RESEARCH PAPER

Securing Cloud Data Storage Using Cryptography And Steganography With Machine Learning

Dinesh Kumar Moriya[1], Dr. Rishikesh Rawat[2]

[1]Research Scholar, Computer Science, Madhyanchal Professional University, Bhopal (M.P.)
[2]Professor; Madhyanchal Professional University, Bhopal (m.p.)

Abstract
Cloud computing provides scalable storage, yet security continues to be a major issue because of malicious data and unauthorized access. Conventional approaches depend on encryption, intrusion detection, or steganography separately, which do not deliver complete security. This paper presents a hybrid technique that integrates machine learning-based data classification with image-based encryption and steganography. The methodology categorizes incoming data as normal, average, and malicious through machine learning, discarding harmful data. Normal and average data are encrypted through a NOR-based operation with a secret key and hidden inside an image using steganography. Experimental results illustrate secure storage, early identification of malicious content, and data confidentiality.

Keywords: Cloud Security, Machine Learning, Cryptography, Steganography, NOR Encryption, Data Classification
How to cite this article: Moriya DK, Rawat R., Securing Cloud Data Storage Using Cryptography And Steganography With Machine Learning. Int J Drug Deliv Technol. 2026;16(77s): 886-890; DOI: 10.25258/ijddt.16.77s.104

1. Introduction

Cloud computing has become a groundbreaking technology that revolutionizes computing and data management from personal desktops and portable devices to centralized data centers. This technology allows applications and services to be delivered over the internet, rather than relying on local resources. The cloud infrastructure, comprising hardware and system software in data centers, provides the backbone for these services, offering scalability, flexibility, and accessibility to users globally.

The evolution of cloud computing has led to the rise of new security concerns, particularly as more sensitive data is stored in the cloud and transmitted across networks. Data privacy, access control, and protection against cyber threats are critical considerations. As a result, various encryption and data protection techniques have been proposed to secure cloud-based information, ensuring that unauthorized users cannot access or tamper with the data.

Steganography is a method used to conceal information within another medium, like text, audio, video, or images, and it plays a role in improving data security during transmission over networks, including cloud environments. In contrast to cryptography, which aims to render information inaccessible to those who do not have authorization, steganography keeps the very existence of the message hidden. This makes steganography a valuable tool for securely transmitting sensitive data in environments like cloud computing, where data privacy is a paramount concern.

A field of artificial intelligence known as machine learning (ML) enables systems to learn using data and progressively improve without direct programming. It applies algorithms that, when provided input data, can identify patterns, make decisions, and predict outcomes.

Literature review of the research papers

Machine learning is broadly applied in areas such as fraud detection, medical diagnosis, recommendation systems, along with image and speech recognition.

Within cloud computing, steganography may be applied to conceal encrypted messages inside media files such as images or videos, ensuring the information stays hidden from casual viewers and possible attackers. For example, the Least Significant Bit (LSB) technique, a simple and widely used steganographic method, embeds sensitive data into the least significant bits of pixels within a cover image. However, as highlighted in research, LSB by itself does not ensure strong security, since it remains susceptible to basic attacks like noise addition or image compression.

2. Related Work

2.1 Traditional Encryption

Encryption algorithms like AES, DES, and RSA provide strong confidentiality but do not detect malicious data. Encrypted malicious content can still compromise systems or cloud resources.

2.2 Machine Learning-Based Detection

ML-based intrusion detection systems can classify data and detect anomalies effectively but do not prevent leakage of sensitive information if storage is unencrypted.

2.3 Steganography-Based Secure Storage

Hiding data in images ensures confidentiality and prevents visual detection but does not identify or block malicious content, leaving the system vulnerable to attacks.

2.4 Problem Identification

None of the existing methods simultaneously detect malicious content and securely store sensitive data. This motivates a hybrid approach.

Paper	Focus Area	Techniques Used	Key Contribution / Outcome
P1	Private cloud security	ML (RF, DT, LR, SGD) + Encryption (AES, 3DES, RC4)	Two-phase model: intrusion detection + data classification with high accuracy
P2	Ad-hoc cloud security	Deep learning + Steganography (V-BOINC)	Secure data transmission with hidden images in unstable cloud systems
P3	Hybrid cloud security	AES, RSA + LSB steganography	Layered model improving confidentiality and integrity
P4	Data classification security	ML (Enhanced KNN + Ensemble) + Hybrid cryptography	Improved classification accuracy and strong encryption
P6	Secure cloud migration	Arithmetic encryption + LSB steganography	Secure data transfer with high PSNR and 94% accuracy
P7	Cloud attack taxonomy	IDS/IPS, ANN, fuzzy logic	Classification of attacks and IDPS-based mitigation strategies
P8	Cloud security challenges	Encryption, IDS, access control	Defense-in-depth strategies for major cloud threats
P9	Image steganography review	RSA, AES, Blowfish + steganography	Comparative study of security vs quality vs capacity
P10	Mobile cloud security	LSB steganography + key-based access	Lightweight secure storage for small-scale data
P11	Cloud security issues	Homomorphic, attribute-based encryption	Mapping of threats to security solutions
P12	Federated cloud security	Encryption + secure query processing	Secure data sharing across multiple clouds
P13	Cloud compliance & risk	Ontology + recommendation system	Helps users select secure/compliant providers
P14	Cloud security review	Cryptography, IAM, blockchain, ML	Emphasizes layered and adaptive security
P15	Cloud fundamentals	Service & deployment models	Overview of cloud benefits and challenges
P16	Cloud data security	One-time pad + steganography	Strong dual-layer confidentiality system
P17	Privacy-preserving security	HE, SMPC, Differential Privacy, FL	Survey of privacy-enhancing technologies
P18	Steganography review	Image, video, protocol steganography	Comparison of embedding techniques and challenges
P19	Advanced security techniques	ML, blockchain, quantum, DNA crypto	Comparative study of modern security approaches
P20	Risk management	PDCA, ISO 27005 frameworks	Need for unified cloud risk framework
P21	Security challenges survey	Encryption, IDS, auditing	Identification of threats and solutions
P22	VM migration security	ML + encryption	Reduced downtime and secure migration
P23	Cloud security survey	Cryptography, access control	Need for integrated security frameworks
P24	Data protection	RSA + DES hybrid encryption	Multi-level encryption improves security
P25	Crypto-stego model	AES, Blowfish + LSB	Multi-layered protection with improved performance
P26	Data confidentiality	RSA, AES + steganography	Dual-layer security for cloud data
P27	Intrusion detection	ML, statistical, anomaly detection	Hybrid anomaly detection improves security
P28	SaaS security	Hybrid cryptography, audits	Emphasis on compliance and secure development

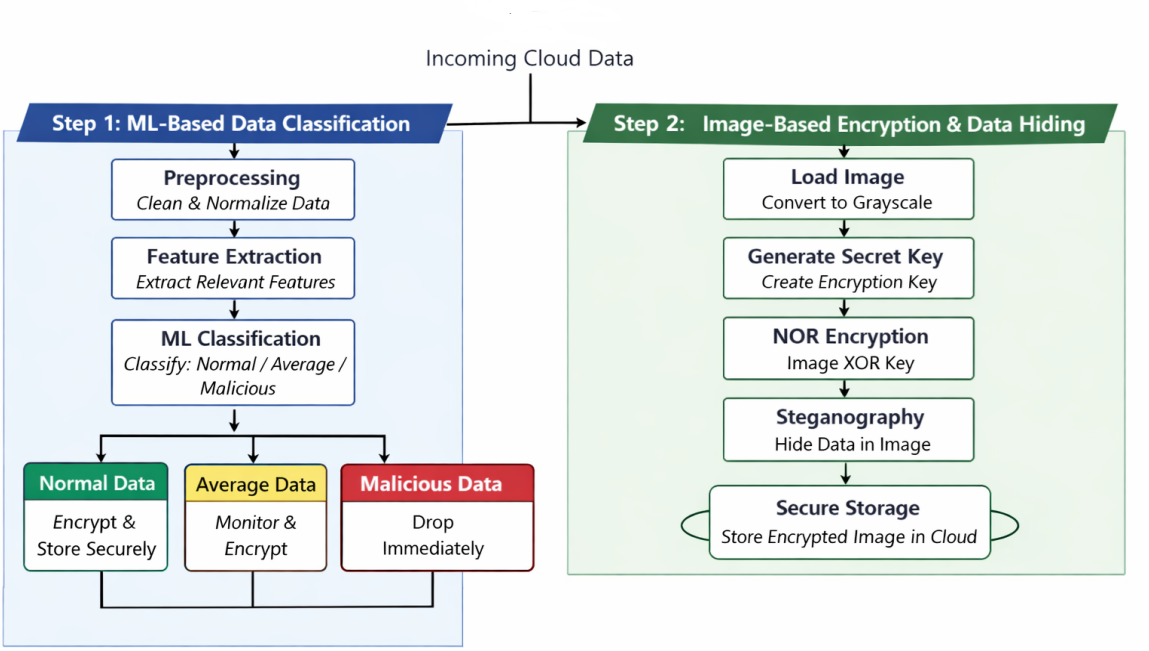
Paper	Focus Area	Techniques Used	Key Contribution / Outcome
P29	ML in cloud security	SVM, ML models	ML improves detection but needs modern datasets
P30	Security strategies	Encryption, IDS, standards	Combined technical and policy solutions
P31	Cybersecurity trends	ML, blockchain, big data	Advanced tools for modern threat detection
P32	Privacy & security	Encryption, access control	Need for multi-layered protection
P33	Security, privacy, trust	Encryption, policy frameworks	Highlights trust and transparency issues

3. Proposed Methodology

Step 1: Machine Learning-Based Data Classification
Incoming cloud data undergoes:
1.Preprocessing: Remove noise, normalize, and clean the data.
2.Feature Extraction: Extract relevant features such as packet size, file behavior, and access patterns.
3.Classification: Use an ML model to classify data as:

- Normal → encrypted and stored securely
- Average → monitored and encrypted
- Malicious → immediately dropped

This ensures early detection of attacks and reduces cloud vulnerabilities.
Step 2: Image-Based Encryption and Data Hiding
1.Load any digital image and convert it to grayscale code.
2.Generate a secret key.
3.Apply NOR operation between the grayscale image code and secret key to produce cipher text.
4.Hide the cipher text in the image using steganography.
5.Store the resulting image in the cloud.



4. Examples

Example 1 – Normal Data

- Input: report.txt
- Gray code: 10110110
- Secret key: 11001010

NOR Operation:
10110110 OR 11001010 = 11111110
NOT(11111110) = 00000001
Cipher text: 00000001 → hidden in image → stored securely.
Example 2 – Malicious Data

- Input: Suspicious packet
- ML Classification: Malicious → Dropped
- Encryption skipped → prevents cloud compromise.

5. Conclusion

The suggested approach introduces a multi-layered cloud security framework that successfully integrates machine learning, cryptography, and steganography to tackle contemporary cloud security issues. By incorporating an initial machine learning-driven classification stage, the system can proactively detect and filter harmful data before it reaches the cloud environment, thereby greatly minimizing the risk of attacks and unauthorized access.
For non-harmful data, the second stage guarantees improved protection through an image-based encryption and data hiding technique. The application of grayscale transformation, secret key creation, and NOR-based encryption, followed by steganography, offers a dual level of security—ensuring that data is not only

encrypted but also hidden within images. This makes it highly resilient to interception, detection, and tampering.
The architecture is effective and practical, as it:

- Blocks malicious data from being processed or stored
- Implements adaptive security based on data sensitivity
- Improves confidentiality through combined encryption and hiding methods.

Overall, the system maintains a strong balance between security, efficiency, and reliability, making it appropriate for secure cloud storage applications. Future enhancements can focus on improving computational efficiency, incorporating advanced deep learning models for better classification accuracy, and reinforcing key management mechanisms to further strengthen robustness.

References

1. Jabbar, A. A., & Bhaya, W. S. (2023). Security of private cloud using machine learning and cryptography. Bulletin of Electrical Engineering and Informatics, 12(1), 561–569. https://doi.org/10.11591/eei.v12i1.4383
2. Mawgoud, A. A., Taha, M. H. N., Abu Talleb, A., & Kotb, A. (2022). Security of private cloud using machine learning and cryptography. Journal of Cloud Computing, 11(97). https://doi.org/10.1186/s13677-022-00339-w
3. Bokhari, N., & Martínez Herráiz, J. J. (2024, April 4). A robust cloud security model leveraging a hybrid of cryptography and steganography. Universidad de Alcalá.
4. Kiran, & Sharma, S. (2017). Enhance data security in cloud computing using machine learning and hybrid cryptography techniques. International Journal of Advanced Research in Computer Science, 8(9), 393–399. https://doi.org/10.26483/ijarcs.v8i9.5042
5. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf
6. Kaur, H., & Kumar, D. (2018). Data migration from private cloud to public cloud using encryption and steganography technique. International Journal of Engineering Sciences & Research Technology, 7(2), 220–226. https://doi.org/10.5281/zenodo.1165928
7. Iqbal, S., Kiah, M. L. M., Dhaghighi, B., Hussain, M., Khan, S., Khan, M. K., & Choo, K. K. R. (2016). On cloud security attacks: A taxonomy and intrusion detection and prevention as a service. Journal of Network and Computer Applications, 74, 98–120. https://doi.org/10.1016/j.jnca.2016.08.016
8. Sanjevi Kumar, A., Rajlingam, A., & Gokila, B. (2023). Study analysis of cloud security challenges and issues in cloud computing technologies. Journal of Science, Computing and Engineering Research, 6(8). https://doi.org/10.46379/jscer.2023.0608002
9. Albalawi, A., & Hamza, N. (2020). A survey on cloud data security using image steganography. International Journal of Advanced Computer Science and Applications, 11(1). https://doi.org/10.14569/IJACSA.2020.0110114
10. Singh, S. K., Manjhi, P. K., & Tiwari, R. K. (2019). Cloud computing security using steganography. Journal of Emerging Technologies and Innovative Research, 6(6), 923–930. Retrieved from https://www.jetir.org
11. Basu, S., Bardhan, A., Gupta, K., Saha, P., Pal, M., Bose, M., Basu, K., Chaudhury, S., & Sarkar, P. (2018). Cloud computing security challenges and solutions—A survey. In Proceedings of the IEEE Conference on Computer Science and Engineering (pp. 1–8). IEEE. https://doi.org/10.1109
12. Khan, I., Reddy, A. Y., Hijab, M., Sridevi, K., Ahmad, S. S., & Shravani, D. (n.d.). Secure and efficient data sharing scheme for multi-user and multi-owner scenario in federated cloud computing. Journal of Theoretical and Applied Information Technology. http://www.jatit.org
13. Kalaiprasath, R., Elankavi, R., & Udayakumar, R. (2017). Cloud security and compliance—A semantic approach in end-to-end security. International Journal on Smart Sensing and Intelligent Systems, Special Issue, 482–489.
14. Chirra, B. R. (2024). Enhancing cloud security through quantum cryptography for robust data transmission. Revista de Inteligencia Artificial en Medicina, 15(1). Retrieved from https://redcrevistas.com/index.php/Revista
15. Cook, A., Robinson, M., Ferrag, M. A., Maglaras, L. A., He, Y., Jones, K., & Janicke, H. (n.d.). Internet of cloud: Security and privacy issues. De Montfort University, School of Computer Science and Informatics, Leicester, U.K.
16. Kumar, L., Mandal, S. K., Srinivasan, S., Singh, O., & Murugan, S. G. (2021). A secure communication with one-time pad encryption and steganography method in cloud. Turkish Journal of Computer and Mathematics Education, 12(10), 5440–5448.
17. Savitha, N., & Sai Kiran, E. (2023). Privacy-preserving techniques for secure cloud computing: A survey of recent advances. International Journal of Scientific Research in Science and Technology, 5(3), 736–745.* https://doi.org/10.32628/IJSRST523103129
18. Akeel Awadg, W., Hashim, A. S., & Hamoud, A. K. (2019). A review of various steganography techniques in cloud computing. University of Thi-Qar Journal of Science, 7(1). Retrieved from http://jsci.utq.edu.iq
19. Rubi, R., Rani, S., Saroha, V. K., & Beniwal, S. (2024). Exploring various data security methods for enhancing security in cloud computing. In Proceedings of the 2024 Second International Conference on Advanced Computing & Communication Technologies (ICACCTech). IEEE.
20. Damenu, T. K., & Balakrishna, C. (2015). Cloud security risk management: A critical review. In 2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies (NGMAST) (pp. 1–6). IEEE.
21. Basu, S., Bardhan, A., Gupta, K., Saha, P., Pal, M., Bose, M., Basu, K., Chaudhury, S., & Sarkar, P. (2018). Cloud computing security challenges and

solutions—A survey. In Proceedings of the IEEE Conference on Computer Science and Engineering. IEEE. https://doi.org/10.1109

22. Haris, R. M., Barhamgi, M., Badawy, A., Nhlabatsi, A., & Khan, K. M. (2025). 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. Expert Systems, 42(e13823). https://doi.org/10.1111/exsy.13823
23. Hammami, H., Brahmi, H., Brahmi, I., & Ben Yahia, S. (2017). Using homomorphic encryption to compute privacy-preserving data mining in a cloud computing environment. In M. Themistocleous & V. Morabito (Eds.), Proceedings of EMCIS 2017 (pp. 397–413). Springer. https://doi.org/10.1007/978-3-319-65930-5_32
24. Sajjan, R. S., Ghorpade, V., & Dalimbkar, V. (2016). A survey paper on data security in cloud computing. International Journal of Computer Sciences and Engineering, 4(Special Issue 4), 1–8. Retrieved from https://www.ijcseonline.org
25. Ibitayo, F. B., Abimbola, O. R., & Oyeladun, M. B. (2022). Securing cloud computing contents with cryptography and steganography. International Journal of Science and Engineering Applications, 11(6), 76–88. https://doi.org/10.7753/IJSEA1106.1002
26. Chandni, C., & Singh, V. (2019). XOR and IP filter-based steganography for secure data transmission in cloud environment. Journal of Emerging Technologies and Innovative Research, 6(6), 41–47. Retrieved from https://www.jetir.org
27. Sari, A. (2015). A review of anomaly detection systems in cloud networks and survey of cloud security measures in cloud storage applications. Journal of Information Security, 6(2), 142–154.* https://doi.org/10.4236/jis.2015.62015
28. Sen, A. K., & Tiwari, P. K. (2017). Security issues and solutions in cloud computing. IOSR Journal of Computer Engineering, 19(2), 67–72.* https://doi.org/10.9790/0661-1902046772
29. Bou Nassif, A., Abu Talib, M., Nasir, Q., Albadani, H., & Dakalbab, F. M. (2021). Machine learning for cloud security: A systematic review. IEEE Access, 9, 29506–29542.* https://doi.org/10.1109/ACCESS.2021.3054129
30. Chauhan, M., & Shiaeles, S. (2023). An analysis of cloud security frameworks, problems and proposed solutions. Network, 3(3), 422–450.* https://doi.org/10.3390/network3030018
31. Jimmy, F. (2024). Cybersecurity vulnerabilities and remediation through cloud security tools. Journal of Artificial Intelligence General Science, 2(1).
32. Darwish, M. A., Yafi, E., Almasri, A. H., & Zuhairi, M. F. (n.d.). Privacy and security of cloud computing: A comprehensive review of techniques and challenges. International Journal of Engineering and Technology.
33. Verma, J. K., & Katti, C. P. (n.d.). View on security, privacy and trust issues in cloud computing environment. International Journal of Latest Trends in Engineering and Technology. Jawaharlal Nehru University, New Delhi, India.