iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

SECURE AND EFFICIENT HEALTHCARE DATA STORAGE: A CRYPTOGRAPHIC FRAMEWORK FOR CLOUD-BASED SYSTEMS

Sunil Kumar Alavilli [1], Bhavya Kadiyala [2], Rajani Priya Nippatla [3], Subramanyam Boyapati[4], Chaitanya Vasamsetty [5], Purandhar. N [6, *]

[1]Sephora, California, USA. Email: sunilkumaralavilli@ieee.org
[2]Parkland Health,Texas, USA. Email: bhavyakadiyala@ieee.org
[3]Kellton Technologies Inc, Texas, USA. Email: rajanipriyanippatla@ieee.org
[4]American Express, Arizona, USA. Email: subramanyamboyapati@ieee.org
[5]Elevance Health, Georiga, USA. Email: chaitanyavasamsetty@ieee.org
[6]Assistant ProfessorDepartment of CSE(Artificial Intelligence)School of Computers
Madanapalle Institute of Technology and Science, MadanapalleCollege code - 69
Andhra Pradesh - 517325, India. Email: purandhar.n@gmail.com

Corresponding Author Name: Purandhar. N Corresponding Author Email: purandhar.n@gmail.com

ABSTRACT
The importance of a secure and efficient means of storing healthcare-related data increases with increasing volumes. Existing frameworks do secure data but, in terms of encryption efficiency and scalability, fail to account for large volumes of data posing a threat. In this work, we have studied a framework for storing health care data securely, adapting solid data protection against contemporary and future threats. The proposed framework for secure healthcare data storage involves data collection in the form of patient records and medical data, secure key generation using CRYSTALS-Kyber for encryption during the transmission of healthcare data, encrypting the data and securely storing it in the cloud environment. The results indicate an encryption strength of 99.5, whereas data integrity received 99.2. The framework scored 98 for adaptability, showing that it can easily handle large volumes of data. Therefore, it meets quantum-resistance requirements and thus supports secure and scalable data solutions for cloud-based environments in healthcare.

Keywords:
Healthcare data, Key Generation, CRYSTALS-Kyber encryption, Cloud Storage.

1. INTRODUCTION

The phenomenon of an explosion of health-related data has led to an increase in reliance on alternative storage mediums such as the cloud for managing patient information [1]. Hospitals, research institutions, and care providers accumulate large quantities of sensitive data, including electronic health records (EHRs), diagnostic images, genomic data, and metrics for real-time patient monitoring [2]. This data serves as an important element in the diagnosis, treatment and personalization of medicine for diseases [3]. This highly sensitive health information stored in cloud settings poses considerable security and privacy issues [4]. It takes names, such as unauthorized access, cyber-attacks and data breaches, among others; there are also many compliance concerns which put a huge share of risk on patient confidentiality [5]. Cloud computing integration promotes easier sharing by health professionals; it is beneficial in increasing accessibility and scalability [6]. These notwithstanding, it has made the decentralized nature of cloud storage stand higher chances of data manipulation, unauthorized exposure and sensitive medical records loss [7]. Thus, it becomes critical to implement advanced security mechanisms to protect stored healthcare data for privacy, integrity and confidentiality [8].

Secure storage and management of sensitive patient information have become more crucial than ever with the transitions of healthcare systems shifting to digital systems. Given the high demand for safe storage of EHRs, medical images and other patient data and growing need for effective cloud-based systems for healthcare providers to store this kind of information, the gains of cloud storage in instances such as scalability, accessibility and cost do come with unwanted concerns such as security risks. Among security risks are data breaches and unauthorized access followed by all-out cyberattacks [9]. The healthcare organizations shall then be demanded to implement stringent encryption and secure data management practices to tackle these issues [10]. Encryption has become an important channel through which most claims of confidentiality and integrity of patient records stored in the cloud are substantiated [11]. Also important is the secured mechanism for key management, which is important for the protection of encryption keys that safeguard sensitive data [12]. Encryption techniques should be always advancing to be strong against future threats including quantum computing. Data privacy and security must not be compromised at all in order to preserve the trust and compliance of healthcare systems.

To prevent unauthorized access to sensitive medical records and data breaches, healthcare organizations should implement stringent security measures. The worth of healthcare data is highly priced and given this fact, an increase in cyber threats with severe consequences to both patients and providers, like ransomware attacks, data leaks, or insider threats, may be observed [13]. Thus, to make such cases of data breaches irrelevant, it is important to implement secure encryption methods, key management strategies and controlled access mechanisms [14]. Furthermore, it is necessary to establish secure data transfer protocols to preserve patient information while transferring data from hospitals to cloud storage or connected medical devices [15]. Data security while accessibility is guaranteed for authorized personnel presents a very complex problem and requires an efficient scalable storage framework [16]. It still remains on top of the concerns of securing patient data stored on clouds against unauthorized disclosures, long-term availability and evolved cyber threats while the digital transformation of healthcare is in full swing [17].

The paper proceeds as follows: Firstly, literature survey gives an overview of existing work on secure healthcare data storage. The next section is the methodology, which describes how data will be collected, keys generated, encryption performed and uploaded on the cloud. The results section examines the performance of the system based on parameters such as encryption time, data integrity and scalability, which is followed by the concluding section that recaps significant findings and future work.

2. LITERATURE SURVEY

Devarajan et al. [18] incorporated these cutting-edge technologies in their research: federated learning and cloud-edge collaborative computing systems. Their research primarily concentrated on developing a multi-national validation architecture for attacks and non-attacks. The study made use of what it termed End-to-End Privacy-Preserving Deep Learning (E2EPPDL) to classify each incident resulting from this study. This E2EPPDL formed the major pillar of this study for attack classification and also kept its activity private.

Cloudlet computing with Edgel-AI: For the health system, Yallamelli and Devarajan [19] developed a hybrid IoT platform that can be integrated with healthcare data processing to secure data sharing, minimize average latency and improve real-time decision making. Besides, advanced artificial intelligence models populate this platform: Random Forest classifiers, Transformer networks and Temporal convolutional networks are incorporated into the Cloudlet with edge, for the distributed processing along this framework.

Ganesan [20] introduced P2DS, a remedy to contain the increasing peril of security threats in financial institutions. It was an advanced cryptographic framework using methods such as Attribute-Based Encryption, Attribute-Based Semantic Access Control and the Proactive Determinative Access algorithm. The research showed its high proficiency in accurate access control, faster threat detection and the efficient encryption of such data. Due to its security and data privacy services, P2DS serves as an authenticated mechanism for the protection of sensitive financial information in the rapidly changing digital ocean.

Devarajan et al. [21] introduced a robust IoMT-and-blockchain-based heart disease monitoring system. The system enabled registration and login of both doctors and patients. At registration, keys were generated for all assigned personnel-whoever they might be. Then, during login, data sensing and sensed data uploads to IPFS, the generation and storage of hashcodes take place in the blockchain. Then again, the Message Authentication Code generation and verification comes in for authentication purposes.

Ganesan [22] focused on ensuring the security of IoT systems through a study on critical node identification, vulnerability assessment, security measure proposal and overall system performance impact analysis. With a quantitative approach toward identifying critical components of IoT systems, a complete vulnerability assessment was carried out. Security measures, such as intrusion detection systems, encryption techniques, access control measures and continuous security audits, were proposed and evaluated for their effectiveness in securing IoT.

Ganesan [23] engineered a service-oriented architecture for the system that operates in a Hadoop-managed server cluster for processing power and data storage. The platform enabled efficient management of educational resources for remote learning through large datasets and high concurrency support. Stress testing demonstrates that the platform is capable of sustaining many users simultaneously and many data transactions reliably under heavy load.

Devarajan et al. [24] have worked out a new method-an innovative approach-in solving the Job Shop Scheduling Problem, using the Heterogeneous Genetic Algorithm (HGA) along with a Hybrid Particle Swarm Optimization (HPSO). The HGA is in fact a combination of the genetic algorithm GAs plus the immune mechanisms like memories and mutation strategies to prevent premature convergence and enhance exploration capabilities. It has been crucial for developing the HPSOs made to improve job sequencing into lesser production time integrating PSO strengths with some genetic operators.

Yallamelli et al. [25] came up with a truly innovative and state-of-the-art approach, which is called Dynamic Mathematical Hybridized Modeling Algorithm for solving work order patching problems of warehousing that are indeed crucial for the entire optimization process involved in any order filling. This is integrated within advanced operational research techniques-a tabu search-related dynamic mathematical hybridized modeling algorithm for solving batching order efficient grouping.

2.1 Problem Statement

The existing works in securing healthcare data in cloud computing have taken giant strides, especially by integrating homomorphic encryption for privacy-preserving data analysis. However, there are still challenges to be faced, like the increased computational overheads raised by homomorphic encryption, which makes it harder to balance data confidentiality with efficient processing [26]. The scalability of the techniques is a problem regarding the current methods of privacy-preserving data analysis when applied for large heaps of healthcare data [27]. This paper proposes the development and thus implementation of more efficient and scalable solutions for privacy-preserving data analysis as an answer to the challenges, thereby promising improved performance and confidentiality in cloud-based healthcare systems.

3.METHODOLOGY

The framework for securing healthcare data in cloud storage is depicted in Figure 1. At the outset, patient records and medical data form the healthcare datasets. Subsequently, the use of CRYSTALS-Kyber for the key generation process produces a public and private key that provides an encryption and decryption process. After that, the acquisition of healthcare data occurs by encrypting such data with CRYSTALS-Kyber before storage. The data is thereafter stored in a cloud environment, making it secure but accessible and scalable. The system also measures the performance of its overall encryption procedure using performance metrics measured against the efficiency of its encryption process, that is, storage space and access speed. This workflow ensures the confidentiality, integrity and post-quantum security in the storage of healthcare data on cloud systems.

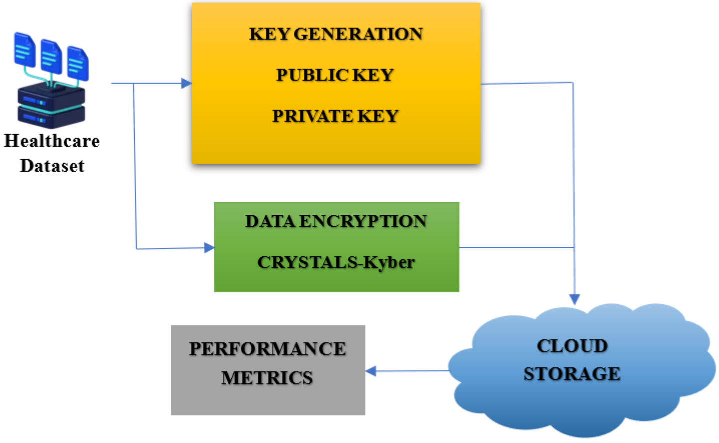

Figure 1: Secure Healthcare data storage using CRYSTALS-Kyber Encryption

3.1 DATACOLLECTION

In collecting data relevant to healthcare, several resources such as electronic health records (EHRs), medical imaging systems, IoT-enabled wearables, patient monitoring sensors and laboratory report systems are used. The data in consideration would comprise structured numerically formatted data records, unstructured clinical note texts and high-resolution medical imaging, all useful for diagnosis and intervention. Preprocessing methods are set in place to maintain data integrity when they come into contact with encryption techniques. In this area, the anonymization of personally identifiable information is another important factor in countering unauthorized access. Furthermore, secure data-sharing agreements with the healthcare bodies magnify security and compliance aspects. The collected data is able to go through an organized process of encryption before secure cloud storage and protection from cyber threats.

3.2 KEY GENERATION

CRYSTALS-Kyber is a post-quantum cryptographic algorithm and lattice-based key encapsulation mechanism for secure key material generation and exchange. In this scheme, a public-private key pair is generated: the public key is used for encryption and the private key for decryption. Then, it uses a key encapsulation mechanism (KEM), which ensures secure derivation and exchange of encryption keys across untrusted networks. Unlike key generators based on classical RSA or elliptic curve cryptography (ECC), Kyber resists quantum attacks and remains secure against attacks from quantum computers. Its operational efficiency, small key size and speed of key generation make it ideal for bulk data encryption. This method secures key exchange and encryption, thus maintaining the data-preservative contemporary security paradigms.

The key generation process in CRYSTALS-Kyber follows these three main steps:

Select a secret key (s) and error term (e) from a small distribution is represented as equation (1),

$$s, e \leftarrow \chi \tag{1}$$

where χ is a noise distribution.

Generate a random matrix A from a predefined set. Compute the public key using the equation (2),

$$pk = A \cdot s + e \bmod q \tag{2}$$

Where, A is a randomly chosen matrix (publicly known). s is the secret key. e is the error term. q is a predefined prime modulus.

The private key is simply expressed as equation (3),

$$sk = s \tag{3}$$

IJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

The private key (s) is chosen randomly and kept secret. The public key (pk) is computed using matrix multiplication with added noise. The security comes from the hardness of solving $pk = A \cdot s + e \bmod q$, even with quantum computers. This process ensures secure key generation for encrypting healthcare data before storage.

3.3 ENCRYPTION

The framework proposed here uses CRYSTALS-Kyber, a post-quantum cryptographic algorithm, for encryption, which is aimed at key exchanges and protecting data. In the first instance, the health data are encrypted with the public key generated in the key generation phase and stored. Health data use an encryption mechanism: KEM, with public key and shared secret key derived during encryption. The ciphertext is sent to the cloud infrastructure to ensure encryption protection against unauthorized access. The CRYSTALS-Kyber algorithm guarantees that, under quantum power, this data remains safe against any algorithm of quantum-based attack. Therefore, the framework provides confidentiality, integrity, and security to sensitive healthcare data throughout the collection and storage phases using this encryption process.

The encryption process in CRYSTALS-Kyber is based on a Key Encapsulation Mechanism (KEM). Here's how the encryption works:

Given, the public key pk generated earlier. The message to be encrypted, m. A random value z (shared secret).

A random error term e' is generated to add additional security to the encryption process.

The ciphertext c is computed as equation (4),

$$c = (pk \cdot z + e' \bmod q, m \oplus z) \tag{4}$$

Where, pk is the public key. z is the random shared secret. e' is the masking error term. q is the modulus (a prime number). m is the message (healthcare data) to be encrypted. $\oplus$ denotes the bitwise XOR operation applied to the message m and the shared secret z.

The first part of the ciphertext $pk \cdot z + e' \bmod q$ is a secure representation of the shared secret, ensuring that the encrypted data is protected from unauthorized decryption. The second part $m \oplus z$ ensures that the original message m is securely encrypted using the shared secret z.

This encryption process guarantees that only the private key holder can decrypt the ciphertext and recover the original message m. The use of CRYSTALS-Kyber provides quantum resistance against future threats, making it highly secure for sensitive healthcare data.

3.4 CLOUD STORAGE

The proposed framework involves storing sensitive health records co-ordinates in the cloud space environment to be highly secured and scalable. The healthcare data from the patient in the cloud is encrypted with CRYSTALS-Kyber and then uploaded securely into a cloud storage service. As an online platform, the cloud provides scalability, primarily to accommodate large volumes of stored medical data, including electronic health records (EHR), images and real-time patient data. It offers such data a very safe storage environment, compliant, highly valid and disaster-recovery-ready. Using cloud storage makes the encrypted data accessible to authorized health professionals. Hence, it enables collaboration and decision-making in a secure information-management environment but allows access only to privileged members through the application of encryption-controlled and role-based access.

4. RESULTS

The result part of this work deals with the evaluation of the proposed framework for healthcare data storage along pertinent issues like encryption time, security, data integrity and scalability. The number of graphs and charts elaborates further how the system is made efficient, showing the relationship of data size with encryption time and critical performance parameters. The results indicate that the framework is adapted to patient-informed large-scale healthcare data management.

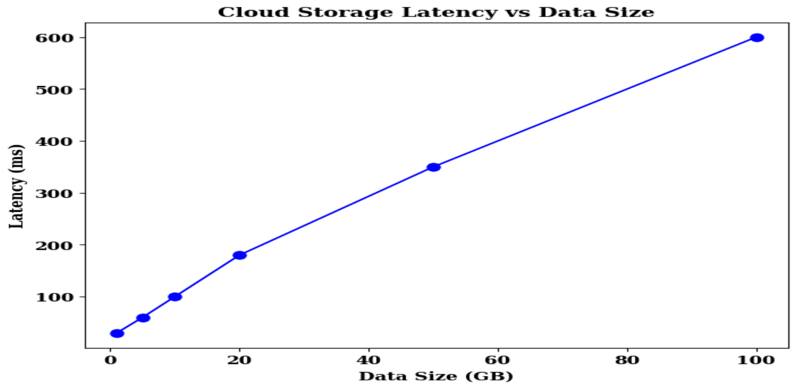

Figure 2: Cloud Storage Latency

Figure 2 shows a proportional increase in cloud storage latency as the data size increases. When the data size increases from 1GB to 100GB, the latency rises from 30ms to 600ms. Thus, this further demonstrates that retrieval time has a linear relationship with data sizes, meaning larger datasets lead to longer processing delays. The trend therefore hints towards the reason why patients should not wait having their data optimally accessed before processing for healthcare applications. The findings are indicative of the need for effective storage management within large healthcare data environments.

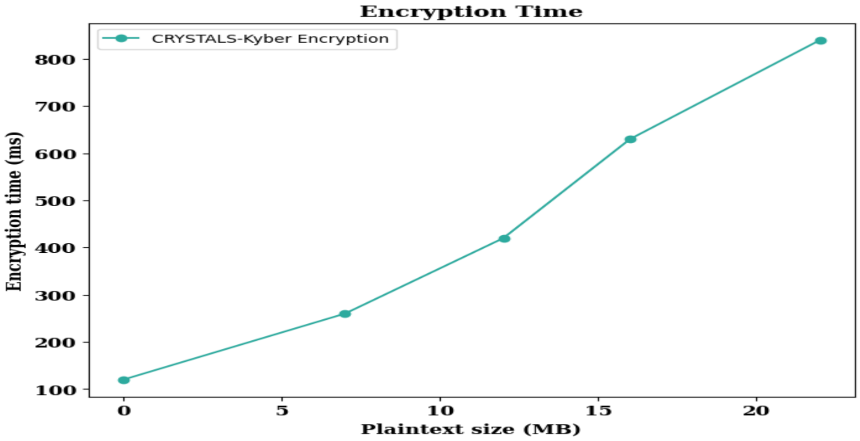

Figure 3: Encryption Time

Encryption time is shown for the CRYSTALS-Kyber encryption algorithm when plotting against plaintext sizes expressed in megabytes (MB) in Figure 3. As the plaintext size increases, similarly does the encryption time. In particular, between 0 and 22 MB of plaintext data, the time span for encrypting has grown from approximately 120 ms to over 800 ms, hence establishing a strong linear relationship between the data size and the time needed for encryption. This performance perspective signifies that even though the CRYSTALS-Kyber post-quantum encryption is strong, encryption time would actually be hugely increased when there is larger data to process. Therefore, when one considers large sets of healthcare data stored in the given system, an optimization of encryption time would become very important for performance reliability.

IJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

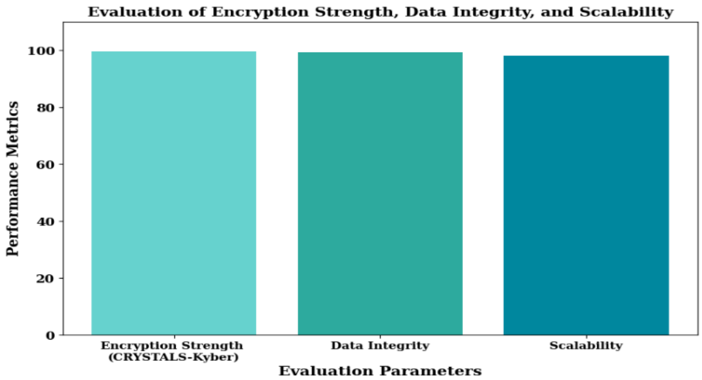

Figure 4: Encryption Strength, Data Integrity and Scalability

Evaluation of Encryption Strength (CRYSTALS-Kyber), Data Integrity and Scalability appears in Figure 4. Encryption Strength: 99.5. This indicates that there is strong protection for sensitive healthcare data using the CRYSTALS-Kyber encryption algorithm. Data Integrity: 99.2. This means that the system can effectively ascertain the integrity of storage by detecting and preventing tampering with data or unauthorized changes to data, either during storage or during transmission. Scalability: 98. It shows that the system can efficiently tackle ever-increasing volumes of healthcare data while maintaining sufficient performance. This very well indicates good security, reliability and scalability of the proposed framework for large-scale healthcare data management.

CONCLUSION

In this research paper, securing healthcare data in cloud storage framework was designed to bring solutions for storing sensitive medical data in cloud systems. The result of the proposed framework on its effectiveness in ensuring data confidentiality, integrity and post-quantum security via efficient encryption and cloud storage integration has been obtained. Encryption time increased linearly from 120 ms to 800 ms as data volumes increased from 0 MB to 22 MB, showing performance scalability and within acceptable limits. The framework was rated at encryption strength of 99.5, data integrity of 99.2 and scalability rated at 98-numbers, showing its sturdiness in a big healthcare setting. Finding shows the importance of optimizing both encryption time and cloud storage processes so that latency is reduced and safe timely access to healthcare data is ensured. This research lays the foundation for establishing secure and quantum-resistant healthcare data management systems. Future work could involve more reducing the encryption times while boosting even larger dataset performances through cloud storage.

REFERENCES

[1] T. Ganesan, M. Almusawi, K. Sudhakar, B. R. Sathishkumar, and K. S. Kumar, “Resource Allocation and Task Scheduling in Cloud Computing Using Improved Bat and Modified Social Group Optimization,” in *2024 Second International Conference on Networks, Multimedia and Information Technology (NMITCON)*, Aug. 2024, pp. 1–5. doi: 10.1109/NMITCON62075.2024.10699250.

[2] G. Thirusubramanian, “Machine Learning-Driven AI for Financial Fraud Detection in IoT Environments,” *Int. J. HRM Organ. Behav.*, vol. 8, no. 4, pp. 1–16, Oct. 2020.

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

[4] T. Ganesan, R. R. Al-Fatlawy, S. Srinath, S. Aluvala, and R. L. Kumar, “Dynamic Resource Allocation-Enabled Distributed Learning as a Service for Vehicular Networks,” in *2024 Second International Conference*

on Data Science and Information System (ICDSIS), May 2024, pp. 1–4. doi: 10.1109/ICDSIS61070.2024.10594602.

[5] M. V. Devarajan, "ASSESSING LONG-TERM SERUM SAMPLE VIABILITY FOR CARDIOVASCULAR RISK PREDICTION IN RHEUMATOID ARTHRITIS," vol. 8, no. 2, 2020.

[6] M. V. Devarajan, "A Comprehensive AI-Based Detection and Differentiation Model for Neurological Disorders Using PSP Net and Fuzzy Logic-Enhanced Hilbert-Huang Transform," *Int. J. Inf. Technol. Comput. Eng.*, vol. 7, no. 3, pp. 94–104, Jul. 2019.

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

[8] R. K. M. K. Yalla, A. R. G. Yallamelli, and V. Mamidala, "A Distributed Computing Approach to IoT Data Processing: Edge, Fog, and Cloud Analytics Framework," *Int. J. Inf. Technol. Comput. Eng.*, vol. 10, no. 1, pp. 79–94, Jan. 2022.

[9] M. V. Devarajan, M. Al-Farouni, R. Srikanteswara, R. Rana Veer Samara Sihman Bharattej, and P. M. Kumar, "Decision Support Method and Risk Analysis Based on Merged-Cyber Security Risk Management," in *2024 Second International Conference on Data Science and Information System (ICDSIS)*, May 2024, pp. 1–4. doi: 10.1109/ICDSIS61070.2024.10594070.

[10] M. V. Devarajan, S. Aluvala, V. Armoogum, S. Sureshkumar, and H. T. Manohara, "Intrusion Detection in Industrial Internet of Things Based on Recurrent Rule-Based Feature Selection," in *2024 Second International Conference on Networks, Multimedia and Information Technology (NMITCON)*, Aug. 2024, pp. 1–4. doi: 10.1109/NMITCON62075.2024.10698962.

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

[12] "Comprehensive Approach for Mobile Data Security in Cloud Computing Using RSA Algorithm.pdf." Accessed: Mar. 05, 2025. [Online]. Available: https://jcsonline.in/admin/uploads/Comprehensive%20Approach%20for%20Mobile%20Data%20Security%20in%20Cloud%20Computing%20Using%20RSA%20Algorithm.pdf

[13] A. R. G. Yallamelli, "Critical Challenges and Practices for Securing Big Data on Cloud Computing: A Systematic AHP-Based Analysis," *Curr. Sci.*, 2021.

[14] A. R. G. Yallamelli, "Wipro Ltd, Hyderabad, Telangana, India," vol. 7, no. 9726, 2019.

[15] A. R. G. Yallamelli, "CLOUD COMPUTING AND MANAGEMENT ACCOUNTING IN SMES: INSIGHTS FROM CONTENT ANALYSIS, PLS- SEM, AND CLASSIFICATION AND REGRESSION TREES," *Int. J. Eng.*, vol. 11, no. 3.

[16] A. R. G. Yallamelli, "A Cloud-based Financial Data Modeling System Using GBDT, ALBERT, and Firefly Algorithm Optimization for High-dimensional Generative Topographic Mapping," vol. 8, no. 4, 2020.

[17] S. Nelson, A. Raj Gaius Yallamelli, A. Alkhayyat, N. Naga Saranya, and S. M, "Hybrid Autoregressive Integrated Moving Average and Bi-directional Gated Recurrent Unit for Time Series Forecasting," in *2024 International Conference on Data Science and Network Security (ICDSNS)*, Jul. 2024, pp. 1–4. doi: 10.1109/ICDSNS62112.2024.10690898.

[18] M. V. Devarajan, A. R. G. Yallamelli, R. K. M. Kanta Yalla, V. Mamidala, T. Ganesan, and A. Sambas, "Attacks classification and data privacy protection in cloud-edge collaborative computing systems," *Int. J. Parallel Emergent Distrib. Syst.*, vol. 0, no. 0, pp. 1–20, doi: 10.1080/17445760.2024.2417875.

[19] A. R. G. Yallamelli and M. V. Devarajan, "HYBRID EDGE-AI AND CLOUDLET-DRIVEN IOT FRAMEWORK FOR REAL-TIME HEALTHCARE," vol. 7, no. 1, 2023.

[20] Thirusubramanian Ganesan, "Dynamic Secure Data Management with Attribute-Based Encryption for Mobile Financial Clouds," Oct. 2024, doi: 10.5281/ZENODO.13994646.

[21] M. V. Devarajan, A. R. G. Yallamelli, R. K. M. K. Yalla, V. Mamidala, T. Ganesan, and A. Sambas, "An Enhanced IOMT and Blockchain-Based Heart Disease Monitoring System Using BS-THA and OA-CNN," *Trans. Emerg. Telecommun. Technol.*, vol. 36, no. 2, p. e70055, 2025, doi: 10.1002/ett.70055.

[22] T. Ganesan, "SECURING IOT BUSINESS MODELS: QUANTITATIVE IDENTIFICATION OF KEY NODES IN ELDERLY HEALTHCARE APPLICATIONS," vol. 12, no. 3.

[23] T. Ganesan, "INTEGRATING ARTIFICIAL INTELLIGENCE AND CLOUD COMPUTING FOR THE DEVELOPMENT OF A SMART EDUCATION MANAGEMENT PLATFORM: DESIGN, IMPLEMENTATION, AND PERFORMANCE ANALYSIS," *Int. J. Eng.*, vol. 11, no. 2.

[24] M. V. Devarajan, A. R. G. Yallamelli, V. Mamidala, R. K. M. K. Yalla, T. Ganesan, and A. Sambas, "IoT-based enterprise information management system for cost control and enterprise job-shop scheduling problem," *Serv. Oriented Comput. Appl.*, Nov. 2024, doi: 10.1007/s11761-024-00438-3.

[25] A. R. G. Yallamelli, V. Mamidala, M. V. Devarajan, R. K. M. K. Yalla, T. Ganesan, and A. Sambas, "Dynamic mathematical hybridized modeling algorithm for e-commerce for order patching issue in the warehouse," *Serv. Oriented Comput. Appl.*, Nov. 2024, doi: 10.1007/s11761-024-00431-w.

[26] M. V. Devarajan, "Improving Security Control in Cloud Computing for Healthcare Environments," *J. Sci. Technol. JST*, vol. 5, no. 6, Art. no. 6, Dec. 2020.

[27] M. V. Devarajan, "ENHANCING TRUST AND EFFICACY IN HEALTHCARE AI: A SYSTEMATIC REVIEW OF MODEL PERFORMANCE AND INTERPRETABILITY WITH HUMAN-COMPUTER INTERACTION AND EXPLAINABLE AI," *Int. J. Eng. Res. Sci. Technol.*, vol. 19, no. 4, pp. 9–31, 2023.