The Evolution of Cloud Security: A Review of Methods and Challenges

Rajneesh Singla, Nand Kishore

UIET, Panjab University, Chandigarh, India

Corresponding author: Rajneesh Singla, Email: eng.singla85@gmail.com

Cloud computing offers scalable and adaptable computing resources, it has completely changed how businesses run. However, security issues have become crucial due to the enormous volumes of data being processed and stored in the cloud. In this paper presents a review of security techniques employed in cloud computing environments. It discusses various aspects including data encryption, access restriction mechanisms, recognize and authentication management, network security measures, and compliance frameworks. Additionally, the study explores emerging technologies like homomorphic encryption and blockchain for enhancing security in the cloud. The analysis emphasizes how crucial a multi-layered security approach is to reducing the risks of insider threats, illegal access, and data breaches. The reviewed studies propose various methods for enhancing cloud security, data encryption, and intrusion detection, showing promising results such as high accuracy and robustness in controlled experiments. However, most approaches face limitations in real-time applicability, adaptability to diverse attack scenarios, or scalability across platforms. While techniques like hybrid encryption, SMOTE-based IDS, and ML-based SSE demonstrate effectiveness, they often struggle with practical deployment challenges such as overhead, unpredictability, or incomplete protection.

Keywords: Cloud computing, Security, Encryption, Blockchain

2025. In Himanshu Mittal (ed.), *Smart Computing and Emerging Technologies*, 35–42. Computing & Intelligent Systems, SCRS, India. DOI: https://doi.org/10.56155/978-81-975670-0-1-4

1 Introduction

1.1 Background

Cloud computing presents numerous benefits compared to traditional networks, enhancing performance and productivity for both consumers and businesses. However, it also encounters various security risks and challenges, significantly influencing individuals' decisions regarding its usage [1]. Potential cloud users should think about a number of security issues before moving their operations and data to cloud platforms. Despite the implementation of several security measures within the cloud, evaluating their effectiveness is crucial for understanding its overall security posture. Security models provide the framework necessary for collecting security information, evaluating various network attack scenarios, and selecting suitable countermeasures. However, due to the more complex privilege boundaries in the cloud compared to traditional networks, automating the functions of these models can be challenging [3]. Presently, because enabling automation is complex, a significant portion of cloud security analysis is conducted manually by security professionals. Nevertheless, this manual approach is time-consuming and susceptible to human error. Hence, automation is essential for cost reduction, time savings, and mitigation of human mistakes. The factors posing a threat to cloud security include:

Unauthorized Use and Exploitation of Cloud Resources*:* While cloud computing offers convenient access to bandwidth and storage, it lacks complete control over resource utilization, leaving room for malevolent users and attackers to exploit vulnerabilities.
Attacks by Malicious Insiders: Often underestimated, attacks by malicious insiders have the potential to cause significant harm across all tiers of cloud infrastructure. A malevolent insider with advanced access rights can take over components of the network and alter private data [5].

Weaknesses in Application Programming Interfaces (APIs): Cloud services offer APIs that facilitate user interaction at various levels, enhancing usability but also introducing complexity. Unfortunately, malicious individuals can exploit vulnerabilities in these APIs to gain unauthorized access [6].

Data Leakage and Loss: Data is frequently transferred and communicated via untrusted networks; data security is a key concern in cloud computing. Weak authentication, inadequate encryption, malfunctioning data centers, and deficiencies in disaster recovery procedures can lead to data loss, exposing clients and industries to significant financial risks due to data theft [7].

Vulnerabilities in Distributed Technology: Cloud computing's multi-tenant architecture allows several users to share on-demand services. However, vulnerabilities in the hypervisor can enable malicious hackers to gain control of legitimate virtual machines, potentially disrupting the normal functioning of the cloud infrastructure [8].

Services and Account Hijacking*:* Malevolent actors can redirect web services to fraudulent websites, gaining access to authentic websites and compromising user credentials. This can lead to identity theft and phishing attempts.

Threats from Anonymous Profiles*:* While cloud services may offer improved security by requiring less maintenance and interaction with hardware and software, organizations risk exposing sensitive data if Compliance Management, Securing Systems, Inspection, patching, logging, and knowledge of internal security measures are not followed diligently [9].

1.2 Security Solutions to Cloud Computing

Once the primary security threats associated with cloud computing have been identified, it can be valuable to explore various cryptographic methods to address specific security concerns. However, the intrinsic characteristics of cloud computing make the problem of data security more complex. Before prospective cloud users can safely migrate their applications or data to the cloud, several security measures must be established. Here are various security services that can be implemented [15]:

User Authentication*:* This process verifies the identity of individuals involved in transactions, while data origin authentication verifies the source of the message [16]. Cloud environments often utilize digital signatures for data origin authentication, requiring knowledge of a secret key to create.

Data Integrity: Maintaining data integrity ensures that unauthorized parties have not altered data. Cryptographic methods including digital signatures and MACs (message authentication codes) can be used to verify the integrity of messages. These methods are particularly useful in cloud environments to safeguard the integrity of forensic data used in investigations [17].

Non-Repudiation: Non-repudiation ensures that a party cannot deny making or sending a transaction or communication. Digital signatures provide proof of message authenticity, as only a party with access to the secret key can create a digital signature [18].

Confidentiality: Confidentiality prevents disclosure by unauthorized means by guaranteeing that information is only available to authorized persons. Cryptography and encryption are effective in establishing confidentiality. Pseudorandom number generation, based on cryptographic methods, is used to create encryption scheme keys.

2 Related Work

The security of cloud computing has improved a lot of the years to adapt to the growing threats in distributed environments. This review literature studies different security approaches, including the traditional cryptographic techniques, ml and dl-based techniques for anomaly detection, Revocable-Based Encryption (RBE) for flexible access control, advanced cryptographic algorithms for improved data security and the blockchain-based frameworks to ensure the transparency and immutability of cloud systems.

2.1 Cryptography Techniques for Clous Data Security

S. Lv, et.al (2023) suggested a MMDSSE technique to encrypt data, which supported manifold users and keywords [21]. The multi-keyword search was executed via an ISO-OR operation for documenting the correlation of keyword with identifier so that a tag was created. A new hybrid data encryption (DE) technique was projected by B. Pushpa, et.al (2020) for protecting the analytical data of medicinal picture [23]. Two Fish Encryption (TFE) method and Blowfish Encryption (BE) technology were integrated and Two-Dimension Discrete Wavelet Transform (2D-DWT) was implemented to secure data. It was advised to use an LS-RQ by Y. Peng, et.al (2022) to preserve the balance between security and efficacy on geographically encrypted data [24]. To manage the geographic data on the public clouds, an index system was used. The confidentiality of the data was maintained in this. An approach was formulated by K. Jaspin, et.al (2021) to encrypt and decrypt the files, utilized for providing an improved level of security [25]. A double encryption technique was implemented to upload the file in cloud. Two algorithms were employed to encrypt the file 2 times. First, the file was encrypted using the AES method, followed by the RSA algorithm.

Table 1. Comparison of Cryptography based Techniques

Author	Year	Technique Used	Results	Limitations
S. Lv, et.al	2023	MMDSSE method	The experiment's findings demonstrated the effectiveness of the suggested approach.	This technique was compatible for satisfying the demands of functions and searchable support.
S. Malhotra, et.al	2023	SSE method based on ML	The suggested approach, which had a CCR of 69.73% and performed well in terms of TPR and FPR.	The method was not applicable on real time cloud platform.
B. Pushpa, et.al	2020	New hybrid data encryption (DE) technique	The outcomes demonstrated the effectiveness of the proposed strategy over a wide range of measures.	This approach was not very adaptable.
Y. Peng, et.al	2022	LS-RQ	The real-time robustness of this strategy was demonstrated by the experimental results.	The overhead factor to transfer data was maximized.
K. Jaspin, et.al	2021	Double encryption technique	The results on DropBox exhibited that the formulated approach was useful for enhancing security level.	This method was unable to figure out how to properly secure the data.

2.2 Deep Learning and Machine Learning based approaches to the Cloud Security

M. Ouhssini, et.al (2024) suggested DeepDefend method to instantly identify and stop DDoS assaults in cloud environments [26]. During testing on the CIDDS-001 traffic dataset, DeepDefend demonstrated rapid and accurate DDoS attack detection as well as excellent entropy prediction accuracy. An enhanced SMOTE (synthetic minority over-sampling technique)-based cloud IDS technique was introduced by M. Bakro, et.al (2023) for tackling the imbalanced data issue [27]. A hybrid method of IG, CS & PSO was implemented to select features. This RF algorithm was introduced to identify and categorize various types of attacks. An AEDL (autoencoder based deep learning) approach was designed by F. J. Abdullayeva, et.al (2021) to detect APT attack [28]. This method leveraged the capability of autoencoders to capture intricate feature correlations within a database, resulting in high classification accuracy. In other work, K. Karthick, et.al (2022) created the Subset Scaling Recursive Factor Feature selection (S2RF2S) method, which uses Lattice Structural access rate to detect DDoS attacks [29]. An innovative method was projected by A. Bhardwaj, et.al (2020) in which stacked sparse AutoEncoder (SSAE) was integrated with DNN (Deep Neural Network) to distinguish between DDoS attack and innocuous network traffic [30]. A well-designed stacking sparse AutoEncoder (AE) was incorporated to learn features.

Table 2. Comparison of ML and DL based Methods

Author	Year	Technique Used	Results	Limitations
M. Ouhssini, et.al	2024	DeepDefend	The results depicted that the suggested model was worked robustly for protecting cloud computing (CC) from DDoS attacks.	This model was ineffective in real-time cloud situations in case of variation and unpredictability of situations.
M. Bakro, et.al	2023	SMOTE-based cloud IDS	The introduced approach offered an accuracy of 98% on UNSW-NB15 and 99% on Kyoto datasets while classifying attacks.	This technique was not tested on extensive datasets having diverse attacks.
F. J. Abdullayeva, et.al	2021	AEDL method	The simulation results exhibited that the designed method had generated more promising results as compared to other methods and offered an accuracy of 98.32% to detect and prevent APT assaults.	This method had not assigned ranks to hosts utilized in exfiltration of data under APT attack.
K. Karthick, et.al	2022	S2RF2S technique	The experiments indicated the supremacy of developed technique for avoiding security issues in Cloud Computing (CC).	This method failed to detect unusual circumstances brought on by DDoS attacks and forecast patterns in typical network traffic..
A. Bhardwaj, et.al	2020	An innovative method of SSAE and DNN	The projected method was performed more robustly on second dataset and offered superior results on initial one.	The time to detect attacks and computing complexity were greater to analyze large data.

2.3 Revocable-Based Encryption (RBE) techniques to the Cloud Security

C. Ge, et.al (2021) presented new framework to address the key revocation issue, which is known as RIB-BPRE [31]. The delegator generated a set of delegates using the re-encryption key, which the proxy for this model might cancel. The performance review confirmed the suggested approach's efficacy and feasibility. RMA-ABE is a successful cloud storage (CS) technique that was proposed by Y. Ming et al. in 2021 [32]. This approach did not require any bilinear pairing processes. Through the use of a version key included in the feature, the attribute revocation was achieved. A RL-ABE model was presented by S. Zhao, et.al (2020) to secure cloud storage [33]. This approach provided a fine-grained access control to user rights so as to obtain shared data, and it was resistant to attacks by quantum algorithms. Two Revocable Hierarchical Identity-based Encryption (RHIBE) techniques were formulated by K. Lee, et.al (2021) in composite-order bilinear groups [34]. A TRAK-CPABE was constructed by M. Bouchaala, et.al (2021) emphasizing monitorability, reversibility, transparency, and key-escrow avoidance [35]. The primary focus of this method was to divide the initial data that was uploaded to the cloud server. The data owner was obliged to retrieve, re-encrypt, and republish the material.

Table 3. Comparison of RBE Techniques to Cloud Data Security

Author	Year	Technique Used	Results	Limitations
C. Ge, et.al	2021	RIB-BPRE framework	The performance review confirmed the suggested approach's efficacy and feasibility.	This framework was not worked effectively when it was designed random oracles.
Y. Ming, et.al	2021	RMA-ABE technique	The proposed technique under study was capable of addressing the IND-CPA.	This technique had not allowed all user to for storing data in the cloud securely.
S. Zhao, et.al	2020	RL-ABE model	The presented model was more effective than prior approaches.	This method was robust only against 2 kinds of attacks.
K. Lee, et.al	2021	Two RHIBE (Revocable Hierarchical Identity-based Encryption) techniques	The outcomes demonstrated the adaptive security of these methods.	The secret key was not generated effectively due to which the requirements of key sanity check (KSC) algorithm were not satisfied.
M. Bouchaala, et.al	2021	TRAK-CPABE algorithm	The experiments' outcomes demonstrated how resilient the developed algorithm was against attacks.	The white-box traceability model lacked efficiency and robustness.

3 Conclusion & Future Work

Cloud computing is often referred to as a model that provides limitless computing services with a pay-as-you-go model. algorithm. The importance of strong security measures in cloud computing systems is emphasized by this review. As businesses depend more and more on the cloud to run their operations, it is critical to guarantee the availability, security, and integrity of data. The multi-faceted approach discussed, encompassing encryption, access controls, authentication mechanisms, and network security measures, illustrates the complexity of safeguarding cloud infrastructures. Moreover, the exploration of emerging technologies suggests promising avenues for addressing evolving security challenges. However, it is clear that security in the cloud is not a one-size-fits-all solution; rather, it requires a tailored and dynamic approach. Organizations must actively engage in risk assessment, implement best practices, and stay abreast of evolving threats to effectively mitigate security risks.Many approaches lack adaptability in unpredictable environments, suffer from scalability limitations, or generate high computational overhead. Techniques that appear effective in simulations may fall short when confronted with diverse and evolving attack scenarios in real-time cloud platforms. Thus, future research should focus on developing more resilient, flexible, and scalable security mechanisms capable of addressing dynamic threats while ensuring efficient performance across varied cloud infrastructures.

References

[1] S. Kannadhasan, R. Nagarajan and S. Thenappan, "Intrusion Detection Techniques Based Secured Data Sharing System for Cloud Computing Using MSVM," 2022 9th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2022, pp. 50-56

[2] N. Ahmad, "Cloud computing: Technology, security issues and solutions," 2017 2nd International Conference on Anti-Cyber Crimes (ICACC), Abha, Saudi Arabia, 2017, pp. 30-35

[3] A. Patel, N. Shah, D. Ramoliya and A. Nayak, "A detailed review of Cloud Security: Issues, Threats & Attacks," 2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 2020, pp. 758-764

[4] G. R. G, R. Santhoshkumar, D. Venkatesan, K. S and P. Santosh Kumar Patra, "Intrusion Detection in Cloud Architecture Using Machine Learning," 2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), Greater Noida, India, 2022, pp. 483-487

[5] K. Soni and S. Kumar, "Comparison of RBAC and ABAC Security Models for Private Cloud," 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon), Faridabad, India, 2019, pp. 584-587

[6] Y. Gajmal and K. P. Thooyamani, "A Survey on Access Controls in Cloud Computing," 2018 4th International Conference on Computing Communication and Automation (ICCCA), Greater Noida, India, 2018, pp. 1-4

[7] R. T. Hameed, A. A. Hussain, O. A. Mohamad, K. A. Zidan, O. T. Hamid and S. A. Salman, "Improved Cloud Computing Security," 2018 1st Annual International Conference on Information and Sciences (AiCIS), Fallujah, Iraq, 2018, pp. 170-175

[8] A. D. Bhagat, S. Basia, K. Sharma and P. Vats, "A Survey of Cloud Architectures: Confidentiality, Contemporary State, and Future Challenges," 2022 3rd International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), Ghaziabad, India, 2022, pp. 1-8

[9] M. Popli and Gagandeep, "A Survey on Cloud Security Issues and Challenges," 2019 6th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2019, pp. 230-235

[10] A. Sharma, U. K. Singh, K. Upreti and D. S. Yadav, "An investigation of security risk & taxonomy of Cloud Computing environment," 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 2021, pp. 1056-1063

[11] W. Shen, J. Yu, M. Yang and J. Hu, "Efficient Identity-Based Data Integrity Auditing with Key-Exposure Resistance for Cloud Storage," in IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 13, pp. 637-645, 2022

[12] M. Yang, T. Gao, W. Xie, L. Jia and T. Zhang, "The Assessment of Cloud Service Trustworthiness State Based on D-S Theory and Markov Chain," in IEEE Access, vol. 10, pp. 68618-68632, 2022

[13] C. Yang, Y. Liu, X. Tao and F. Zhao, "Publicly Verifiable and Efficient Fine-Grained Data Deletion Scheme in Cloud Computing," in IEEE Access, vol. 8, pp. 99393-99403, 2020

[14] L. Cao, R. Li, X. Ruan and Y. Liu, "Defending Against Co-Residence Attack in Energy-Efficient Cloud: An Optimization Based Real-Time Secure VM Allocation Strategy," in IEEE Access, vol. 10, pp. 98549-98561, 2022

[15] H. Attou, A. Guezzaz, S. Benkirane, M. Azrour and Y. Farhaoui, "Cloud-Based Intrusion Detection Approach Using Machine Learning Techniques," in Big Data Mining and Analytics, vol. 6, no. 3, pp. 311-320, September 2023

[16] H. Jin, Z. Li, D. Zou and B. Yuan, "DSEOM: A Framework for Dynamic Security Evaluation and Optimization of MTD in Container-Based Cloud," in IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 3, pp. 1125-1136, 1 May-June 2021

[17] X. Ouyang, Y. Xu, Y. Mao, Y. Liu, Z. Wang and Y. Yan, "Blockchain-Assisted Verifiable and Secure Remote Sensing Image Retrieval in Cloud Environment," in IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing, vol. 16, pp. 1378-1389, 2023

[18] B. Celiktas, I. Celikbilek and E. Ozdemir, "A Higher-Level Security Scheme for Key Access on Cloud Computing," in IEEE Access, vol. 9, pp. 107347-107359, 2021

[19] R. R. Irshad et al., "A Multi-Objective Bee Foraging Learning-based Particle Swarm Optimization Algorithm for Enhancing the Security of healthcare data in cloud system," in IEEE Access, vol. 12, no. 1, pp. 94-100, 2023

[20] D. Ramesh,B. Rama, “Flexible And Efficient Encryption Scheme For Data Dynamics On Encrypted Outsourced Data To Public Cloud”, 2019, International Journal of Scientific & Technology Research, Volume 8, Issue 10

[21] S. Lv, H. Tan and M. Wang, “A dynamic conjunctive keywords searchable symmetric encryption scheme for multiple users in cloud computing”, Computer Communications, vol. 209, pp. 239-248, 10 July 2023

[22] S. Malhotra and W. Singh, “An efficacy analysis of data encryption architecture for cloud platform”, Procedia Computer Science, vol. 218, pp. 989-1002, 31 January 2023

[23] B. Pushpa, "Hybrid Data Encryption Algorithm for Secure Medical Data Transmission in Cloud Environment," 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 2020, pp. 329-334

[24] Y. Peng, L. Wang, J. Cui, X. Liu, H. Li and J. Ma, "LS-RQ: A Lightweight and Forward-Secure Range Query on Geographically Encrypted Data," in IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 1, pp. 388-401, 1 Jan.-Feb. 2022

[25] K. Jaspin, S. Selvan, S. Sahana and G. Thanmai, "Efficient and Secure File Transfer in Cloud Through Double Encryption Using AES and RSA Algorithm," 2021 International Conference on Emerging Smart Computing and Informatics (ESCI), Pune, India, 2021, pp. 791-796

[26] M. Ouhssini, K. Afdel and A. Abarda, “DeepDefend: A comprehensive framework for DDoS attack detection and prevention in cloud computing”, Journal of King Saud University - Computer and Information Sciences, vol. 36, no. 2, pp. 781-790, 4 February 2024

[27] M. Bakro et al., "An Improved Design for a Cloud Intrusion Detection System Using Hybrid Features Selection Approach With ML Classifier," in IEEE Access, vol. 11, pp. 64228-64247, 2023

[28] F. J. Abdullayeva, “Advanced Persistent Threat attack detection method in cloud computing based on autoencoder and softmax regression algorithm”, Array, vol. 10, pp. 56-62, 21 April 2021

[29] K. Karthick, G. Kiruthiga and R. Radha, “A Subset Scaling Recursive Feature Collection Based DDoS Detection Using Behavioural Based Ideal Neural Network For Security In A Cloud Environment”, Procedia Computer Science, vol. 215, pp. 509-518, 2022

[30] A. Bhardwaj, V. Mangat and R. Vig, "Hyperband Tuned Deep Neural Network With Well Posed Stacked Sparse AutoEncoder for Detection of DDoS Attacks in Cloud," in IEEE Access, vol. 8, pp. 181916-181929, 2020

[31] C. Ge, Z. Liu, J. Xia and L. Fang, "Revocable Identity-Based Broadcast Proxy Re-Encryption for Data Sharing in Clouds," in IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 3, pp. 1214-1226, 1 May-June 2021

[32] Y. Ming, B. He and C. Wang, "Efficient Revocable Multi-Authority Attribute-Based Encryption for Cloud Storage," in IEEE Access, vol. 9, pp. 42593-42603, 2021

[33] S. Zhao, R. Jiang and B. Bhargava, "RL-ABE: A Revocable Lattice Attribute Based Encryption Scheme Based on R-LWE Problem in Cloud Storage," in IEEE Transactions on Services Computing, vol. 15, no. 2, pp. 1026-1035, 1 March-April 2022

[34] K. Lee, “Revocable hierarchical identity-based encryption with adaptive security”, Theoretical Computer Science, vol. 40, no. 8, pp. 2142-2151, 2021

[35] M. Bouchaala, C. Ghazel and L. AzzouzSaidane, “TRAK-CPABE: A novel Traceable, Revocable and Accountable Ciphertext-Policy Attribute-Based Encryption scheme in cloud computing”, Journal of Information Security and Applications, vol. 275, no. 13, pp. 364-372, 2021