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)

DEC 2024 ISSUE52 VOL 23

www.misan-jas.com

journal.m.academy@uomisan.edu.iq

رقم الايداع في دار الكتب والوثائق بغداد 1326 في 2009

الصفحة	فهرس البحوث	ت
15 – 1	**The Relationship Between Periodontitis Severity and MCP-1, IL-6 Levels in Gingival Crevicular Fluid** Mohammed Faisal Ali Ghada Ibrahim Taha	1
29 – 16	**Organizational Reflection and Its Impact on Strategic Performance: An Analytical Research in the General Company for Electrical and Electronic Industries** Ayman Abdul Sattar Jasim Aamer Fadous Azib Al-Lami	2
42 - 30	**Convolutional Neural Networks in Detection of Plant Diseases** Shaymaa Adnan Abdulrahman	3
57 - 43	**Gestural and Facial Expression Feedback in Motivating EFL Learners to Learn Grammar** Inas Kamal Yaseen	4
67 - 58	**The Effect of Titanium Oxide Nanotubes on the Surface Hardness of a Three-** **Dimensional Printed Denture Base Material** Anwr Hasan Mhaibes Ihab Nabeel Safi	5
81 - 68	**Myofunctional Appliance for Class III Malocclusion: A review** Maryam S. Al-Yasari Layth M. Kareem Ihab N. Safi Mustafa S. Tukmachi Zahra S. Naji	6
91 - 82	**The Intertwined Trajectory between Gender and Psychic Anxiety in Chimamanda Ngozi Adichie's Americanah** Tahseen Ali Mhodar Hayder Ali Abdulhasan	7
104 - 92	**The Role of Digital Human Resource Management Practices in Achieving Employee Well-being: An Analytical Study within the Civil Aviation Authority** Ayman Kadhum Al-Qaraghouli Ali Hasson Al-Taee Sinan Fadhel Hamad	8
113 - 105	**Employing the Frontload Vocabulary Strategies in Enhancing Iraqi EFL Students' Vocabulary Retrieval Abilities** Aswan Fakhir Jasim	9
122 - 114	**Assessment of the surface hardness of high-impact polymethylmethacrylate following long-term dipping in clove oil solution** Karrar Salah Al-Khafagi Wasmaa Sadik Mahmood	10

133 - 123	**Improved Machine Learning Techniques for Precise DoS Attack Forecasting in Cloud Security** Yasir Mahmood Younus Ahmed Salman Ibraheem Murteza Hanoon Tuama wahhab Muslim mashloosh	11
147 - 134	**The Impact of Using Menus Strategy on the Performance of Iraqi University Students in English as a Foreign Language in Writing Composition** Ansam Ali Sadeq	12
167 - 148	**Attitudes of students in the Department of General Science in the College of Basic Education towards electronic tests** Shaimaa Jasim Mohammed	13
188 - 168	**The Systemic Heterogeneity in Adnan Al-Sayegh's Poetry – with Reference to Group (Text Dice)** Abdulrahman Abdullah Ahmed	14
198 - 189	**Legal Means Employed by the Iraqi and French Legislators to Deter Abuse of Office: A Comparative Study** Mahdi Khaghani Isfahani Jaafar Shakir Hussein	15
208 - 199	**Challenges of the social and structural identity in the Middle East)Iraq as a model(** Yousif Radhi Kadhim	16
226 - 209	**Evaluation of the Susceptibility of some Eggplant Varieties and the Role of Their Biochemical Compounds in Resistance to the Leafhopper *Amrasca biguttula*** Fayroz T. Lafta Aqeel Alyousuf Hayat Mohammed Ridhe Mahdi	17
241 - 227	**The Effect of Using Modern Technologies on the Interaction of Middle School Students in Geography** Ali Fakhir Hamid	18
252 - 242	**Narrative themes in the papers of Atyaf Sanidah, the novel (I may be me) as a mode** Raad Huwair Suwailem	19

272 - 253	**The Role of Composing the Soundtrack for the Dramatic Film (Psychopath): An Analytical Study** Seerwan Mohammad Mustafa Abdulnaser Mustafa Ibrahim	**20**
287 - 273	**The psychological connotations of poetic images in the poetry of Rahim Al-Gharabawi** Salam Radi Jassim Al-Amiri Mehdi Nasseri Haider Mahallati	**21**
311 - 288	**Pedagogical Knowledge Competencies Among Students/Teachers in the Mathematics Department and Their Relationship to Professional Motivation** Duha Hamel Hussei Haider Abdel Zahra Alwan	**22**
323 - 312	**Derivatives in douaa Alahad: a semantic morphologicalstudy** Zahraa shehab Ahmed	**23**
330 - 324	**The effect of biological control agents in controlling the larval stages of *Spodoptera littoralis* in Basra Governorate** Zahraa J. Khadim and Ali Zachi Abdulqader	**24**

Misan Journal for Academic studies
مجلة ميسان للدراسات الاكاديمية
Vol 23 Issue 52 Dec 2024
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 costeffective 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

Yet, if we follow the evolution of cybersecurity, distribution denial of service attacks (DDoS)Musa,2018) will continue to represent a permanent risk to the availability and security of cloud-based services. The cloud environment has affected the traditional structure and approach of many businesses and organizations that relied heavily on hardware; this caused them to become victims of cyber-attacks that try to inundate a network or system with fake data that they have obtained, which proves to be catastrophic. As DDoS attacks continue to increase in complexity and scale, conventional methods of DDoS attack detection and mitigation are seldom adequate. The use of machine learning (ML) (Ahmed,2024) has emerged as a useful method for protecting cloud computing systems from distributed denial of service attacks. Machine learning-based DDoS attack forecasting uses an algorithm's processing capacity to analyze vast amounts of real-time network traffic information. By training models on historical data that includes both normal network usage patterns and known distributed denial of service attacks, machine learning algorithms learn to identify trends and outliers that can indicate future attacks. The companies are able to Predict and respond to Distributed denial of service (DDoS) attacks before they can bring down their services(S.Liu,2022)

One of the most significant advantages of machine learning-based DDoS attack prediction systems is their ability to learn and adapt to new threats. Unlike static, rule-based approaches, machine learning models can learn from fresh data and in real time, uncovering new attack paths and zero-day vulnerabilities. This adaptability is critical because attack methods and cloud environments are always changing, with new vulnerabilities and methods of attack seemingly appearing from nowhere. Some distinct techniques are used in ML-based DDoS attack prediction systems. This domain includes supervised, unsupervised, and semi-supervised learning methods. Supervised learning methods such as Random Forests and Support Vector Machines (SVM) (Ahmed,2024), will require training on datasets with initiation labels for both benign and dangerous network traffic. Unsupervised learning techniques such as clustering and anomaly detection algorithms are capable of exposing network outliers without labeled data. Hybrid systems combining supervised and unsupervised learning methodologies allow for enhanced detection precision and scalability. These approaches mix a larger corpus of unlabeled data with a smaller corpus of labelled data. The effective deployment of machine learning-based techniques to forecast distributed denial of service attacks requires the integration with cloud security architecture (Sambangi,2020). With the help of cloud-native machine learning services and platforms, businesses can collect and analyze the network traffic data and respond taking appropriate actions by minimizing response delays. This is particularly useful since machine-learning based detection systems, when coupled with existing security mechanisms such as firewalls, IDSs, and so on, can add an extra level of defense to protect from distributed denial of service attacks. ML-based DDoS attack prediction systems have enormous potential, but as well certain limitations and challenges. Collecting high-quality labeled training data can be even harder on the wide range of dynamic cloud environments. In addition, machine learning models may also be affected by adversarial manipulation and evasion attacks. In targeted attacks, adversaries create malicious traffic specifically tailored to evade machine learning-based security systems.

A combination of measures is required to meet these challenges successfully (Ahmed,2023). It calls for research collaboration between academics, business leaders, and cybersecurity professionals to design and train until well-loved adversarial robustness strategies, along with the necessary robust machine learning algorithms to support them academically. Collaboratively, we can enhance cloud security by implementing machine learning to defend against distributed denial of service (DDoS) attacks to maintain uptime of cloud-based services. We can achieve this through collaborative efforts to solve these challenges. In addition, DDoS attack prediction techniques based on machine learning are well-suited for cloud environments as well since such environments are dynamic and require a lot of resources, and the scalability and computational efficiency of the proposed model is a good match. This enables organizations to analyze massive volumes of network traffic data in real-time using machine learning algorithms to detect and respond to DDoS attacks quickly. This is especially important in cloud environments, where the amount of data transmitted over the network can vary immensely and traditional detection methods are unlikely to be able to handle it.

Furthermore, these machine-learning-based methods for predicting the distributed denial of service attacks (Jamil,2018) act as an advance precautionary measure for the field of cyber security. This approach helps businesses prepare for potential threats by preventing attacks from affecting cloud services availability. Machine learning algorithms can trigger automatic responses or alerts to cybersecurity specialists. This is done by monitoring the connections in network traffic for any abnormal activity before attacks from the junk robots which calls for distributed denial of service attacks are received. This preventative measure helps business organizations to safeguard their cloud infrastructure from DDoS attacks and mitigate their impact. Machine learning-based prediction algorithms can not only successfully identify and diminish the effect of managed denial-of-service attacks, but additionally offer insight into the specifics of cyber risk. Machine learning models can analyze network traffic data to detect patterns and trends allowing them to find new weaknesses, attack vectors, and threats against cloud infrastructure. Companies can leverage this information to improve prevention, and aid in developing stronger security practices.

Both Enhancing Cloud Security and Developing Algorithms to Detect DDoS Attacks Using Machine Learning require a lot of teamwork and the open exchange of information (Ahmed,2023). Collaborating data, sharing insights and ideas and exchanging best practices enables cybersecurity professionals, academicians and stake holders in the industry to come together and formulate solutions with better detection and mitigation capabilities. In cloud security, sharing ideas and innovating are being done through open-source initiatives, collaborative research and industrial partnerships. This paper presents an ML-based approach to identify DoS attack attack in cloud environment. "This makes it concrete that the supervised learning models can solve the problem of security in cloud system when comes to the use of the dataset which is UNSW and ISOT with prediction accuracy as high as 99.6%.

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) applied a supervised learning approach to identify DDoS attacks in cloud environments. Methods, such as Decision Trees and Support Vector Machines (SVMs) are examples of these. The authors train a prediction algorithm with a set of labeled datasets that could contain an example of malicious and benign network traffic. This allows them to achieve a stunning level of accuracy. One of the many caveats of the study is the use of labeled datasets that may not reflect the real distribution of DDoS attack scenarios observed in cloud systems. "Also, the scalability of supervised learning methods may become a challenge when processing high volumes of real-time network traffic data.

Khatun et al. (2024) offer an overview of using machine learning techniques to mitigate security risks in IoT-Healthcare systems and provide insights into ways in which similar approaches could strengthen frameworks for the security of cloud systems. Risk mitigation strategies and their adaptation in the fight against attacks such as DDoS, thus highlighting the need for effective anomaly detection to adequately protect interlaced systems.

To predict distributed denial of service attacks in the cloud networks, Chen, Lee et al. give in their article an anomaly detection approach (Chen, 2023). Network DDoS attacks can be uniquely characterized based on the unusual patterns found in network behavior, and using unsupervised learning techniques, such as K-means clustering and Isolation Forest, can be used to identify potential DDoS attacks. Anomaly detection algorithms may have a hard time differentiating real distributed denial of service attacks from genuine anomalies, which results in false positives. Moreover, the effectiveness of these approaches can be affected by the quality of the feature representation and the anomaly detection algorithm used.

A hybrid machine learning model is proposed by (Daniel, 2021) which employs a combination of supervised, unsupervised and semi-supervised learning techniques. In cloud security, this approach is used for DDoS attack detection. The authors are seeking a model which would better predict and permit consistent detection of multiple types of distributed denial of service attacks. Keeping many learning algorithms together in a single model may make it more computationally complex and introduce overhead. Also, selecting the best algorithms and tuning hyperparameters can be hard.

The authors of (Yang, 2021) presented a deep learning based method to detect distributed denial of service attacks in different cloud environments. In this configuration, they make use of LSTM networks and CNNs. By learning practices from the network traffic data, the system can classify DDoS which will automatically predict DDoS in real-time. Deep learning model training will often needs large scale labeled training set to be prepared, and the corresponding computing resources: they may not always be patient to slap in the cloud. Additionally, it is hard to explain why deep learning models made certain predictions because of their black nature. It validates the ensemble learning techniques including Gradient Boosting and Random Forests as effective methods for predicting DDoS attacks within cloud security (Heo, 2023). The goal of the authors is to take many weak learners, and combine them into one model that predicts well. However, the ensemble learning systems may require more computer resources and higher computational complexity in training and inference studies. Moreover, the range of these models can be difficult to manage enabling the best ensemble method. Extending recent progress, Abdallah et al. (2024) investigate the use of machine and deep learning techniques in for detecting anomalies within cloud networks. (Empirical Evaluation of Evasion Attacks and Defense Mechanisms on DDoS Attack Prediction, 2021) have been researching on adversarial robustness techniques to make machine learning based distributed denial of service attack prediction systems more resistant to evasion attacks. The authors apply adversarial training and input sanitization to mitigate the risk of attackers manipulating the network traffic. These adversarial robustness tactics can leverage the prediction models to be more complex and expensive to infer. How effective these techniques are can also vary depending on the experience and adaptability of those who carry out the attacks.

III.Dataset

At the Cyber Range Lab of the Australian Centre for Cyber Security (ACCS), using IXIA PerfectStorm software; the UNSW-NB-15 dataset (Thakkar,2020) created with a key objective of generating a mixture of real-time ordinary actions and synthetic new attack behaviors from network traffic. This was done in order to reconstruct the dataset. Raw network captures of 100 GB was recorded using the tcpdump application. This dataset consists of 9 different types of attacks, namely: fuzzers, analysis, backdoors, DOS attacks, exploits, generic approaches, reconnaissance, shellcode, worms. In total, twelve methods are also developed to produce the grand total of 49 class-labeled attributes (Alduailij,2022). Some examples of network monitoring tools are Argus and Bro-IDS. A detailed description regarding types of attacks and their features can be found in (Rajapraveen,2021) Statistics for normal and abnormal packets can be inspected from Tables I, which is shown 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%

ISOT dataset had been compiled from two different datasets where one of the datasets is from the malicious traffic collected by the French Honeynet project chapter (Alzahrani,2021). In these analyses, both the Storm and Waledac botnets contributed their data [22]. To additional capture a true representation of benign, normal activity, two distinct datasets have been fused together. Hungarian firm For the first data set, we primarily used Traffic Data from Ericsson Research (Mishra,2021), while also including data from Lawrence Berkeley National Laboratory (LBNL) (Thakkar, 2022) as the second data set. The shown counts involve 22 unique subnets, and were gathered between October 2004 and January 2005. Table II: An overview of the ISOT dataset statistics. The next section will elaborate the results we obtained when we employed numerous significant supervised machine learning algorithms to the two datasets that we fused together.

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 sorts using similarities of the data points in to sets; it is an unsupervised learning method.| For example, K-means clustering can process network traffic patterns and find unusual clusters which may indicate the presence of denial-of-service attacks.

D. Isolation Forest

A specific type of anomaly detection method is called an Isolation Forest method, in this a data point is divided into N number of divisions, where value of N can differ from 1 to n, and a case is isolated according to randomly selected characteristics. Isolation Forest is another algorithm that can be used to prevent DOS attacks as it will treat instances that require fewer splits to isolate as anomalies.

E. Bayesian Machine Learning

Bayesian methods provide a rich framework for representing uncertainty and for integrating prior knowledge into predictive models. Methods and approaches to Bayesian statistics are used interchangeably. We use Bayesian Machine Learning techniques to forecast DoS attacks. This approach consists of collecting uncertainty from network traffic data and leveraging it to make probabilistic forecasts.

F. Random Forests

Random Forests is an ensemble learning model which combines many decision trees to make predictions. To combine the predictions of individual trees on the tree, Random Forests are trained-up to improve accuracy and robust forecasting, making this ensemble method suitable for DoS attack prediction.

G. GBM (Gradient Boosting Machines)

One of the models GBM builds prediction models iteratively. It is an ensemble learning method. This way, successive models correct the mistakes of the previous ones. GBM offers two complimentary functions that make it very suitable for detection of denial of service attacks: high prediction accuracy and identification of complex correlations.

An implementation of this method aims to categorize traffic data as suspicious, normal, or unknown, and infer accordingly through the performance metrics listed below. The definitions of performance parameters are given in Table III. This table IV represents the formulae for performance matrix.

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

Algorithms such as Support Vector Machine, k-means, Decision tree Random Forest, and also Naïve Bayes were used to train and test the dataset. In table V we can see how the confusion matrix is used to evaluate the classifiers, where k-means produced an overall accuracy of 95.6%, Decision tree an accuracy of 94.4%, Random forest got an accuracy of 99.6%, Support vector machine gave a score of 97.8% and Naïve bayes provided an accuracy of 98.2%. That being said, due to the imbalanced data specificity, recall and accuracy all should be seen as equally relevant. Testing-out these different algorithms. Compared to Random Forest, the SVM has higher values for recall, accuracy, fmeasure specificity, and f measure. In Fig. it is shown a visual representation of the data collected from the testing phase. 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

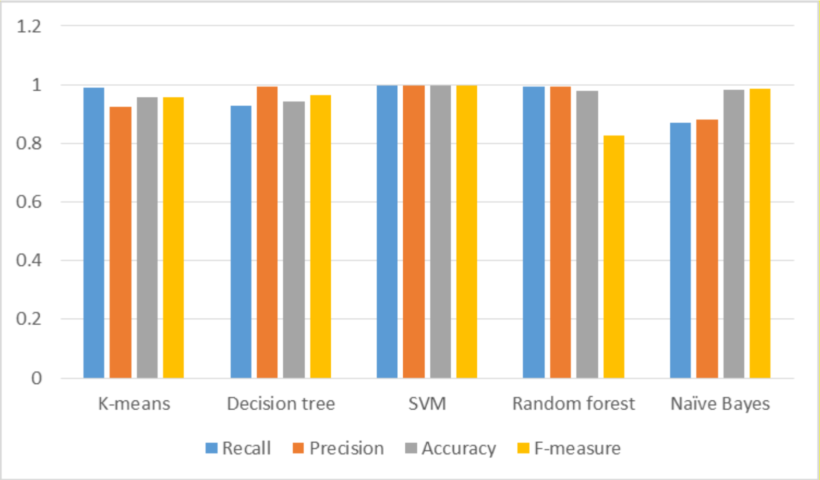

Fig. 1. Graphical representation of results during the testing phase.

VI.Conclusions

An assessment overview of these Cloud-computing security threats is essential for finding how these risks can impact actual use cases of Cloud-based scenarios. Nothing is better than taking time to revive the security parameters of cloud computing by making online services and browsers a little more secure. So based on the SLR results this is derived from. So, the security of the cloud can be reinforced as part of the ongoing evolution. The underlying protocols, standards, and tools in cloud situations can reinforce these foundations. Cloud computing has swept the IT industry by a sea change. It offers a host of benefits to businesses and organizations alike. Cloud computing comes with several benefits, but it is prone to security vulnerabilities. So there are various hindrances in cloud computing adoption with the most vital being security. Security issues and attacks have been well-known to both vendors and customers. It is primarily the work of many researchers who have displayed numerous threats, attacks, and security problems that make cloud computing quite difficult to implement. Cloud has unique features like resource sharing, resource pooling and facing, and security related issues which cause the challenges and problems in security. The cloud security risks and attacks are evaluated according to the provider's security issues. Security issues associated with cloud computing are among the most critical and one of the most paramount reasons considered to hinder its development. We have traversed a lot of ground in this article about the various threats or technology security threats of cloud computing. The supervised machine learning models learned on the UNSW dataset. We then evaluate these models on the ISOT dataset. The results of our research are showcased along with the corresponding confusion matrices of the algorithm for denial-of-service and probing attacks. For predicting DoS attacks, we are 99.6 percent effective. The presentation of our work is intended to argue that further research into machine learning needs to be conducted to demonstrate the approach can be applied to cloud security.

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 AlKadhum College (IKC). His research interests include Machine learning and Deep learning.