International Research Journal of Management Science & Technology



ISSN 2250 – 1959(0nline)
2348 – 9367 (Print)

An Internationally Indexed Peer Reviewed & Refereed Journal

www.IRJMST.com
www.isarasolutions.com

Published by iSaRa Solutions

Review on Detection of DDoS Attacks using Machine Learning for Cloud Security

Chhaya Makhijani
(Research Scholar)

Yogendra Yati
Assistant Professor
Deptt. of Computer. Sc. &Appl.
S.V. (Auto.) PG College,
Bairagarh Bhopal (M.P.)

Anil Kumar Gupta
HOD, Department of Computer Science, UTD,
Barkatullah University,
Bhopal (M.P.)

Abstract

The rapid growth of cloud computing has revolutionized data storage, processing, and service delivery but has also intensified cybersecurity challenges, particularly Distributed Denial of Service (DDoS) attacks, data breaches, and privacy violations. This study synthesizes findings from 29 research papers published between 2017 and 2025 that explore how Machine Learning (ML) and cryptographic techniques enhance cloud security. The review identifies DDoS detection, intrusion detection systems (IDS), and data encryption as the most actively researched domains. Frequently used ML algorithms include Support Vector Machines (SVM), Random Forest, Decision Trees, and Naïve Bayes, while deep learning models such as CNN, RNN, and LSTM are emerging for complex attack detection. Studies report high accuracy levels (up to 99%) using datasets like KDD Cup'99, CICIDS2017, and CICDDoS2019. Despite these advancements, challenges persist in dataset relevance, real-time detection, and integration with IoT and big data environments. The review concludes that hybrid models combining machine learning, cryptography, and intelligent automation represent the future of robust, scalable, and adaptive cloud security systems.

Keywords:- Cloud Computing , Support Vector Machines (SVM), Random Forest, Decision Trees, Naïve Bayes, Deep learning, Machine Learning , KDD, IDS, DDOS.

Introduction

Cloud computing has become a critical backbone of modern digital infrastructure, enabling scalable, cost-effective, and on-demand access to computing resources. However, its distributed nature and resource-sharing capabilities have made it increasingly susceptible to a wide range of cyber threats, including Distributed Denial of Service (DDoS) attacks, data breaches, malware injection, and unauthorized access. Traditional security mechanisms often fail to keep pace with the dynamic and large-scale nature of these threats, necessitating more intelligent, automated, and adaptive security approaches.

Cloud computing security issues are also important now that society is moving to the digital information age. As more and more users connect to the Internet, it attracts many cybercriminals. This includes authorizing network administrative control to access network information. The task of network security does not require ensuring the security of terminal systems only, but of the entire network. Need for Key Management in Cloud Encryption

provides data protection, while key management enables access to protected data. Data encryption in transit, at rest and on backup media is highly recommended. In particular, information to hide your information. Both encryption and key management are critical to the security of applications and data stored in the cloud.

Recent advancements in machine learning (ML) and cryptography have introduced innovative solutions to address these challenges. ML models can learn from historical data to detect anomalies, predict attacks, and adapt to new threat patterns, while cryptographic techniques ensure data confidentiality and integrity during transmission and storage. This integration of ML and cryptography has driven significant progress in intrusion detection systems (IDS), threat classification, and secure data management across cloud platforms. This paper presents a comprehensive synthesis of 29 research works that examine the application of machine learning and cryptographic methods in enhancing cloud computing security. It categorizes these studies into key domains such as DDoS detection, intrusion prevention, encryption-based data protection, and big data analytics. The review identifies prevailing trends, evaluates algorithmic performance, and highlights current limitations and future research directions for building resilient, intelligent, and secure cloud infrastructures.

Literature Review

The paper [1] 2021 presents a systematic review of 63 studies exploring how machine learning (ML) enhances cloud security by Ali Bou Nassif et.al. It identifies 11 major research areas, with DDoS attacks and data privacy being the most investigated. Common ML techniques include Support Vector Machines (SVM), K-Nearest Neighbors (KNN), and Random Forest, used to detect intrusions, anomalies, and vulnerabilities. Evaluation metrics like accuracy and true positive rate dominate, with datasets such as KDD Cup'99 widely used. The study highlights the need for updated datasets, deep learning integration, and hybrid models to strengthen future cloud protection strategies.

The paper [2] by Zekri et al. (2017) proposes a machine learning-based approach to detect and mitigate Distributed Denial of Service (DDoS) attacks in cloud computing environments. It highlights the increasing threat of DDoS attacks that exploit cloud vulnerabilities, affecting service availability and network performance. The authors designed a C4.5 decision tree algorithm integrated with signature-based detection for improved accuracy and automatic identification of flooding attacks. Comparative experiments using other ML techniques demonstrate that the C4.5 model effectively enhances detection accuracy and reduces false positives, providing a reliable defense mechanism for ensuring cloud security and service continuity.

The study [3] by Aroosh Amjad et al. (2019) presents an effective approach for detecting and mitigating DDoS attacks in cloud computing using machine learning algorithms. The authors employ Naïve Bayes and Random Forest classifiers to distinguish between malicious and normal packets. Using ParrotSec OS and Wireshark, they simulate and analyze DDoS traffic to train and test datasets. Results show that Naïve Bayes outperforms Random Forest in detecting false positives and identifying abnormal packets efficiently. The proposed model strengthens cloud security by enhancing detection accuracy, reducing vulnerabilities, and maintaining service availability in cloud-based environments.

C. Bagyalakshmi and Dr. E. S. Samundeeswari (2020) [4] proposed a machine-learning-based intrusion detection framework for classifying DDoS attacks in cloud computing environments using the NSL-KDD dataset. The study employs Learning Vector Quantization (LVQ) and Principal Component Analysis (PCA) for feature selection, followed by classifiers such as Naïve Bayes, Support Vector Machine, and Decision Tree. Results indicate that the LVQ-based Decision Tree model achieved the highest detection accuracy of 98.7%, outperforming other approaches. The work highlights the crucial role of machine learning in enhancing cloud security, enabling efficient detection of DDoS threats while optimizing computational resources.

A. A. Alsirhani, A. M. Alghamdi, and A. S. Alqahtani in 2021 study [5], developed a machine learning-based framework to detect DDoS attacks in cloud computing environments. The research used six ML algorithms—KNN, SVM, Naïve Bayes, Decision Tree, Random Forest, and Logistic Regression—implemented via WEKA using the CICDDoS2019 dataset. Results show that Random Forest and Decision Tree achieved the highest accuracy in classifying normal and malicious traffic. The study emphasizes that ML significantly improves cloud security by enhancing detection accuracy and reducing false alarms. The authors recommend future work integrating IoT defence and hybrid ML approaches for stronger cloud protection.

"Cyber Security Vulnerabilities and Remediation Through Cloud Security Tools" (FNU Jimmy, 2024) [6], the author examines how cloud computing, machine learning, and advanced analytics can mitigate rising cyber threats such as DDoS attacks. The study outlines the increasing sophistication of cybercriminals exploiting vulnerabilities in cloud-based systems and networks. It emphasizes the integration of AI, deep learning, and blockchain to enhance intrusion detection, malware defense, and data protection. Despite progress, challenges remain in securing data integrity, mitigating ML biases, and preventing cloud-based attacks. The paper advocates a combined technical and managerial approach for future cyber resilience.

Ganesh Rathod, Vikrant Sabnis, and Jay Kumar Jain (2024) [7] present a comprehensive comparative study on Intrusion Detection Systems (IDS) in cloud computing using machine learning (ML) algorithms. The paper explores traditional rule-based IDS (Snort, Suricata, Bro, OSSEC) and ML-based IDS (SVM, CNN, LSTM, and hybrid models). ML-based IDSs demonstrate higher accuracy and lower false positive rates, effectively detecting complex and previously unseen threats, including DDoS attacks. The study concludes that integrating ML with IDS can significantly enhance cloud security, though challenges such as large training data requirements and computational complexity persist.

"AI-Based Intrusion Detection System in Cloud Computing" by Kalpana Verma, 2024, [8] the study proposes a neural network–based intrusion detection system (IDS) that leverages machine learning to enhance cloud computing security. It highlights the growing complexity of cyber threats, including DDoS attacks, and emphasizes the need for adaptable, intelligent detection models. The research evaluates multiple machine learning algorithms—Random Forest, Naive Bayes, J48, Bayesian Network, and Random Tree—using the CICIDS2017 dataset, achieving high accuracy in anomaly detection. Results demonstrate that feature selection significantly improves IDS performance. The paper concludes that AI-driven IDS frameworks offer scalable and efficient protection in cloud environments.

"Network Intrusion Detection Systems in Cloud Computing Environments" (IJACSA, 2024), [9] the paper reviews advancements in intrusion detection systems (IDS) tailored for cloud-based infrastructures by Sina Ahmadi. It explores hybrid detection techniques combining signature-based and anomaly-based methods to improve accuracy and reduce false positives. The integration of AI and machine learning models, including neural networks and federated learning, enhances detection efficiency for emerging cyber threats. The study also highlights trends in cloud-native IDS such as microservice-based architectures, containerization, and data privacy compliance. By leveraging machine learning and cloud technologies, the research underscores improved scalability, adaptability, and resilience against DDoS and evolving cyberattacks.

In [10] "Enhancing Security and Performance in Live VM Migration: A Machine Learning-Driven Framework with Selective Encryption for Enhanced Security and Performance in Cloud Computing Environments" Haris et al., 2025, the authors propose a hybrid framework integrating machine learning and selective encryption to improve security and efficiency during live virtual machine migration in cloud computing. The approach predicts optimal migration times while encrypting only sensitive data, maintaining confidentiality without sacrificing performance. Experimental results show a 51.82% reduction in downtime and 72.73% faster migrations.

The study highlights that intelligent ML-driven encryption significantly enhances cloud computing reliability, scalability, and protection against attacks such as DDoS and data interception.

The paper [11] by M. Chauhan and S. Sharma (2023) provides an extensive comparative review of cloud security frameworks such as NIST, COBIT5, ISO 27017, CSA STAR, and AWS Well-Architected. It highlights major cloud computing threats including DDoS attacks, insecure APIs, insider threats, and account hijacking. The study emphasizes that no single framework can address all cloud security challenges; instead, a combination of controls ensures better protection of data integrity, confidentiality, and availability. The authors advocate for robust authentication, encryption, continuous monitoring, and risk management to strengthen organizational cloud security posture.

Rajesh Bingu and S. Jothilakshmi in [12] 2023 study propose an ensemble-based deep learning framework to enhance intrusion detection in cloud computing and Software-Defined Networking (SDN) environments. The model integrates K-means clustering with classifiers like CNN, LSTM, RNN, GRU, and DNN to improve accuracy and reduce false alarms. Tested on CICIDS-2018 and SDN-based DDoS datasets, it achieved up to 99.68% accuracy and strong F1-scores. The approach effectively detects DDoS attacks and other malicious intrusions while minimizing computational complexity, outperforming traditional standalone deep learning models in cloud-based intrusion detection.

Joel Emmanuel Mulepa and Dr. Glorindal Selvam in 2023 study, [13] and propose a Proficient Network Intrusion Detection System (PNIDS) that integrates machine learning techniques with rule-based and anomaly-based detection to improve cybersecurity defenses. The system identifies threats such as DDoS attacks, malware, phishing, and port scanning by analyzing network traffic patterns. It employs models that learn normal and abnormal behaviors to minimize false alarms and enhance detection accuracy. Evaluation metrics such as F1 score, AUC, and false positive rate validate the

system's efficiency. The proposed framework strengthens network resilience and supports proactive, automated threat response.

Mahmood A. Al-Shareeda, Selvakumar Manickam, and Murtaja Ali Saare in 2023 study, [14] analyze and compare machine learning (ML) and deep learning (DL) methods for detecting DDoS attacks in network environments. The research examines algorithms such as Naïve Bayes, SVM, Decision Tree, K-Means, ANN, CNN, and RNN, emphasizing their accuracy, scalability, and adaptability in intrusion detection systems (IDS).
Results show that while ML performs effectively with smaller datasets, DL outperforms ML for large-scale data and complex attack patterns. The authors conclude that integrating DL techniques significantly improves detection accuracy and resilience against evolving DDoS threats.

Sanjevi Kumar A., A. Rajalingam, and B. Gokila in 2023 study, [15] analyze the security challenges and issues in cloud computing technologies. The paper highlights major threats such as data breaches, data loss, account hijacking, insecure APIs, DDoS attacks, and malicious insiders. It explains that cloud computing's multi-tenant and shared environment increase vulnerability to cyber threats. The authors propose countermeasures including encryption, intrusion detection, access control, redundancy, and regular monitoring to strengthen cloud security. The paper concludes that while complete protection is unattainable, proactive security strategies can substantially reduce risks in cloud computing environments.

The paper [16] authored by Manjunath C R et al. (2022) presents a novel machine learning-based approach for detecting DDoS attacks in cloud computing environments. It uses data preprocessing for noise removal and dimensionality reduction, followed by feature extraction and classification via a ResNet-101 based Kernel Extreme Learning Machine (KELM). The method achieves high detection accuracy, data delivery ratio, and transaction rate, demonstrating improved performance over existing techniques. It addresses the critical challenge of securing cloud-based services against disruptive DDoS attacks through intelligent machine learning architectures, enhancing cloud security and operational reliability.

In the paper [17] in 2022 "Comprehensive Overview of DDoS Attack in Cloud Computing Environment Using Different Machine Learning Techniques", Sherwin Kati, Abhishek Ove, Bhavana Gotipamul, Mayur Kodche, and Prof. Swati Jaiswal discuss how the rapid adoption of cloud computing increases vulnerability to Distributed Denial of Service (DDoS) attacks. The authors explain how attackers flood cloud servers with massive illegitimate traffic, making services inaccessible to legitimate users. The paper reviews different detection and prevention techniques, including statistical models, intrusion detection systems, filtering methods, and machine learning-based classification. The study concludes that although progress has been made, more robust and adaptive defense mechanisms are still required.

The paper [18] in 2019 "Big Data Security: A Review of Encryption Techniques in Big Data" by M. Geethanjali and Dr. P. Madhubala discusses the rapid growth of big data and the resulting challenges in storing, processing, and protecting massive, diverse datasets

The authors describe how traditional systems struggle to handle large structured and unstructured data generated from social media, IoT, and cloud environments. The study highlights the importance of security and privacy in big data analytics and reviews encryption approaches such as Identity-Based Encryption, Attribute-Based Encryption, and Homomorphic Encryption. The paper concludes that stronger, scalable security mechanisms are needed to safeguard big data in cloud systems.

The paper [19] in 2020 "Machine Learning Solutions for Analysis and Detection of DDoS Attacks in Cloud Computing Environment" by Abdul Raoof Wani, Q. P. Rana, and Nitin Pandey focuses on detecting and mitigating Distributed Denial of Service (DDoS) attacks in cloud platforms. The authors explain how cloud computing environments are highly vulnerable due to resource sharing and open access. The study generates a dataset in a CloudStack environment using the Tor Hammer attack tool and analyzes it with machine learning algorithms including SVM, Random Forest, Naïve Bayes, Decision Tree, K-Means, and C4.5. Results show that SVM and C4.5 provide the highest detection accuracy, making them effective for intrusion detection.

The paper [20] in 2020 "A Survey on Cloud Data Security using Image Steganography" by Afrah Albalawi and Nermin Hamza discusses how cloud computing provides flexible and cost-efficient services, but storing sensitive data in the cloud raises serious security concerns. The authors review the use of image steganography as a method to enhance data confidentiality by hiding secret data within images, making it difficult for attackers to detect. The paper compares several recent steganography-based cloud security techniques based on their algorithms, advantages, and limitations. The study concludes that while many methods ensure security, achieving high capacity, strong invisibility, and high-quality stego images simultaneously remains a challenge for future research.

The paper [21] in 2018 "Information Security in Big Data" by Naseema Shaik, Mubeena Shaik, Nada Ahmed Mohammad, and Fatima Ahmed Alomari highlights the growing importance of securing large-scale data environments. The authors explain that big data offers valuable insights for business growth but also increases exposure to cyber threats and hacking attempts. They describe major security challenges across data entry, storage, and output stages, emphasizing the need for encryption, strong access control, intrusion detection, and secure distributed frameworks like Hadoop. The paper concludes that organizations must adopt proactive security strategies and continuous monitoring to protect sensitive information and ensure reliable big data operations.

The paper [22] in 2016 "Encryption and Decryption Based Information Security in Big Data" by G. Vihari and P. Ramaiah Chowdary discusses the rising need to secure sensitive data in big data environments where large volumes of information are collected, stored, and processed. The authors emphasize that traditional security measures such as usernames and passwords are insufficient to prevent unauthorized access. To enhance data privacy, the paper proposes using encryption before storing data in the database and decrypting it only when needed. The system is implemented using the SHA-3 encryption algorithm, which ensures strong data protection. The study concludes that encryption-based approaches provide reliable security and improve data confidentiality in big data applications.

The paper [23] in 2024 “A Survey of Cryptographic Approaches to Securing Big-Data Analytics in the Cloud” by Sophia Yakoubov, Vijay Gadepally, Nabil Schear, Emily Shen, and Arkady Yerukhimovich discusses the security challenges faced when performing large-scale data analytics in cloud environments. The authors explain that although cloud computing provides scalability and efficiency, it also introduces risks related to data confidentiality and integrity. The paper presents a model of cloud data processing and examines three key cryptographic techniques: Homomorphic Encryption, Verifiable Computation, and Secure Multi-Party Computation. Each method offers different strengths in protecting data during storage and computation. The authors conclude that further improvements are needed to make these methods practical for real-world large-scale cloud systems.

The paper [24] in 2023 “Cloud DDoS Attack Detection Model with Data Fusion & Machine Learning Classifiers” by Lal Mohan Pattnaik, Pratik Kumar Swain, Suneeta Satpathy, and Aditya N. Panda presents a fusion-based approach to detect Distributed Denial of Service (DDoS) attacks in cloud environments. The authors explain that cloud computing’s open and scalable nature makes it vulnerable to large-scale attacks. To improve detection accuracy, the study integrates data fusion techniques with machine learning classifiers such as Decision Tree, Naïve Bayes, SVM, and KNN. Using the CIC-DDoS2019 dataset, results show that the Decision Tree classifier achieved the highest accuracy of 99%, demonstrating its effectiveness in identifying cloud DDoS attacks.

The paper [25] in 2019 "Smart Detection: An Online Approach for DoS/DDoS Attack Detection Using Machine Learning" by Francisco Sales de Lima Filho et al. (2019) presents a novel machine learning-based system for real-time detection of DoS and DDoS attacks. The system uses random traffic sampling and a Random Forest classifier to identify a wide range of attacks including TCP, UDP, and HTTP floods with high accuracy. Evaluated on multiple benchmark datasets, it achieves detection rates above 80%-100%, low false alarm rates, and high precision without requiring infrastructure upgrades. The approach balances scientific advances and industrial practicality, promising scalable and privacy-preserving cloud and network security.

The paper [26] "A Secure Communication with One Time Pad Encryption and Steganography Method in Cloud" by Lalit Kumar, Sanjeev Kumar Mandal, Srinivasan S, Omkar Singh, and Sabari Giri Murugan in 2021 explores enhancing cloud data security by combining cryptography and steganography. It highlights challenges in protecting cloud data confidentiality and integrity amid increasing cyber threats. The proposed approach leverages Blowfish encryption and steganography to shield sensitive information, ensuring secure data transmission and storage. The method maintains data secrecy by hiding encrypted data within objects like images, resisting unauthorized access. This unified model offers a robust security mechanism for cloud environments while addressing shared responsibility in cloud security.

The paper [27] "DDoS Attack Detection using Machine Learning Techniques in Cloud Computing Environments" by Marwane Zekri, Said El Kafhali, Noureddine Aboutabit, and Youssef Saadi in 2017 presents a machine learning-based system for detecting DDoS attacks in cloud environments. Using the C4.5 decision tree algorithm combined with signature detection techniques, the method

effectively identifies flooding attacks targeting network layers 3 and 4. The system achieves high detection accuracy (up to 98.8%) and low detection time, outperforming other classifiers like Naive Bayes and K-Means. This approach provides a scalable, efficient solution for securing cloud services from DDoS threats.

The paper[28] "Survey and Performance Analysis of Machine Learning Based Security Threats Detection Approaches in Cloud Computing" by Rajesh Keshavrao Sadavarte1, Dr. G. D. Kurundkar in 2021, works to find research paper based on technique that used Support Vector Machine (SVM), Decision Tree (DT), Naive Bayes (NB), Random Forests (RF) and the K-Nearest neighbour (KNN).

The paper titled [29] "Big Data Analytic Using Machine Learning Algorithms for Intrusion Detection System: A Survey" by Abdulnaser A. Hagar, Deepali G. Chaudhary, Ali A. Al-Bakhrani, and Bharti W. Gawali in 2021 presents a comprehensive survey on the use of big data analytics and machine learning algorithms for intrusion detection systems (IDS). It reviews eight key machine learning algorithms used for IDS, discusses various intrusion detection techniques and systems, and highlights commonly used datasets. The paper emphasizes the importance of improving IDS accuracy and efficiency to detect diverse cyberattacks, including DDoS, in cloud and network environments. It also explores challenges in data processing and feature selection.

Results:

After detail studies result shows in table 1 Types of count of Literature studies and figure 1 shows types of count of Literature studies in graphical form. Table 2 shows number of authors in the Literature studies and figure 2 shows number of authors in the Literature studies in graphical form. In Table 3 it shows total 29 literature studied year wise (Between 2015- 2025)

And figure 3 shows total 29 literature studied year wise (Between 2015- 2025) in graphical form.

S.No.	Types of Literature	No of literature
1	Journal	21
2	Article	6
3	Conference	2

Table 1: Types of count of Literature studies

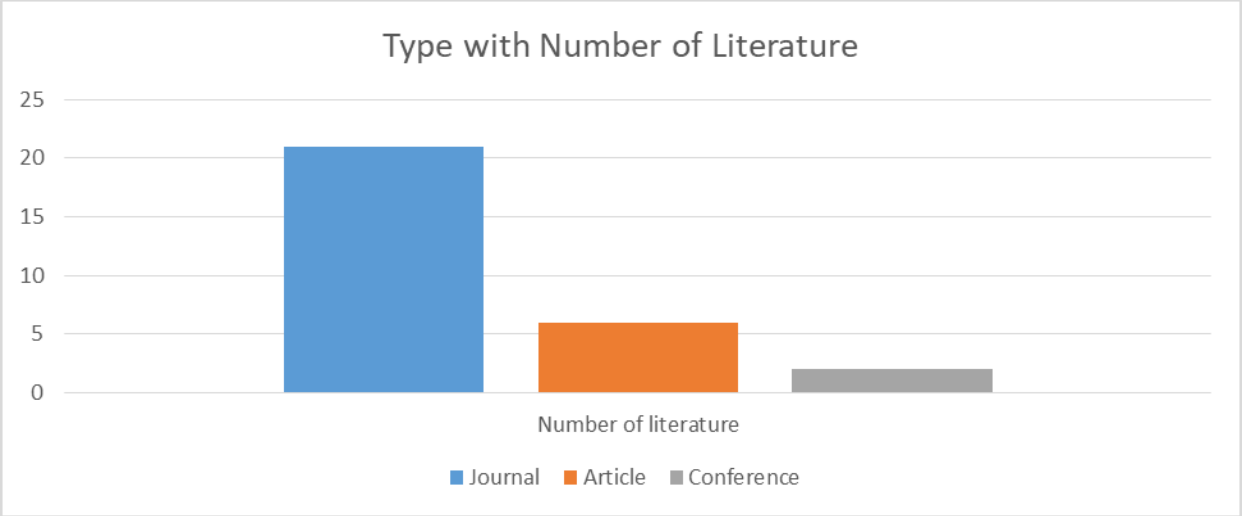


Figure 1: Types of count of Literature studies in graphical form

S.No.	No. of Authors	In Respective total no. of literature
1	1	3
2	2	7
3	3	6
4	4	5
5	5	7
6	6	1
7	7	0
8	8	0
9	9	0

Table 2: Number of authors in the Literature studies

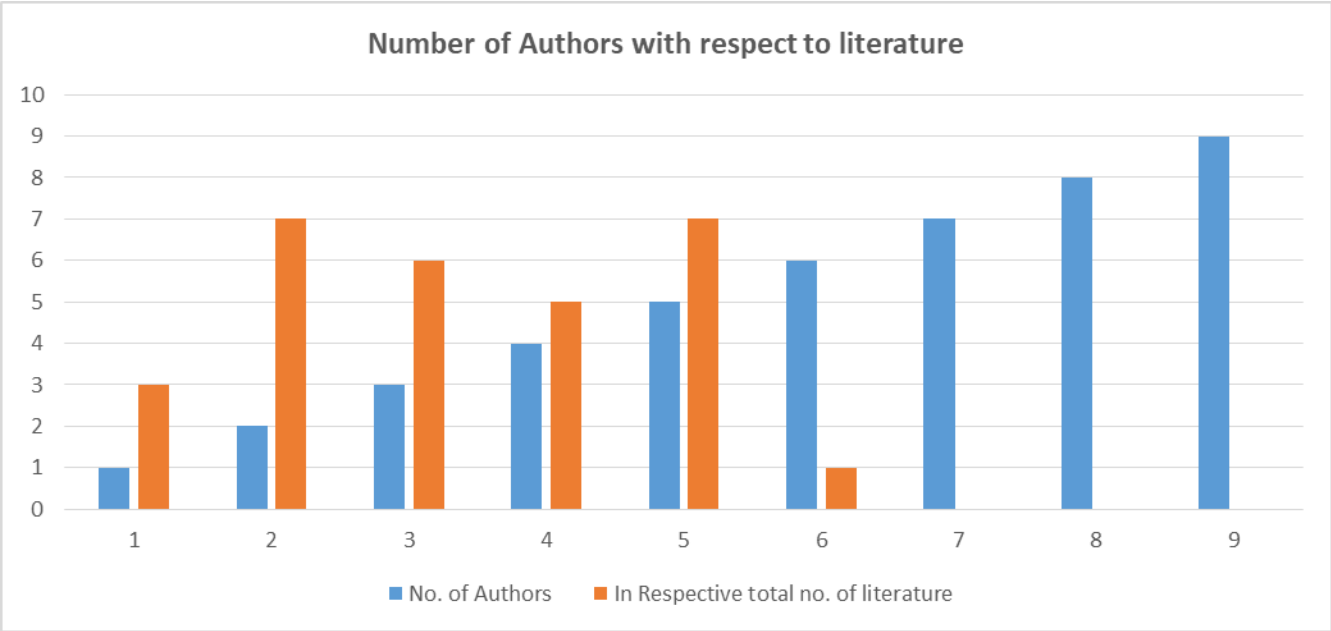


Figure 2: Number of authors in the Literature studies in graphical form

S.No.	Year	No of literature
1	2015	0
2	2016	1
3	2017	2
4	2018	1
5	2019	3
6	2020	4
7	2021	4
8	2022	2
9	2023	6
10	2024	5
11	2025	1

Table 3:- Total 29 literature studied year wise (Between 2015- 2025)

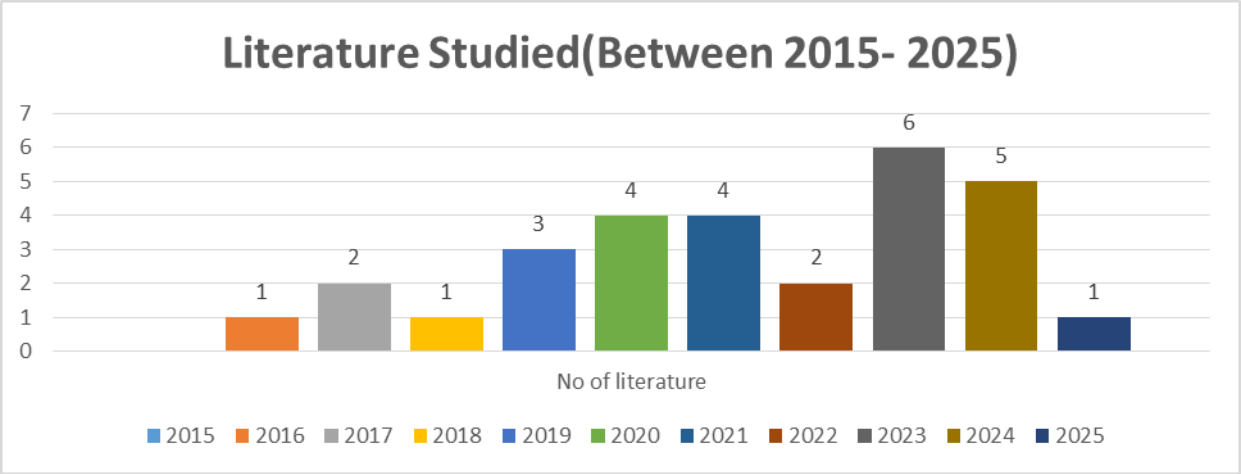


Figure 3:- Total 29 literature studied year wise (Between 2015- 2025) in graphical form

Conclusion

The reviewed studies collectively demonstrate that machine learning and cryptography play pivotal roles in strengthening the security of cloud computing environments. ML-based systems have achieved high detection accuracy against DDoS and other cyberattacks, improving system reliability and response efficiency. Techniques like Random Forest, SVM, Decision Tree, and Naïve Bayes remain dominant due to their accuracy and interpretability, while deep learning models such as CNN, LSTM, and RNN are proving superior in handling large, complex datasets. Meanwhile, cryptographic methods, including homomorphic encryption, SHA-3, and steganography, continue to secure data integrity and privacy.

However, persistent challenges such as outdated datasets, limited adaptability to emerging threats, and the computational cost of deep learning highlight the need for hybrid, scalable, and real-time defense architectures. Future research should focus on integrating ML with blockchain, IoT, and federated learning to enable autonomous, distributed, and privacy-preserving security models. The

convergence of these technologies will be vital in establishing a next-generation secure cloud ecosystem capable of defending against evolving cyber threats. Details of research as shown in table 4, total literature studied and occurrence of keywords in the research paper.

Paper id	No of authors	Journal or conference paper	Key Word count
1	5	Journal	"DDoS Attacks" → 13 times "Machine Learning" → 38 times "Cloud Security" → 22 times "Cloud Computing" → 31 times
2	4	Journal	DDoS Attacks 48 Machine Learning 21 Cloud Security 8 Cloud Computing 19
3	4	Article	DDoS Attacks 37 Machine Learning 12 Cloud Security 6 Cloud Computing 28
4	2	Journal	DDoS Attacks 15 times Machine Learning 17 times Cloud Security 2 times Cloud Computing 14 times
5	2	Article	DDoS Attacks 46 Machine Learning 23 Cloud Security 8 Cloud Computing 20
6	1	Journal	DDoS Attacks 5 times Machine Learning 12 times Cloud Security 4 times Cloud Computing 7 times
7	3	Journal	DDoS Attacks 2 times Machine Learning 44 times Cloud Security 5 times Cloud Computing 36 times
8	1	Journal	DDoS Attacks 3 times Machine Learning 18 times Cloud Security 2 times Cloud Computing 11 times
9	1	Journal	DDoS Attacks 1 time Machine Learning 15 times Cloud Security 3 times Cloud Computing 9 times
10	5	Article	DDoS Attacks 1 time Machine Learning 26 times Cloud Security 2 times Cloud Computing 19 times
11	2	Journal	DDoS Attacks 1 time Machine Learning 0 times Cloud Security 22 times Cloud Computing 38 times
12	2	Journal	DDoS Attacks 6 times Machine Learning 11 times Cloud Security 0 times Cloud Computing 13 times

13	2	Journal	DDoS Attacks 2 times Machine Learning 12 times Cloud Security 0 times Cloud Computing 3 times
14	3	Journal	DDoS Attacks 33 times Machine Learning 26 times Cloud Security 0 times Cloud Computing 2 times
15	3	Journal	DDoS Attacks 1 time (mentioned under "Denial-of-Service" section as DDoS) Machine Learning 0 times Cloud Security 9 times Cloud Computing 24 times
16	6	Journal	DDoS Attacks 8 times DDoS (general occurrences) 32 times Machine Learning 9 times Cloud Security 0 times Cloud Computing 5 times
17	5	Journal	DDoS Attacks 6 times Machine Learning 2 times Cloud Security 0 times Cloud Computing 8 times
18	2	Journal	DDoS Attacks 0 times Machine Learning 0 times Cloud Security 0 times Cloud Computing 5 times
19	3	Journal	DDoS Attacks 15 times Machine Learning 11 times Cloud Security 0 times Cloud Computing 13 times
20	3	Journal	DDoS Attacks 0 times Machine Learning 0 times Cloud Security 0 times Cloud Computing 17 times
21	3	Journal	"DDoS Attacks" appears 0 times. "Machine learning" is mentioned 1 time. "Cloud Security" is mentioned 1 time. "Cloud computing" is mentioned 1 time.
22	2	Journal	DDoS Attacks 0 times Machine Learning 0 times Cloud Security 0 times Cloud Computing 2 times
23	5	Conference	DDoS Attacks 0 times Machine Learning 0 times Cloud Security 0 times Cloud Computing 13 times
24	4	Article	DDoS Attacks 26 times Machine Learning 42 times Cloud Security 11 times Cloud Computing 18 times
25	5	Article	The term "DDoS Attacks" (or variations such as "DDoS attack," "DoS attacks") appears approximately 87 times. "Machine learning" occurs around 41 times.

			"Cloud Security" is mentioned 6 times. Cloud computing" is mentioned 8 times
26	5	Article	DDoS Attacks" occurs 0 times. "Machine learning" occurs 0 times. "Cloud Security" is mentioned 5 times. "Cloud computing" appears 34 times.
27	4	Conference	DDoS Attacks" are mentioned approximately 1 time. "Machine learning" is mentioned approximately 16 times. "Cloud Security" appears around 2 times. "Cloud computing" is referenced about 4 times.
28	5	Journal	"DDoS Attacks" occur 16 times. "Machine learning" is mentioned 167 times. "Cloud Security" appears 57 times. "Cloud computing" appears 134 times.
29	4	Journal	"DDoS Attacks" is mentioned approximately 20 times. "Machine learning" appears around 180 times. "Cloud Security" is mentioned about 15 times. "Cloud computing" is mentioned roughly 40 times.

Table 4:- Total literature studied shows occurrence of keywords in the research

References:-

[1] A. Bou Nassif, M. A. Talib, Q. Nasir, H. Albadani, and F. M. Dakalbab, "Machine Learning for Cloud Security: A Systematic Review," *IEEE Access*, vol. 9, pp. –, Jan. 2021, doi: 10.1109/ACCESS.2021.3054129.

[2] M. Zekri, S. El Kafhali, N. Aboutabit, and Y. Saadi, "DDoS Attack Detection Using Machine Learning Techniques in Cloud Computing Environments," *Proc. CloudTech Conf.*, Settat, Morocco, Oct. 2017, doi: 10.1109/CloudTech.2017.8284731.

[3] A. Amjad, T. Alyas, U. Farooq, and M. A. Tariq, "Detection and Mitigation of DDoS Attack in Cloud Computing Using Machine Learning Algorithm," *EAI Endorsed Transactions on Scalable Information Systems*, 2020.

[4] C. Bagyalakshmi and E. S. Samundeeswari, "DDoS Attack Classification on Cloud Environment Using Machine Learning Techniques with Different Feature Selection Methods," *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 9, no. 5, pp. –, Sept.–Oct. 2020, doi: 10.30534/ijatcse/2020/60952020.

[5] R. J. Alzahrani and A. Alzahrani, "Security Analysis of DDoS Attacks Using Machine Learning Algorithms in Networks Traffic," *Electronics*, vol. 10, no. 23, p. 2919, 2021, doi: 10.3390/electronics10232919.

[6] Deloitte, "Cyber Security Vulnerabilities and Remediation Through Cloud Security Tools," *Journal of Artificial Intelligence General Science (JAIGS)*, vol. 2, no. 1, Mar. 2024.

[7] G. Rathod, V. Sabnis, and J. K. Jain, "Intrusion Detection System (IDS) in Cloud Computing Using Machine Learning Algorithms: A Comparative Study," *Grenze International Journal of Engineering and Technology*, Jan. 2024.

[8] K. Verma, "AI-Based Intrusion Detection System in Cloud Computing," *Journal of Emerging Technologies and Innovative Research (JETIR)*, vol. 11, no. 4, Apr. 2024, ISSN: 2349-5162.

[9] S. Ahmadi, "Network Intrusion Detection in Cloud Environments: A Comparative Analysis of Approaches," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 15, no. 3, 2024, doi: 10.14569/IJACSA.2024.0150301.

[10] R. M. Haris, M. Barhamgi, A. Badawy, A. Nhlabatsi, and K. M. Khan, "Enhancing Security and Performance in Live VM Migration: A Machine Learning-Driven Framework with Selective Encryption," *Expert Systems*, vol. 42, e13823, 2025, doi: 10.1111/exsy.13823.

[11] M. Chauhan and S. Shiaeles, "An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions," *University of Portsmouth*, UK, 2023.

[12] R. Bingu and S. Jothilakshmi, "Design of Intrusion Detection System Using Ensemble Learning Technique in Cloud Computing Environment," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 14, no. 5, 2023.

[13] J. E. Mulepa and G. Selvam, "Proficient Intrusion Detection System Using Machine Learning," *International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)*, vol. 3, no. 1, Apr. 2023, doi: 10.48175/IJARSCT-9072.

[14] M. A. Al-Shareeda, S. Manickam, and M. A. Saare, "DDoS Attacks Detection Using Machine Learning and Deep Learning Techniques: Analysis and Comparison," *Bulletin of Electrical Engineering and Informatics*, vol. 12, no. 2, pp. 930–939, Apr. 2023, doi: 10.11591/eei.v12i2.4466.

[15] S. Kumar A., A. Rajlingam, and B. Gokila, "Study Analysis of Cloud Security Challenges and Issues in Cloud Computing Technologies," *Journal of Science, Computing and Engineering Research (JSCER)*, vol. 6, no. 8, Aug. 2023, doi: 10.46379/jscer.2023.0608002.

[16] M. C. R. Manjunath, K. Rathor, N. Kulkarni, P. P. Patil, M. S. Patil, and J. Singh, "Cloud-Based DDoS Attack Detection Using Machine Learning Architectures: Understanding the Potential for Scientific Applications," *International Journal of Intelligent Systems and Applications in Engineering (IJISAE)*, vol. 10, no. 2s, pp. 268–271, 2022.

[17] S. Kati, A. Ove, B. Gotipamul, M. Kodche, and S. Jaiswal, "Comprehensive Overview of DDoS Attack in Cloud Computing Environment Using Different Machine Learning Techniques," Proc. PCCOE, Pune, India, 2021.

[18] M. Geethanjali and P. Madhubala, "Big Data Security: A Review of Encryption Techniques in Big Data," International Journal of Computational Intelligence and Informatics, vol. 9, no. 3, Dec. 2019.

[19] A. Raoof Wani, Q. P. Rana, and N. Pandey, "Machine Learning Solutions for Analysis and Detection of DDoS Attacks in Cloud Computing Environment," *International Journal of Engineering and Advanced Technology (IJEAT)*, vol. 9, no. 3, Feb. 2020.

[20] A. Albalawi and N. Hamza, "A Survey on Cloud Data Security Using Image Steganography," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 11, no. 1, 2020.

[21] N. Shaik, M. Shaik, N. A. Mohammad, and F. A. Alomari, "Information Security in Big Data," *International Journal of Engineering Research and General Science*, vol. 6, no. 5, Sept.–Oct. 2018.

[22] G. Vihari and P. R. Chowdary, "Encryption and Decryption Based Information Security in Big Data," *Anveshana's International Journal of Research in Engineering and Applied Sciences (AIJREAS)*, vol. 1, no. 9, Sept. 2016.

[23] S. Yakoubov, V. Gadepally, N. Schear, E. Shen, and A. Yerukhimovich, "A Survey of Cryptographic Approaches to Securing Big-Data Analytics in the Cloud," *IEEE*, 2014.

[24] L. M. Pattnaik, P. K. Swain, S. Satpathy, and A. N. Panda, "Cloud DDoS attack detection model with data fusion and machine learning classifiers," EAI Endorsed Transactions on Scalable Information Systems, Faculty of Emerging Technologies, Sri Sri University, Cuttack, India, and Center for AI & ML, SOA University, Bhubaneswar, India.

[25] F. S. de Lima Filho, F. A. F. Silveira, A. de M. Brito Junior, G. Vargas-Solar, and L. F. Silveira, "Smart detection: An online approach for DoS/DDoS attack detection using machine learning," Research Article, Federal University of Rio Grande do Norte, Natal, Brazil, and Centre National de la Recherche Scientifique (CNRS), LIG Grenoble, France, Oct. 2019.

[26] L. Kumar, S. K. Mandal, S. Srinivasan, O. Singh, and S. G. Murugan, "A secure communication with one time pad encryption and steganography method in cloud," Turkish Journal of Computer and Mathematics Education, vol. 12, no. 10, pp. 5440–5448, 2021.

[27] M. Zekri, S. El Kafhali, N. Aboutabit, and Y. Saadi, "DDoS attack detection using machine learning techniques in cloud computing environments," Research Article, National School of Applied Sciences, Hassan 1st University, Settat, Morocco.

[28] Sadavarte, R. K., & Kurundkar, G. D. (n.d.). *Survey and performance analysis of machine learning based security threats detection approaches in cloud computing*. **International Journal of Scientific Research in Computer Science, Engineering and Information Technology**, *49*. https://doi.org/10.32628/CSEIT217538

[29] A. Hagar, D. G. Chaudhary, A. A. Al-Bakhrani, and B. W. Gawali, "Big data analytic using machine learning algorithms for intrusion detection system: A survey," International Journal of Mechanical and Production Engineering Research and Development (IJMPERD), vol. 10, no. 3, pp. 6063–6084, Jun. 2020.

ISARA INSTITUTE OF MANAGEMENT & PROFESSIONAL STUDIES

WWW.IIMPS.IN

EARN YOUR

MBA



Accreditation & Ranking

UGC / NCTE Approved.

INFO@IIMPS.IN

011-41005174

RESEARCH GATEWAY

STOP PLAGIARISM

1 Submit your content in Word File.

2 Get report in 48 hrs.

3 *Missing content or references will be fixed.

4 Citation for your work.

5 Get accurate user friendly report.

researchgateway.in | info@researchgateway.in

+91-9205579779

AROGYAM ONLINE

Arogyam Ayurveda

Holistic Healing through herbs

100% NATURAL

PARIVARTAN PSYCHOLOGY CENTER

COLOR PSYCHOLOGY : HOW COLOR AFFECT YOUR CHILD

BLUE — Calms your Child's Mind & Body

YELLOW — Promotes Concentration, Stimulates the Memory

PINK — Evokes Empathy, makes your Child Calm

RED — Excites and energizes your Child's body

GREEN — Improves Reading speed and Comprehension

www.parivartan4u.com

Confuse about your children's future?

भारतीय भाषा, शिक्षा, साहित्य एवं शोध

ISSN 2321 – 9726

WWW.BHARTIYASHODH.COM

INTERNATIONAL RESEARCH JOURNAL OF MANAGEMENT SCIENCE & TECHNOLOGY

ISSN – 2250 – 1959 (0) 2348 – 9367 (P)

WWW.IRJMST.COM

INTERNATIONAL RESEARCH JOURNAL OF COMMERCE, ARTS AND SCIENCE

ISSN 2319 – 9202

WWW.CASIRJ.COM

INTERNATIONAL RESEARCH JOURNAL OF MANAGEMENT SOCIOLOGY & HUMANITIES

ISSN 2277 – 9809 (0) 2348 - 9359 (P)

WWW.IRJMSH.COM

INTERNATIONAL RESEARCH JOURNAL OF SCIENCE ENGINEERING AND TECHNOLOGY

ISSN 2454-3195 (online)

WWW.RJSET.COM

INTEGRATED RESEARCH JOURNAL OF MANAGEMENT, SCIENCE AND INNOVATION

ISSN 2582-5445

WWW.IRJMSI.COM

JOURNAL OF LEGAL STUDIES,POLITICS AND ECONOMICS RESEARCH

WWW.JLPER.COM