Archives available at journals.mriindia.com

ITSI Transactions on Electrical and Electronics Engineering

ISSN: 2320-8945

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

Taneesha Varathan

Assistant Professor, Department of Computer Science and Engineering, Lagoon Polytechnic of Technology, Maldives

Email: taneesha.varathan@lpt-mv.net

Peer Review Information

Submission: 02 April 2025

Revision: 23 April 2025

Acceptance: 11 May 2025

Keywords

Cloud Computing Security, Giant Trevally Optimizer, Quantum Convolutional Neural Network, Cloud Data Encryption, Artificial Intelligence Security, Secure Data Retrieval.

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.

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.

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

Sadeeq and Abdulazeez (2022) introduced the Giant Trevally Optimizer (GTO), a novel population-based metaheuristic optimization algorithm inspired by the hunting behaviour of giant trevally fish. The algorithm uses exploration and exploitation strategies to efficiently search large solution spaces and identify optimal solutions for complex optimization problems. Experimental evaluations demonstrated that GTO outperforms several well-known optimization algorithms in solving benchmark engineering problems. The researchers highlighted the algorithm's strong convergence speed and global search capability, making it suitable for complex optimization tasks such as cloud resource allocation and security parameter optimization.

Man (2023) proposed a neural network-based encryption framework for cloud data security. The study addressed several vulnerabilities associated with traditional cloud encryption methods and introduced a neural network-driven image encryption scheme capable of generating highly complex encryption patterns. The results showed that neural network-based encryption significantly improves resistance to cryptographic attacks and enhances cloud data confidentiality.

Research on hybrid quantum-classical convolutional neural networks has shown promising results for secure cloud computation. One study proposed an encryption framework where image data is encrypted before being processed by a quantum convolutional neural network. The encrypted data can still be processed by the neural network while maintaining privacy protection. Experimental results demonstrated that the proposed system protects input data without affecting algorithm accuracy.

Kadry et al. (2023) proposed an optimized quantum neural network intrusion detection system for cloud security. The system integrates quantum neural networks with optimization algorithms to detect malicious activities in cloud infrastructures. Experimental results showed that the proposed system achieved detection accuracy of up to 98.5%, demonstrating the effectiveness of quantum neural networks for improving cloud cybersecurity systems.

Zhang, Wang, and Liu (2021) proposed a deep learning-based encryption mechanism for secure cloud storage systems. The authors developed a convolutional neural network (CNN) model capable of generating complex encryption patterns for protecting sensitive cloud data. The CNN architecture was used to transform input data into encrypted representations before storing it in cloud servers. Experimental results showed that the proposed system significantly improved resistance against brute-force and cryptographic attacks compared with traditional encryption techniques. The study concluded that deep learning-based encryption frameworks can enhance data confidentiality while maintaining acceptable computational performance in cloud computing environments.

Kumar and Kumar (2022) introduced a deep learning-based intrusion detection system for cloud computing infrastructures. Their framework employed deep neural networks to analyse network traffic and detect malicious activities in real time. The system utilized feature extraction and classification techniques to identify cyber threats such as Distributed Denial of Service (DDoS) attacks, malware injection, and unauthorized access attempts. Experimental evaluations demonstrated that the proposed system achieved high detection accuracy and reduced false alarm rates compared with traditional rule-based intrusion detection systems. The researchers emphasized the importance of artificial intelligence in improving cloud security architectures.

Sharma, Gupta, and Singh (2023) investigated the use of nature-inspired optimization algorithms for enhancing cloud computing security. Their research evaluated several metaheuristic optimization techniques, including particle swarm optimization, genetic algorithms, and grey wolf optimizer, for optimizing encryption parameters and improving system performance. The results indicated that optimization algorithms can significantly improve resource allocation efficiency and reduce computational overhead in cloud infrastructures. The study highlighted the potential of metaheuristic algorithms for designing secure and efficient cloud security frameworks.

Chen and Zhao (2021) explored the application of quantum machine learning for cloud data encryption systems. The researchers proposed a hybrid encryption architecture that integrates quantum neural networks with classical cryptographic algorithms to improve cloud data security. The system utilized quantum feature encoding techniques to generate secure cryptographic keys and protect sensitive information during transmission. Experimental results demonstrated that the proposed quantum-based encryption framework provides stronger protection against cryptanalysis compared with classical encryption methods.

Alqahtani, Alzahrani, and Alshamrani (2022) proposed an artificial intelligence-driven cybersecurity framework for cloud computing environments. The system utilized machine learning algorithms to continuously monitor network traffic and identify anomalies that may indicate cyberattacks. The framework incorporated predictive security mechanisms capable of detecting potential threats before they cause damage to cloud infrastructures. Experimental results showed that the AI-based security system significantly improves threat detection rates and enhances overall system reliability.

Alazab, Venkatraman, and Watters (2021) investigated the use of deep learning techniques for improving cloud cybersecurity systems. The authors proposed a hybrid intrusion detection system combining convolutional neural networks and recurrent neural networks to analyse cloud network traffic and detect malicious activities. The system was trained using large cybersecurity datasets and demonstrated strong performance in detecting cyber threats such as malware, phishing attacks, and unauthorized access attempts. Experimental results showed that the proposed model achieved high detection accuracy and reduced false positives compared with traditional signature-based security mechanisms. The study emphasized that deep learning models can significantly enhance the effectiveness of cloud security frameworks.

Khan, Alqahtani, and Alsubhi (2022) developed a machine learning-based secure cloud storage framework that integrates cryptographic techniques with intelligent monitoring systems. The proposed architecture uses machine learning algorithms to analyse data access patterns and detect abnormal user behaviour within cloud infrastructures. The system also applies encryption mechanisms to protect sensitive data during storage and retrieval processes. Experimental results demonstrated that combining machine learning with encryption techniques improves cloud data confidentiality and reduces the risk of unauthorized access.

Zhou, Chen, and Huang (2023) proposed a quantum key distribution-based cloud security architecture designed to improve secure communication between cloud servers and users. Their framework uses quantum cryptographic principles to generate encryption keys that cannot be intercepted without detection. The study demonstrated that quantum key distribution provides extremely high security levels for cloud communication systems and significantly reduces the risk of data interception during transmission. The researchers concluded that quantum cryptography will play a major role in the development of next-generation cloud security infrastructures.

Patel and Patel (2021) analysed the effectiveness of metaheuristic optimization algorithms for cloud resource allocation and security management. Their study evaluated several optimization techniques, including genetic algorithms, particle swarm optimization, and ant colony optimization, for improving task

scheduling and resource management in cloud environments. The results showed that optimization algorithms significantly improve system performance and reduce computational overhead. The authors emphasized that optimization-based strategies are essential for maintaining efficient and secure cloud infrastructures.

Singh and Chatterjee (2022) proposed a blockchain-enabled secure cloud storage framework integrated with artificial intelligence techniques. The system combines blockchain technology with deep learning-based anomaly detection models to enhance data integrity and transparency in cloud environments. Blockchain ensures that all data transactions are securely recorded, while the AI model continuously monitors system behaviour for suspicious activities. Experimental evaluations demonstrated that the proposed framework effectively prevents unauthorized data modification and improves overall cloud security.

Gupta and Sharma (2020) investigated the application of machine learning techniques for improving access control mechanisms in cloud computing environments. The researchers developed a cloud security framework that utilizes supervised learning algorithms to analyse user authentication patterns and detect suspicious access attempts. The proposed model employed classification algorithms to identify abnormal login behaviour and potential insider threats. Experimental results showed that the machine learning-based access control system significantly improved the security of cloud infrastructures by detecting unauthorized access attempts in real time. The study concluded that intelligent monitoring systems can play an important role in enhancing secure cloud data storage and retrieval mechanisms.

Wang, Zhang, and Liu (2021) proposed a privacy-preserving cloud computing model based on homomorphic encryption and artificial intelligence techniques. The system allows cloud servers to process encrypted data without decrypting it, thereby maintaining data privacy during computation. The authors integrated deep learning algorithms with homomorphic encryption to optimize data processing performance and improve encryption efficiency. Experimental results demonstrated that the proposed system provides strong privacy protection while maintaining acceptable computational overhead. The study highlighted the importance of privacy-preserving technologies in secure cloud computing architectures.

Rahman, Hassan, and Hossain (2022) introduced an AI-driven anomaly detection framework for cloud cybersecurity. The proposed model uses deep neural networks to analyse network traffic patterns and identify abnormal behaviour associated with cyber threats. The system applies feature extraction techniques and pattern recognition algorithms to detect malicious activities such as data breaches, malware injection, and distributed denial-of-service attacks. Experimental evaluations showed that the AI-based anomaly detection system significantly improves threat detection accuracy compared with traditional security systems.

Lee and Kim (2023) explored the application of quantum neural networks for improving cryptographic security in cloud computing systems. Their research proposed a hybrid encryption architecture combining classical cryptographic algorithms with quantum machine learning models. The quantum neural network generates complex encryption keys using quantum feature encoding techniques, which enhances resistance against brute-force attacks and cryptanalysis. The study concluded that quantum machine learning techniques can significantly improve encryption strength and will play an important role in future cloud security architectures.

Abdullah, Alqahtani, and Alshahrani (2021) proposed a hybrid cloud security framework integrating artificial intelligence and metaheuristic optimization algorithms. The framework uses optimization algorithms to tune the parameters of machine learning models for improved threat detection performance. The proposed system continuously monitors cloud network traffic and identifies suspicious activities using intelligent classification algorithms. Experimental results showed that the hybrid approach significantly improves detection accuracy while maintaining efficient resource utilization in cloud infrastructures.

Ali, Khan, and Vasilakos (2020) examined security challenges and intelligent solutions for cloud computing infrastructures. Their study analysed various cybersecurity threats in cloud environments, including data leakage, unauthorized access, and malicious insider attacks. The researchers proposed an artificial intelligence-based cloud security architecture that utilizes machine learning algorithms to monitor network activities and detect abnormal behaviour patterns. The proposed system continuously analyses cloud network traffic and automatically identifies suspicious activities associated with cyber threats. Experimental results indicated that AI-driven security frameworks significantly enhance the ability to

detect and mitigate cyberattacks in cloud computing systems.

Li, Zhang, and Chen (2021) proposed a convolutional neural network-based encryption framework for secure cloud data transmission. The model transforms sensitive data into encrypted feature representations using CNN-based encoding techniques before transmitting the data to cloud servers. The proposed approach increases the complexity of encryption keys and makes it extremely difficult for attackers to perform cryptanalysis. Experimental evaluations demonstrated that the CNN-based encryption system provides higher security levels compared with traditional cryptographic techniques while maintaining efficient data transmission performance.

Hassan and Kaur (2022) conducted a comprehensive study on metaheuristic optimization algorithms for cloud resource management and security optimization. The authors analysed several nature-inspired optimization algorithms such as particle swarm optimization, grey wolf optimizer, and whale optimization algorithm. The study concluded that optimization algorithms can significantly improve cloud performance by optimizing resource allocation, load balancing, and task scheduling processes. Furthermore, optimization techniques can also be applied to improve encryption parameters and enhance cloud security mechanisms.

Zhang, Li, and Wang (2023) investigated the use of quantum cryptography for secure cloud communication systems. Their research proposed a cloud communication framework based on quantum key distribution (QKD) for generating highly secure encryption keys. The system uses quantum cryptographic principles to detect eavesdropping attempts during data transmission. Experimental results demonstrated that QKD-based encryption systems provide extremely high security levels and can effectively protect sensitive cloud data from interception attacks.

Reddy and Kumar (2021) developed a machine learning-based authentication and access control framework for secure cloud data management. The proposed system analyses user login patterns and behavioural characteristics to detect suspicious authentication attempts. The framework implements classification algorithms to identify abnormal access patterns and automatically enforce security policies. Experimental results showed that the proposed model improves cloud data protection by preventing unauthorized access and strengthening authentication mechanisms.

Sun, Yu, and Zhao (2020) investigated the application of deep learning-based encryption techniques for secure cloud data transmission. The researchers proposed a convolutional neural network-based encryption model that transforms plaintext data into highly complex encrypted representations before storage or transmission. The CNN architecture generates dynamic encryption patterns that significantly increase the complexity of the encryption keys. Experimental results demonstrated that the proposed encryption framework improves resistance against statistical attacks and brute-force cryptanalysis while maintaining efficient computational performance. The study concluded that deep learning-based encryption systems provide a promising solution for enhancing the confidentiality of cloud-stored data.

Mahmood and Abbas (2021) proposed an artificial intelligence-driven cybersecurity model for cloud computing environments. Their framework integrates machine learning algorithms with traditional security mechanisms to detect anomalies and cyber threats in cloud networks. The system continuously monitors network activities and uses classification algorithms to identify abnormal patterns associated with malicious attacks. Experimental evaluations demonstrated that AI-based security models significantly improve threat detection accuracy and reduce the risk of data breaches in cloud infrastructures.

Kaur and Singh (2022) explored the role of nature-inspired optimization algorithms in improving cloud computing performance and security. The researchers evaluated multiple metaheuristic algorithms, including grey wolf optimizer, whale optimization algorithm, and particle swarm optimization, for optimizing cloud resource allocation and task scheduling. The study concluded that optimization algorithms can enhance system efficiency, reduce resource consumption, and improve the overall performance of cloud infrastructures. These algorithms also contribute to strengthening security frameworks by optimizing encryption parameters and system configurations.

Cheng and Liu (2023) investigated quantum machine learning techniques for enhancing cryptographic security in cloud computing systems. Their study proposed a hybrid architecture combining quantum neural networks with classical machine learning models to generate secure encryption keys for cloud data protection. The system utilizes quantum feature encoding to improve cryptographic strength and resistance against cyberattacks. Experimental results showed that quantum machine learning-

based encryption systems provide higher levels of security compared with classical cryptographic approaches.

Ahmed, Khan, and Al-Hassan (2022) developed an AI-based predictive cybersecurity framework for protecting cloud storage systems. The proposed model uses deep learning algorithms to analyse network traffic patterns and identify potential cyber threats before they occur. The system incorporates anomaly detection techniques and predictive analytics to detect suspicious activities such as unauthorized access and data leakage. Experimental results demonstrated that the AI-driven cybersecurity framework significantly improves threat detection rates and enhances the reliability of cloud storage infrastructures.

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