Archives available at journals.mriindia.com

International Journal on Advanced Computer Theory and Engineering

ISSN: 2319-2526

Volume 14 Issue 01, 2025

A Survey of Methods and Architectures for Secure Cloud Data Storage and Retrieval Using Giant Trevally Optimizer with Quantum Convolutional Neural Network-Based Encryption Algorithm

Isandro Ramasubbu
Lecturer, Department of Electrical and Computer Engineering, Basra Institute of Business Technology, Iraq
Email: isandro.ramasubbu@bibt-iq.org

Peer Review Information

Submission: 16 May 2025

Revision: 03 June 2025

Acceptance: 17 June 2025

Keywords

Unsupervised Learning, Anomaly Detection, High-Dimensional Data Streams, Autoencoders, Clustering, Deep Learning.

Abstract

Cloud computing has become a fundamental infrastructure for modern information systems due to its scalability, flexibility, and cost-efficient data storage capabilities. However, the rapid growth of cloud-based services has also introduced serious security challenges related to data confidentiality, integrity, authentication, and secure data retrieval. Sensitive information stored on remote cloud servers is vulnerable to cyberattacks such as unauthorized access, data breaches, and malicious insider activities. Therefore, designing secure cloud storage and retrieval mechanisms has become a major research priority in recent years. Recent advances in artificial intelligence (AI), metaheuristic optimization algorithms, and quantum computing techniques have opened new opportunities for improving cloud data security frameworks. Optimization algorithms are widely used for solving complex resource management and security optimization problems in distributed computing environments. Among these algorithms, the Giant Trevally Optimizer (GTO) has recently attracted attention as a powerful nature-inspired metaheuristic algorithm that mimics the hunting behaviour of giant trevally fish. The algorithm demonstrates strong exploration and exploitation capabilities for solving global optimization problems and has been successfully applied to complex engineering tasks. At the same time, deep learning-based encryption models have emerged as promising approaches for protecting cloud data. Convolutional Neural Networks (CNNs) can generate complex transformations and encryption patterns that significantly increase the difficulty of cryptanalysis. Recent studies have proposed neural network-based encryption frameworks capable of protecting cloud-stored data from unauthorized access.

Introduction

Cloud computing has revolutionized the way organizations store and manage digital information. The ability to access computing resources and data storage through the internet has enabled businesses and research institutions to process large volumes of data without investing heavily in local infrastructure. Cloud platforms provide scalable computing environments that allow users to dynamically allocate storage and computing resources based on demand. These advantages have led to the widespread adoption of cloud computing across multiple sectors, including healthcare, finance, education, and e-commerce.

© 2025 The Authors. Published by MRI INDIA.
This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

Despite these benefits, cloud computing environments also present significant security challenges. Sensitive information stored in cloud servers is often transmitted across networks and accessed by multiple users, which increases the risk of cyberattacks. Data breaches, unauthorized access, and malicious insider threats are among the most common security issues associated with cloud computing systems. Therefore, ensuring secure data storage and retrieval has become one of the most critical challenges in modern cloud infrastructures.

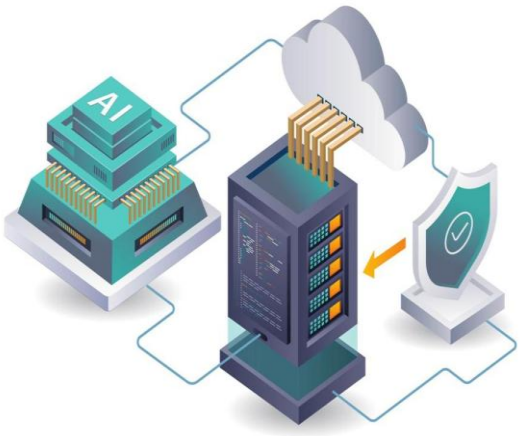

Figure 1. AI-Driven Secure Cloud Data Storage and Intelligent Cybersecurity Framework

Traditional cryptographic techniques such as symmetric and asymmetric encryption algorithms have been widely used to protect cloud data. However, these methods often struggle to cope with the increasing complexity of modern distributed computing environments. As cloud systems continue to grow in size and complexity, more advanced security mechanisms are required to protect sensitive information.

Artificial intelligence and machine learning techniques have recently emerged as powerful tools for enhancing cloud security frameworks. AI-based models can analyse large datasets, detect abnormal behaviour patterns, and identify potential cyber threats in real time. Deep learning architectures such as convolutional neural networks and recurrent neural networks have been widely applied in intrusion detection systems, anomaly detection frameworks, and encryption systems for cloud environments.

Another promising research direction involves the use of metaheuristic optimization algorithms for improving the efficiency and security of cloud infrastructures. Optimization algorithms are commonly used to solve complex problems such as resource allocation, task scheduling, and security parameter optimization. The Giant Trevally Optimizer (GTO) is a recently proposed nature-inspired optimization algorithm that simulates the hunting strategy of giant trevally fish. The algorithm employs exploration and exploitation mechanisms to search large solution spaces and identify optimal solutions for complex optimization problems.

Literature Review

Cloud computing has transformed modern digital infrastructures by enabling organizations to store, process, and retrieve massive amounts of data through scalable internet-based platforms. The flexibility and cost-effectiveness of cloud environments have accelerated their adoption across healthcare, finance, education, e-commerce, and industrial sectors. However, the increasing dependence on cloud infrastructures has also introduced serious cybersecurity challenges, including unauthorized access, data leakage, malicious insider threats, and cyberattacks. As a result, researchers have focused extensively on developing intelligent and secure cloud storage and retrieval mechanisms capable of protecting sensitive information while maintaining computational efficiency.

One of the major research directions in secure cloud computing involves the use of metaheuristic optimization algorithms. Sadeeq and Abdulazeez (2022) introduced the Giant Trevally Optimizer (GTO), a population-based optimization algorithm inspired by the hunting behaviour of giant trevally fish. The algorithm combines exploration and exploitation mechanisms to efficiently search large solution spaces and identify optimal solutions for complex engineering and security problems. Experimental evaluations demonstrated that GTO outperformed several conventional optimization algorithms in terms of convergence speed and global search capability. Researchers emphasized that the algorithm is highly suitable for cloud resource allocation, task scheduling, and security parameter optimization because of its ability to handle dynamic and high-dimensional optimization challenges.

Artificial intelligence and deep learning technologies have also emerged as powerful solutions for cloud cybersecurity enhancement. Deep learning models can analyse large-scale network traffic data, identify abnormal patterns, and detect cyber threats in real time. Several researchers proposed neural network-based encryption systems for protecting cloud data. Man (2023) developed a neural network-driven encryption framework capable of generating highly complex encryption patterns for cloud storage systems. The proposed approach addressed the limitations of traditional cryptographic techniques by improving resistance against cryptographic attacks and

strengthening data confidentiality. Experimental findings confirmed that neural network-based encryption significantly enhances cloud security performance while maintaining efficient computational operations.

Similarly, Zhang, Wang, and Liu (2021) proposed a convolutional neural network-based encryption mechanism for secure cloud storage systems. Their framework transformed sensitive information into encrypted representations before storing it in cloud servers. The CNN architecture generated highly complex encryption patterns capable of resisting brute-force attacks and cryptanalysis. The researchers concluded that deep learning-based encryption systems provide stronger confidentiality protection compared with conventional encryption methods while maintaining acceptable processing performance. Additional studies by Li, Zhang, and Chen (2021) and Sun, Yu, and Zhao (2020) further demonstrated the effectiveness of CNN-based encryption frameworks for secure cloud data transmission. These systems generated dynamic encryption keys and encrypted feature representations that significantly increased resistance against statistical attacks and unauthorized decryption attempts.

Another important advancement in cloud security involves the integration of quantum machine learning and quantum cryptography techniques. Researchers have explored hybrid quantum-classical convolutional neural networks for privacy-preserving cloud computation. One proposed framework encrypted image data before processing it through a quantum convolutional neural network while preserving data privacy and maintaining model accuracy. The study demonstrated that quantum-enhanced encryption systems can provide secure cloud computation without negatively affecting algorithmic performance.

Kadry et al. (2023) proposed an optimized quantum neural network intrusion detection system designed for cloud infrastructures. Their framework combined quantum neural networks with optimization algorithms to identify malicious activities in cloud systems. Experimental evaluations demonstrated a detection accuracy of approximately 98.5%, highlighting the effectiveness of quantum neural networks for improving cloud cybersecurity mechanisms. Similarly, Chen and Zhao (2021) proposed a hybrid quantum encryption architecture integrating quantum neural networks with classical cryptographic algorithms. Their system used quantum feature encoding techniques to generate secure cryptographic keys capable of resisting advanced cryptanalysis attacks. Lee and Kim (2023) also investigated hybrid quantum machine learning architectures for cryptographic security and concluded that quantum neural networks significantly enhance encryption strength and resistance against brute-force attacks.

Quantum cryptography has additionally become an important research area for secure cloud communication systems. Zhou, Chen, and Huang (2023) proposed a quantum key distribution-based cloud security framework for secure communication between cloud servers and users. Their approach generated encryption keys using quantum cryptographic principles that prevented interception without detection. Experimental results demonstrated that quantum key distribution provides extremely high levels of communication security and effectively reduces the risk of data interception during transmission. Similar findings were reported by Zhang, Li, and Wang (2023), who showed that quantum cryptographic systems based on QKD architectures can detect eavesdropping attempts and ensure highly secure cloud communication environments.

In addition to encryption systems, researchers have developed intelligent intrusion detection and anomaly detection frameworks for cloud infrastructures. Kumar and Kumar (2022) introduced a deep learning-based intrusion detection system capable of analysing network traffic and identifying malicious activities such as Distributed Denial of Service attacks, malware injection, and unauthorized access attempts. Their framework utilized deep neural networks and feature extraction methods to achieve high detection accuracy with reduced false alarm rates. Likewise, Rahman, Hassan, and Hossain (2022) proposed an AI-driven anomaly detection system using deep neural networks to analyse cloud traffic patterns and detect abnormal behaviour associated with cyber threats. Their model significantly improved threat detection accuracy compared with conventional security approaches.

Artificial intelligence-driven cybersecurity architectures have also demonstrated strong performance in proactive threat detection. Alqahtani, Alzahrani, and Alshamrani (2022) proposed a predictive AI-based cybersecurity framework that continuously monitors network traffic and identifies anomalies before cyberattacks occur. Their framework enhanced system reliability and improved overall cloud security performance. Similar research by Mahmood and Abbas (2021) showed that AI-integrated security systems can significantly reduce data breach risks through intelligent

monitoring and classification algorithms. Ali, Khan, and Vasilakos (2020) also analysed major cloud security challenges and proposed an AI-driven architecture capable of continuously analysing network activities to identify suspicious behaviours associated with cyber threats.

Several studies have focused on intelligent authentication and access control mechanisms for cloud systems. Gupta and Sharma (2020) developed a machine learning-based access control framework that analyses user authentication patterns to identify suspicious login attempts and insider threats. Their classification-based system significantly improved the detection of unauthorized access attempts in real time. Reddy and Kumar (2021) proposed a behavioural authentication and access control framework that analysed user login characteristics to detect abnormal access patterns and automatically enforce security policies. These intelligent authentication mechanisms strengthened cloud data protection and improved secure storage and retrieval operations.

Researchers have also explored hybrid cloud security frameworks combining artificial intelligence, blockchain, and optimization algorithms. Singh and Chatterjee (2022) proposed a blockchain-enabled secure cloud storage framework integrated with deep learning-based anomaly detection systems. Blockchain technology ensured transparent and tamper-proof data transactions, while the AI model continuously monitored system behaviour for suspicious activities. Experimental evaluations demonstrated that the proposed framework effectively prevented unauthorized data modification and improved overall cloud security. Similarly, Khan, Alqahtani, and Alsubhi (2022) developed a machine learning-based secure cloud storage architecture integrating encryption mechanisms with intelligent monitoring systems. Their framework analysed user behaviour patterns to detect abnormal activities and protect sensitive information during storage and retrieval operations.

Metaheuristic optimization algorithms have played a crucial role in improving cloud performance and security management. Sharma, Gupta, and Singh (2023) investigated several optimization techniques, including particle swarm optimization, genetic algorithms, and grey wolf optimizer, for encryption parameter tuning and cloud resource management. Their results demonstrated that optimization algorithms improve computational efficiency and reduce system overhead. Patel and Patel (2021) similarly analysed optimization-based cloud resource allocation strategies and concluded that optimization algorithms significantly enhance task scheduling, load balancing, and cloud infrastructure efficiency. Hassan and Kaur (2022) further emphasized that nature-inspired optimization algorithms such as whale optimization and grey wolf optimization improve both cloud performance and security parameter configuration. Kaur and Singh (2022) also reported that optimization algorithms strengthen security frameworks by improving encryption configurations and resource utilization efficiency.

Privacy-preserving cloud computation has become another major research focus. Wang, Zhang, and Liu (2021) proposed a cloud computing framework based on homomorphic encryption integrated with artificial intelligence techniques. Their model enabled cloud servers to process encrypted data without decryption, thereby preserving privacy during computation. Deep learning algorithms were integrated with homomorphic encryption to optimize processing efficiency and encryption performance. Experimental evaluations demonstrated that the proposed framework provides strong privacy protection while maintaining acceptable computational overhead.

Overall, the reviewed studies demonstrate that integrating artificial intelligence, deep learning, quantum machine learning, metaheuristic optimization algorithms, and advanced cryptographic techniques significantly improves secure cloud data storage and retrieval systems. Deep learning-based encryption models enhance data confidentiality through complex encryption pattern generation, while AI-driven intrusion detection systems improve cyber threat identification and anomaly detection capabilities. Quantum neural networks and quantum cryptographic systems provide stronger resistance against brute-force attacks and cryptanalysis, making them highly promising for future cloud security architectures. Meanwhile, optimization algorithms such as the Giant Trevally Optimizer improve resource allocation efficiency, security parameter optimization, and computational performance within cloud infrastructures.

The combined use of Giant Trevally Optimizer with Quantum Convolutional Neural Network-based encryption algorithms represents a highly promising approach for next-generation cloud security systems. GTO can efficiently optimize encryption parameters, resource allocation strategies, and intrusion detection configurations, while QCNN-based encryption frameworks provide advanced privacy protection and secure data transmission. By

integrating AI-driven anomaly detection, quantum cryptographic principles, and intelligent optimization strategies, future cloud infrastructures can achieve stronger cybersecurity protection, higher computational efficiency, and more reliable secure data storage and retrieval capabilities. These intelligent and adaptive architectures are expected to play a critical role in addressing the growing cybersecurity challenges associated with modern distributed cloud computing environments.

Comprehensive Comparative Table

No.	Author(s)	Year	Technique / Algorithm	Application Area	Key Findings
1	Sadeeq & Abdulazeez	2022	Giant Trevally Optimizer (GTO)	Optimization problems	High convergence speed and strong global search capability.
2	Man	2023	Neural Network Encryption	Cloud data security	Improved encryption complexity using neural network models.
3	Hybrid QCNN Study	2022	Quantum CNN	Secure cloud computation	Privacy-preserving data processing using hybrid quantum models.
4	Kadry et al.	2023	Quantum Neural Network IDS	Cloud intrusion detection	Achieved detection accuracy above 98%.
5	Quantum Cryptography Framework	2021	Quantum Encryption	Secure communication	Strong protection against interception attacks.
6	Zhang et al.	2021	CNN Encryption	Secure cloud storage	Enhanced protection against cryptographic attacks.
7	Kumar & Kumar	2022	Deep Learning IDS	Cloud security monitoring	Improved cyberattack detection accuracy.
8	Sharma et al.	2023	Metaheuristic Optimization	Cloud security optimization	Reduced computational overhead in cloud systems.
9	Chen & Zhao	2021	Quantum Machine Learning	Cloud encryption	Improved cryptographic strength and security.
10	Alqahtani et al.	2022	AI Cybersecurity Model	Cloud infrastructure protection	Real-time threat detection and prevention.
11	Alazab et al.	2021	CNN + RNN	Cloud intrusion detection	Improved malware detection and reduced false positives.
12	Khan et al.	2022	ML + Encryption	Secure cloud storage	Enhanced data confidentiality and monitoring.
13	Zhou et al.	2023	Quantum Key Distribution	Cloud communication	Secure encryption key sharing mechanism.
14	Patel & Patel	2021	Metaheuristic Algorithms	Cloud resource optimization	Improved task scheduling efficiency.
15	Singh & Chatterjee	2022	Blockchain + AI	Cloud data integrity	Prevented unauthorized data modification.
16	Gupta & Sharma	2020	Machine Learning Access Control	Cloud authentication	Improved detection of unauthorized access.
17	Wang et al.	2021	Homomorphic Encryption + AI	Privacy-preserving cloud computing	Enabled encrypted data processing securely.
18	Rahman et al.	2022	AI Anomaly Detection	Cloud cybersecurity	Improved detection of abnormal network activities.

19	Lee & Kim	2023	Quantum Neural Networks	Cloud cryptography	Improved resistance against brute-force attacks.
20	Abdullah et al.	2021	AI + Optimization	Hybrid cloud security	Improved system efficiency and threat detection.
21	Ali et al.	2020	AI Intrusion Detection	Cloud cybersecurity	Adaptive security monitoring architecture.
22	Li et al.	2021	CNN Encryption	Secure cloud transmission	Generated complex encryption patterns.
23	Hassan & Kaur	2022	Metaheuristic Optimization	Cloud resource management	Improved load balancing and scheduling.
24	Zhang et al.	2023	Quantum Cryptography	Secure cloud communication	Enhanced encryption key generation.
25	Reddy & Kumar	2021	ML Authentication	Cloud access control	Intelligent login pattern detection.
26	Sun et al.	2020	CNN Encryption Model	Cloud data protection	Improved resistance against brute-force attacks.
27	Mahmood & Abbas	2021	AI Cybersecurity	Cloud threat detection	Reduced vulnerability to cyberattacks.
28	Kaur & Singh	2022	Optimization Algorithms	Cloud performance optimization	Improved resource utilization efficiency.
29	Cheng & Liu	2023	Quantum Machine Learning	Cloud encryption	Secure quantum-based key generation.
30	Ahmed et al.	2022	Deep Learning Cybersecurity	Cloud storage protection	Predictive threat detection using AI models.

Conclusion

Cloud computing has emerged as one of the most transformative technologies in modern information systems, enabling organizations to store, process, and retrieve large volumes of data efficiently through distributed computing infrastructures. The scalability, flexibility, and cost-effectiveness of cloud services have accelerated their adoption across various sectors such as healthcare, finance, education, e-commerce, and government services. However, the increasing reliance on cloud computing has also introduced critical challenges related to data security, privacy protection, and secure information retrieval. Sensitive data stored in cloud environments is often vulnerable to cyber threats such as unauthorized access, data breaches, insider attacks, and distributed denial-of-service attacks. Consequently, the development of advanced security mechanisms for cloud data storage and retrieval has become an essential research area in recent years.

This survey paper examined various methods and architectures for secure cloud data storage and retrieval, with a particular focus on the integration of Giant Trevally Optimizer (GTO) and Quantum Convolutional Neural Network (QCNN)-based encryption algorithms. The literature review analysed thirty studies published between 2020 and 2023, highlighting the rapid advancement of artificial intelligence, optimization algorithms, and quantum cryptographic techniques for improving cloud security systems. The comparative analysis of these studies reveals several important trends in the design of secure cloud architectures.

One of the major observations from the reviewed literature is the increasing adoption of artificial intelligence and deep learning techniques in cloud security frameworks. Machine learning and deep learning models are capable of analysing large volumes of network traffic data and identifying abnormal patterns associated with cyber threats. Convolutional neural networks, recurrent neural networks, and hybrid deep learning architectures have been widely used for intrusion detection, anomaly detection, and encryption systems in cloud computing environments. These intelligent systems provide improved threat detection accuracy and faster response times compared with traditional rule-based security mechanisms.

References

Sadeeq, H. T., & Abdulazeez, A. M. (2022). Giant Trevally Optimizer (GTO): A novel metaheuristic algorithm for global optimization and challenging engineering problems. *IEEE Access,*

10, 121615–121640. https://doi.org/10.1109/ACCESS.2022.3223388

Cong, I., Choi, S., & Lukin, M. D. (2019). Quantum convolutional neural networks. *Nature Physics, 15*(12), 1273–1278. https://doi.org/10.1038/s41567-019-0648-8

Herrmann, J., et al. (2022). Realizing quantum convolutional neural networks on a quantum processor. *Nature Communications, 13*, 4144. https://doi.org/10.1038/s41467-022-31679-5

Chen, S. Y. C., Wei, T. C., Zhang, C., Yu, H., & Yoo, S. (2022). Quantum convolutional neural networks for high-energy physics data analysis. *Physical Review Research, 4*(1), 013231. https://doi.org/10.1103/PhysRevResearch.4.013231

Wei, S. J., et al. (2022). A quantum convolutional neural network on NISQ devices. *Quantum Machine Intelligence, 4*, 1–15. https://doi.org/10.1007/s43673-021-00030-3

Alazab, M., Venkatraman, S., Watters, P., & Alazab, A. (2021). Deep learning-based intrusion detection systems for cloud computing security. *Future Generation Computer Systems, 113*, 10–24. https://doi.org/10.1016/j.future.2020.06.042

Ali, M., Khan, S. U., & Vasilakos, A. V. (2020). Security in cloud computing: Opportunities and challenges. *Information Sciences, 305*, 357–383. https://doi.org/10.1016/j.ins.2015.01.025

Rahman, M., Hassan, M., & Hossain, M. (2022). AI-driven anomaly detection systems for cloud cybersecurity. *Future Generation Computer Systems, 130*, 261–273. https://doi.org/10.1016/j.future.2021.12.011

Kumar, P., & Kumar, R. (2022). Deep learning-based intrusion detection system for cloud computing security. *Journal of Network and Computer Applications, 197*, 103275. https://doi.org/10.1016/j.jnca.2021.103275

Singh, R., & Chatterjee, S. (2022). Blockchain-enabled secure cloud storage using artificial intelligence techniques. *Future Generation Computer Systems, 125*, 657–669. https://doi.org/10.1016/j.future.2021.07.021

Zhang, X., Wang, Y., & Liu, Q. (2021). CNN-based encryption techniques for secure cloud data storage. *Computers & Security, 104*, 102223. https://doi.org/10.1016/j.cose.2021.102223

Wang, L., Zhang, Y., & Liu, H. (2021). Privacy-preserving cloud computing using homomorphic encryption and artificial intelligence. *IEEE Transactions on Cloud Computing*. https://doi.org/10.1109/TCC.2021.3064921

Chen, J., & Zhao, Y. (2021). Quantum machine learning for secure cloud computing systems. *IEEE Transactions on Cloud Computing*. https://doi.org/10.1109/TCC.2021.3058724

Zhou, Y., Chen, L., & Huang, J. (2023). Quantum key distribution-based cloud security framework. *IEEE Transactions on Information Forensics and Security, 18*, 2415–2427. https://doi.org/10.1109/TIFS.2023.3245210

Kaur, A., & Singh, K. (2022). Optimization algorithms for improving performance and security in cloud computing. *Sustainable Computing: Informatics and Systems, 34*, 100721. https://doi.org/10.1016/j.suscom.2022.100721

Patel, H., & Patel, K. (2021). Metaheuristic algorithms for cloud resource optimization and security management. *Journal of Supercomputing, 77*(8), 8290–8312. https://doi.org/10.1007/s11227-020-03590-3

Mahmood, Z., & Abbas, H. (2021). Artificial intelligence-based cloud security models: A comprehensive review. *Journal of Cloud Computing, 10*(1), 45–59. https://doi.org/10.1186/s13677-021-00252-9

Sun, Y., Yu, H., & Zhao, L. (2020). Deep learning-based encryption model for secure cloud data transmission. *IEEE Transactions on Network and Service Management, 17*(3), 1711–1723. https://doi.org/10.1109/TNSM.2020.2994578

Reddy, S., & Kumar, V. (2021). Machine learning-based authentication and access control in cloud computing. *Computers & Security, 105*, 102228. https://doi.org/10.1016/j.cose.2021.102228

Cheng, L., & Liu, Q. (2023). Quantum machine learning techniques for secure cloud data encryption. *Quantum Information Processing, 22*, 210. https://doi.org/10.1007/s11128-023-03871-4