Journal of Science and Technology
ISSN: 2456-5660 Volume 10, Issue 03 (March -2025)
www.jst.org.in *DOI:https://doi.org/10.46243/jst.2025.v10.i03.pp20- 27*

Fortifying Cloud Security with Advanced Data Encryption Technique

Karthikeyan Parthasarathy
Technical Architect, LTIMindtree, Tampa, FL, United States
karthikeyan11.win@gmail.com

Naresh Kumar Reddy Panga
Engineering Manager, Virtusa Corporation, New York, NY, USA
nareshpangash@gmail.com

Jyothi Bobba
Lead IT Corporation, Illinois, USA
jyobobba@gmail.com

Ramya Lakshmi Bolla
Software Developer, ESB Technologies, Round Rock, Texas, USA
ramyabolla.lakshmi@gmail.com

Rajeswaran Ayyadurai
IL Health & Beauty Natural Oils Co Inc, California, USA
rajeswaranayyadurai@arbpo.com

R. Hemnath
Assistant Professor, Kaamadhenu Arts and Science College, Sathyamangalam, India
drhemnathr87@gmail.com

To Cite this Article

Karthikeyan Parthasarathy[1], Naresh Kumar Reddy Panga[2], Jyothi Bobba[3], Ramya Lakshmi Bolla[4], Rajeswaran Ayyadurai[5] R. Hemnath[6] "**Fortifying Cloud Security with Advanced Data Encryption Technique**" *Journal of Science and Technology, Vol. 10, Issue 03-March 2025, pp20-27*

Article Info

Received: 29-12-2024 Revised: 07-03-2025 Accepted: 18-03-2025 Published:28 -03-2025

ABSTRACT

The rapid growth of cloud computing has introduced several challenges regarding the securing of sensitive data. Traditional encryption methods such as those proposed by AES and RSA are unable to efficiently perform with the scale of large cloud environments as they have high computational cost. Recent advancements that have been made in encryption methods, especially concerning homomorphic encryption, appear to unravel an unprecedented potential since they provide capabilities for performing computations on encrypted data without the need to decrypt it thus assuring the privacy and integrity of data. However, they are still associated with adding computational overhead, and that will definitely pose various challenges for real-time cloud data processing. The setup proposed in this paper is a complete framework that integrates homomorphic encryption within a cloud security environment. It evaluates the effectiveness of homomorphic encryption in the cloud for aspects pertaining to performance and security, especially in terms of scalability as well with processing huge amounts of sensitive data while ensuring much efficiency in performance. Further, the framework includes some prior processing like normalization so as to optimize efficiency in encryption performance. A comprehensive security analysis is undertaken toward measuring the resistance of such encryption under numerous attack scenarios, and the effect of quantum computing applications on the proposed method of encryption is also discussed in this regard. This paper presents a thorough study of performance in conjunction with security trade-offs and, the overall development of a secure and efficient cloud data processing model.

Keywords: Cloud security, Homomorphic encryption, Performance metrics, Data privacy, Encryption overhead.

1. INTRODUCTION

The security of sensitive information has turned into a major concern within organizations and individual users alike during the cloud-computing era. [1] While organizations increasingly utilize cloud computing for data storage and processing, their exposure to cyber threats and subsequent rise in risks engaged includes data breaches, unauthorized accesses, and tampering.[2] Conventional security techniques such as firewalls and access control methods may not be sufficient in protecting cloud-held data because of the convoluted, distributed nature of cloud environments. [3] Therefore, the existence of strong encryption techniques is a prerequisite for ensuring data privacy, confidentiality, and integrity while being stored and transmitted to mitigate all of these risks.[4] Advanced encryption mechanisms, including homomorphic encryption, may be one way to reflect a promising avenue to

enhance cloud security while enabling computations on the encrypted data without exposing it to any unauthorized access [5]. The advanced data encryption techniques are assessed in this write-up for their role in strengthening cloud security. [6] It thoroughly analyses the case of application of advanced ethical means like homomorphic encryption in securing sensitive data and providing a capacity for secure computation. [7]

Exploring several encryption algorithms and assessing their performances, security and scalability with respect to cloud environment, this research aims at bringing out the bite of such advanced techniques in addressing the upcoming security challenges. [8] Thus this paper makes a thorough analysis to get into the discussions on how such encryption methods can successfully guard cloud data from emerging threats and further throw light on practical implementation and the future of cloud security in such a digital world. [9] As cloud computing will change and develop, the requirement for advanced methods of encryption will keep on increasing along with the expected need for new innovative solutions to forestall the risks likely to be caused in matters security. [10] Above all quantum-resistant encryption comes into play when the advances in quantum computing have to be counter by maintaining data safe over the long run. [11] The study also investigates overheads in calculation incurred during the implementation of these approaches in the cloud environment, as well as the trade-offs between performance and security. [12] It presents real-world use cases of the encryption modalities, illustrating their capacity to address specific security challenges of different industries. [13] Key management and scalability of encryption are some of the issues addressed to cover the entire spectrum of cloud security's present state. [14] It aims, thus, with making this holistic view of encryption in the cloud, to fuel the debate further on future secure infrastructures based on clouds. [15]

PROBLEM STATEMENT

The rapid growth of cloud computing has imposed paramount challenges in safeguarding sensitive data in the cloud [31]. While traditional encryption schemes offer adequate protection, they nonetheless prove inadequate with respect to performance scalability owing to high computational cost-these schemes have shortcomings for real complex operations over large cloud environments [32]. Furthermore, there exists a potential and growing risk from quantum computing to existing encryption schemes. These factors point to more inefficiency requiring cutting-edge superior encryption techniques that can securely do large-scale data without compromising system performance [33]. Though homomorphic encryption stands to be a potential candidate, the computational overhead involved continues to be a great deal of trouble for cloud deployments requiring both real-time data processing and secure computations [34]. This requires building a comprehensive framework that achieves advanced encryption coupled with cloud performance metrics and good security analysis for data protection in the contemporary cloud environment [35]**.**

Objective

- To develop an advanced cloud security framework that integrates homomorphic encryption techniques to secure sensitive data while maintaining the ability to perform computations on encrypted data.
- To evaluate the performance of homomorphic encryption in cloud environments, focusing on scalability, computational efficiency, and system overhead.
- implement data preprocessing and normalization techniques to ensure effective data handling and enhance the performance of the encryption process.
- To assess the effectiveness of the encryption scheme through performance metrics, ensuring that the framework meets the necessary standards of data protection without compromising cloud system performance.
- To deploy the encryption system on cloud infrastructure and analyse its security, identifying potential vulnerabilities and proposing improvements for robust data protection.
- To conduct a security analysis that evaluates the resilience of the encryption technique against various types of cyber-attacks and ensures that sensitive data remains protected under different threat scenarios.

2. LITERATURE SURVEY

Cloud security is of utmost importance as more organizations are depending on clouds for both data storage and computing. Most organizations use AES and RSA as their traditional methods for encrypting sensitive information in the cloud [16]. However, these techniques suffer from certain limitations and constraints imposed by large-scale cloud environments since they are highly computationally expensive and not scalable. As a result, more advanced encryption methods are fast gaining attention, especially as developments in homomorphic encryption [17]. This is because homomorphic encryption is based on the principle of abstracting the operation needed to perform on the encrypted data, thereby ensuring confidentiality without the need to decrypt. Hence, such a solution can become very useful in cloud environments where sensitive data processing must be done without compromising the data itself [18].

Advanced encryption techniques, still, encounter deployment challenges in cloud computing. Homomorphic encryption guarantees a secure structure for data, but it greatly increases computation complexity [19]. The research so far has focused on optimizing such encryption methods to reduce overheads while keeping them robust [20]. Moreover, so-called quantum-resistant encryption algorithms have recently gained prominence in development because quantum computing would break typical encryption schemes such as RSA. Researchers now focusing on lattice-based cryptography and other quantum resistance methods work towards future-proofing cloud security against this threat of quantum computing [21].

Key management is another important segment of cloud encryption. Reduction in the chance of unauthorized accessing and enhancement of the security of encryption keys have been the aspects considered in many research works to engineer distributed and hierarchical key management systems [22]. Such systems would mainly target extensive scale cloud environments to democratize access to security and efficiency in key management [23]. In addition, end-to-end encryption at the cloud's doorsteps until it is viewed only by those authorized has been suggested to protect even more sensitive data passing and storage action [24].

The machine learning integration is further researched in conjunction with other high-end approaches in the quest for balancing security and performance in cloud encryption [25]. Such methods minimize encryption overhead while detecting possible threats because of the combination of encryption and anomaly detection with other AI-driven methods. Other areas of cloud security researched are edge computing and closer data processing to the source besides reducing latency in some critical applications where real-time protection is needed [26]. The latest development has fused blockchain technology with encryption mechanisms to increase security level through decentralization and immutability of transaction logs [27].

Finally, lightweight encryption methods are developed to secure IoT devices and low-power edge computing environments, where traditional encryption methods fail due to resource constraints. These encryption methods are optimized for networks in which devices have very limited processing capabilities, and therefore these methods ensure that encryption does not affect device performance substantially [28]. Further, multi-layered encryption frameworks have been proposed so that different encryption levels are applied according to the sensitivity of the data, thus increasing security levels in the cloud [29]. Ongoing research continues to address scalability, performance, and security in the cloud as it continues to evolve to develop privacy-preserving techniques such as secure multi-party computation (SMPC) and differential privacy [30].

3. PROPOSED METHDOLOGY

Figure 1: illustrates the workflow of a cloud security system, starting with data collection, where relevant data is gathered from various sources. The data then moves to data preprocessing, where it undergoes normalization to standardize the values for effective processing. The next step is encryption, specifically using homomorphic encryption, which allows secure computation on encrypted data without needing decryption, ensuring confidentiality. After encryption, the system evaluates performance metrics to assess the system's efficiency and accuracy. Simultaneously, cloud deployment occurs, ensuring that the system is operational within a cloud environment. Finally, security analysis is performed to identify vulnerabilities and ensure the system’s robustness against potential threats. This complete process helps in ensuring both performance and security within a cloud infrastructure.

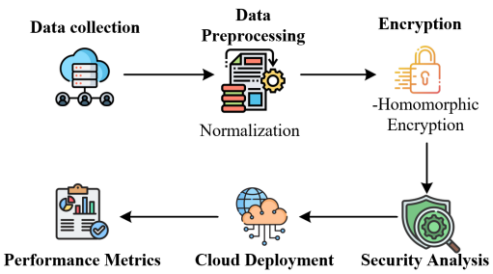

Figure 1: Cloud Security

3.1 DATA COLLECTION

Data Collection encompasses the collection of pertinent cloud data that can be used to represent real-world scenarios for testing purposes in respect to encryption. Such data will typically comprise sensitive information,

such as transaction logs, user access records, network traffic data, and other confidential resources stored in the cloud. The dataset can also comprise data from cloud service providers, IoT devices, or security logs. For encryption testing to be effective, the data must range over a significant span in types of sensitive information: it should be collected from veritable sources or generated from simulations, imitating genuine cloud security conditions which means that the encryption techniques can be evaluated on data that is realistic in terms of its credibility and potential security threats.

3.2 DATA PREPROCESSING

The purification of the collected data has to yield effective encryption tests on it. In general, cleansing the collected data for exploitation generally means deleting non-duplicate data, legacy or wrong measurements or irrelevant information. By imputation, the other way is used to deal with the absence of these values. Normalized, are applicable to numerical data, while encoding should also be used for categorical data. In order to remove unnecessary information, feature selection is done in locating the most critical attributes that matter with respect to the assessment of encryption methods. To prepare for robust encryption, such data would be rendered usable and mark accuracy or efficiency in further advances in security assessment.

3.2.1 Normalization

Normalization refers to a preprocessing procedure in which numerical variables fall to a certain range, commonly between 0 and 1, so that all features are treated equally concerned with the analysis. It is very relevant in cases of data of different magnitudes where it prevents some features from dominating simply because they are larger. A typical method of normalization is Min-Max Scaling, which transforms every feature x to a certain value x' according to the eqn1:

$$x' = \frac{x - \min(x)}{\max(x) - \min(x)} \quad (1)$$

Where: x is the original value of the feature, $\min(x)$ is the minimum value of the feature, $\max(x)$ is the maximum value of the feature.

3.3 ENCRYPTION

Encryption is the process of altering plaintext data to output scrambled data, unreadable without the necessary access or authorization. This will use cryptographic algorithms to generate keys which convert sensitive input into ciphertext forms that can be misunderstood and not be read without the appropriate decryption key. It might either be symmetric wherein the same keys will be used for encryption-decryption purposes such as AES or asymmetric wherein two different keys would be used-one for encryption while the other is for decryption like RSA. In short, encryption aims to keep private, maintain integrity on data, and protect the entry of unauthorized persons into data information that are sensitive most especially in cloud computing where data are stored over the internet without and during sending.

3.3.1 Homomorphic Encryption

Homomorphic encryption is a special encryption method such that it allows computations to be performed directly on the ciphertext without the need to decrypt it first. This property enables secure data processing in situations where sensitive data must be kept private, such as in cloud computing, while at the same time, the data may be analysed or computed upon. The result of the computation on encrypted data remains encrypted, and only the party that has been authorized and has the decryption key can decrypt that result to obtain final output. Parlier Homomorphic Encryption is a typical example that allows addition. Given two encrypted values $E(x)$ and $E(y)$, the homomorphic property allows for the encrypted result of their sum to be computed eqn2:

$$E(x + y) = E(x) \cdot E(y) \quad (2)$$

Where $E(x)$ and $E(y)$ are the encrypted values of x and y, and the product of these ciphertexts $E(x) \cdot E(y)$ is the encrypted result of $x + y$. This ability to perform operations directly on encrypted data is critical for privacy-preserving computations in sensitive environments.

3.4 SECURITY ANALYSIS

Security analysis pertains to the evaluation of encryption techniques and comprehensive cloud security regarding their effectiveness, robustness, and resistance to all forms of cyber threats and vulnerabilities. This would mean identifying any possible weaknesses in the encryption methods and testing how well they defend sensitive data

against any attack, such as brute force, side-channel, man-in-the-middle, or replay attacks. Security analysis also involves penetration testing to simulate attacks and assess how well the encryption withstands various attack scenarios. This would also mean verifying encryption algorithms against security standards to assure data confidentiality, integrity, and authentication, and resistance to advanced attacks, including computationally intensive quantum computing-based decrypting techniques. Such analyses would thus ensure that security measures put in place are actually functioning in the interest of protecting cloud data from unauthorized access and breaches.

3.4.1 Vulnerability Testing

The procedures for identifying, analysing, and mitigating security weaknesses in systems, networks, or applications that may be exploited by malicious parties are classified as Vulnerability Testing. This testing includes the use of a variety of non-exhaustive techniques such as automated scanning, manual penetration test methods, or security audits to detect vulnerabilities such as software bugs, misconfigurations, or flaws in encryption protocols. Vulnerability testing aims to identify several potential entry points for cyberattacks, including SQL injection, cross-site scripting, and unauthorized access to sensitive data. With the identification of specific vulnerabilities, corrective measures can be initiated by organizations, such as applying patches, improving configurations, and enhancing encryption in order to mitigate the risk of exploitation and strengthen the overall security posture of the calendar system.

3.5 CLOUD DEPLOYMENT

Cloud Deployment is the process of establishing and configuring cloud systems and services to host applications, store data or provide resources over the internet. The process involves the selection of a cloud service model (IaaS, PaaS, or SaaS) and subsequently choosing a cloud deployment model (public, private, hybrid, or multi-cloud) pertaining to the organization's requirements regarding security, scalability, and flexibility. During cloud deployment, organizations would configure their cloud environment, ensuring the appropriate networking and security measures as well as resource allocations to fulfil business objectives. In addition, this process involves integration of cloud services with systems currently in use, data migration, and continuous performance monitoring for optimizations. Thus, good cloud deployment guarantees that applications are accessible, secure, and scalable to provide on-demand resources while allowing for infrastructure cost reduction.

4. RESULT AND DISCUSSION

Figure 2: shows the Encryption Execution Time for two different encryption methods: AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman), and shows the increase in the data size. The x-axis indicates the size of the data in kilobytes (KB), while the y-axis shows time in milliseconds taken for encryption execution as it increases against the data size. The blue line represents AES, which is relatively stable and low for increasingly larger data sizes. On the other hand, the orange line, signifying RSA, soars up even with small data sizes, meaning very large amounts of time will be required even for small data sizes if RSA is used for the encryption process. This makes AES more efficient in terms of execution time when compared to RSA, particularly on larger data sets.

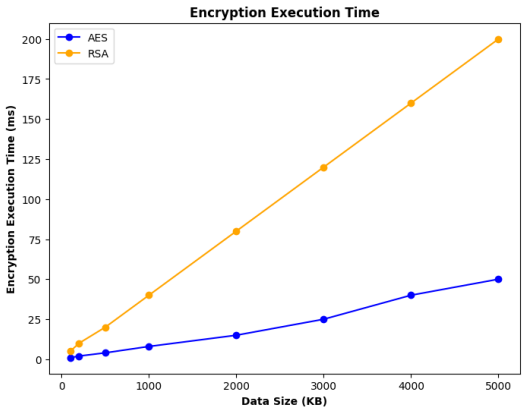

Figure 2: Encryption Execution Time

Figure 3: depicts Throughput Performance Comparison for a 30-minute time duration. The x-axis differentiates time intervals in minutes, while the y-axis denotes throughput percentage, a measure of system efficiency. A rise in throughput with time indicates a green line toward a positive trend. The beginning throughput percentage is about 10%, moving toward 90% at the end of the 30-min mark. This shows an increase in the system performance as time progresses from low throughput to high throughput percentage, indicating improved performance or data-processing capacity with time within this particular process.

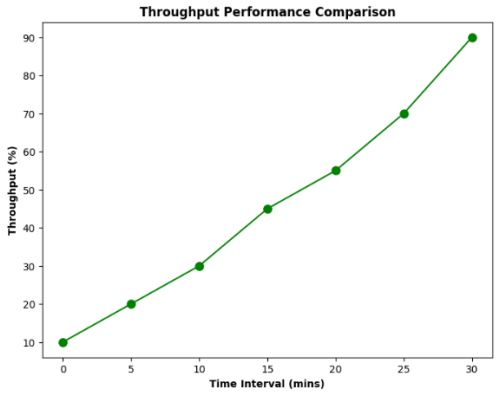

Figure 3: Throughput Performance

5. CONCLUSION

The paper gives a full framework for strengthening security in the cloud through advanced data encryption methods, mainly homomorphic encryption. The study points out the increased difficulties in cloud computing environments, in which traditional data encryption methods such as AES and RSA are having trouble performing in a scalable manner. Although homomorphic encryption assures good data secrecy and computation, it introduces very high computational overheads that must be taken into consideration in real time data processing. This framework gracefully incorporates this encryption scheme and tests its efficiency, scalability, and security with respect to cloud environments. The deliberations highlighted a trade-off between performance and security aspects. Homomorphic encryption, providing solid protection against data breaches and unauthorized access, shows promise but has challenges due to computational overhead requiring optimization approaches to lessen its effect on cloud performance. The study also addresses the threats posed by quantum computing and stresses the need for encryption algorithms resistant to quantum attacks. In conclusion, this framework lends credence to future efforts aimed at bolstering cloud security by guaranteeing that the sensitive nature of the data can be securely processed in the cloud without degrading its performance, meanwhile flagging toward potential directions for advancement in protection for cloud data.

6. REFERENCE

[1] K. Dondapati, “Lung’s cancer prediction using deep learning,” Int. J. HRM Organ. Behav., vol. 7, no. 1, pp. 1–10, Jan. 2019.

[2] B. R. Gudivaka, “BIG DATA-DRIVEN SILICON CONTENT PREDICTION IN HOT METAL USING HADOOP IN BLAST FURNACE SMELTING,” Int. J. Inf. Technol. Comput. Eng., vol. 7, no. 2, pp. 32–49, Apr. 2019.

[3] P. Alagarsundaram and N. Carolina, “Implementing AES Encryption Algorithm to Enhance Data Security in Cloud Computing,” vol. 7, no. 2, 2019.

[4] A. R. G. Yallamelli, “Wipro Ltd, Hyderabad, Telangana, India,” vol. 7, no. 9726, 2019.

[5] N. S. Allur, “Genetic Algorithms for Superior Program Path Coverage in software testing related to Big Data,” Int. J. Inf. Technol. Comput. Eng., vol. 7, no. 4, pp. 99–112, Dec. 2019.

[6] Alavilli, S. K. (2020). Predicting heart failure with explainable deep learning using advanced temporal convolutional networks. *International Journal of Computer Science Engineering Techniques, 5*(2), March-April.

[7] *Panga, N. K. R. (2020). Leveraging heuristic sampling and ensemble learning for enhanced insurance big data classification.* International Journal of Financial Management (IJFM), *9(1), 15-26.*

[8] M. R. Sareddy "Next-Generation Workforce Optimization: The Role of AI and Machine Learning," vol. 5, no. 5, 2020.

[9] Gudivaka, R. L. (2020). Robotic process automation meets cloud computing: A framework for automated scheduling in social robots. *IMPACT: International Journal of Research in Business Management (IMPACT: IJRBM)*, 8(4), 49-62.

[10] Gudivaka, R. K. (2020). Robotic process automation optimization in cloud computing via two-tier MAC and Lyapunov techniques. International Journal of Business and General Management (IJBGM), 9(5), 75-92.

[11] D. P. Deevi, "ARTIFICIAL NEURAL NETWORK ENHANCED REAL-TIME SIMULATION OF ELECTRIC TRACTION SYSTEMS INCORPORATING ELECTRO-THERMAL INVERTER MODELS AND FEA," Int. J. Eng., vol. 10, no. 3.

[12] Chetlapalli, H. (2021). Enhancing test generation through pre-trained language models and evolutionary algorithms: An empirical study. *International Journal of Computer Science and Engineering (IJCSE)*, 10(1), 85-96.

[13] Dondapati, K. (2020). Clinical implications of big data in predicting cardiovascular disease using SMOTE for handling imbalanced data. *Journal of Cardiovascular Disease Research, 11*(9), 191-202.

[14] N. S. Allur, "Enhanced Performance Management in Mobile Networks: A Big Data Framework Incorporating DBSCAN Speed Anomaly Detection and CCR Efficiency Assessment," vol. 8, no. 9726, 2020.

[15] D. P. Deevi, "REAL-TIME MALWARE DETECTION VIA ADAPTIVE GRADIENT SUPPORT VECTOR REGRESSION COMBINED WITH LSTM AND HIDDEN MARKOV MODELS," J. Sci. Technol. JST, vol. 5, no. 4, Art. no. 4, Aug. 2020.

[16] A. R. G. Yallamelli, "Improving Cloud Computing Data Security with the RSA Algorithm," vol. 9, no. 2, 2021.

[17] S. Kodadi, "ADVANCED DATA ANALYTICS IN CLOUD COMPUTING: INTEGRATING IMMUNE CLONING ALGORITHM WITH D-TM FOR THREAT MITIGATION," Int. J. Eng. Res. Sci. Technol., vol. 16, no. 2, pp. 30–42, Jun. 2020.

[18] K. Dondapati, "INTEGRATING NEURAL NETWORKS AND HEURISTIC METHODS IN TEST CASE PRIORITIZATION: A MACHINE LEARNING PERSPECTIVE," Int. J. Eng., vol. 10, no. 3.

[19] Koteswararao Dondapati, "Leveraging Backpropagation Neural Networks and Generative Adversarial Networks to Enhance Channel State Information Synthesis in Millimetre Wave Networks," Oct. 2024, doi: 10.5281/ZENODO.13994672.

[20] Kalyan Gattupalli, "Optimizing 3D Printing Materials for Medical Applications Using AI, Computational Tools, and Directed Energy Deposition," Oct. 2024, doi: 10.5281/ZENODO.13994678.

[21] N. S. Allur and W. Victoria, "Big Data-Driven Agricultural Supply Chain Management: Trustworthy Scheduling Optimization with DSS and MILP Techniques," Curr. Sci., 2020.

[22] N. S. Allur, "Phishing Website Detection Based on Multidimensional Features Driven by Deep Learning: Integrating Stacked Autoencoder and SVM," J. Sci. Technol. JST, vol. 5, no. 6, Art. no. 6, Dec. 2020.

[23] S. S. Kethu, K. Corp, and S. Diego, "AI and IoT-Driven CRM with Cloud Computing: Intelligent Frameworks and Empirical Models for Banking Industry Applications," vol. 8, no. 1, 2020.

[24] P. Alagarsundaram, "PHYSIOLOGICAL SIGNALS: A BLOCKCHAIN-BASED DATA SHARING MODEL FOR ENHANCED BIG DATA MEDICAL RESEARCH INTEGRATING RFID AND BLOCKCHAIN TECHNOLOGIES," vol. 9, no. 9726, 2021.

[25] M. V. Devarajan and C. Solutions, "AN IMPROVED BP NEURAL NETWORK ALGORITHM FOR FORECASTING WORKLOAD IN INTELLIGENT CLOUD COMPUTING," vol. 10, no. 9726, 2022.

[26] Mamidala, V. (2021). Enhanced security in cloud computing using secure multi-party computation (SMPC). *International Journal of Computer Science and Engineering (IJCSE)*, 10(2), 59-72.

[27] N. K. R. Panga, "Optimized Hybrid Machine Learning Framework for Enhanced Financial Fraud Detection Using E-Commerce Big Data," vol. 11, no. 2.

[28] R. Ayyadurai, "Big Data Analytics and Demand-Information Sharing in E- Commerce Supply Chains: Mitigating Manufacturer Encroachment and Channel Conflict," vol. 15, no. 3, 2021.

[29] R. K. Gudivaka, "Enhancing 3D Vehicle Recognition with AI: Integrating Rotation Awareness into Aerial Viewpoint Mapping for Spatial Data," Curr. Sci., 2022.

[30] H. Nagarajan and H. M. Khalid, "OPTIMIZING SIGNAL CLARITY IN IOT STRUCTURAL HEALTH MONITORING SYSTEMS USING BUTTERWORTH FILTERS," vol. 7, no. 5, 2022.

[31] S. Kodadi, "Big Data Analytics and Innovation in E-Commerce: Current Insights, Future Directions, and a Bottom-Up Approach to Product Mapping Using TF-IDF," Int. J. Inf. Technol. Comput. Eng., vol. 10, no. 2, pp. 110–123, May 2022.

[32] M. V. Devarajan, "DATA-DRIVEN TECHNIQUES FOR REAL-TIME SAFETY MANAGEMENT IN TUNNEL ENGINEERING USING TBM DATA," vol. 7, no. 3.

[33] Chetlapalli, H. (2023). Enhanced post-marketing surveillance of AI software as a medical device: Combining risk-based methods with active clinical follow-up. *IMPACT: International Journal of Research in Engineering & Technology, 11*(6), 1-14.

[34] Poovendran, A. (2024). Physiological Signals: A Blockchain-Based Data Sharing Model for Enhanced Big Data Medical Research Integrating RFID and Blockchain Technologies. Journal of Current Science, 9(2), 9726-001X.

[35] Sitaraman, S. R. (2020). Optimizing Healthcare Data Streams Using Real-Time Big Data Analytics and AI Techniques. International Journal of Engineering Research and Science & Technology, 16(3), 9-22.