jas.com

journal.m.academy@uomisan.edu.iq

رقم الايداع في دار الكتب والوثائق بغداد 1326 في 2009

Misan Journal for Academic studies
Vol 23 Issue 52 Dec 2024
مجلة ميسان للدراسات الاكاديمية
مجلد 23 العدد 52 كانون الأول 2024

ISSN (Print) 1994-697X
ISSN (Online) 2706-722X

DOI:
https://doi.org/10.54633/2333-023-052-011

Improved Machine Learning Techniques for Precise DoS Attack Forecasting in Cloud Security

Yasir Mahmood Younus [1], Ahmed Salman Ibraheem [2], Murteza Hanoon Tuama [3]
and wahhab Muslim mashloosh [4]
[1.2.3.4] Department of Computer Techniques Engineering, Imam Al-Kadhum College (IKC), Baghdad, Iraq
Corresponding Author : [1]yasir.mahmood@iku.edu.iq
ORCID ID: https://orcid.org/0009-0007-2602-6005

Abstract:

One of the fundamental motives of Cloud based computing for the use of technologies of current era that based on Internet. The concept of cloud computing has exploded in popularity, and the reason for this is the cost-effective transmission, storage, and intensive computation that it offers. The goal is to provide end-users with remote storage and data analysis capabilities utilising shared computer resources, lowering an individual's overall cost. Consumers, on the other hand, are still hesitant to use this technology owing to security and privacy concerns. This paper provides a thorough overview of the different risks and technological security problems associated with cloud computing. We use the UNSW dataset to train the supervised machine learning models. We then test these models with ISOT dataset. The algorithm's accuracy for DoS and probe attacks was investigated, and the findings were given as confusion matrices. Cloud computing has changed the technological scope by offering cost-effective transmission, storage, and computation. It's security especially on Distributed Denial of Service Attacks remains a major concern. This study uses two datasets, UNSW and ISOT, to train and test supervised machine learning models for the prediction of DoS attacks. The model used achieved a remarkable accuracy of 99.6%. These findings present the ability of machine learning to improve cloud security in the near term.We have achieved an accuracy of 99.6% to predict a DoS attack. We present our results and argue that more research in the field of machine learning is still required for its applicability to the cloud security.

Keywords: Attack, Cloud security, Dos, Machine learning, Malicious threats.

Introduction

Even though cybersecurity is constantly evolving, distribution denial of service attacks (DDoS) (Musa,2018) remain a constant threat to the availability and security of cloud-based services. Organizations and businesses relying on cloud infrastructure are vulnerable to attacks that aim to flood a network or system with fraudulent data, which can have

devastating consequences. Due to the increasing complexity and magnitude of distributed denial of service (DDoS) attacks, traditional methods for detecting and mitigating these attacks are often inadequate. To better protect cloud computing systems against distributed denial of service attacks, machine learning (ML) (Ahmed,2024) has become an effective tool. Methods for foretelling DDoS attacks that rely on machine learning use the computational power of algorithms to sift through enormous amounts of real-time network traffic data. Training models using historical data that includes both typical network activity and known occurrences of distributed denial of service attacks teaches machine learning algorithms to spot trends and outliers that presage future attacks.

Companies can now anticipate and respond to distributed denial of service (DDoS) attacks before they cause major disruptions to their services (Liu,2022).

The ability of distributed denial of service (DDoS) attack prediction systems based on machine learning to adapt and evolve in reaction to new threats is one of its most notable advantages. In contrast to static rule-based approaches, machine learning models can learn from new data in real-time, allowing them to discover previously unseen attack pathways and zero-day vulnerabilities. Because both attack techniques and cloud environments are in a constant state of flux, with new vulnerabilities and attack methodologies appearing seemingly out of nowhere, this adaptability is crucial. Machine learning-based DDoS attack prediction systems use a number of distinct methods. Supervised, unsupervised, and semi-supervised learning methods are all part of this category. Training supervised learning methods like Random Forests and Support Vector Machines (SVM) (Ahmed,2024) requires labeled datasets that include examples of both benign and dangerous network traffic. The algorithms are trained using these datasets. Clustering and anomaly detection procedures are examples of unsupervised learning methods that can identify network outliers without labeled data. Hybrid systems that combine supervised and unsupervised learning techniques improve detection accuracy and scalability. These methods combine a bigger set of unlabeled data with a smaller set of labelled data.

Integration with cloud security architecture is crucial for the effective deployment of machine learning-based techniques to forecast distributed denial of service attacks (Sambangi,2020). Businesses can analyze network traffic data in real-time and respond to potential risks with minimal delays by using cloud-native machine learning platforms and services. When combined with existing security mechanisms like firewalls and intrusion detection systems, machine learning-based detection systems can provide an additional defense against distributed denial of service attacks. There is a lot of promise in ML-based DDoS attack prediction systems, but there are also certain limitations and challenges. Obtaining high-quality labeled training data can be challenging, particularly in different and dynamic cloud environments. Furthermore, adversarial manipulation and evasion attacks might potentially affect machine learning models. Malicious traffic specifically designed to evade security systems based on machine learning is created by the adversary in an effort to evade detection in targeted attacks.

A multi-faceted approach is necessary to tackle these challenges successfully (Ahmed,2023). Academics, business leaders, and cybersecurity professionals should work together to develop and implement adversarial robustness strategies, as well as robust machine learning algorithms. Working together, we can strengthen cloud security by using machine learning to ward off distributed denial of

service (DDoS) attacks and keep cloud-based services up and running. Collaboratively resolving these challenges will enable us to achieve this. Also, cloud environments are dynamic and resource-intensive, therefore DDoS attack prediction techniques based on machine learning are a good fit because of their scalability and computational efficiency. With the use of machine learning algorithms, companies can detect and respond to distributed denial of service attacks quickly by analyzing massive volumes of network traffic data in real-time. This scalability is of the utmost importance in cloud environments, where network traffic volumes might fluctuate greatly, and traditional detection methods cannot be able to cope.

In addition, techniques for predicting distributed denial of service attacks (Jamil,2018) that are based on machine learning provide a preventative measure for cybersecurity. Preventing attacks from impacting the availability of cloud services is the goal of this approach, which helps businesses prepare for potential threats. Automatic responses or alerts to cybersecurity specialists can be triggered by machine learning algorithms. This is achieved by keeping a close eye on the patterns of network traffic and identifying any irregularities that might indicate coming distributed denial of service attacks. Business organizations can protect their cloud infrastructure against DDoS attacks and mitigate their impact by using this preventative measure. Not only can machine learning-based prediction algorithms successfully detect and lessen the impact of distributed denial-of-service attacks, but they also give light on the specifics of cyber dangers. The patterns and trends in network traffic data can be studied by machine learning models to identify new vulnerabilities, attack vectors, and threats to cloud infrastructure. Firms can use this knowledge to better prepare for future cyber attacks and to help create security measures that are even stronger.

Improving cloud security and creating algorithms to detect DDoS attacks using machine learning both rely heavily on teamwork and the free flow of information (Ahmed,2023). By exchanging information, insights, and best practices, cybersecurity professionals, academics, and industry stakeholders can work together to create better detection and mitigation solutions. When it comes to cloud security, ideas can be shared, and innovations can be made via open-source initiatives, collaborative research, and industrial partnerships.In this paper, a machine learning concept for detecting DoS attacks in cloud surroundings is introduced. When applied with the UNSW and ISOT datasets, it shows prediction accuracy up to 99.6%, proving explicitly that supervised learning models can solve the issue of security in cloud systems."

A. Contributions

Following are the contributions of our research work,

- In this research work, a proactive and scalable approach to enhancing cloud security is to use machine learning-based techniques for anticipating distributed denial-of-service attacks.
- By using algorithms to examine network traffic patterns and identify anomalies, organizations can detect and mitigate distributed denial of service (DDoS) attacks in real time. This aids in reducing the impact of these dangers on the reliability and accessibility of services hosted in the cloud.
- Machine learning-based distributed denial of service attack prediction systems in cloud environments have the potential to become more effective and resilient with further study and collaboration, even in the face of present limitations.

II.Literature Review

(Wang, 2018) used supervised learning techniques to detect distributed denial of service attacks in cloud systems. Decision Trees and Support Vector Machines (SVMs) are two examples of such methods. Labeled datasets including examples of harmful and benign network traffic are used by the authors for training prediction algorithms. Because of this, they are able to attain a remarkable degree of precision. Among the study's many caveats is its reliance on labeled datasets, which could not be representative of the actual range of DDoS attack scenarios seen in cloud systems. When dealing with massive volumes of real-time network traffic data, the scalability of supervised learning methods can also be an issue.

In their article, Khatun et al. (2024) provide an overview of how machine learning techniques can address security risks in IoT-Healthcare systems, offering insights into how similar approaches might enhance cloud security frameworks. The study discusses risk mitigation strategies and their applicability in combating attacks, including DDoS, which emphasizes the importance of robust anomaly detection in securing interconnected systems.

In order to foresee distributed denial of service attacks in cloud networks, Chen, Lee, et al. provide an anomaly detection method in their article (Chen, 2023). Unsupervised learning techniques, such as K-means clustering and Isolation Forest, can help find the out-of-the-ordinary patterns in network data that point to DDoS attacks. True distributed denial of service attacks and actual anomalies can be difficult for anomaly detection algorithms to distinguish, which might lead to false positives. In addition, the feature representation quality and the anomaly detection algorithm utilized could impact the efficacy of these approaches.

Research by (Daniel, 2021) presents a hybrid machine learning technique that integrates supervised, unsupervised, and semi-supervised learning approaches. In cloud security, this method is meant to identify DDoS attacks. A more accurate prediction model that can consistently detect different types of distributed denial of service attacks is the goal of the authors. Combining many learning algorithms into one model might potentially lead to more computational complexity and overhead. It can also be challenging to choose the optimal combination of algorithms and adjust hyperparameters.

A technique for detecting distributed denial of service attacks in cloud environments that is based on deep learning is presented in a paper by (Yang, 2021). This setup employs LSTM networks and Convolutional Neural Networks (CNNs). The program can predict DDoS attacks in real-time by automatically learning traits from data on network traffic. Training deep learning models requires a lot of labeled training data and computing resources, which aren't always readily available in the cloud. Furthermore, it can be difficult to understand the reasoning behind the predictions made by deep learning models due to their limited interpretability.

Research by (Heo, 2023) examines how well ensemble learning methods like Gradient Boosting and Random Forests predict DDoS attacks in cloud security. The authors aim to improve the prediction accuracy by combining many weak learners into one model. When it comes to training and inference, ensemble learning systems can potentially need more computer resources and see an increase in computational complexity. Furthermore, it can be challenging to handle the diversity of these models and pick the optimum ensemble approach.

Building on recent advancements, Abdallah et al. (2024) explore the application of machine and deep learning techniques for anomaly detection in cloud networks. Their study highlights the potential of scalable and precise detection mechanisms while emphasizing challenges such as balancing computational costs and ensuring reliability in dynamic cloud environments.

In order to make distributed denial of service attack prediction systems that rely on machine learning more resistant to evasion attacks, (Kachavimath, 2021) have been studying adversarial robustness tactics. The authors use adversarial training and input sanitization to lessen the possibility of attackers tampering with network traffic. Prediction models can become more complicated and expensive to compute as a result of adversarial robustness tactics. The amount of experience and adaptability of those who carry out the attacks can also affect how effective these techniques are.

III.Dataset

Using an IXIA PerfectStorm software at the Cyber Range Lab of the Australian Centre for Cyber Security (ACCS), the UNSW-NB-15 dataset (Thakkar,2020) was developed with the purpose of developing a blend of real-time normal activities and synthetic modern attack behaviors from network traffic. In order to build the dataset, this was done. Using the tcpdump application, 100 GB of raw network data was recorded. This dataset contains nine distinct types of attacks: fuzzers, analysis, backdoors, DOS attacks, exploits, generic approaches, reconnaissance, shellcode, and worms. To generate a grand total of 49 class-labeled attributes, twelve methods are also developed (Alduailij,2022). Tools for keeping tabs on networks include Argus and Bro-IDS. We can find a more detailed description of the types of attacks and their characteristics in (Rajapraveen,2021) We can examine the statistics for the normal and abnormal packets in Table I, which is given as below in UNSW dataset.

TABLE I. UNSW dataset statistics

Dataset	Total records	Normal	Anomalous
Training	175342	56000	119341
Testing	82332	37000	45332
Total	257674	93000	164674
Percentages	100%	36.1%	63.9%

Two separate datasets, one of which includes malicious traffic from the French Honeynet project chapter, were combined to form the ISOT dataset (Alzahrani,2021). Both the Storm and Waledac botnets provided the data used in these analyses [22]. To further ensure an authentic portrayal of benign, everyday traffic, two separate datasets have been integrated. Hungarian firm Ericsson Research's Traffic Lab provided the first dataset (Mishra,2021), while LBNL's Lawrence Berkeley National Laboratory (LBNL) provided the second one (Thakkar,2022). These numbers include 22 different subnets and were compiled over the course of three months, from October 2004 to January 2005. An overview of the ISOT dataset's statistics can be seen in the table II. The results that we obtained from combining these two datasets with many important supervised machine learning techniques will be detailed in the section that follows.

TABLE II. ISOT dataset statistics

Traffic type	Unique flows	Percentages
Training	55904	3.33%
Testing	1619520	96.66%
Total	1675424	100%

IV.Methodology

A. Support Vector Machines (SVM)

Classification issues, including the prediction of denial-of-service attacks, are well-suited to SVM, a popular supervised learning approach. The hyperplane that Statistical Vector Machines (SVMs) produce allows them to distinguish between legitimate and malicious network traffic.

B. Decision Trees

By dividing the feature space according to the values of the characteristics within it, decision trees can create a tree-like structure that can be utilized for categorization. Decision tree-based models are used to effectively capture intricate decision boundaries and identify patterns indicative of denial-of-service attacks.

C. K-means Clustering

The K-means clustering algorithm organises data points into sets according to their similarities; it is an unsupervised learning method. K-means clustering can analyze network traffic patterns and identify out-of-the-ordinary clusters that might indicate the presence of denial-of-service attacks.

D. Isolation Forest

One form of anomaly detection methodology is the Isolation Forest method, which separates data points into divisions and isolates cases by randomly selecting characteristics. Isolation Forest works well to prevent DOS attacks because it treats instances that need fewer splits to isolate as anomalies.

E. Bayesian Machine Learning

Bayesian methods provide a probabilistic framework for describing uncertainty and incorporating prior knowledge into prediction models. Bayesian methodologies and approaches are interchangeable terms. One possible application of Bayesian Machine Learning techniques is to forecast DoS attacks. Gathering uncertainty from network traffic data and using it to make probabilistic predictions is one of these methods.

F. Random Forests

As an ensemble learning model, Random Forests combine many decision trees to provide predictions. The technique of pooling the predictions of individual trees on the tree allows Random Forests to boost forecast accuracy and robustness, making them effective for DoS attack prediction.

G. Gradient Boosting Machines (GBM)

A technique called GBM builds prediction models sequentially. It is an ensemble learning approach. Using this approach, subsequent models fix the errors of their predecessors. High prediction accuracy and complicated correlation identification are two capabilities that GBM brings to the table when it comes to identifying denial of service attacks.

The goal of this approach is to classify traffic data as either suspicious, normal, or unknown, and then draw conclusions based on the performance indicators provided below. Table III presents the performance parameter definitions. Formulae for performance matrix is shown in table IV.

TABLE III. Performance parameter DEFINITIONS

TP (True Positives)	The model's accurate prediction of positive class outcomes is represented by the True Positive Value.
FP (False Positives)	The model's ability to effectively predict the negative class's outcomes is shown by the True Negative Value.
TN (True Negatives)	The term "False Positive Value" refers to the model's incorrect prediction of positive class outcomes.
FN (False Negatives)	The model's incorrectly predicted negative class outcomes are represented by the False Negative Value.

TABLE IV. Formulae for Performance Matrix.

Accuracy	$\frac{(TP+TN)}{(TP+TN+FP+FN)}$
Precision	$\frac{TP}{(TP+FP)}$
Recall	$\frac{TP}{(TP+FN)}$
Specificity	$\frac{TN}{(TN+FP)}$
F measure	$\frac{2TP}{(2TP+FP+FN)}$

V.Results

Support Vector Machine, k-means, Decision tree Random Forest, and Naïve Bayes were among the algorithms used for training and testing purposes on the dataset. We can see the results of using the confusion matrix to evaluate the classifiers in Table V. A total accuracy of 95.6% was found for k-means, 94.4% for Decision tree, 99.6% for Random Forest, 97.8% for Support Vector Machine, and 98.2% for Naïve Bayes. Due to the imbalanced data, specificity, recall, and accuracy should all be considered equally relevant. Analyzing these various algorithms. In comparison to Random Forest, the Support Vector Machine (SVM) performs better across the board, including recall, accuracy, f-measure specificity, and f measure. A visual representation of the data collected during testing can be shown in Fig. 1.

TABLE V. Calculated Performance Metric's Results.

ML Techniques	Recall	Precision	Accuracy	F-measure
K-means	0.99	0.923	0.956	0.958
Decision tree	0.928	0.992	0.944	0.965
SVM	0.997	0.997	0.996	0.997
Random forest	0.994	0.993	0.978	0.828
Naïve Bayes	0.87	0.882	0.982	0.987

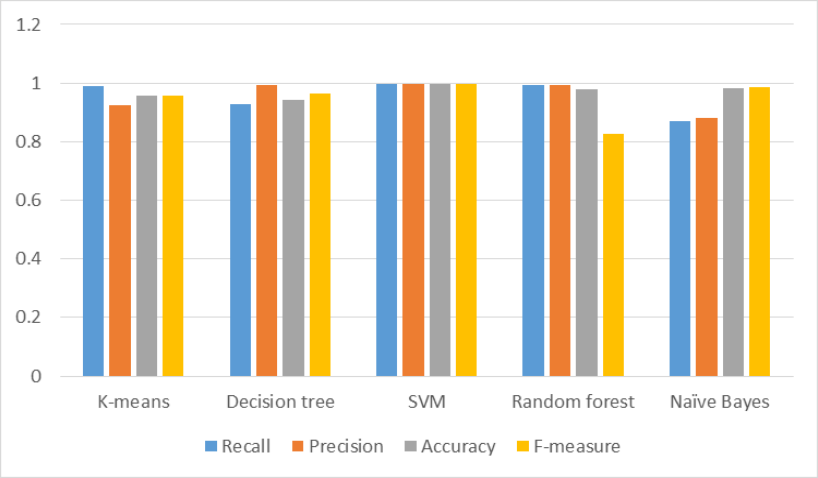

Fig. 1. Graphical representation of results during the testing phase.

VI.Conclusions

A comprehensive analysis of the cloud computing security threats is required to determine how these risks can affect real-world cloud-based situations. In order to make cloud computing more secure, it is recommended to enhance the security features of online services and browsers. This is derived from the results obtained using SLR. Thus, as part of the continuing development, the cloud's security can have its foundations fortified. The standards, underlying protocols, and tools used in cloud situations provide support for these foundations. A sea change has occurred in the IT industry as a result of cloud computing. Businesses and organizations alike get a plethora of benefits from it. While cloud computing does provide many advantages, it is nevertheless vulnerable to security breaches. Consequently, there are a lot of obstacles to cloud computing adoption, the most critical of which is security. Security issues and attacks have been public knowledge among both vendors and customers. The research has shown that there are a lot of threats, attacks, and security issues that make it hard to use cloud computing. The unique characteristics of the cloud, such as resource sharing and pooling, as well as other security-related issues, give rise to challenges and problems with security. According to the provider's security concerns, a range of cloud security risks and attacks are analyzed. One of the main reasons thought to be delaying the development of cloud computing is the associated security issues, which are among the most critical. We have covered all the bases when it comes to the many dangers and technological security concerns associated with cloud computing in this essay. We have used the UNSW dataset to train the supervised machine learning models. Then, we do an evaluation of these models using the ISOT dataset. We used confusion matrices to show the findings of our study on the algorithm's accuracy against denial-of-service and probing attacks. In terms of forecasting DoS attacks, we have a 99.6 percent success rate. We argue that more research into machine learning is required to establish its applicability to cloud security via the presenting of our results.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] N. Musa, "A conceptual framework of IT security governance and internal controls," in *Cyber Resilience Conference (CRC)*, Putrajaya, Malaysia, 2018, pp. 1-4: IEEE. DOI: 10.17576/apjitm-2018-0702(02)-06

[2] A. A. Ahmed et al., "Secure AI for 6G Mobile Devices: Deep Learning Optimization Against Side-Channel Attacks," *IEEE Transactions on Consumer Electronics*, 2024. DOI: 10.1109/TCE.2024.3372018

[3] Z. Liu, L. Qian, and S. Tang, "The prediction of DDoS attack by machine learning," in *Third International Conference on Electronics and Communication; Network and Computer Technology (ECNCT 2021)*, Harbin, China, 2022, vol. 12167, pp. 681-686: SPIE. DOI: 10.1117/12.2628658

[4] A. Abbas Ahmed, M. Kamrul Hasan, S. Azman Mohd Noah, and A. Hafizah Aman, "Design of Time-Delay Convolutional Neural Networks (TDCNN) Model for Feature Extraction for Side-Channel Attacks," *International Journal of Computing Digital Systems*, vol. 15, no. 1, pp. 1-9, 2024. DOI: 10.12785/ijcds/160127

[5] S. Sambangi and L. Gondi, "A machine learning approach for DDoS (distributed denial of service) attack detection using multiple linear regression," in *14th International Conference on Interdisciplinarity in Engineering*, Târgu Mureș, Romania, 2020, p. 51: MDPI. DOI: 10.3390/proceedings2020063051

[6] A. A. Ahmed, M. K. Hasan, N. S. Nafi, A. H. Aman, S. Islam, and S. A. Fadhil, "Design of Lightweight Cryptography based Deep Learning Model for Side Channel Attacks," in *33rd International Telecommunication Networks and Applications Conference*, Melbourne, Australia, 2023, pp. 325-328: IEEE. DOI: 10.1109/ITNAC59571.2023.10368560

[7] A. Jamil and Z. M. Yusof, "Information security governance framework of Malaysia public sector," *Asia-Pacific Journal of Information Technology Multimedia*, vol. 7, no. 2, pp. 85-98, 2018. DOI: 10.17576/apjitm-2018-0702-07

[8] A. A. Ahmed, M. K. Hasan, N. S. Nafi, A. H. Aman, S. Islam, and M. S. Nahi, "Optimization Technique for Deep Learning Methodology on Power Side Channel Attacks," in *33rd International Telecommunication Networks and Applications Conference*, Melbourne, Australia, 2023, pp. 80-83: IEEE. DOI: 10.1109/ITNAC59571.2023.10368481

[9] L. Wang, "Understanding Cloud Application Security Via Measurements," *PhD. Thesis*, The University of Wisconsin-Madison, Madison, Wisconsin, 2018.

[10] Chen, Lee, et al., "Defense Mechanism based on Game Theory for Securing Cloud Infrastructure against Co-Resident DoS Attacks," *International Journal of Systems Management Innovation Adoption*, vol. 13, no. 22, p. 8, 2023.

[11] A. Daniel and M. O. Momoh, "A computer security system for cloud computing based on encryption technique," *Computer Engineering Applications Journal*, vol. 10, no. 1, pp. 41-54, 2021. DOI: 10.18495/comengapp.v10i1.354

[12] Y. Yang, W. Shen, B. Ruan, W. Liu, and K. Ren, "Security challenges in the container cloud," in *Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, Atlanta, GA, USA, 2021, pp. 137-145: IEEE. DOI: 10.1109/TPSISA52974.2021.00016

[13] Heo, et al., "MyData Cloud: Secure Cloud Architecture for Strengthened Control Over Personal Data," *Research Square*, no. PREPRINT (Version 1), 16 August 2023. DOI: 10.21203/rs.3.rs-3250636/v1

[14] Kachavimath and Narayan, "A Deep Learning-Based Framework for Distributed Denial-of-Service Attacks Detection in Cloud Environment," in *Advances in Computing and Network Communications*, Singapore, 2021, pp. 605-618: Springer. DOI: 10.1007/978-981-33-6977-1_44

[15] S. Reddy and Shyam, "A machine learning based attack detection and mitigation using a secure SaaS framework," *Journal of King Saud University-Computer Information Sciences*, vol. 34, no. 7, pp. 4047-4061, 2022. DOI: 10.1016/j.jksuci.2020.10.005

[16] A. Aljuhani, "Machine learning approaches for combating distributed denial of service attacks in modern networking environments," *IEEE Access*, vol. 9, pp. 42236-42264, 2021. DOI: 10.1109/ACCESS.2021.3062909

[17] U. A. Butt et al., "A review of machine learning algorithms for cloud computing security," *Electronics*, vol. 9, no. 9, p. 1379, 2020. DOI: 10.3390/electronics9091379

[18] Sudar, et al., "Detection of Distributed Denial of Service Attacks in SDN using Machine learning techniques," in *International Conference on Computer Communication and Informatics (ICCCI)*, Coimbatore, India, 2021, pp. 1-5: IEEE. DOI: 10.1109/ICCCI50826.2021.9402517

[19] Alduailij et al., "Machine-learning-based DDoS attack detection using mutual information and random forest feature importance method," *Symmetry*, vol. 14, no. 6, p. 1095, 2022. DOI: 10.3390/sym14061095

[20] Rajapraveen and Pasumarty, "A Machine Learning Approach for DDoS Prevention System in Cloud Computing Environment," in *IEEE International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS)*, Bangalore, India, 2021, pp. 1-6: IEEE. DOI: 10.1109/CSITSS54238.2021.9683768

[21] Alzahrani et al., "Security analysis of DDoS attacks using machine learning algorithms in networks traffic," *Electronics*, vol. 10, no. 23, p. 2919, 2021. DOI: 10.3390/electronics10232919

[22] Revathi, et al., "A machine learning based detection and mitigation of the DDOS attack by using SDN controller framework," *Wireless Personal Communications*, vol. 127, pp. 1-25, 2022. DOI: 10.1007/s11277-021-09071-1

[23] Mishra, et al., "Classification based machine learning for detection of DDoS attack in cloud computing," in *IEEE International Conference on Consumer Electronics (ICCE)*, Las Vegas, NV, USA, 2021, pp. 1-4: IEEE.

[24] A. Thakkar and R. Lohiya, "A Review of the Advancement in Intrusion Detection Datasets," *Procedia Computer Science*, vol. 167, pp. 636-645, 2020. DOI: 10.1016/j.procs.2020.03.330

[25] M. A. Khatun, S. F. Memon, C. Eising, and L. L. Dhirani, "Machine Learning for Healthcare-IoT Security: A Review and Risk Mitigation," *IEEE Access*, vol. 11, pp. 145869-145896, 2024. DOI: 10.1109/ACCESS.2024.3274872

[26] A. M. Abdallah, A. Alkaabi, G. B. Alameri, S. H. Rafique, N. S. Musa, and T. Murugan, "Cloud Network Anomaly Detection Using Machine and Deep Learning Techniques—Recent Research Advancements," *IEEE Access*, vol. 12, pp. 56749-56773, 2024. DOI: 10.1109/ACCESS.2024.3298146

Yasir Mahmood Younus received the B.Sc. degree in Computer Techniques Engineering from Alrafidain university college, and the M.Sc. degree in Computer Software Engineering from Ferdowsi University, in 2021. He is Computer Techniques Engineering, Imam Al-Kadhum College (IKC). His research interests include Machine learning and Deep learning.

Ahmed Salman Ibraheem received the B.Sc. degree in computer science from the University of Baghdad, and the M.Sc. degree in computer science from, IZU - South Tehran Branch, in 2023. From Junuary 2023 to July 2024, he was a Lecturer with the Imam Al-Kadhum College, Baghdad, Iraq.

Murteza Hanoon Tuama received the B.Sc. degrees in computer science from the Science College, University of Basrah, Iraq, in 2010, respectively, and the MSc. degree from the Imam Reza International University of Science and Technology, Iran, in 2022. He is Computer Techniques Engineering, Imam Al-Kadhum College (IKC). His research interests include Machine learning and Deep learning**.**

Wahhab Muslim mashloosh received the B.Sc. degrees in computer science from the Science College, University of Imam alsadk Iraq, in 2008,2009 respectively, and the MSc. degree from the Imam Reza International University of Science and Technology, Iran, in 2022. He is Computer Techniques Engineering, Imam Al-Kadhum College (IKC). His research interests include Machine learning and Deep learning.