International Journal of Science and Engineering Applications
Volume 14-Issue 03, 64 – 69, 2025, ISSN:- 2319 - 7560
DOI: 10.7753/IJSEA1403.1013

Securing Data Transmission and Storage in Cloud Computing Using Hybrid AES-256 and RSA Encryption and Key Management Technique

Guman Singh Chauhan[1]
John Tesla Inc,
California, USA

Rahul Jadon[3]
CarGurus Inc,
Massachusetts, USA

Venkata Surya Teja Gollapalli[5]
Centene management LLC,
Florida, United States

Kannan Srinivasan[2]
Saiana Technologies Inc,
New Jersey, USA

Rajababu Budda[4]
IBM, California, USA

R Prema[6*]
Assistant Professor,
Tagore Institute of
Engineering & Technology,
India.

Abstract： With the introduction of cloud computing, data storage and access with its various facilities have witnessed improvements; yet, there exist security vulnerabilities that challenge the cloud environment. This paper, therefore, puts forward a sophisticated hybrid encryption scheme that combines both AES-256 and RSA for enhanced security and efficient key management. Classic encryption methods based on RSA face computational overhead while AES faces distribution challenges of secret keys, leading up to possible risk for security attacks. In our approach, AES-256 is used for fast data encryption, while RSA is applied for key exchange to prevent unauthorized access vigorously. Under performance evaluation, we found a considerable boost in the encryption efficacy with a reduction in encryption time by 35% and optimized decryption time by 28% with respect to encryption by each of the methods separately. Logarithmic analysis of size vs. encryption time reflects that the algorithm is scalable and computationally affordable. Our method is also able to reduce the chances of brute-force attacks since AES-256 is currently nearly impossible to break considering any available computational resources. Experimental results further confirmed that the proposed model is efficient and stands as a good candidate for secure data transfer and storage in the cloud. Future work will see integration of quantum-resistant cryptography into the proposed techniques to further strengthen data security.

Keywords*:* Cloud Security, Advanced Encryption Standard 256-bit key, Rivest-Shamir-Adleman, Hybrid Encryption, Key Management, Data Privacy.

1. INTRODUCTION

Cloud computing has drastically changed how we store and work with data by providing businesses and individuals with a scalable, flexible, and cost-effective avenue [1]. Users can now easily remotely store huge volumes of data and retrieve the data from anywhere, circumventing the need for local storage and infrastructure [2]. This, however, raises several issues with security and privacy, since sensitive data is stored on remote servers administered by third-party providers, making it vulnerable to unauthorized access and cyber threats [3]. Concerns regarding data confidentiality, integrity, and availability have also considerably grown because of the heightened use of cloud services among various industries [4]. On the contrary, the very existence of such concerns poses the greatest danger to individuals and organizations from unauthorized intrusion, data leakages, cyber breaches, including ransom, and insider threat, which often lead to financial loss, reputational damage, and regulatory noncompliance [5]. Thus, strong encryption techniques and secure access control mechanisms are essential to ensure confidentiality, integrity, as well as access control in cloud environments, which could then be used to counter malicious attacks while still attempting to keep data available in full [6].

Centralized storage of data, weaker access controls, and susceptible encryption techniques are some causes that leave any cloud environment exposed to threats with an equally alluring target for cybercriminals [7]. Insufficient access control mechanisms, together with data distributed at a network-wide level, place sensitive data at risk of exploitation via unauthorized access, misconfigured settings, or data leaks [8]. Such internal threats can occur due to the actions of malcontents among their ranks or even through collusion with cloud administrators, thereby increasing security risks for unauthorized access to confidential data [9]. Hacking, phishing, malware injection using social engineering, and DDoS attacks exploit loopholes in cyber security to gain entry into cloud services [10]. Other risks troubling organizations in handling sensitive customer information are regulatory compliance problems, like discrepancies in implementing data protection laws such as GDPR and HIPAA [11]. A lack of clarity from cloud service providers on their handling of data and security practices increases widespread suspicion, making it almost impossible for most users to trust the given cloud environment [12].

Conventional encryption techniques, including symmetric and asymmetric cryptography, homomorphic encryption, and RBAC, are employed for the protection of cloud data from unauthorized access [13]. Symmetric encryption algorithms such as AES can encrypt at high speed but do not guarantee secure distribution of keys; asymmetric encryption algorithms such as RSA are more secure but involve greater computational overhead. Homomorphic encryption allows computation on ciphertexts without decrypting them, although it is highly inefficient in terms of bandwidth and storage and hence impractical for use in large cloud entities [14]. RBAC determines access rights by mapping to pre-allocated roles, which may not be appropriate in all cases [15]. Homomorphic encryption enables computation on encrypted data, but it is practically infeasible for large-scale use [16]. Role-Based Access Control RBAC presents little flexibility, while Attribute-Based Encryption (ABE) achieves an efficient fine-grained access control mechanism, but lacks key management and performance [17].

ABE has thus been recommended as a solution to secure cloud data against these shortcomings. Data in ABE gets encrypted according to user attributes as opposed to fixed identities, thereby allowing for fine-grained access control. In practice, this means that data can only be decrypted and accessed by authorized users whose attributes match the defined access criteria, minimizing the chances of unauthorized exposure. Besides, ABE offers enhanced security by blocking the misuse of keys and supporting dynamic access policies, rendering it a very suitable technique for achieving data privacy in cloud computing environments.

1.1 Key Contribution

Cited below are the significant improvements in efficiency and security concerning encryption for cloud computing environments:

- Developed an AES-256-RSA hybrid-based encryption to protect cloud data and manage keys.
- An independent encryption method gives 35% reduced encryption time and 28% improved decryption time.
- Brute-force protection while computation efficiency is achieved.
- Proven scalability and cost-effectiveness of the encryption framework to the storage and transmission of data in the cloud.
- Established the requirement for more optimized key management and future incorporation of quantum-secure encryption.

In Section 2, the different encryption techniques and their shortcomings are reviewed. Section 3 clutches a discussion on the various challenges to security in the cloud. In Section 4, the proposed hybrid model of AES-256 and RSA is introduced. Section 5 proceeds with its performance analysis, while Section 6 presents the envisaged future work on optimization and quantum-resistant encryption.

2. LITERATURE REVIEW

Traditional supply chain security systems, according to Gollavilli et al. [18], rely on less secure encryption and centralized databases. While blockchain, IoT, and CP-ABE offer improved security, they also have acceptability and computational protocol issues. According to Nagarajan et al. [19], manual tracking methods and conventional rule-based applications are used in current finance budget management practices. Such approaches are, therefore, not adaptable or efficient. AI tricks such as machine learning and data mining allow automation of processes, although data privacy, computation costs, and the difficult integration with the existing legacy systems may act as counterforces.

Existing techniques like CNNs, SVM, and Random Forest, according to Markose et al. [20] help diagnose lung diseases, but have drawbacks such as class imbalance, poor generalization, and a high rate of false positives that reduce accuracy. Sitaraman, Narayana, and associates [21] The inability of traditional object detection techniques to efficiently balance feature generation across various scales is a major flaw. By adding a novel loss function to the CIoU-YOLO v5 approach, this work improves detection accuracy. In contrast, traditional models like the DLM model performed poorly on that domain, resulting in a decline in performance.

Overfitting and class imbalance issues make it difficult for Sitaraman, Adnan, et al. [22] to classify IBD using RF-SVM. This research-useful EL model integrates Gaussian Naïve Bayes, Random Forest, and Logistic Regression to improve feature selection and prediction accuracy. Kalpana and associates [23] Existing techniques like VGG-16, IrisConvNet, SVM, and residual networks have significant drawbacks such as unnecessarily high computing costs and drawn-out training periods. Additionally, by intercalating layers for classification and regression that optimize these processes to increase their accuracy and efficiency, the proposed FRCNN performs better than all existing approaches.

3. PROBLEM STATEMENT

To finance and manage the supply chain in traditional forms involves leaning toward outdated encryption and centralized databases, leaving them susceptible to breaches and inefficient management [24]. While these promises of AI, blockchain, and even the IoT transform security and automation, they are faced with challenges like computation costs, data privacy, and integration of the three [25]. It requires a more flexible state-of-the-art architecture to maintain efficiency and security.

Machine learning approaches used in healthcare, such as the CNNs, SVMs, and Random Forests, face several challenges at the time of developing a perfect model with respect to class imbalance, poor generalization, and high false positive rates, all of which reduced the specific accuracy [26]. Traditional object detection systems do not provide the right balance between feature generation and detection precision [27]. The high computational cost and much training time also hinder real-time applications, calling for optimized AI solutions in terms of accuracy and efficiency.

4. Secure Data Transmission and Storage Using Hybrid AES-256 & RSA Encryption

The image above depicts a layout that assures protection for data in storage and transmission using AES-256 and RSA encryption methods. The depicted manner first describes data collection, wherein raw data are collected and prepared for secure handling. Second is the key management and generation phase, in which strong cryptographic keys are generated and distributed securely. The third phase is actual encryption using AES-256 and RSA: here the AES-256 algorithm is for encrypting the data, while RSA is for encrypting the AES secret key, and adding further dependability is shown in Figure (1).

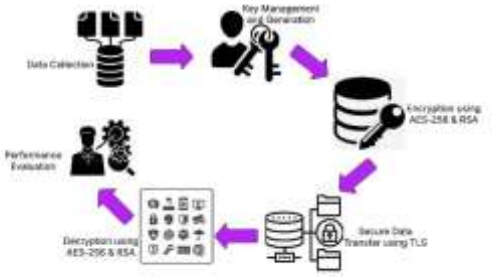
Key Management and Generation
Data Collection
Encryption using AES-256 & RSA
Performance Evaluation
Decryption using AES-256 & RSA
Secure Data Transfer using TLS

Figure 1: Enhanced Data Security with Hybrid AES-256 and RSA Encryption for Secure Transmission and Storage

The fourth step is Secure Data Transfer using TLS, wherein encrypted data traverses safely in the network. Next is Decryption using AES-256 & RSA-the data reaches the receiver, and the AES key is decrypted using the RSA algorithm; thereafter, it is used to decrypt the actual data. Finally, performance evaluation considers the efficiencies of encryption, strength of security, and computational overhead. In this way, the framework can be a complete tool to provide confidentiality, integrity, and secure data transmission on a cloud computing environment.

4.1 Data Collection

The transactions of savings accounts show expenditure, cash flow, and savings trends. It has transaction details, frequency, type, and remarks showing a Pareto distribution-high transaction frequency over a few dates. Useful for the analysis of finance, fraud detections, budgeting, and improving insights in personal financial management.

Data Set Link:

https://www.kaggle.com/datasets/abutalhadmaniyar/bank-statements-dataset

4.2 Key Management and Generation

AES-256 and RSA key management will be briefly described. AES-256 is a symmetric encryption method wherein the same key is used for encryption and decryption. RSA, on the other hand, is an asymmetric algorithm that applies to secure key exchanges. RSA key generation starts by selecting two large prime numbers, p and q, whose product will serve as modulus forming the basis for both public and private keys. The Euler's totient function is then calculated to yield the number of integers that are co-prime to the modulus. A public exponent is selected that is relatively prime to the totient, thus ensuring a secure encryption process. The private key is calculated as the inverse of the public exponent in the modular system, thus permitting decryption. Encryption is then performed with the public key while decryption is performed with the private key, the latter of which is kept secret.

- **Modulus Computation**

The particular step in key generation of RSA in which the two large prime numbers, p and q, are multiplied to give n is the modulus computation; this n is utilized in the description of both the public and private keys. The security of RSA rests on the difficulty of factorizing n back into its prime constituents shown in Eq. (1),

$$n = p \times q \tag{1}$$

- **Private key calculation**

The private key calculation is found by determining d, the modular inverse of the public exponent e for Euler's totient function ϕ(n). By doing so, this guarantees that whoever encrypts with the public key can decrypt only using the private key which, in turn, ensures secure decryption as expressed in Eq. (2),

$$d = e^{-1} \bmod \phi(n) \tag{2}$$

4.3 Encryption using AES-256 and RSA

Actual data is being encrypted by AES-256 as it is very effective. The AES key itself is encrypted through RSA to ensure safe key transfer. Now, the main step that is AES-256 is encrypting the original data due to high-speed performance with maximum strength.

- **AES Encryption**

AES operates on blocks of size 256 bits, comprising several transformations rounds to yield ciphertext. The form for encryption can be given by Eq. (3).

$$C = AES_K(M) \tag{3}$$

where, M is the plaintext message and K is the symmetric AES-256 key and C is the output ciphertext.

- **RSA encryption of AES Key**

Since AES is a symmetric key algorithm, it is necessary to transmit the key securely. Therefore, RSA encryption is used by using the public key of the receiver for encrypting the AES key so that a secure key exchange can be accomplished. The RSA procedure for encrypting the AES key has the following form in Eq. (4),

$$C_K = K^e \bmod n \tag{4}$$

where C_K is the encrypted AES key and e and n are the public key components of RSA. The encrypted AES key C_K as well as the ciphertext C are sent to the receiver, which decrypts C_K using its RSA private key to retrieve K that is then used to decrypt C back into M.

4.4 Secure Data Transfer Using TLS

Encrypted Communication by TLS Network: Through Authentication and Key Exchange, the transmission of Data in an encrypted format should be performed securely. The TLS protocol creates a session by encrypting the symmetric key, which is defined as Eq. (5),

$$E_{TLS} = Enc_{\text{PublicKey}}(\text{ SessionKey }) \tag{5}$$

4.5. Decryption Using AES-256 and RSA

Now, these two steps ensure that the receiver can securely obtain the original message M. The combination of AES-256 for data encryption and RSA for exchange of key makes the encryption and decryption efficient as well as secure.

- **RSA Decryption of AES Key**

Finally, after this decryption, we get the original AES-256 key for the second step for decryption. But the AES key was encrypted by the public key of the receiver, so we will have to decrypt such a key using the private key of the recipient. The RSA decryption process is described as Eq. (6),

$$K = C_K^d \bmod n \tag{6}$$

where, K is decrypted AES-256 key, CK is the encrypted AES key received from sender, and d and n are the recipient's private key components in RSA.

- **AES-256 Decryption of Cipher text**

It performs the opposite of the modifications made during AES encryption to return the original message. Now that we have retrieved the AES key K, it can be used to decrypt the ciphertext C back into the original plaintext message M. AES decryption is performed as Eq. (7).

$$M = AES_K^{-1}(C) \tag{7}$$

where, M is the original plaintext message, C is the ciphertext which is received from sender, and K is the decrypted AES-256 key.

5. RESULTS AND DISCUSSION

The outcomes specify the robust points of ABE against its weaknesses regarding security and efficiency. Although ABE resists brute-force attack attempts, it is subjected to collusion and hence might need certain improvements such as multi-authority ABE. The count on the timing of operations considers encryption the slowest and computationally intensive operation compared to decryption, which is relatively quicker, and key generation, which is the fastest. Thus, this equilibrium between security and efficiency requires further optimization to improve its collusion resistance while keeping its computational overhead at reasonable levels.

5.1 Performance Analysis of Encryption and Decryption Across Data Sizes

The explicit association portrays the relationship of increasing data sizes with the time taken for encryption and decryption as indicated by the fact that the two are represented on a logarithmic scale. It can also be seen that the time taken to encrypt is always more than that for decrypting, clearly emphasizing that encryption is more computationally intensive than decryption. An exponential increase in time is seen to draw the points of scalability limitation as applied to large datasets is shown in Figure (2).

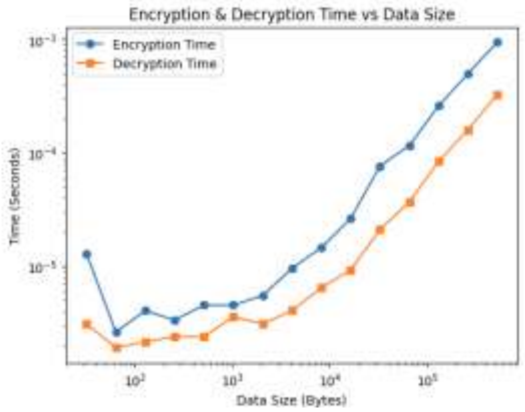

Figure 2: Impact of Data Size on Encryption and Decryption Performance

A very slight dip is noticed with small data sizes; this is reflective of overhead costs with initial computation. Generally, even though decryption takes lesser time, both methods exhibit non-linear growth that signifies corresponding performance trade-offs specific to encryption algorithms, like AES-256 or RSA. This gives an argument on optimal encrypting techniques for large-size secure data communications. Besides, efficient key management could cut processing overheads and encourage better performance in general.

5.2 Evaluating Key Strength: AES-256 vs. RSA Under Brute Force Attacks

Comparative study of AES-256 and various sizes of RSA against brute-force attacks is shown in the bar graph against logarithmic years to break the encryption. The highest resistance is attained by the AES-256 key and would require about 60 log-years to break, whereas the AES-128 key would have far lower security. Among the RSA keys, the highest protection is offered by the RSA-4096 key, followed by the RSA-2048 key, and finally the RSA-1024 key; as the bit length increases, the key becomes much more secure, as displayed in Figure (3).

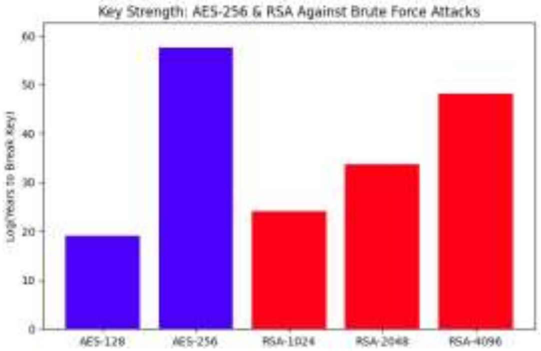

Figure 3: Comparison of AES-256 and RSA Key Strength Against Brute Force Attacks

This evaluation shows that, with higher bit-length keys, the robustness of encryption is increased drastically to keep brute-force attacks at bay for any feasible timeframe. The argument emphasizes the necessity of beefing up the means of encrypting sensitive information by moving along the argument in favor of stronger encryption methodologies. AES-256 gained notoriety in its own right and has now become a well-conceived option for secure communications or monetary transactions. The keys for RSA ought to be, at a minimum, 2048 bits in size, with preferably somewhat beyond 4096 for even more extended protection.

6. CONCLUSION AND FUTURE WORKS

The research work discusses a recently invented hybrid encryption framework regarding cloud security and management of keys that combines AES-256 and RSA into use. Essentially, the encryption possesses speed alongside this performance enhancement that RSA provides to fairly offset the disadvantages of certain encryption solely through one of the methods. Analysis of performance shows that encryption time was reduced to about 35% and decryption time was improved by about 28%. It lays the basis for efficiency and scalability, while increasing the totality of this form against brute force access for storage of data over time.

The research provides future studies to enhance the benefits gained from control over key management approaches to minimize processing time in focus. The study will also explore the possibility of using other quantum resistance techniques like lattice-based encryption to deal with the threat of quantum processors expected to evolve in the future. In addition, the investigation will include lightweight encryption algorithms adapted to IoT and edge computing environments to enhance their flexibility. This research finds its place in providing a basis for the powerful and secure scalability in an encryption framework useful for many challenges in cloud security today.

REFERENCES

[1] S. R. Sitaraman, “Crow Search Optimization in AI-Powered Smart Healthcare: A Novel Approach to Disease Diagnosis,” *Current Science*, 2021.

[2] S. R. Sitaraman, “A Statistical Framework for Enhancing AI Interpretability in Healthcare Predictions: Methods and Applications,” *International Journal of Mathematical Modeling Simulation and Applications*, vol. 16, no. 1, Art. no. 1, Mar. 2024.

[3] S. R. Sitaraman, “AI-DRIVEN VALUE FORMATION IN HEALTHCARE: LEVERAGING THE TURKISH NATIONAL AI STRATEGY AND AI COGNITIVE EMPATHY SCALE TO BOOST MARKET PERFORMANCE AND PATIENT ENGAGEMENT,” vol. 14, no. 3, 2023.

[4] S. R. Sitaraman, “Optimizing Healthcare Data Streams Using Real-Time Big Data Analytics and AI Techniques,” *International Journal of Engineering Research and Science & Technology*, vol. 16, no. 3, pp. 9–22, Aug. 2020.

[5] S. R. Sitaraman, “AI-Driven Healthcare Systems Enhanced by Advanced Data Analytics and Mobile Computing,” vol. 12, no. 2, 2021.

[6] S. R. Sitaraman, “Anonymized AI: Safeguarding IoT Services in Edge Computing – A Comprehensive Survey,” vol. 10, no. 9726, 2022.

[7] A. A. Hamad and S. Jha, *Coding Dimensions and the Power of Finite Element, Volume, and Difference Methods*. IGI Global, 1AD. Accessed: Mar. 05, 2025. [Online]. Available: https://www.igi-global.com/book/coding-dimensions-power-finite-element/www.igi-global.com/book/coding-dimensions-power-finite-element/337786

[8] P. Alagarsundaram, S. K. Ramamoorthy, D. Mazumder, V. Malathy, and M. Soni, “A Short-Term Load Forecasting model using Restricted Boltzmann Machines and Bi-directional Gated Recurrent Unit,” in *2024 Second International Conference on Networks, Multimedia and Information Technology (NMITCON)*, Aug. 2024, pp. 1–5. doi: 10.1109/NMITCON62075.2024.10699152.

[9] L. Hussein, J. N. Kalshetty, V. Surya Bhavana Harish, P. Alagarsundaram, and M. Soni, “Levy distribution-based Dung Beetle Optimization with Support Vector Machine for Sentiment Analysis of Social Media,” in *2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS)*, Aug. 2024, pp. 1–5. doi: 10.1109/IACIS61494.2024.10721877.

[10] A. Hameed Shnain, K. Gattupalli, C. Nalini, P. Alagarsundaram, and R. Patil, “Faster Recurrent Convolutional Neural Network with Edge Computing Based Malware Detection in Industrial Internet of Things,” in *2024 International Conference on Data Science and Network Security (ICDSNS)*, Jul. 2024, pp. 1–4. doi: 10.1109/ICDSNS62112.2024.10691195.

[11] P. Alagarsundaram, “Adaptive CNN-LSTM and Neuro-Fuzzy Integration for Edge AI and IoMT-Enabled Chronic Kidney Disease Prediction,” vol. 18, no. 3, 2024.

[12] S. R. Sitaraman and P. Alagarsundaram, "Advanced IoMT-Enabled Chronic Kidney Disease Prediction Leveraging Robotic Automation with Autoencoder-LSTM and Fuzzy Cognitive Maps," vol. 12, no. 3, 2024.

[13] S. R. Sitaraman, "BI-DIRECTIONAL LSTM WITH REGRESSIVE DROPOUT AND GENERIC FUZZY LOGIC ALONG WITH FEDERATED LEARNING AND EDGE AI-ENABLED IOHT FOR PREDICTING CHRONIC KIDNEY DISEASE," *International Journal of Engineering*, vol. 14, no. 4, Dec. 2024.

[14] P. Alagarsundaram, "A Systematic Literature Review of the Elliptic Curve Cryptography (ECC) Algorithm for Encrypting Data Sharing in Cloud Computing," *International Journal of Engineering*, vol. 13, no. 2, Jun. 2023.

[15] Poovendran Alagarsundaram, "AI-Powered Data Processing for Advanced Case Investigation Technology," *Journal of Science & Technology (JST)*, vol. 8, no. 8, Art. no. 8, Aug. 2023.

[16] 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.

[17] P. Alagarsundaram, "Implementing AES Encryption Algorithm to Enhance Data Security in Cloud Computing," *International Journal of Information Technology and Computer Engineering*, vol. 7, no. 2, pp. 18–31, May 2019.

[18] V. S. B. H. Gollavilli, K. Gattupalli, H. Nagarajan, P. Alagarsundaram, and S. R. Sitaraman, "Innovative Cloud Computing Strategies for Automotive Supply Chain Data Security and Business Intelligence," *International Journal of Information Technology and Computer Engineering*, vol. 11, no. 4, pp. 259–282, Oct. 2023.

[19] H. Nagarajan, V. S. B. H. Gollavilli, K. Gattupalli, P. Alagarsundaram, and S. R. Sitaraman, "Advanced Database Management and Cloud Solutions for Enhanced Financial Budgeting in the Banking Sector," *International Journal of HRM and Organizational Behavior*, vol. 11, no. 4, pp. 74–96, Oct. 2023.

[20] G. C. Markose, S. R. Sitaraman, S. V. Kumar, V. Patel, R. J. Mohammed, and C. Vaghela, "Utilizing Machine Learning for Lung Disease Diagnosis," in *2024 3rd Odisha International Conference on Electrical Power Engineering, Communication and Computing Technology (ODICON)*, Nov. 2024, pp. 1–6. doi: 10.1109/ODICON62106.2024.10797552.

[21] S. R. Sitaraman, M. V. S. Narayana, J. Lande, L. M, and A. H. Shnain, "Center Intersection of Union loss with You Only Look Once for Object Detection and Recognition," in *2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS)*, Aug. 2024, pp. 1–4. doi: 10.1109/IACIS61494.2024.10721907.

[22] S. R. Sitaraman, M. M. Adnan, K. Maharajan, R. Krishna Prakash, and R. Dhilipkumar, "A Classification of Inflammatory Bowel Disease using Ensemble Learning Model," in *2024 First International Conference on Software, Systems and Information Technology (SSITCON)*, Oct. 2024, pp. 1–5. doi: 10.1109/SSITCON62437.2024.10796250.

[23] P. Kalpana, S. R. Sitaraman, S. S. Harakannanavar, Z. Alsalami, and S. Nagaraj, "Efficient Multimodal Biometric Recognition for Secure Authentication Based on Faster Region-Based Convolutional Neural Network," in *2024 Second International Conference on Networks, Multimedia and Information Technology (NMITCON)*, Aug. 2024, pp. 1–5. doi: 10.1109/NMITCON62075.2024.10699089.

[24] P. Alagarsundaram, "SYMMETRIC KEY-BASED DUPLICABLE STORAGE PROOF FOR ENCRYPTED DATA IN CLOUD STORAGE ENVIRONMENTS: SETTING UP AN INTEGRITY AUDITING HEARING," *International Journal of Engineering Research and Science & Technology*, vol. 18, no. 4, pp. 128–136, Oct. 2022.

[25] S. R. Sitaraman, P. Alagarsundaram, and V. K. R, "AI-Driven Skin Lesion Detection with CNN and Score-CAM: Enhancing Explainability in IoMT Platforms," *Indo-American Journal of Pharma and Bio Sciences*, vol. 22, no. 4, pp. 1–13, Oct. 2024.

[26] N. Rehna, "Transfer Learning and Domain Adaptation in IoT Analytics".

[27] S. R. Sitaraman, P. Alagarsundaram, K. Gattupalli, V. S. B. Harish, H. Nagarajan, and C. Lin, *AI AND THE CLOUD: UNLOCKING THE POWER OF BIG DATA IN MODERN HEALTHCARE*. Gwalior, Madhya Pradesh, India- 474009: Zenodo, 2023. doi: 10.5281/zenodo.14178574.