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

Securing Cloud Computing through the Integration of Machine Learning and Cryptography: A Comprehensive Review

Meena Malviya
Research Scholar
Barkatullah University,
Bhopal (M.P.) India
Email
meenamalviyanew@gmail.com
(Corresponding author)

Yogendra Yati
Asst. Prof, Department of Computer science and application S.V (Auto.) PG college, Bairagarh, Bhopal (M.P.) India

Anil Gupta
Department of Computer science
UTD, Barkatullah University,
Bhopal (M.P.) India

Abstract
The rapid advancement of cloud computing has revolutionized data storage, accessibility, and scalability but has also intensified concerns over data confidentiality, integrity, and authentication. This review examines thirty-three research papers published between 2010 and 2025, focusing on the convergence of Machine Learning (ML), Artificial Intelligence (AI), and Cryptography for enhancing cloud security. Studies reveal that ML models such as Decision Trees, Support Vector Machines, Neural Networks, and Reinforcement Learning significantly improve anomaly detection, intrusion prevention, and data classification. Cryptographic algorithms particularly AES, RSA, ECC, and hybrid models continue to provide strong encryption and authentication mechanisms. Recent trends emphasize the adoption of hybrid frameworks combining cryptography, steganography, and ML to secure multi-cloud and IoT environments. The findings indicate that the fusion of ML intelligence and cryptographic strength creates adaptive, privacy-preserving, and resilient cloud ecosystems capable of mitigating modern cyber threats.

Keywords
Cloud computing, data confidentiality, integrity, authentication, Machine Learning (ML), Artificial Intelligence (AI), Cryptography etc.

Introduction
Cryptography-related attacks and defences. It also discusses future directions for machine learning in strengthening information security systems Cloud computing has emerged as the backbone of modern information technology, enabling on-demand access to computing resources, data storage, and services over the internet. However, as organizations increasingly migrate to the cloud, challenges such as unauthorized access, data leakage, malware, and Distributed Denial of Service (DDoS) attacks have become critical security concerns. Traditional cryptographic Cryptography-related attacks and defences. It also discusses future directions for machine learning in strengthening information security systems methods like AES, RSA, and DES offer robust protection but lack the adaptive intelligence to counter evolving cyber threats. To address these limitations, researchers have turned to Machine Learning (ML) and Artificial Intelligence (AI) techniques for dynamic threat detection, anomaly prediction, and automated response systems.
This review paper synthesizes 33 key studies from 2010 to 2025 that explore the integration of ML and cryptographic mechanisms in securing cloud infrastructures. The selected works examine diverse security frameworks, including encryption–steganography hybrids, AI-driven identity and access

management systems, and privacy-preserving ML models. The discussion highlights how ML enhances traditional cryptographic methods through real-time learning, data-driven analytics, and predictive modelling. Furthermore, the review identifies gaps related to data privacy, adversarial robustness, and computational efficiency offering insights for future research in developing unified, intelligent cloud security architectures.

Literature Review

The paper titled[1] in 2021"Adaptability of Machine Learning in Cryptography," authored by Veerpal Kaur, Gagandeep Kaur, Gamini Dhiman, Ruchika Bindal, and Mukul Kumar Mishra, explores the integration of machine learning techniques into cryptography to enhance network security. It highlights the rising trend of machine learning applications across industries and particularly in security domains like cryptanalysis and intrusion detection. The study covers various machine learning methods (supervised, unsupervised, reinforcement) and their applications in This comprehensive [5] in 2024 study by Deepak Dasaratha Rao et al. explores the use of machine learning (ML) for cybersecurity threat detection against evolving threats.

The paper by [2] Nur Syuhada Selamat titled in 2019 "Comparison of malware detection techniques using machine learning" discusses the increasing complexity of malware and the application of machine learning (ML) techniques for detection. It emphasizes static analysis methods based on PE file features, utilizing classifiers like Decision Tree, K-NN, and SVM. The study finds that Decision Tree achieves the highest detection accuracy of 99% with a low false positive rate, outperforming other algorithms. The research demonstrates that machine learning, combined with static analysis, provides an efficient way to identify malware without executing the code, enhancing cybersecurity measures.

The article titled [3] in 2023 "Cloud data security and various cryptographic algorithms" is authored by Yahia Alemami, Ali M. Al-Ghonmein, Khaldun G. Al-Moghrabi, and Mohamad Afendee Mohamed. It reviews cloud computing's widespread adoption and emphasizes cloud data security challenges. The study compares encryption algorithms such as AES, DES, RSA, Blowfish, and IDEA in terms of security, memory use, and speed. AES is recognized as the fastest and most suitable for encrypting large data volumes, while Blowfish requires the least memory. The authors conclude that hybrid encryption methods combining AES and Blowfish offer enhanced security for cloud data protection.

The paper by [4] Bokhari Nabil and José Javier Martínez Herráiz in 2024 discusses a security model for hybrid cloud computing that combines cryptography and steganography to protect data privacy and security. It highlights the benefits and vulnerabilities of hybrid cloud environments, proposing a solution that uses RSA, AES cryptographic algorithms, and Least Significant Bit steganography. The model adds layers of security with backup and recovery mechanisms. It also explores future enhancements involving artificial intelligence and machine learning to strengthen cloud security in dynamic environments Rebet Jones in 2024 [8] explores the intersection of Artificial Intelligence (AI) and cloud in dynamic cloud computing environments. It highlights ML's superiority over traditional rule-based methods in identifying sophisticated cyber threats like malware, DDoS, and unauthorized access. The paper reviews supervised, unsupervised, and ensemble learning techniques to enhance detection accuracy and resilience against adversarial attacks. Challenges such as data quality, model updating, and adversarial robustness are discussed. The study demonstrates ML's potential to significantly improve cloud security, encouraging further research in integrating ML with existing security frameworks for real-world applications.

Bhaskaran and Achar (2025) [6] investigate the application of machine learning (ML) techniques to improve cloud security through enhanced threat detection and mitigation. The study analyzes key cloud vulnerabilities such as unauthorized access, data breaches, and denial-of-service attacks, highlighting ML models including Support Vector Machines, Artificial Neural Networks, and K-Nearest Neighbors. Results demonstrate that ML-based security significantly bolsters cloud security by enabling early threat identification and effective mitigation strategies. This research provides valuable insights into optimizing ML models and developing robust security frameworks for cloud computing environments.

This paper explores [7] in 2024 the use of Artificial Intelligence (AI) and Machine Learning (ML) to optimize data access and security in cloud computing environments. It highlights AI's role in intelligent data retrieval, anomaly detection, and adaptive access control, improving speed, accuracy, and user experience. The study discusses AI-driven semantic search, predictive data pre-fetching, and behaviour-based access control mechanisms that enforce real-time security policies. Challenges such as data privacy, model interpretability, and computational complexity are addressed. The authors conclude AI and ML are pivotal in enhancing cloud data management, security, and user-centricity in modern cloud architectures the paper [11] 2024 explores the intersection of artificial intelligence (AI) and cloud security, presenting AI-driven solutions as the future for

Paulraj et al. in 2023 propose [15] a robust system for secure cross-cloud data migration and user anonymity leveraging an Admission Control safeguarding sensitive data in the digital age. It discusses leveraging AI algorithms and machine learning techniques to adapt and evolve cloud security to counter emerging threats in real-time, enhancing detection, prevention, and response capabilities. Key approaches such as anomaly detection, threat intelligence analysis, and behaviour analytics are highlighted for their effectiveness in mitigating risks and ensuring regulatory compliance. The work also addresses challenges and ethical considerations including transparency and accountability associated with AI-driven cloud security.

Ali Abdulsattar Jabbar and Wesam Sameer Bhaya [12] 2023 propose a secure private cloud model that leverages machine learning (ML) and cryptography to protect cloud data. The model operates in two phases: detecting malicious traffic using ML algorithms like random forest and decision tree, then classifying and encrypting data based on importance using AES, 3DES, and RC4 encryption. The approach uses datasets UNSW-NB15 and BBC News for training and testing. Results show 100% detection accuracy for attacks and 98% accuracy in data classification, demonstrating an effective security solution for private cloud environments.

Priyanka Rajan Kumar and Sonia Goel [13] in 2023 propose a hybrid security model combining elliptic curve cryptography (ECC), advanced encryption standard (AES), and logistic regression to enhance data security in Fog computing environments. The model addresses security and privacy challenges by encrypting data before cloud storage and employing machine learning for data classification. Experimental results demonstrate the model's efficiency in encryption/decryption time and strong avalanche effect, validating its suitability for Fog settings. The approach balances data protection and computational efficiency, making it practical for realistic IoT and distributed computing applications.

Ahmed A. Mawgoud and co-authors in 2022 [18] present a deep learning and steganography-based framework to enhance data security in ad-hoc Policy (ACP) and key agreement protocol based on anonymous identity. The approach employs Multi-Agent Reinforcement Learning (MARL) for

effective anonymity classification and security enhancement. The model facilitates trust among cloud providers and optimizes secure resource sharing, reducing computation and communication overheads compared to existing methods. Performance evaluation shows superior accuracy, resource utilization, and response times, demonstrating strong potential for practical cloud computing security applications and privacy-preserving data migration Sanjevi Kumar A, A. Rajlingam, and B. Gokila in 2023 [16] analyze cloud security challenges amid the growing adoption of cloud computing technologies. The paper discusses prevalent threats such as data breaches, loss, account hijacking, insecure APIs, denial-of-service, and malicious insiders. It highlights the importance of implementing strong security measures including encryption, access controls, intrusion detection, and multi-factor authentication. While emphasizing shared infrastructure risks in cloud models like SaaS, PaaS, and IaaS, the authors propose innovative countermeasures to enhance cloud security and mitigate vulnerabilities for service providers and users alike

K. Srinivas Rao and Dr. V. Harsha Shastri [17] in 2023 review various cryptography techniques used to secure cloud data. The study covers encryption algorithms, including hybrid cryptographic models, attribute-based and message digest methods, highlighting their role in ensuring data privacy and integrity in cloud environments. Challenges in encryption, key management, and prevention of unauthorized access are discussed. The authors emphasize the need for advanced, efficient cryptographic solutions to counter emerging security threats in cloud computing infrastructures. The review also compares different algorithms regarding security, efficiency, and applicability in cloud data protection.

like feature selection, model training, and updates are handled by the **cloud**, and lightweight prediction runs on IoT devices. The system adapts ML models based on device capacity, improving efficiency while maintaining strong security.

cloud computing systems using the V-BOINC platform. The model focuses on securing cloud data transmissions by integrating advanced steganographic techniques with adaptive learning models to detect and mitigate threats. The research aims to reinforce privacy and confidentiality in cloud environments, addressing the growing challenges of data breaches and unauthorized access in dynamic distributed computing infrastructures.

The paper [19] “Leveraging AI for Enhanced Identity and Access Management in Cloud-Based Systems to Advance User Authentication and Access Control” in 2024 by Godwin Nzeako and Rahman Akorede Shittu explores how Artificial Intelligence strengthens cloud-based Identity and Access Management (IAM). It discusses the integration of AI and machine learning for adaptive authentication, anomaly detection, and dynamic access control. The study highlights AI’s role in improving data integrity, scalability, and real-time security in cloud environments. Through literature reviews and case studies across finance, healthcare, and government, it concludes that AI-driven IAM enhances security, compliance, and efficiency while ensuring a user-centric approach.

The paper [20] in 2021 “Study of Machine Learning for Cloud Assisted IoT Security as a Service” by Maram Alsharif and Danda B. Rawat proposes a cloud-based framework to enhance IoT device security using machine learning (ML). It introduces Cloud Model as a Service (MaaS) to offload heavy ML tasks—such as model building, training, and validation—from resource-limited IoT devices to the cloud. IoT devices perform lightweight operations like feature extraction and anomaly prediction, while the cloud handles continuous learning and updates. This architecture

improves intrusion detection efficiency, scalability, and performance, ensuring secure IoT environments despite limited computing resources on edge devices.

This paper [21] in 2021 discusses how **machine learning** can enhance security for **IoT devices** by providing efficient intrusion detection systems. Due to resource limitations in IoT devices, running full ML models locally is difficult. To solve this, the authors propose a **cloud-based Model-as-a-Service (MaaS)** framework, where heavy tasks like feature selection, model training, and updates are handled by the **cloud**, and lightweight prediction runs on IoT devices. The system adapts ML models based on device capacity, improving efficiency while maintaining strong security. The paper concludes with emerging security challenges and suggests future improvements for more reliable and secure cloud computing . Experiments show that reduced feature sets and cloud support make ML-based IoT security more practical and scalable.

This paper [22] in 2020 discusses the increasing role of **cloud computing** in modern data storage and processing environments and highlights its security challenges. As more organizations shift to the cloud, ensuring data confidentiality, integrity, and privacy becomes critical. The study emphasizes how **machine learning** techniques can enhance security by detecting threats, anomalies, and unauthorized access more efficiently. It also explains different cloud service models and deployment layers, focusing on the need for secure authentication and access control. The authors argue that integrating intelligent security mechanisms can provide scalable and reliable protection for cloud-based systems in real-world applications.

This paper [23] in 2020 focuses on enhancing **data security in cloud computing** by combining **machine learning** classification techniques with **cryptography**. The authors highlight that cloud environments are vulnerable to unauthorized access and data breaches, making confidentiality and access control essential. They propose using an improved **Ensemble Learning model** alongside **K-Nearest Neighbor (KNN)** to automatically classify data based on sensitivity levels. For securing highly confidential data, the system integrates **RSA encryption** with **HMAC** authentication, ensuring integrity and protection against tampering. The proposed approach improves accuracy, reduces encryption time, and enhances overall cloud data security.

This paper [24] 2021 provides a detailed review of **cloud computing security**, focusing on current challenges and research directions. The authors explain the essential characteristics and service models of cloud computing and highlight security concerns such as data privacy, integrity, and availability. The study classifies prior research into three major areas: **encryption methods**, **machine learning-based security approaches**, and **big data protection** in cloud environments. Various algorithms, such as AES, RSA, ANN, SVM, and optimization techniques, are reviewed for their effectiveness in securing cloud systems.

The paper [28] in 2018 proposes a **Cryptographically Privacy-Preserving Extreme Learning Machine (CPP-ELM)** designed for secure data classification in cloud systems. The authors emphasize that many organizations rely on environments.

This paper [25] in 2020 presents a survey on **cloud data security** using **image steganography** techniques. As cloud computing grows in use, ensuring data confidentiality and preventing unauthorized access have become major challenges. The authors explain how **image steganography** can hide sensitive data inside images, making it difficult for attackers to detect. The paper reviews multiple steganography models and compares them based on encryption methods, data hiding capacity, image quality, and resistance to attacks. Results show that while many approaches offer

strong **security**, limitations remain in **capacity**, **quality**, and processing overhead. The authors suggest improving future techniques to balance security, quality, and efficiency.

This paper addresses [26] in 2019 **data security in cloud computing**, particularly for **mobile cloud environments**. The authors highlight that as cloud services grow, ensuring confidentiality and privacy becomes a major concern. The paper proposes the use of **image steganography** to conceal sensitive information within images before uploading them to the cloud. This method hides data in such a way that it becomes difficult for attackers or cloud administrators to detect. The system embeds both data and a secret key into an image, allowing only authorized users to retrieve it. The approach is lightweight, suitable for mobile devices, and improves security without heavy encryption overhead.

This paper [27] in 2018 provides a detailed survey of **cloud computing security challenges** and existing solutions. It explains how cloud services offer flexibility, scalability, and reduced cost, but also introduces new risks due to virtualization, remote data storage, and multi-tenant environments. The authors categorize security issues into **confidentiality, integrity, and availability**, highlighting threats such as unauthorized access, data leakage, VM attacks, and DDoS. Various defence approaches, including encryption, access control, trusted computing, virtualization security frameworks, and auditing mechanisms, are reviewed. The paper concludes that although many solutions exist, **significant gaps remain**, requiring further research into trust, policy enforcement, and cross-domain security.

While steganography hides secret data within images. Individually, these techniques may be **machine learning** for data analysis, but privacy risks arise when sensitive data is outsourced. To solve this, the model uses **homomorphic encryption** and multi-party computation so that training can occur on **encrypted data** without revealing original information. The approach distributes computation among multiple parties and reconstructs the classification model securely. The study demonstrates that effective machine learning can be achieved while preserving **data confidentiality** in cloud environments.

This paper [29] in 2018 focuses on the role of **machine learning** in enhancing data **privacy and security**. The authors explain that as the volume of online and cloud data grows, traditional security techniques are often insufficient against new types of cyber-attacks. The paper reviews how machine learning algorithms such as classification, clustering, anomaly detection, and neural networks can analyze usage patterns to detect intrusions and prevent unauthorized access. It highlights both the strengths and limitations of machine learning, noting issues like training data dependency and adversarial attacks. The paper concludes that integrating adaptive ML-based security models can significantly improve data protection.

According to [30] in 2017 **A. S. Pavithra and M. S. Vijayalakshmi**, cloud computing offers scalable and on-demand services but faces serious security threats involving unauthorized access and data leakage. The paper presents an in-depth review of **cryptographic techniques** such as AES, RSA, and ECC for securing cloud data transmission and storage. It also discusses the potential of **machine learning** in enhancing anomaly detection and adaptive encryption methods. The authors conclude that integrating **cryptography** with **cloud computing** infrastructure significantly improves data confidentiality, integrity, and trust between cloud providers and users.

The paper [31] in 2017 titled "Information Security: A Review on Steganography with Cryptography for Secured Data Transaction" by Kodge B. G. from Swami Vivekanand Mahavidhyalaya, India, presents a combined approach of cryptography and steganography to

enhance data security. Cryptography converts plain text into coded form, vulnerable, but combined, they provide strong security by encrypting and hiding data, making unauthorized decoding difficult. The method is particularly useful for confidential communication and protecting data from hackers and crackers.

The paper [32] in 2016 "On cloud security attacks: A taxonomy and intrusion detection and prevention as a service" by Salman Iqbal, Miss Laiha Mat Kiah, Babak Dhaghighi, Muzammil Hussain, Suleman Khan, Muhammad Khurram Khan, and Kim-Kwang Raymond Choo provides a comprehensive taxonomy of security attacks specific to cloud computing service models including SaaS, PaaS, and IaaS. It discusses new attack vectors and vulnerabilities emerging from cloud architectures and highlights intrusion detection and prevention as critical services. The authors review various attack types such as DoS, authentication attacks, and malware injection, emphasizing the importance of layered defense and effective security policies in cloud ecosystems. They also address open challenges in cloud security research and suggest mitigation strategies for enhanced trust and safety.

The paper [33] in 2016 "A Secure Data Classification Model in Cloud Computing Using Machine Learning Approach" by Kulwinder Kaur and Vikas Zandu presents a framework to address security issues in cloud computing by classifying data based on its sensitivity using machine learning. Sensitive data is encrypted using hybrid steganography methods before storing on the cloud to ensure confidentiality and integrity. The study applies boosting supervised algorithms for accurate data classification and uses image sequencing password authentication to enhance cloud access security. Simulation results show improvement over traditional methods in classification accuracy and encryption time, demonstrating the effectiveness of their approach.

Results

1. For the above literature review total 32 research papers studied in which 28 journal 3 articles and 1 conference have studied as shown in Table 1 and Fig.1 presents the graphical representation of the types of literature considered in this review.

S.No.	Types of Literature	No of literature
1	Journal	28
2	Article	3
3	Conference	1

Table 1

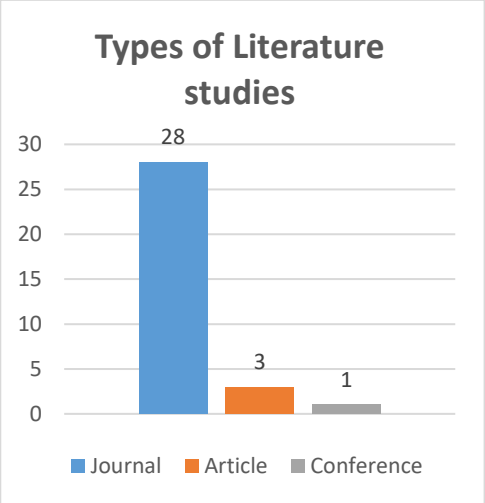


Figure 1

2. Table 2 shows about the details of no. of authors wise literature papers studied. In total 32 literature studied considered publication year between 2015- 2025. Figure 2 shows Number of authors in the considered in Literature studies in graphical form.

SNo.	No. of Authors	In Respective total no. of literature
1	1	3
2	2	14
3	3	3
4	4	5
5	5	4
6	6	0
7	7	1
8	8	1
9	9	1

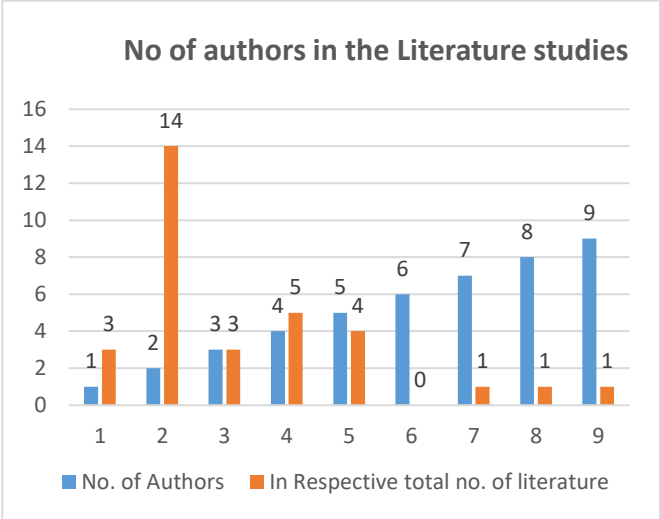


Table 2 **Figure 2**

3. Table 3 shows total numbers of papers considered and studied year wise. Figure 3 shows no. of literature (total 32 literature) studied year wise (Between 2015- 2025) in graphical form.

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

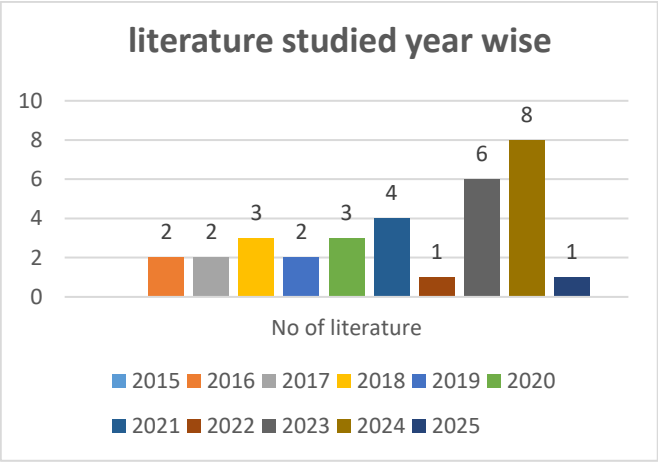


Table 3 **Figure 3**

4. Table 4 shows paper wise occurrence of keyword in research that considered in the studied.

Paper id	No of authors	Journal or conference paper	Key Word count
1	**5**	Journal	cloud computing": 6 times "machine learning": 126 times "cryptography": 50 times
2	**2**	Journal	cloud computing": 4 times "machine learning": 117 times "cryptography": 75 times
3	**4**	Journal	cloud computing": 85 times "machine learning": 7 times "cryptography": 52 times
4	**2**	Journal	"cloud computing": 58 times "machine learning": 7 times "cryptography": 31 times
5	**5**	Journal	cloud computing": 73 times "machine learning": 116 times "cryptography": 31 times
6	**2**	Journal	"cloud computing": 65 times "machine learning": 60 times "cryptography": 14 times
7	**2**	Journal	cloud computing": 45 times "machine learning": 42 times "cryptography": 15 times
8	**1**	Journal	"cloud computing": 57 times "machine learning": 38 times (included under AI technologies) "cryptography": 18 times
9	**1**	Journal	"cloud computing": 92 times "machine learning": 60 times "cryptography": 26 times
10	**4**	Journal	"cloud computing": 56 times "machine learning": 42 times "cryptography": 10 times
11	**1**	Journal	cloud computing" → 7 occurrences "machine learning" → 39 occurrences "cryptography" → 1 occurrence
12	**2**	Journal	"cloud computing" → 3 times "machine learning" → 18 times "cryptography" → 6 times
13	**2**	Journal	"cloud computing" → 4 times "machine learning" → 15 times "cryptography" → 12 times
15	**4**	Journal	"cloud computing" → 21 times "machine learning" → 2 times "cryptography" → 1 time
16	**3**	Journal	cloud computing": 52 times "machine learning": 7 times "cryptography": 15 times
17	**2**	Journal	"cloud computing" → 16 times "machine learning" → 1 time "cryptography" → 126 times
18	**4**	Journal	cloud computing": 9 times "machine learning": 0 times

			"cryptography": 0 times
19	**2**	Journal	"cloud computing": 3 times "machine learning": 0 times "cryptography": 0 times
20	**2**	Journal	cloud computing": 0 times "machine learning": 3 time "cryptography": 0 times
21	**5**	Journal	cloud computing 5 times machine learning 20 times cryptography 0 times
22	**8**	Journal	cloud computing 62 times machine learning 26 times cryptography 0 times
23	**3**	Journal	cloud computing 11 times machine learning 7 times cryptography 6 times
24	**2**	Journal	cloud computing 86 times machine learning 20 times cryptography 2 times
25	**2**	Journal	cloud computing 17 times machine learning 0 times cryptography 2 times
26	**3**	Journal	cloud computing 17 times machine learning 0 times cryptography 4 times
27	**9**	Journal	cloud computing 31 times machine learning 0 times cryptography 0 times
28	**2**	Journal	Cloud Computing 2 Machine Learning 13 Cryptography 0
29	**4**	Journal	Cloud Computing 2 times Machine Learning 50 times Cryptography 0 times
30	**2**	Journal	Cloud Computing 28 times Machine Learning 6 times Cryptography 19 times
31	**1**	Journal	Cloud computing → 0 times Machine learning → 0 times Cryptography → 39 times
32	**7**	Journal	Cloud computing → 65 times Machine learning → 1 time Cryptography → 2 times
33	**2**	Journal	Cloud computing → 36 times Machine learning → 10 times Cryptography → 3 times

Table 4

Conclusion

The reviewed literature underscores that integrating Machine Learning and Cryptography offers a promising pathway toward building intelligent, secure, and scalable cloud environments. ML algorithms enable proactive threat detection, adaptive security policy enforcement, and automated

incident response, while cryptographic techniques ensure data confidentiality, integrity, and authenticity. Together, they form a multi-layered defense mechanism capable of addressing emerging challenges in cloud and IoT ecosystems. However, several limitations persist, including data dependency, algorithmic transparency, and encryption overheads. Future research should emphasize privacy-preserving learning, federated AI systems, and lightweight cryptographic protocols to enhance cloud resilience. Overall, the convergence of ML and cryptography represents a transformative approach to achieving robust, intelligent, and trustworthy cloud computing security.

REFERENCES

[1] V. Kaur, G. Kaur, G. Dhiman, R. Bindal, and M. K. Mishra, "Adaptability of Machine Learning in Cryptography," *Solid State Technology*, vol. 63, no. 4, pp. 1–8, 2020.

[2] N. S. Selamat and F. H. M. Ali, "Comparison of Malware Detection Techniques Using Machine Learning Algorithm," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 16, no. 1, pp. 435–440, Oct. 2019.

[3] Y. Alemami, A. M. Al-Ghonmein, K. G. Al-Moghrabi, and M. A. Mohamed, "Cloud Data Security and Various Cryptographic Algorithms," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 13, no. 2, pp. 1867–1879, Apr. 2023.

[4] B. Nabil and J. J. Martínez Herráiz, "A Robust Cloud Security Model Leveraging a Hybrid of Cryptography and Steganography," *Universidad de Alcalá*, Apr. 2024.

[5] D. D. Rao, "Cybersecurity Threat Detection Using Machine Learning in Cloud-Based Environments: A Comprehensive Study," *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 12, no. 1, pp. 1–8, Jan. 2024.

[6] S. V. Bhaskaran and S. Achar, "A Study of Evolving Cloud Computing Data Security: A Machine Learning Perspective," *Business Review*, vol. 10, no. 3, pp. 1–15, 2025, doi: 10.26668/businessreview/2025.v10i3.5315.

[7] C. Wei and L. Mei, "Improving Data Access in Cloud Computing Environments Through AI and Machine Learning," *Journal of Innovative Technologies*, vol. 7, 2024.

[8] R. Jones, "The Impact of AI on Secure Cloud Computing: Opportunities and Challenges," *Indonesian Journal of Computer Science*, vol. 13, no. 4, pp. 4708–4715, Aug. 2024.

[9] H. Sharma, "The Role of Artificial Intelligence and Machine Learning in Strengthening Cloud Security: A Comprehensive Review and Analysis," *International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE)*, vol. 13, no. 8, pp. 1–8, Aug. 2024.

[10] I. Zziwa, A. Ilolo, K. C. Nwafor, and D. O. T. Ihenacho, "Cloud Computing and AI in Cybersecurity Forensics: Leveraging Data Analytics for Enhanced Threat Detection and Incident Response," *International Journal of Research Publication and Reviews*, vol. 1, pp. 1–10, 2024.

[11] H. Rehan, "AI-Driven Cloud Security: The Future of Safeguarding Sensitive Data in the Digital Age," *Journal of Artificial Intelligence General Science (JAIGS)*, vol. 1, no. 1, Jan. 2024.

[12] A. A. Jabbar and W. S. Bhaya, "Security of Private Cloud Using Machine Learning and Cryptography," *Bulletin of Electrical Engineering and Informatics*, vol. 12, no. 1, pp. 561–569, Feb. 2023.

[13] P. R. Kumar and S. Goel, "Integrating Machine Learning Algorithms with an Advanced Encryption Scheme: Enhancing Data Security and Privacy," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 12, pp. 1–8, 2023.

[14] P. Mell and T. Grance, *The NIST Definition of Cloud Computing (Special Publication 800-145)*, National Institute of Standards and Technology, 2011.

[15] D. Paulraj, S. Neelakandan, M. Prakash, and E. Baburaj, "Admission Control Policy and Key Agreement Based on Anonymous Identity in Cloud Computing," *Journal of Cloud Computing: Advances, Systems and Applications*, vol. 12, art. no. 71, 2023.

[16] 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, pp. 1–8, Aug. 2023.

[17] K. S. Rao and V. H. Shastri, "A Review on Various Cryptography Techniques in Cloud Security," *Dogo Rangsang Research Journal*, vol. 13, no. 4, pp. 1–10, Apr. 2023.

[18] A. A. Mawgoud, M. H. N. Taha, A. A. Talleb, and A. K. Khaled, "A Deep Learning-Based Steganography Integration Framework for Ad-Hoc Cloud Computing Data Security Augmentation Using the V-BOINC System," *Journal of Cloud Computing: Advances, Systems and Applications*, vol. 11, art. no. 97, 2022.

[19] G. Nzeako and R. A. Shittu, "Leveraging AI for Enhanced Identity and Access Management in Cloud-Based Systems to Advance User Authentication and Access Control," *World Journal of Advanced Research and Reviews*, vol. 24, no. 3, pp. 1661–1674, Dec. 2024.

[20] M. Alsharif and D. B. Rawat, "Study of Machine Learning for Cloud-Assisted IoT Security as a Service," *Sensors*, vol. 21, no. 1034, 2021.

[21] M. U. Sana, Z. Li, F. Javaid, H. B. Liaqat, and M. U. Ali, "Enhanced Security in Cloud Computing Using Neural Network and Encryption," *IEEE Access*, vol. 9, pp. 1–10, Oct. 2021, doi: 10.1109/ACCESS.2021.3122938.

[22] U. A. Butt et al., "A Review of Machine Learning Algorithms for Cloud Computing Security," *Electronics*, vol. 9, no. 1379, pp. 1–25, 2020.

[23] A. A. Ahmed, M. I. T. Hussan, and V. Bollapalli, "Upgrade Data Security in Cloud by Machine Learning and Cryptography Techniques," *International Journal of Engineering and Advanced Technology (IJEAT)*, vol. 8, no. 6, pp. 1–6, Aug. 2019.

[24] Z. Salman and M. Hammad, "Securing Cloud Computing: A Review," *International Journal of Computing and Digital Systems*, vol. 10, no. 1, pp. 1–10, Apr. 2021.

[25] 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, pp. 1–8, 2020.

[26] S. K. Singh, P. K. Manjhi, and R. K. Tiwari, "Cloud Computing Security Using Steganography," *Journal of Emerging Technologies and Innovative Research (JETIR)*, vol. 6, no. 6, pp. 923–930, Jun. 2019.

[27] S. Basu et al., "Cloud Computing Security Challenges and Solutions – A Survey," *Institute of Engineering and Management, Kolkata*, pp. 1–10, 2019.

[28] F. O. Çatak and A. F. Mustacoglu, "Cryptographically Privacy-Preserving Extreme Learning Machine for Cloud Systems," *Proceedings on Privacy Enhancing Technologies*, vol. 2018, no. 3, pp. 123–142, 2018.

[29] E. Hesamifard, H. Takabi, M. Ghasemi, and R. N. Wright, "Privacy-Preserving Machine Learning as a Service," *Proceedings on Privacy Enhancing Technologies*, vol. 2018, no. 3, pp. 123–142, 2018.

[30] K. Kiran and S. Sharma, "Enhance Data Security in Cloud Computing Using Machine Learning and Hybrid Cryptography Techniques," *International Journal of Advanced Research in Computer Science*, vol. 8, no. 9, pp. 1–8, Nov.–Dec. 2017.

[31] B. G. Kodge, "Information Security: A Review on Steganography with Cryptography for Secured Data Transaction," *International Journal of Scientific Research in Network Security and Communication (IJSRNSC)*, vol. 5, no. 6, pp. 1–6, Dec. 2017.

[32] S. Iqbal et al., "On Cloud Security Attacks: A Taxonomy and Intrusion Detection and Prevention as a Service," *Journal of Network and Computer Applications*, vol. 80, pp. 1–15, 2017.

[33] K. Kaur and V. Zandu, "A Secure Data Classification Model in Cloud Computing Using Machine Learning Approach," *International Journal of Grid and Distributed Computing*, vol. 9, no. 8, pp. 13–22, 2016.

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