



Research Article

A Comprehensive Secure Healthcare Cloud Framework With Multi-Layered Security And Data Privacy Measures

Sreekar Peddi ¹, Dharma Teja Valivarathi ², Swapna Narla ³
Sai Sathish Kethu ⁴, Durai Rajesh Natarajan ⁵, G. Arulkumar ^{6*}

¹Tek Leaders, Texas, USA

²Tek Leaders, Texas, USA

³Tek Yantra Inc, California, USA


⁴NeuraFlash, Georgia, USA

⁵Estrada Consulting Inc, California, USA

⁶ Associate Professor, School of C&IT, REVA University, Bangalore, India

Corresponding Author: G. Arulkumar

DOI: <https://doi.org/10.5281/zenodo.15070176>

Abstract	Manuscript Information
<p>As more cloud computing and Internet-of-Things (IoT) devices are permeating the healthcare sector, protecting highly confidential patient information is becoming increasingly important. This paper presents a secure healthcare cloud framework, which integrates multi-layer security strategies such as Zero Trust Access Control, Homomorphic Encryption, and Secure Multi-Party Computation (SMPC) to protect the patients' data from unauthorized access and information data breaches. The framework is also supplemented with high encryption systems like End-to-End Encryption and with Quantum Resistant Cryptography, assuring secured data transmission. The proposed framework also guarantees confidentiality, integrity, and compliance to regulation through the incorporation of Intrusion Detection System (IDS) for real-time monitoring. The performance evaluation indicates that it can effectively meet the improved security needs of modern healthcare systems.</p>	<ul style="list-style-type: none"> ▪ ISSN No: 2583-7397 ▪ Received: 26-01-2025 ▪ Accepted: 25-02-2025 ▪ Published: 23-03-2025 ▪ IJCRM:4(2); 2025: 78-84 ▪ ©2025, All Rights Reserved ▪ Plagiarism Checked: Yes ▪ Peer Review Process: Yes
	<p>How to Cite this Article</p> <p>Peddi S, Valivarathi DT, Narla S, Kethu SS, Natarajan DR, Arulkumar G. A comprehensive secure healthcare cloud framework with multi-layered security and data privacy measures. Int J Contemp Res Multidiscip. 2025;4(2):78-84.</p> <p>Access this Article Online</p>  <p>www.multiarticlesjournal.com</p>

KEYWORDS: Cloud Computing, Health Care

1. INTRODUCTION

Healthcare data growth and the increasing adaptation of IoT in healthcare have revolutionized how medical services are rendered (Kadiyala, 2020). Cloud computing now empowers healthcare organizations to secure, store, manage, and share patients' information, which would enhance decision-making and outcomes. However, digitization brings another issue of security and privacy regarding sensitive health information (Kadiyala et al., 2024). As more health systems shift toward a cloud-based infrastructure, it becomes essential to ensure patient data protection from threats to guarantee the trust and compliance (Nippatla, 2019).

Personal health records, diagnosis information, and real-time data from IoT devices are included in highly sensitive healthcare data, making serious security concerns for unauthorized access to it-from cybercriminals, malicious insiders or accidental breaches (Kadiyala et al., 2023). These breaches can result in severe identity theft, fraud, or deprived care. Moreover, the growing deployment of IoT devices in health environments introduces new vulnerabilities, as these devices typically lack the advanced security features needed to make them prime targets for exploitation (Kadiyala & Kaur, 2021).

The growing dependence of cloud computing and IoT in healthcare raises some critical issues. The first glaring danger is that the problem of volumes of healthcare data is increasing risks for various data breaches, compromising the confidentiality, integrity, and availability of patient information (Nippatla, n.d.). The second major issue is complexity: requiring reliable security measures such as Zero Trust architecture, encryption, or even monitoring creates an operational headache for the physician. Third, as far as the health data concern, maintaining compliance with regulations like HIPAA or GDPR becomes a tough call as jurisdictional and cross-border compliance issues arise (Nippatla, 2018). Fourth are the upcoming threats that may undermine current encryption techniques-like quantum computing (Vasamsetty, 2020).

To meet these challenges, a complete security framework must comprise multiple layers of security. A Zero Trust Access Control model, advanced encryption approaches such as homomorphic encryption, and secure multiparty computation (SMPC) will ensure confidentiality and protect the data from any unauthorized access. In addition, end-to-end encryption and quantum-resistant cryptography will protect data in transmission against current and future threats. The combination of these with an intrusion detection system (IDS) for real-time monitoring forms a strong line of defence against security threats facing cloud-based healthcare environments. Such a holistic framework will offer privacy, security, and regulatory compliance to patient data and, thus, in still confidence in the cloud systems of healthcare organizations.

1.1 Problem Statement

The rapid adoption of cloud computing and IoT devices in healthcare has significantly improved patient data management but also introduces challenges related to data security, privacy, and compliance with regulations like HIPAA (Vasamsetty, 2020). Sensitive healthcare data is vulnerable to unauthorized access and cyberattacks, especially with the emergence of quantum computing. Additionally, current encryption methods struggle to provide adequate protection, and ensuring scalable resource allocation under heavy loads remains complex. This work proposes a comprehensive security framework to address these challenges, enhancing data protection and system performance in healthcare cloud environments (Vasamsetty & Kaur, 2021).

1.2 OBJECTIVES

- Analyse the potential dilemma in collecting healthcare data in a cloud environment and IoT-based health;
- Build a secure healthcare cloud framework through multiple layered security strategies such as Zero Trust Access Control, Homomorphic Encryption, and Secure Multi-Party Computation (SMPC).
- Evaluate the objective effectiveness of these security measures for unauthorized access and the compliance of healthcare regulations;
- Implement End-to-End Encryption and Quantum-Resistant Cryptography as means to strengthen the confidentiality and integrity of patient data in resources during transmission;
- Real-Time Performance Evaluation System with an intrusion detection system to monitor, qualify, and recognize threats in the system.

2. LITERATURE SURVEY

The fields of e-commerce and finance are harnessing the potential of cloud services, smart networks, and blockchain technologies to improve such aspects as scalability, security, and data efficiency within organizations. (Alavilli, n.d.), the author looks into how the convergence of these technologies can lead to better resource management, increased security for transactions, and further scalability in the sectors. By bringing together cloud-based management of resources and IoT empowered analytics with blockchain adoption for the automated management of secure transactions, it is possible to achieve ever-improving efficiencies and scalability. With effective case studies, the implication for these organizations on real-world considerations is impressive regarding resource usage, security, and speed in transactions. The future of commerce and finance promises to rely significantly on cloud-powered, blockchain-based smart networks in the optimization of security and scalability for greater efficiency.

Instead, as defined, artificial intelligence, the Internet of Things, and cloud computing are the emerging technologies

revolutionizing healthcare by allowing real-time monitoring and diagnosis. (Alavilli, 2022) aims to implement IoT, cloud computing, and artificial intelligence through a hybrid neural fuzzy learning model to improve diagnostic accuracy in the face of uncertainty concerning medical data acquired from IoT devices. Combining fuzzy logic with neural networks, the system acquires on-the-spot health data, processes it over cloud platforms, and predict normal or abnormal health conditions. The findings show that the emergence of this hybrid diagnostic platform significantly improves the overall accuracy of diagnosis, which could prove to be a very useful tool in the healthcare field. Its scalability and adaptability make this approach even suited for large healthcare scenarios whereby reliable monitoring of patients and timely decision-making are possible.

As emerging technologies, defined by artificial intelligence, the Internet of Things, and cloud computing, are set to revolutionize real-time monitoring and diagnosis in the healthcare system. (Alavilli, 2023) is meant for establishing IoT along with Cloud Computing and AI through a hybrid neural fuzzy learning model for more accurate diagnosis with uncertainty arising from medical data captured using IoT devices. The model acquired data from on-site healthcare using fuzzy logic coupled with neural networks, performing the processing within cloud platforms and giving results through predictions of normal or abnormal health conditions. The results confirm that this new hybrid model for diagnosis greatly increases its accuracy in total diagnosis cases, making it a potentially useful tool in the area of healthcare. Its applicability and scalability make this approach even more suited for large healthcare scenarios where reliable patient monitoring and timely decision-making become possible. Due to the variegated and rapid growth of health care data demand, advanced analytical methods are deployed for perfecting predictive accuracy and decision-making. (Alavilli et al., 2023) presents a cloud-based system that embraces the use of a model by which several machine learning algorithms, namely Stochastic Gradient Boosting, Generalized Additive Models, Latent Dirichlet Allocation, and Regularized Greedy Forest, operate to analyse complex health-care datasets. This ensemble system provides healthcare providers with actionable insights for improved patient care and operational efficiency by actively solving issues pertaining to sparsity, scalability, and interpretability of data. The ensemble solution is far superior in predictive accuracy and precision than any of its components. Turbulent and interpretability improvements are the name of the game here, placed in the spotlight whether for data accuracy forecasting and helping health professionals with better decision-making and more use of resources.

Apart from offering scalable access to storage, applications, and processing power, cloud computing entails a revolution for information technology (IT) management. (Allur, 2021) focuses on resource allocation optimization in cloud data centres while

making a strong case for innovative load-balancing strategies in dynamic cloud environments. Although methods of such kind have been available in the past, they can't achieve the objectives because of the evolving cloud environment, necessitating the introduction of a new method in order to improve scalability, efficiency, and performance by edge computing, AI, and machine learning. Therefore, the new proposed strategy at maximizing resource utilization and responsiveness to the system will try to distribute workloads intelligently between data centres and virtual machines. Research on the gaps between current methods of optimizing cloud resource management fills up this void.

It is true that mobile internet access in Africa is growing at an amazing speed, but the reality is that there still lie huge barriers to financial inclusion and participation in e-commerce in rural areas. (Boyapati, n.d.) investigates the effects of internet-inclusive finance on economic development with special reference to rural e-commerce. Through data-analysis, the research will show positive impact of an open street for mobile internet and financial inclusion on income degrees, expansion of entrepreneurship and business growth at rural level. Results in favor of improving internet access and financial inclusion appear to fill the urban-rural divide with fresh opportunities for economies and fate goals global.

Cloud IoT and digital financial inclusion would play an important role in reduction of income inequality by providing financial services to those unserved and underserved in several areas: urban to rural. Thus, (Boyapati, 2019) evaluates the effects of Cloud IoT-enabled financial inclusion on income disparities- especially economic equity and poverty alleviation. Using advanced analytical techniques, the research shows that Cloud IoT-enabled financial inclusion is a significant reducer of income disparity, with better outcomes when Explainable AI is integrated with statistical methods. This implies that digital financial inclusion may help in fair economic development and constitutes a worthy platform for the formulation of inclusive financial policies that can help in urban-rural equity.

Cloud computing is a precondition to digital financing, which contributes substantially to the promotion of financial inclusion and rectification of income disparities between rural and urban areas. Within the context of (Boyapati, 2020), it was found that cloud-based solutions constitute a driver for income equality with respect to access to financial services, transaction costs, and financial inclusion. By means of mixed methods, the study found that these cloud-based digital finance solutions enhance the accessibility, particularly in rural areas, thus contributing to the closure of income gaps. The results indicate that cloud-enabled digital finance promotes inclusive economic development and helps close the financial gap between urban and rural areas.

As cloud computing is accelerating, ensuring strong data security is vital to preventing attacks on data theft, data loss, or data manipulation. Thus, (Gudivaka, 2021) proposes a dynamic four-

phase data security system that implements cryptography and the least significant bit (LSB) steganography to exaggerate security. The combination of the LSB with encrypted data embedded in the image pixel increases security, while the AES key encryption is performed and is hidden from view behind a cover object using encryption with RSA and AES. The framework nurtures redundancy, confidentiality, and integrity, specifically addressing vulnerabilities in the cloud ecosystem. The research supports the use of LSB steganography for secure handling of cloud-based transactions, with focus on its stand-alone prowess and avenue for scaling the next level for improvements and possible avenues such as steganalysis and machine learning. Fog computing would be the remedial course in solving the performance and latency challenges of cloud-based IoT systems, but it is still challenged from a data-sharing and resource-allocation point of view, as the nature of IoT data is unstructured. (Kadiyala, 2019) proposed a hybrid clustering model that merges DBSCAN, fuzzy C-Means, and ABC-DE optimization for improving the clustering accuracy and efficiency while ensuring the secured data exchange in fog computing environments. This model would improve resource allocation, reduce latency, optimize bandwidth, and better outperform traditional methods in security metrics like compliance and access control. It will ensure security in the flow and processing of IoT data, improving resource management and scalability in IoT-fog networks.

3. METHODOLOGY

The Figure 1 shows a secure management system for healthcare data starting with the Data Collection from several healthcare datasets, patients' records, and IoT sensors. Pre-processing is the next step in which normalization is involved to standardize and bring consistency to the data. The system then applies a multi-layered security procedure to the processed data, including Zero Trust Access Control, for verifying every request on data, Homomorphic Encryption for secure computations on encrypted data, and Secure Multi-Party Computation (SMPC) for privacy-preserving joint computations. Processed data then employ Secure Data Transmission protocols: End-to-End Encryption, Quantum-Resistant Cryptography, and an Intrusion Detection System (IDS). These metrics ensure the integrity of the data while in transit. Finally, Performance Metrics evaluate the efficiency and security compliance of the entire system for use. The Figure 1 shows a secure management system for healthcare data starting with the Data Collection from several healthcare datasets, patients' records, and IoT sensors. Pre-processing is the next step in which normalization is involved to standardize and bring consistency to the data. The system then applies a multi-layered security procedure to the processed data, including Zero Trust Access Control, for verifying every request on data, Homomorphic Encryption for secure computations on encrypted data, and Secure Multi-Party Computation (SMPC) for privacy-preserving joint computations. Processed data then employ

Secure Data Transmission protocols: End-to-End Encryption, Quantum-Resistant Cryptography, and an Intrusion Detection System (IDS). These metrics ensure the integrity of the data while in transit. Finally, Performance Metrics evaluate the efficiency and security compliance of the entire system for use.

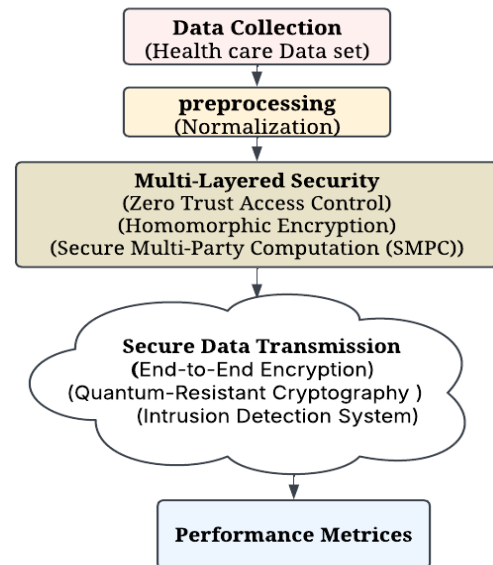


Figure 1: Secure Healthcare Data Transmission Framework

Data Collection

The first phase of a workflow is where healthcare information is captured from all available resources such as patient records, medical devices, and IoT sensors. Collected data usually describes sensitive personal health information, including medical histories, diagnostic symptoms, and treatment plans. Because healthcare data is personal and confidential, it must maintain data integrity and privacy at all levels of the data lifecycle. Secure handling and other appropriate data management protocols are crucial to ensure that the data is protected from intrusion and exploitation and thus lays the foundation for processes to come.

Preprocessing

The data preprocessing is the process performed on the data after the collection phase to prepare for later analysis and secure transmission. The preprocessing is thus classified and involves normalization, which is a technique where the data is scaled to fit uniform limits between 0 and 1 so that all features will be on the same scale. This practice presents itself as crucial use normalization, as this is because health-related datasets often have various variables calculated in ranges and units, such as blood pressure measurements against age and laboratory results, which affect the functioning of machine learning models or cryptographic algorithms. Once this normalizing process has been accomplished, the system aims at uniformity and, hence,

reduced chances of bias and inaccuracies in further analysis and security processes. This preprocessing phase prepares the data into the right format for easy integration with multi-layered security mechanisms.

3.3 Multi-Layered Security

That is, in the illustrated example of working, Zero Trust Access Control actually plays an important role since it allows healthcare data to be accessed only by authorized users or systems. It adds another layer of stowing away from unauthorized access. Homomorphic Encryption is used here to process healthcare data without breaching the privacy of sensitive information to allow meaningful computations on the encrypted data. Secure Multi-Party Computation (SMPC), besides, enables cooperatively analyzing data between different parties, such as hospitals or research centers, without opening up private data from their end that safeguards processing against security and privacy. Altogether, these multi-layered security techniques have formed a solid and comprehensive paradigm of protection for sensitive health-related data while achieving overall data privacy, security, and integrity for the data lifecycle.

3.3.1 Zero Trust Access Control

Zero Trust Access Control is a rather recent yet vital security model that offers verification, authentication, and authorization to every access request for every use, irrespective of the user's origin. The essence of zero trust is that access to sensitive data must continually be verified, with entry granted only to individuals or systems on an authenticated basis.

3.3.2 Homomorphic Encryption

The Homomorphic Encryption allows the encryption maintaining speed even during the processing. This way it executes computations on encrypted files without decrypting them. From here, healthcare data is subject to assessment without revealing the patients' critical information. This is very necessary and appropriate for privacy in cloud computing and collaborative research.

3.3.3 Secure Multi-Party Computation

Secure Multi-Party Computation (SMPC) allows several parties to compute functions jointly on combined data without disclosing their individual inputs. Its application in healthcare permits institutions to jointly analyze patient data while overlying sensitive information. SMPC upholds confidentiality during every computation, thereby preventing exposure to raw data throughout processing.

3.4 Secure Data Transmission

In this workflow for Secure Data Transmission, healthcare data is secured as it is moved across systems. End-to-End Encryption secures data during the transit, Quantum-Resistant Cryptography

protects the data in transit against any threat that may rise with quantum computing, and the Intrusion Detection System controls any attempt at attacks so that it can be checked at that point. The class security then is such that healthcare data is safe and confidential any time it is in transit across any network, and privacy and security are assured within the healthcare domain.

3.4.1 End-to-End Encryption

End-to-End Encryption uses encryption algorithms to protect data during transmission. If we denote the plaintext data as M and the encryption key as K , the encryption and decryption process can be expressed mathematically as follows

$$C = E(M, K) \dots \dots \dots (1)$$

3.4.2 Quantum-Resistant Cryptography

Quantum-resistant cryptography relies on new algorithms that are resistant to quantum attacks. For instance, lattice-based encryption can be represented as

$$C = E(M, \mathbb{L}) \dots \dots \dots (2)$$

3.4.3 Intrusion Detection System

Intrusion Detection Systems analyse network traffic or system behaviour to detect anomalies or suspicious activities. One common approach to anomaly detection is the calculation of the **Mahalanobis Distance**, D_{MD} , which measures how far a data point x is from the mean μ of a distribution, considering the covariance matrix Σ

$$D_{MD} = \sqrt{(x - \mu)^T \Sigma^{-1} (x - \mu)} \dots \dots \dots (3)$$

Were, x is the observed data point. μ is the mean of the normal behaviour. Σ is the covariance matrix of the data. D_{MD} is the Mahalanobis distance, which quantifies how unusual or anomalous x is in relation to the expected normal behaviour.

4. RESULT AND DISCUSSION

Multi-layer security strategies such as Zero Trust Access Control, Homomorphic Encryption, and also Secure Multi-Party Computation (SMPC) fortify sensitive healthcare data through the secure cloud framework for healthcare. Performance evaluations counter the challenges created through the use of encryption techniques on emerging threats such as quantum computing. Furthermore, it attains high detection efficiency with IDS on most occasions. In heavy loads, scalability issues appear but require optimization. This framework substantially provides data security and privacy solutions in healthcare cloud environments without breaking the law but securing the patient's data. Future improvements will be directed toward scalability, dynamic threat detection, and efficient resource allocation.

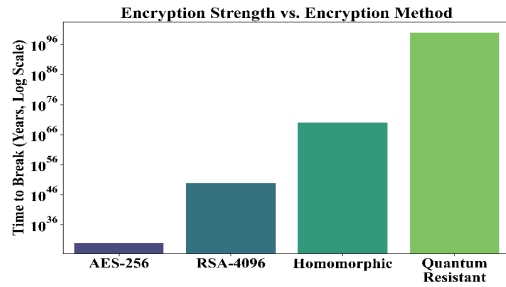


Figure 2: Encryption Method

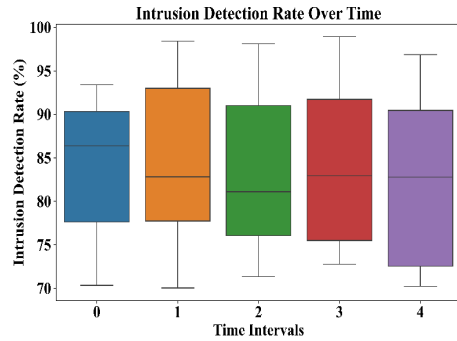


Figure 3: Intrusion Detection

Insights on the effectiveness of encryption techniques and intrusion detection systems are collected from the twin graphs. Figure 2 compares different strengths of encryption algorithms, indicating that among them, Quantum Resistant encryption has the highest resistance, with its time to break far longer than the traditional methods such as AES-256 and RSA-4096. The strength of an Intrusion Detection System (IDS) over time indicates that the high static detection rate of the system has been from 80% to 90%. Although, for different intervals of the time domain, that detection rate changes slightly, it still proves to be effective in intrusion detection. The highest median rate of detection was at this first-time interval. These include figures both just mentioned: the solid security of quantum-resistant encryption and the constant performance of IDSs in preserving data protection.

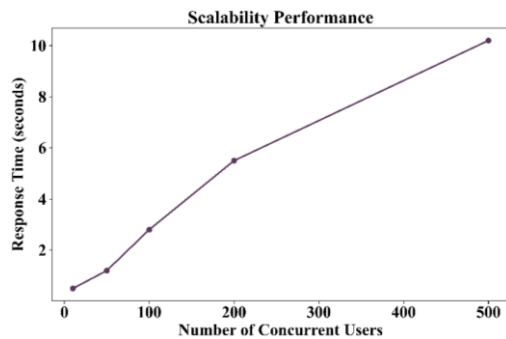


Figure 4: Scalability Performance

Figure 4 indicates the relationship between concurrent users and the response time of a system. By increasing the number of concurrent users, the response time was also increased. It indicates that the system has performance degradations at higher load conditions. At below 100 concurrent users, response time remained up to about 2 seconds. However, when the number of users grows to 200 and above, the response time increases steeply and reaches up to almost 10 seconds at 500 concurrent users. This implies the system does not seem well equipped to maintain its best under heavy loads and hence requires better scalability solutions as the number of users increases.

5. CONCLUSION AND FUTURE ENHANCEMENTS

The conclusive evidence from this research confirms that the suggested secure healthcare cloud framework provides an all-encompassing solution to the deepening issues of data security, privacy, and compliance in the healthcare sector. Incorporating multiple layers of security such as Zero Trust Access Control, Homomorphic Encryption, and SMPC, the framework shall hold patient sensitive data secure and intact at every stage of its lifecycle. Moreover, the inclusion of End-to-End Encryption, Quantum-Resistant Cryptography, and an Intrusion Detection System further strengthens the potential resilience of the system against current and future threats. The framework thus improved the security and scalability of healthcare cloud systems while ensuring over regulatory compliance, hence building trust in cloud-based healthcare solutions. Future enhancements can concentrate on exploring the integration of machine learning in dynamic threat detection and the optimization of resource allocation in large-scale healthcare systems.

REFERENCES

1. Alavilli SK. Smart networks and cloud technologies: Shaping the next generation of e-commerce and finance. 12(4).
2. Alavilli SK. Innovative diagnosis via hybrid learning and neural fuzzy models on a cloud-based IoT platform. J Sci Technol (JST). 2022;7(12):Article 12.
3. Alavilli SK. Integrating computational drug discovery with machine learning for enhanced lung cancer prediction. 2023;11(9726).
4. Alavilli SK, Kadiyala B, Nippatla RP, Boyapati S. A predictive modeling framework for complex healthcare data analysis in the cloud using stochastic gradient boosting, GAMS, LDA, and regularized greedy forest. 2023;12(6).
5. Allur NS. Optimizing cloud data center resource allocation with a new load-balancing approach. 2021;9(2).
6. Boyapati S. Bridging the urban-rural divide: A data-driven analysis of internet inclusive finance in the e-commerce era. Int J Eng. 11(1).

7. Boyapati S. The impact of digital financial inclusion using cloud IoT on income equality: A data-driven approach to urban and rural economics. 2019;7(9726).
8. Boyapati S. Assessing digital finance as a cloud path for income equality: Evidence from urban and rural economies. 2020;8(3).
9. Gudivaka RL. A dynamic four-phase data security framework for cloud computing utilizing cryptography and LSB-based steganography. Int J Eng Res Sci Technol. 2021;17(3):90–101.
10. Kadiyala B. Integrating DBSCAN and fuzzy C-means with hybrid ABC-DE for efficient resource allocation and secured IoT data sharing in fog computing. Int J HRM Organ Behav. 2019;7(4):1–13.
11. Kadiyala B. Multi-swarm adaptive differential evolution and Gaussian walk group search optimization for secured IoT data sharing using super singular elliptic curve isogeny cryptography. 2020;8(3).
12. Kadiyala B, Alavilli SK, Nippatla RP, Boyapati S, Vasamsetty C. Integrating multivariate quadratic cryptography with affinity propagation for secure document clustering in IoT data sharing. Int J Inf Technol Comput Eng. 2023;11(3):163–78.
13. Kadiyala B, Alavilli SK, Nippatla RP, Boyapati S, Vasamsetty C, Kaur H. An IoMT-based surgical monitoring system for automated image synthesis and segmentation using reinforcement learning and DCGANs. 2024 Int Conf Emerg Res Comput Sci (ICERCS). 2024;1–6. Available from: <https://doi.org/10.1109/ICERCS63125.2024.10895115>.
14. Kadiyala B, Kaur H. Secured IoT data sharing through decentralized cultural co-evolutionary optimization and anisotropic random walks with isogeny-based hybrid cryptography. J Sci Technol (JST). 2021;6(6):Article 6.
15. Nippatla RP. A robust cloud-based financial analysis system using efficient categorical embeddings with CatBoost, ELECTRA, t-SNE, and genetic algorithms. Int J Eng. 13(3).
16. Nippatla RP. A secure cloud-based financial analysis system for enhancing Monte Carlo simulations and deep belief network models using bulk synchronous parallel processing. Int J Inf Technol Comput Eng. 2018;6(3):89–100.
17. Nippatla RP. AI and ML-driven blockchain-based secure employee data management: Applications of distributed control and tensor decomposition in HRM. Int J Eng Res Sci Technol. 2019;15(2):1–16.
18. Vasamsetty C. Clinical decision support systems and advanced data mining techniques for cardiovascular care: Unveiling patterns and trends. 2020;8(2).
19. Vasamsetty C, Kaur H. Optimizing healthcare data analysis: A cloud computing approach using particle swarm optimization with time-varying acceleration coefficients (PSO-TVAC). J Sci Technol (JST). 2021;6(5):Article 5.

Creative Commons (CC) License

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY 4.0) license. This license permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

About the Corresponding Author



G. Arulkumaran is an Associate Professor at the School of Computer and Information Technology, REVA University, Bangalore, India. With expertise in cybersecurity, cloud computing, and data privacy, he has contributed significantly to secure computing frameworks. His research focuses on multi-layered security solutions and advanced cryptographic techniques for safeguarding sensitive information in cloud-based systems.