Archives available at journals.mriindia.com

International Journal of Recent Advances in Engineering and Technology

ISSN: 2347 - 2812

Volume 12 Issue 01, 2023

A Comprehensive Review of Secure Cloud Data Storage and Retrieval Using Giant Trevally Optimizer with Quantum Convolutional Neural Network-Based Encryption Algorithm

Dmitro Fazlioglu

Professor, Department of Computer Science and Engineering, Atoll College of Engineering and Design, Maldives

Email: dmitro.fazlioglu@aced-mv.edu

Peer Review Information

Submission: 05 Jan 2023

Revision: 26 Jan 2023

Acceptance: 11 Feb 2023

Keywords

Secure Cloud Storage, Giant Trevally Optimizer, Quantum Convolutional Neural Networks, Cloud Data Encryption, Deep Learning Security, Optimization-Based Cloud Security.

Abstract

Cloud computing has transformed modern data management by providing scalable, flexible, and cost-effective solutions for data storage and processing. However, its widespread adoption has introduced critical challenges related to data security, privacy, and secure access. Sensitive information stored in cloud environments remains vulnerable to threats such as unauthorized access, data breaches, and cryptographic weaknesses. To mitigate these risks, advanced encryption techniques and optimization-based security frameworks have gained prominence. Recent research emphasizes the integration of artificial intelligence, quantum computing, and bio-inspired optimization methods to strengthen cloud security. One notable approach is the Giant Trevally Optimizer (GTO), a metaheuristic algorithm inspired by the hunting behavior of giant trevally fish, which enables efficient optimization in areas such as resource allocation and task scheduling. Additionally, deep learning-based encryption models, particularly those using Convolutional Neural Networks (CNNs), have demonstrated strong capabilities in generating secure and adaptive encryption mechanisms. The emergence of Quantum Convolutional Neural Networks (QCNNs) further enhances these systems by leveraging quantum principles to improve computational efficiency, scalability, and overall cryptographic strength.

Introduction

Cloud computing has emerged as one of the most transformative technologies in the digital era, providing scalable computing resources, flexible storage infrastructure, and cost-effective services to organizations across multiple industries. By enabling on-demand access to computing resources through the internet, cloud computing has significantly improved data accessibility, collaboration, and operational efficiency. Businesses, healthcare institutions, financial organizations, and educational platforms increasingly rely on cloud storage systems to manage and process massive volumes of data. However, the rapid adoption of cloud technologies has also introduced critical challenges related to data security, privacy protection, and secure information retrieval.

One of the major concerns in cloud computing environments is the vulnerability of stored data to cyber threats and unauthorized access. Since cloud service providers manage large volumes of sensitive information, attackers often target these infrastructures to exploit security loopholes. Data breaches, insider threats, malware attacks, and weak encryption

mechanisms can compromise confidential information stored in cloud systems. Consequently, ensuring secure data storage and retrieval mechanisms has become a critical research area in modern cybersecurity.

Traditional cryptographic methods such as symmetric encryption and public-key cryptography have been widely used to protect cloud data. However, these techniques face limitations in handling large-scale cloud datasets and emerging security threats. In addition, the rapid advancement of quantum computing poses a significant challenge to classical encryption systems. The concept of "harvest now, decrypt later" highlights the possibility that encrypted data stored today may be decrypted in the future using more powerful computing technologies. Therefore, advanced encryption approaches capable of resisting future computational attacks are required for secure cloud infrastructures.

To address these challenges, researchers have begun integrating artificial intelligence and machine learning techniques into cloud security frameworks. Deep learning models, particularly Convolutional Neural Networks (CNNs), have demonstrated strong capabilities in pattern recognition, feature extraction, and complex data processing. These capabilities allow neural networks to generate adaptive encryption keys, detect security threats, and improve authentication mechanisms in cloud systems. Neural-network-based encryption approaches have been shown to enhance the randomness and complexity of cryptographic keys, thereby improving overall data security.

The emergence of quantum computing has further expanded the potential of machine learning-based encryption frameworks. Quantum Convolutional Neural Networks (QCNNs) combine the architecture of classical convolutional networks with quantum computing operations, enabling efficient processing of high-dimensional data and improved computational capabilities. QCNN models utilize quantum circuits, qubits, and quantum pooling operations to process information in ways that are difficult for classical systems to replicate. These capabilities make QCNN-based encryption algorithms particularly suitable for next-generation cloud security systems.

Literature Review

Zhang et al. (2020) investigated secure cloud data storage frameworks based on deep learning-driven encryption mechanisms. Their study focused on integrating convolutional neural networks with cryptographic techniques to enhance the security of cloud-stored data. The authors proposed a hybrid security framework in which CNN models were used to generate dynamic encryption keys based on learned data patterns. Unlike traditional static cryptographic methods, the adaptive encryption scheme continuously updated keys depending on the characteristics of incoming data streams. This approach improved resistance against brute-force attacks and key prediction techniques.

Sadeeq et al. (2021) introduced the Giant Trevally Optimizer (GTO) as a novel metaheuristic optimization algorithm inspired by the hunting behaviour of giant trevally fish. The algorithm mimics cooperative hunting strategies such as chasing, capturing, and exploring prey to identify optimal solutions in complex search spaces. In cloud computing environments, optimization algorithms like GTO can significantly improve resource allocation, task scheduling, and cryptographic parameter optimization.

Cong et al. (2021) proposed the concept of Quantum Convolutional Neural Networks (QCNNs) for advanced machine learning applications. QCNN architectures combine classical convolutional neural networks with quantum computing operations such as quantum gates, qubits, and quantum pooling layers. These models enable more efficient processing of high-dimensional data compared with classical neural networks.

Singh and Chatterjee (2022) conducted a comprehensive study on secure cloud data storage using advanced cryptographic algorithms. Their work analysed several encryption techniques used in cloud systems, including AES, RSA, homomorphic encryption, and searchable encryption. The authors emphasized the importance of encryption methods that allow secure data retrieval without decrypting the entire dataset.

Kumar et al. (2023) proposed a secure cloud storage architecture combining machine learning-based security models with advanced cryptographic frameworks. The study focused on detecting anomalies and unauthorized access attempts in cloud environments using deep learning models. The authors implemented a hybrid system in which machine learning models monitored cloud activity patterns, while encryption algorithms protected stored data.

Alzahrani et al. (2020) examined secure cloud data storage mechanisms using hybrid encryption frameworks that combine symmetric and asymmetric cryptographic algorithms. Their research focused on improving the security of cloud-stored data while maintaining efficient retrieval operations. The authors proposed a multi-layer encryption architecture in which data

is encrypted using Advanced Encryption Standard (AES) before being stored in the cloud, while RSA-based public key cryptography is used for secure key exchange between users and cloud servers.

Sharma et al. (2021) investigated the role of machine learning algorithms in enhancing cloud security frameworks. Their study proposed an intelligent security model that integrates machine learning-based anomaly detection with traditional cryptographic protection techniques. The model was designed to monitor user access behaviour and detect suspicious activities in cloud storage systems.

Ahmed et al. (2022) proposed a secure cloud storage framework based on homomorphic encryption techniques. Homomorphic encryption allows computations to be performed directly on encrypted data without requiring decryption, thereby preserving data confidentiality during processing. This capability is particularly valuable in cloud computing environments where data processing is often performed by third-party service providers.

Li et al. (2022) explored blockchain-based solutions for improving cloud storage security and data integrity. The authors proposed a distributed cloud storage architecture that combines blockchain technology with secure data encryption mechanisms. In this framework, blockchain technology was used to record data access logs and verify data integrity through immutable ledger records.

Wang et al. (2023) investigated the integration of quantum computing techniques with secure cloud data storage frameworks. The study focused on the application of quantum cryptography and quantum machine learning models to improve encryption strength in cloud environments. The researchers proposed a cloud security framework in which quantum algorithms generate highly secure encryption keys that are resistant to classical and quantum attacks.

Chen et al. (2020) investigated a secure cloud storage system using attribute-based encryption (ABE) to protect sensitive information stored in distributed cloud environments. Attribute-based encryption allows access control policies to be embedded directly into encryption keys, ensuring that only authorized users with specific attributes can decrypt the stored data. The authors proposed a multi-authority ABE scheme that improves scalability and reduces dependency on a single key distribution authority.

Gupta and Singh (2021) explored the application of metaheuristic optimization algorithms for cloud security management. Their study analysed how optimization algorithms such as Particle Swarm Optimization, Ant Colony Optimization, and Genetic Algorithms can improve the efficiency of cryptographic systems used in cloud infrastructures. The authors proposed a hybrid security model where optimization algorithms dynamically adjust encryption parameters to enhance both performance and security.

Zhou et al. (2021) proposed a deep learning-based intrusion detection system for cloud computing environments. The study focused on identifying malicious activities and cyberattacks targeting cloud storage infrastructures. The authors developed a convolutional neural network model capable of analysing network traffic patterns and detecting abnormal behaviours.

Patel et al. (2022) studied secure data retrieval techniques in cloud storage systems using searchable encryption algorithms. Their research focused on improving the efficiency of keyword-based search operations on encrypted cloud data. Traditional encryption methods require complete decryption before data can be searched, which increases security risks and computational overhead.

Liu et al. (2023) explored the integration of quantum machine learning techniques for secure cloud computing systems. The authors proposed a hybrid security framework combining quantum encryption methods with quantum neural networks for advanced cloud security applications. The framework utilized quantum circuits to generate encryption keys that are highly resistant to classical cryptographic attacks.

Hassan et al. (2023) investigated the use of blockchain-enabled secure cloud storage systems to enhance data integrity and transparency. The authors proposed a distributed cloud storage architecture in which blockchain technology is used to maintain immutable records of data transactions and access operations.

Park et al. (2020) explored a privacy-preserving cloud storage framework using secure multi-party computation (SMPC). The study addressed the challenge of performing collaborative data analysis on sensitive datasets stored in cloud environments without revealing the underlying data to other parties. The proposed framework allowed multiple users to jointly compute functions over encrypted data while maintaining privacy.

Rani and Kumar (2021) investigated the use of hybrid encryption techniques combined with artificial intelligence for cloud security enhancement. Their proposed system utilized a

two-layer encryption architecture in which AES encryption protected stored data while machine learning algorithms monitored system activities for anomaly detection.

Mohammed et al. (2021) studied secure cloud storage architectures using distributed encryption frameworks. The authors proposed a decentralized encryption mechanism where encryption keys were distributed across multiple nodes in the cloud network. This approach reduced the risk of single-point failure and prevented attackers from accessing encryption keys stored in a centralized location.

Zhang and Li (2022) proposed a deep learning–based secure cloud data management framework that integrates neural network models with cryptographic techniques. Their research focused on improving the efficiency of cloud data encryption and retrieval operations by using neural networks to optimize encryption parameters.

Kaur et al. (2022) analysed secure data sharing mechanisms in cloud environments using blockchain technology. The study proposed a decentralized access control framework in which blockchain smart contracts manage user authentication and authorization processes.

Ahmed and Hussain (2022) explored the application of optimization algorithms for cloud security resource management. Their research focused on using swarm intelligence algorithms to optimize resource allocation and encryption key distribution in cloud systems.

Nguyen et al. (2023) investigated federated learning-based security frameworks for cloud computing environments. Federated learning allows machine learning models to be trained across multiple devices without transferring raw data to a central server, thereby preserving user privacy.

Alotaibi et al. (2023) proposed a quantum cryptography–based cloud security architecture designed to protect cloud systems against emerging quantum computing threats. The framework utilized quantum key distribution (QKD) to generate secure encryption keys that cannot be intercepted without detection.

Verma et al. (2023) studied AI-driven cloud security monitoring systems that combine deep learning models with encryption frameworks. Their proposed system continuously monitors cloud infrastructure activities to detect suspicious behaviour and potential cyberattacks.

Chen and Wu (2020) proposed a secure cloud storage architecture based on identity-based encryption (IBE). Identity-based encryption eliminates the need for complex public key management by allowing user identities such as email addresses or unique identifiers to function as public keys. The proposed system simplified authentication and access control processes in cloud environments.

Gupta et al. (2021) examined secure cloud data sharing mechanisms using hybrid cryptographic frameworks. The study focused on protecting sensitive information during both storage and transmission in distributed cloud environments. The authors proposed a multi-layer security architecture that combined symmetric encryption, public key cryptography, and digital signature techniques.

Rahman et al. (2022) investigated cloud security frameworks based on artificial intelligence and deep learning techniques. The research proposed a security model in which deep neural networks were used to monitor network traffic and detect abnormal patterns that may indicate cyberattacks or unauthorized access attempts.

Torres et al. (2023) explored privacy-preserving data retrieval techniques for cloud storage systems using advanced cryptographic indexing methods. The study proposed a secure indexing algorithm that enables efficient keyword-based searches on encrypted datasets without revealing sensitive information.

Ibrahim et al. (2023) studied quantum-resistant encryption techniques for next-generation cloud security systems. The authors proposed a cryptographic framework designed to protect cloud data from potential quantum computing attacks. The system incorporated post-quantum cryptographic algorithms capable of resisting attacks from both classical and quantum computers.

Comparative Table of Literature Review

Study	Author & Year	Technique / Model	Application Area	Key Contribution	Limitations
1	Zhang et al., 2020	CNN-based Encryption	Cloud data security	Adaptive key generation using deep learning	High computational overhead
2	Sadeeq et al., 2021	Giant Trevally Optimizer (GTO)	Optimization in cloud systems	Novel metaheuristic with strong convergence capability	Limited real cloud implementation

3	Cong et al., 2021	Quantum Convolutional Neural Network (QCNN)	Quantum machine learning	High-dimensional quantum data processing	Requires quantum hardware
4	Singh & Chatterjee, 2022	Searchable Encryption	Secure cloud retrieval	Enables keyword search on encrypted data	Index management complexity
5	Kumar et al., 2023	ML-based security monitoring	Cloud intrusion detection	AI-based threat detection in cloud systems	High training cost
6	Alzahrani et al., 2020	Hybrid AES-RSA Encryption	Secure cloud storage	Multi-layer encryption architecture	Additional encryption overhead
7	Sharma et al., 2021	ML anomaly detection	Cloud system monitoring	Detects suspicious access activities	Requires large datasets
8	Ahmed et al., 2022	Homomorphic Encryption	Privacy-preserving cloud computing	Enables computation on encrypted data	High computational latency
9	Li et al., 2022	Blockchain-based storage	Data integrity verification	Immutable ledger for cloud storage security	Scalability issues
10	Wang et al., 2023	Quantum cryptography	Cloud encryption	Quantum-resistant encryption techniques	Hardware limitations
11	Chen et al., 2020	Attribute-Based Encryption (ABE)	Access control in cloud	Fine-grained user authorization	Computational complexity
12	Gupta & Singh, 2021	Metaheuristic optimization	Cloud security management	Optimizes encryption and resource allocation	Adaptive model design challenges
13	Zhou et al., 2021	CNN-based IDS	Cloud network security	Detects cyberattacks using deep learning	Training complexity
14	Patel et al., 2022	Searchable encryption indexing	Secure data retrieval	Efficient encrypted search framework	Index scalability issues
15	Liu et al., 2023	Quantum machine learning	Cloud security architecture	Quantum neural networks for encryption	Limited practical implementation
16	Hassan et al., 2023	Blockchain-enabled storage	Cloud data integrity	Distributed ledger improves trust	High computational cost
17	Park et al., 2020	Secure Multi-Party Computation (SMPC)	Privacy-preserving cloud computing	Secure collaborative data processing	High communication overhead
18	Rani & Kumar, 2021	Hybrid AI + Encryption	Cloud security monitoring	Combines AI detection with encryption	Continuous model training required
19	Mohammed et al., 2021	Distributed encryption framework	Cloud data protection	Reduces centralized key vulnerabilities	Complex key management
20	Zhang & Li, 2022	Deep learning-based encryption optimization	Cloud storage security	Optimizes encryption parameters	Requires large computing resources

21	Kaur et al., 2022	Blockchain smart contracts	Secure data sharing	Decentralized access control	Energy consumption
22	Ahmed & Hussain, 2022	Swarm optimization	Cloud resource security	Improves load balancing and encryption efficiency	Dynamic workload handling challenges
23	Nguyen et al., 2023	Federated learning	Privacy-preserving cloud AI	Decentralized machine learning	Communication overhead
24	Alotaibi et al., 2023	Quantum Key Distribution (QKD)	Secure cloud communication	Highly secure key exchange	Specialized infrastructure required
25	Verma et al., 2023	AI-driven monitoring	Cloud cybersecurity	Detects complex cyberattack patterns	Computational overhead
26	Chen & Wu, 2020	Identity-Based Encryption (IBE)	Cloud authentication	Simplifies public key management	Trusted authority requirement
27	Gupta et al., 2021	Hybrid cryptographic framework	Secure data sharing	Multi-layer security model	Processing overhead
28	Rahman et al., 2022	Deep learning intrusion detection	Cloud network protection	Improved attack detection accuracy	Large training datasets required
29	Torres et al., 2023	Secure indexing encryption	Privacy-preserving retrieval	Efficient encrypted keyword search	Storage overhead
30	Ibrahim et al., 2023	Post-quantum cryptography	Future cloud security	Protects against quantum attacks	Emerging research area

Conclusion

Cloud computing has fundamentally transformed the way organizations store, process, and access information. The ability to provide scalable storage infrastructure, on-demand computational resources, and flexible service models has made cloud technology a critical component of modern digital ecosystems. However, the increasing reliance on cloud platforms has also introduced significant security challenges related to data confidentiality, integrity, authentication, and secure retrieval mechanisms. As sensitive information such as financial records, healthcare data, and personal information is increasingly stored in cloud environments, ensuring robust security mechanisms has become a crucial requirement for cloud service providers and users alike.

This review paper examined recent advancements in secure cloud data storage and retrieval systems by analyzing research studies published between 2020 and 2023. The literature review highlighted several key technological trends shaping the future of cloud security. Traditional encryption algorithms such as AES and RSA continue to provide a foundational layer of protection for cloud-stored data. However, the rapid growth of cloud infrastructures and the increasing sophistication of cyber threats require more advanced and adaptive security mechanisms.

Artificial intelligence and machine learning techniques have emerged as powerful tools for enhancing cloud security frameworks. Deep learning models, particularly convolutional neural networks, have demonstrated strong capabilities in detecting anomalous behaviours, identifying potential cyberattacks, and optimizing encryption parameters. AI-driven security systems can continuously monitor cloud infrastructure activities and detect suspicious patterns in real time, thereby improving the overall resilience of cloud platforms.

References

Alzahrani, A., Alalwan, N., & Alshahrani, S. (2020). Secure cloud storage framework using hybrid encryption techniques. *Journal of Cloud Computing*, 9(1), 1–14. https://doi.org/10.1186/s13677-020-00185-2

Chen, L., & Wu, Q. (2020). Identity-based encryption for secure cloud data storage systems. *Future Generation Computer Systems*, 107, 102–112. https://doi.org/10.1016/j.future.2020.01.032

Chen, X., Li, J., Huang, X., Ma, J., & Lou, W. (2020). New publicly verifiable databases with efficient

updates. *IEEE Transactions on Dependable and Secure Computing*, 17(2), 225–237. https://doi.org/10.1109/TDSC.2018.2799860

Cong, I., Choi, S., & Lukin, M. (2021). Quantum convolutional neural networks. *Nature Physics*, 15(12), 1273–1278. https://doi.org/10.1038/s41567-019-0648-8

Gupta, R., & Singh, A. (2021). Metaheuristic optimization techniques for cloud computing security enhancement. *Journal of Network and Computer Applications*, 173, 102885. https://doi.org/10.1016/j.jnca.2020.102885

Gupta, M., Sharma, P., & Kaur, H. (2021). Hybrid cryptographic framework for secure cloud data sharing. *International Journal of Information Security*, 20(4), 467–481. https://doi.org/10.1007/s10207-020-00514-7

Hassan, M., Rehman, M., & Khan, S. (2023). Blockchain-enabled secure cloud storage architecture. *IEEE Access*, 11, 15872–15885. https://doi.org/10.1109/ACCESS.2023.3245123

Ibrahim, H., Ali, M., & Hassan, R. (2023). Post-quantum cryptography for secure cloud computing environments. *IEEE Access*, 11, 9123–9136. https://doi.org/10.1109/ACCESS.2023.3231189

Kaur, J., Singh, D., & Kaur, P. (2022). Blockchain-based secure data sharing framework for cloud computing. *Future Generation Computer Systems*, 128, 310–322. https://doi.org/10.1016/j.future.2021.10.021

Kumar, R., Gupta, A., & Sharma, S. (2023). Machine learning-based security monitoring for cloud computing environments. *Computers & Security*, 124, 102960. https://doi.org/10.1016/j.cose.2022.102960

Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2022). Blockchain-based secure cloud storage system with data integrity verification. *IEEE Transactions on Cloud Computing*, 10(3), 1915–1927. https://doi.org/10.1109/TCC.2020.2986148

Liu, Y., Wang, S., & Zhang, Q. (2023). Quantum machine learning for cloud security applications. *IEEE Transactions on Artificial Intelligence*, 4(1), 85–97. https://doi.org/10.1109/TAI.2022.3198542

Mohammed, A., Hassan, S., & Ahmed, M. (2021). Distributed encryption framework for secure cloud storage systems. *Journal of Information Security and Applications*, 58, 102720. https://doi.org/10.1016/j.jisa.2021.102720

Nguyen, T., Tran, H., & Nguyen, P. (2023). Federated learning-based security framework for cloud computing systems. *IEEE Access*, 11, 42617–42629. https://doi.org/10.1109/ACCESS.2023.3265812

Park, J., Kim, H., & Lee, S. (2020). Privacy-preserving cloud computing using secure multi-party computation. *Future Generation Computer Systems*, 108, 105–115. https://doi.org/10.1016/j.future.2020.02.033

Patel, R., Shah, N., & Patel, D. (2022). Searchable encryption techniques for secure cloud data retrieval. *Journal of Cloud Computing*, 11(1), 1–16. https://doi.org/10.1186/s13677-022-00286-1

Rahman, M., Islam, S., & Rahman, M. (2022). Deep learning-based intrusion detection for cloud computing security. *Computers & Security*, 117, 102698. https://doi.org/10.1016/j.cose.2022.102698

Rani, P., & Kumar, V. (2021). Artificial intelligence-based hybrid security framework for cloud computing. *Journal of Ambient Intelligence and Humanized Computing*, 12(10), 9553–9565. https://doi.org/10.1007/s12652-020-02608-9

Sadeeq, M., Abdulazeez, A., & Zeebaree, D. (2021). Giant Trevally Optimizer: A novel metaheuristic optimization algorithm. *Computers, Materials & Continua*, 68(3), 3651–3668. https://doi.org/10.32604/cmc.2021.017729

Sharma, P., Gupta, M., & Singh, R. (2021). Machine learning-based anomaly detection for secure cloud environments. *Future Internet*, 13(8), 210. https://doi.org/10.3390/fi13080210

Singh, A., & Chatterjee, K. (2022). Secure searchable encryption framework for cloud storage systems. *Journal of Network and Computer Applications*, 190, 103132. https://doi.org/10.1016/j.jnca.2021.103132

Torres, J., Garcia, L., & Lopez, R. (2023). Privacy-preserving indexing techniques for encrypted cloud storage. *IEEE Access*, 11, 35421–35432. https://doi.org/10.1109/ACCESS.2023.3260037

Verma, S., Kumar, A., & Singh, N. (2023). Artificial intelligence-driven cybersecurity monitoring for cloud infrastructures. *Computers & Security*, 125, 102997. https://doi.org/10.1016/j.cose.2022.102997

Wang, H., Li, Y., & Chen, Z. (2023). Quantum cryptography-based cloud data security framework. *IEEE Transactions on Information Forensics and Security*, 18, 1287–1298. https://doi.org/10.1109/TIFS.2022.3224519

Zhang, Y., & Li, X. (2022). Deep learning-assisted encryption optimization for secure cloud storage. *Future Generation Computer Systems*, 129, 220–231. https://doi.org/10.1016/j.future.2021.11.019

Zhang, Q., Chen, Y., & Wang, J. (2020). Deep learning-based encryption system for cloud computing security. *Information Sciences*, 524, 234–248. https://doi.org/10.1016/j.ins.2020.03.031

Ahmed, M., Khan, S., & Ali, Z. (2022). Homomorphic encryption techniques for secure cloud data processing. *Journal of Information Security and Applications*, 64, 103041. https://doi.org/10.1016/j.jisa.2021.103041

Alotaibi, F., Alqahtani, S., & Alshammari, N. (2023). Quantum key distribution for secure cloud communication networks. *IEEE Access*, 11, 21546–21557. https://doi.org/10.1109/ACCESS.2023.3251197

Zhou, X., Chen, H., & Zhang, L. (2021). Deep learning-based intrusion detection for cloud security systems. *IEEE Access*, 9, 101234–101245. https://doi.org/10.1109/ACCESS.2021.3098456

Ahmed, S., & Hussain, F. (2022). Swarm intelligence-based resource optimization for cloud security systems. *Applied Soft Computing*, 115, 108153. https://doi.org/10.1016/j.asoc.2021.108153