https://doi.org/10.46335/IJIES.2025.10.3.8 **e-ISSN: 2456-3463**
Vol. 10, No. 3, 2025, PP. 33-39

International Journal of Innovations in Engineering and Science, www.ijies.net

Searchable and Secure Data Sharing in E-Healthcare Using Proxy Re-Encryption

Rahul Manohar Patil[1], Tejashree D. Suryawanshi[2], Manish Madhukar Patil[3]

[1]Associate Professor and Head, Department of Electronics and Telecommunication Engineering
NES's Gangamai College of Engineering. Nagaon, Dhule (Maharashtra), India
[2] M.E. Student Gangamai college of Engineering, Nagaon, Dhule (Maharashtra), India
[3]Associate Professor, Department of Electronics and Telecommunication Engineering
NES's Gangamai College of Engineering. Nagaon, Dhule (Maharashtra), India

Email of corresponding Author: ***rahuletc.gcoe@gmail.com***

Received on: 19 April, 2025 *Revised on: 12 May ,2025* *Published on: 14 May,2025*

Abstract – *In modern e-healthcare ecosystems, patients frequently share their sensitive Personal Healthcare Records (PHRs) with healthcare providers via cloud platforms to ensure real-time access and effective treatment. However, outsourcing such critical data to third-party cloud servers poses significant challenges concerning privacy, data security, and controlled access. To address these issues, this paper implements and evaluates the DSAS (Data Sharing and Authorized Searchable) framework—an advanced cryptographic system that combines Searchable Encryption (SE) with Conditional Proxy Re-Encryption (CPRE). The framework enables fine-grained access delegation, efficient encrypted keyword-based search, and proxy-invisible re-encryption, ensuring data confidentiality even in untrusted cloud environments. Experimental evaluation demonstrates that the proposed approach achieves superior security features such as proxy invisibility, condition hiding, and collusion resistance, while maintaining computational efficiency suitable for resource-constrained devices. This research substantiates DSAS as a practical and scalable solution for secure data sharing in cloud-based e-healthcare systems.*

Keywords *Searchable Encryption, Conditional Proxy Re-Encryption, Cloud Security, Personal Health Records (PHRs), e-Healthcare, Data Privacy, Keyword Search, Proxy Invisibility*

INTRODUCTION

The integration of cloud computing and mobile sensor technologies has significantly transformed healthcare delivery, enabling real-time patient monitoring, teleconsultation, and data-driven diagnosis. Modern e-healthcare systems leverage wearable devices, mobile applications, and cloud platforms to collect and store vast volumes of patient data—collectively termed Personal Heacords (PHRs). These data repositories empower physicians and researchers to analyze patient health conditions, formulate treatment plans, and perform medical research. However, the remote storage of PHRs on third-party cloud servers introduces critical concerns related to data privacy, secure access control, and efficient search capabilities. Traditional encryption techniques, while effective in preserving data confidentiality, create obstacles for usability—particularly in scenarios that require keyword-based data retrieval or access delegation. In dynamic healthcare environments, authorized professionals such as substitute doctors or external researchers may require timely access to specific subsets of a patient's encrypted medical data. Ensuring access while safeguarding privacy, preventing misuse, and sustaining performance is a complex challenge in data sharing.

To address these challenges, this research adopts the DSAS (Data Sharing and Authorized Searchable)

https://doi.org/10.46335/IJIES.2025.10.3.8 e-ISSN: 2456-3463
Vol. 10, No. 3, 2025, PP. 33-39

framework. DSAS integrates Searchable Encryption (SE) to support efficient encrypted keyword searches and Conditional Proxy Re-Encryption (CPRE) to enable secure delegation of access rights under predefined conditions. Furthermore, DSAS introduces robust security mechanisms such as proxy invisibility, condition hiding, and collusion resistance— critical features for protecting sensitive healthcare data in untrusted environments.

This paper presents the design, implementation, and performance evaluation of the DSAS framework in a simulated e-healthcare environment. The results demonstrate that DSAS not only enhances privacy and access control but also supports practical deployment through efficient cryptographic operations. This work contributes a robust foundation for building secure, scalable, and patient-centric data-sharing platforms in e-healthcare.

RELATED WORK

The rising adoption of cloud computing in e-healthcare environments has created a paradigm shift in how medical data is stored, accessed, and utilized. However, the inherent risks associated with outsourcing Personal Healthcare Records (PHRs) to third-party cloud platforms—such as unauthorized access and privacy breaches—have led researchers to explore advanced cryptographic mechanisms that can ensure both security and usability.

Searchable Encryption (SE)

Searchable Encryption allows users to perform keyword-based search operations over encrypted data without needing to decrypt the entire dataset. The concept was pioneered by Boneh et al. [1], who proposed the Public Key Encryption with Keyword Search (PEKS) scheme, enabling keyword queries in a public-key encrypted environment. Abdalla et al. [2] extended this idea by introducing consistency notions, ensuring deterministic search results across encrypted datasets. Later, Baek et al. [3] improved practicality by eliminating the need for secure channels between the user and the server.

In the e-healthcare context, Yang et al. [4] designed a privacy-preserving cloud storage system using SE that enables secure keyword searches without revealing sensitive data. Yasnoff [5] proposed decentralized healthcare storage architecture to mitigate the risk of data breaches in centralized repositories.

Proxy Re-Encryption (PRE)

Proxy Re-Encryption (PRE) facilitates secure delegation of decryption rights from one user to another without exposing the plaintext to intermediaries. The foundational PRE scheme was proposed by Blaze et al. [6], followed by a unidirectional variant introduced by Ateniese et al. [7], which prevents the proxy from reversing the re-encryption operation. Green and Ateniese[8] further extended the model by incorporating identity-based cryptographic primitives, enhancing security against chosen ciphertext attacks.

Conditional Proxy Re-Encryption (CPRE)

To overcome the overly permissive access granted by PRE, Conditional Proxy Re-Encryption (CPRE) was introduced. Seo et al. [9] proposed the first proxy-invisible CPRE scheme where ciphertexts re-encrypted under certain conditions were indistinguishable from original encryptions. Fang et al. [10, 11] introduced fuzzy CPRE schemes that enabled flexible access policies based on overlapping attribute sets. However, most of these schemes revealed the embedded conditions to the proxy, thus compromising patient privacy.

Proxy Searchable Re-Encryption (PRES)

To unify search and delegation, Shao et al. [13] proposed Proxy Searchable Re-Encryption (PRES), where both keyword search and decryption rights can be securely delegated. However, this approach lacked condition hiding and proxy invisibility. Weng et al. [14, 15] addressed this limitation by binding re-encryption keys to specific access conditions, but they too failed to guarantee complete privacy of the embedded conditions.

Privacy-Preserving E-Healthcare Systems

Recent works such as Fu et al. [16] combined fog and cloud architectures to enable secure and efficient search across distributed medical datasets. While such systems offer enhanced performance, they often fall short in terms of fine-grained access control and collusion resistance. Bhatia et al. [18,19] proposed certificateless proxy re-encryption schemes tailored for mobile healthcare, although they did not fully achieve condition-hiding or proxy-invisible capabilities. Yang and Ma [12] presented a CPRE model that supports both condition hiding and keyword search but suffered from high computational overhead.

https://doi.org/10.46335/IJIES.2025.10.3.8 **e-ISSN: 2456-3463**
Vol. 10, No. 3, 2025, PP. 33-39

International Journal of Innovations in Engineering and Science, www.ijies.net

Collectively, these studies indicate that no single system simultaneously offers proxy invisibility, condition hiding, CCA-security, and efficient keyword search—an essential combination for scalable and secure e-healthcare platforms. The DSAS framework aims to bridge this gap by integrating SE and CPRE with enhanced cryptographic techniques.

PROPOSED SYSTEM

The proposed system is based on the DSAS (Data Sharing and Authorized Searchable) framework, which integrates advanced cryptographic mechanisms to facilitate secure data sharing and keyword-based search over encrypted medical records in e-healthcare systems. It addresses core challenges such as unauthorized access, inefficient retrieval, collusion risk, and lack of fine-grained access control in cloud-based Personal Healthcare Record (PHR) management.

System Architecture and Entities

The architecture of DSAS comprises four major entities: the patient, the doctor-in-charge (Alice), a delegate doctor (Bob), and the cloud server. Patients are responsible for collecting personal healthcare data through wearable sensors or mobile health applications. Before uploading to the cloud, these records are encrypted using the doctor's public key to ensure privacy. The doctor-in-charge acts as the primary healthcare provider who can access the full dataset. When necessary, she can delegate partial access rights to another healthcare professional (Bob) without revealing the content or compromising the integrity of the original data. The cloud server, while responsible for storing and searching encrypted data, operates in a semi-trusted model — it follows protocols but may attempt to infer private data.

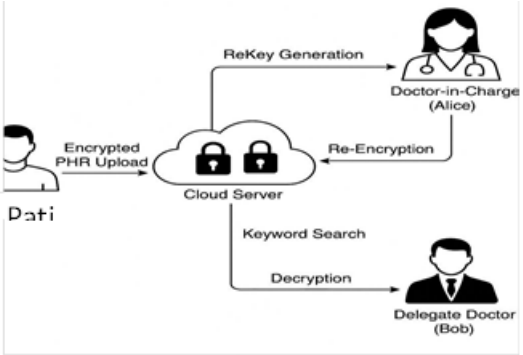

Fig. 1 System Architecture

System Workflow

The DSAS framework operates through four sequential phases: system setup, data encryption, conditional delegation with re-encryption, and secure data retrieval via keyword search.

In the setup phase, a security parameter (λ) is initialized, and each participant generates their cryptographic public-private key pairs. A global public parameter set is also shared among all entities, enabling consistent encryption and re-encryption operations.

During the data collection and encryption phase, the patient's device continuously generates health data. Each data record is encrypted using the public key of the doctor-in-charge. Simultaneously, important keywords (e.g., medical conditions, test results) are extracted from the data and encrypted using a searchable encryption algorithm to create secure indices. These encrypted PHRs and indices are uploaded to the cloud server for storage, ensuring that no plaintext is visible to the server.

The delegation and re-encryption phase enable temporary access delegation without exposing the original decryption key. If the doctor-in-charge becomes unavailable, she generates a conditional proxy re-encryption key using her private key, the delegate's public key, and an access condition (e.g., data related only to "pneumonia"). This re-encryption key is sent to the cloud server, which uses it to transform only the cipher texts matching the condition. The cloud, however, remains unaware of the access condition due to the system's condition-hiding property. Furthermore, the framework ensures proxy invisibility—making it impossible for external observers or attackers to distinguish between original and re-encrypted cipher texts.

In the final retrieval and search phase, the delegate doctor generates a trapdoor (i.e., a search token) for a specific keyword using his private key. The cloud server uses this token to perform a secure search over the encrypted indices and returns matching cipher texts. The delegate then decrypts the authorized records using his private key. Importantly, only the data satisfying the delegation condition are accessible, preventing unauthorized access even in case of collusion between the server and the delegate.

https://doi.org/10.46335/IJIES.2025.10.3.8 e-ISSN: 2456-3463
Vol. 10, No. 3, 2025, PP. 33-39

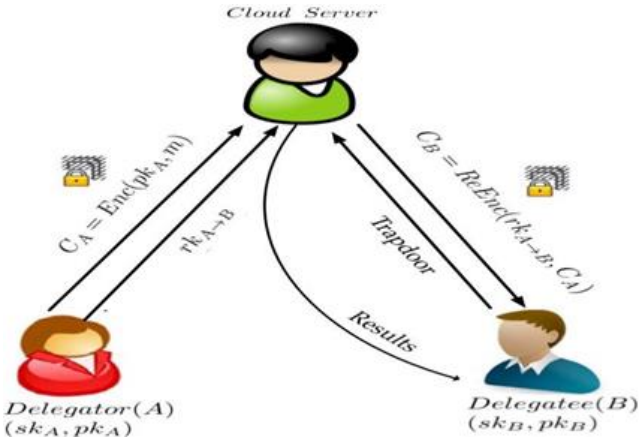

Fig. 2 System Model

Cryptographic Framework

DSAS employs a combination of pairing-based cryptographic algorithms to implement secure functionalities. These include system initialization (Setup), key generation (KeyGen), data encryption (Enc), conditional re-encryption key generation (ReKeyGen), cipher text transformation (ReEnc), trapdoor generation (Trapdoor), keyword search (Test), and final decryption (Dec). Each function operates efficiently, even on resource-constrained platforms like Raspberry Pi, ensuring the framework's suitability for real-world deployment.

Example Scenario

To illustrate the system in practice, consider a patient uploading encrypted medical records that include details of multiple conditions. These records are encrypted under Alice's public key and stored on the cloud. Before going on leave, Alice delegate's access to Bob, a colleague, by generating a re-encryption key conditioned on the keyword "pneumonia." The cloud re- encrypts only those records that meet this condition and enables Bob to search using a secure trapdoor. Bob is able to retrieve and decrypt only the relevant data while remaining blind to other unrelated information, and the cloud server remains unaware of the access context.

Algorithm Implementation

Algorithm 1: Secure PHR Sharing and Retrieval using DSAS Framework

Input:

PHR m, keyword w, Patient's private key skP, Doctor Alice's public key pkA, Delegate Doctor Bob's public key pkB, Condition c (e.g., disease name)

Output:

Encrypted PHR CT uploaded to cloud, re-encrypted CT' accessible to Bob

Step 1: Setup

- Generate key pairs (pkP, skP), (pkA, skA), (pkB, skB)
- Initialize global parameters param ← Setup(λ)

Step 2: Encryption by Patient

- Extract keyword w from PHR m
- CT ← Enc(pkA, m, w)
- Upload (CT, index(w)) to Cloud Server

Step 3: Delegation by Doctor Alice

- Alice selects condition c (e.g., "pneumonia")
- rk ← ReKeyGen(skA, pkB, c)
- Send rk to Cloud Server

Step 4: Proxy Re-Encryption by Cloud

- If keyword in CT matches condition c: CT' ← ReEnc(rk, CT)

Step 5: Keyword Search by Bob

- tw ← Trapdoor(skB, w)

- If Test(CT', tw) == 1:
  m' ← Dec(skB, CT')
-Else:
  return "No Access"

Return: Decrypted record m' accessible only if keyword & condition match

Once access has been conditionally delegated, the delegate doctor performs a secure search and decryption operation using the trapdoor mechanism. Algorithm 2 outlines this process, showing how trapdoors are generated, tested against encrypted indices, and used for decrypting relevant PHRs.

Algorithm 2: Trapdoor Generation, Keyword Matching, and Decryption in DSAS

Input:

https://doi.org/10.46335/IJIES.2025.10.3.8 e-ISSN: 2456-3463
Vol. 10, No. 3, 2025, PP. 33-39

Keyword w, Delegate Doctor Bob's private key skB, Re-encrypted ciphertext CT', Cloud Server, Search index

Output:

Decrypted PHR m' if search condition is matched

Step 1: Trapdoor Generation

- Bob selects search keyword w
- tw ← Trapdoor(skB, w)

Step 2: Keyword Matching at Cloud

- Cloud receives trapdoor tw
- For each encrypted index in cloud:

If Test (CT', tw) == 1:

Return CT' to Bob

Else:

Skip to next record

Step 3: Decryption by Bob

- Upon receiving CT' from cloud:

m' ← Dec(skB, CT')

- If m' is valid:

Return m'

- Else:

Return "Unauthorized or No Match"

Return: Retrieved PHR record m' if condition and keyword are satisfied

RESULTS AND PERFORMANCE EVALUATION

This section presents experimental results.

Experimental Setup

To evaluate the practicality and efficiency of the DSAS framework, a simulated cloud-based e-healthcare environment was created. The implementation focused on validating security features, computation cost, and operational feasibility under realistic conditions.

The hardware setup consisted of a personal computer acting as a cloud server, equipped with an Intel Core i5-8250U processor, 8 GB RAM, and Windows 11. The system employed bilinear pairing-based cryptography using the PBC library and Type A pairing curves.

Security Analysis

The DSAS framework was evaluated against standard security properties critical for e- healthcare systems:

• **Data Privacy:** All PHRs are encrypted using public-key cryptography before being uploaded to the cloud. Since the decryption keys are never shared with the cloud, the data remains confidential even in case of server compromise.

• **Proxy Invisibility:** The cloud server cannot distinguish between original and re- encrypted ciphertexts. This protects the availability status of the delegator (Doctor Alice) and prevents inference attacks.

• **Condition Hiding**: Sensitive medical conditions embedded as delegation criteria (e.g., "HIV", "Cancer") are not visible to the proxy or unauthorized users.

• **Collusion Resistance:** Even if the cloud server colludes with the delegate doctor, they cannot derive the delegator's private key or decrypt unauthorized data.

• **CCA Security:** The framework is secure against chosen ciphertext attacks, ensuring robustness even under active attack scenarios.

Performance Evaluation

Performance was measured across multiple cryptographic operations and compared with baseline schemes like FSGW and YM.

Table 1. - Performance Evaluation

Operation	DSAS	FSGW	YM
Key Generation	2 Exponentiations	4 Exp	1 Exp
Encryption + Index Encryption	5 G + 2 GT Ops	3 G + 2 GT	3 G + 1 GT
ReKey Generation	1 G + 2 GT	4 G	2 G
Re-Encryption	3 Pairings	5 Pairings	2 Pairings
Trapdoor Generation	1 G Op	2 G	1 G
Keyword Search (Test)	1 Pairing	2 Pairings	1 Pairing
Decryption	1 Pairing	1 Pairing	1 Pairing

Note: G = Group operation; GT = Target group operation; Exp = Exponentiation

Graphical Analysis

https://doi.org/10.46335/IJIES.2025.10.3.8 **e-ISSN: 2456-3463**
Vol. 10, No. 3, 2025, PP. 33-39

International Journal of Innovations in Engineering and Science, www.ijies.net

Graphical plots were generated to illustrate the computational overhead of different operations. DSAS demonstrated near-linear scalability and outperformed FSGW in both encryption and re-encryption phases while offering stronger privacy guarantees.

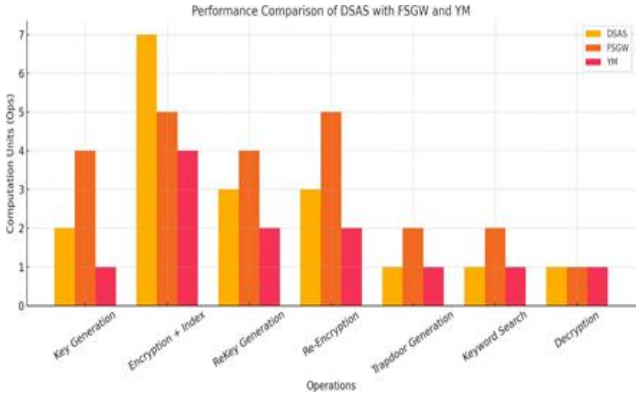

Fig. 3: Performance Comparison of DSAS with FSGW and YM

Figure 3 illustrates the computational efficiency of DSAS compared to two existing frameworks, FSGW and YM, across various cryptographic operations. DSAS requires fewer group operations and pairings for key generation, re-encryption, and keyword search, showcasing its lightweight design. While FSGW and YM impose higher computational loads for encryption and re-key generation, DSAS maintains a more balanced and optimized overhead. This validates DSAS as a secure yet computationally efficient solution suitable for real-time healthcare applications, particularly on resource-constrained devices.

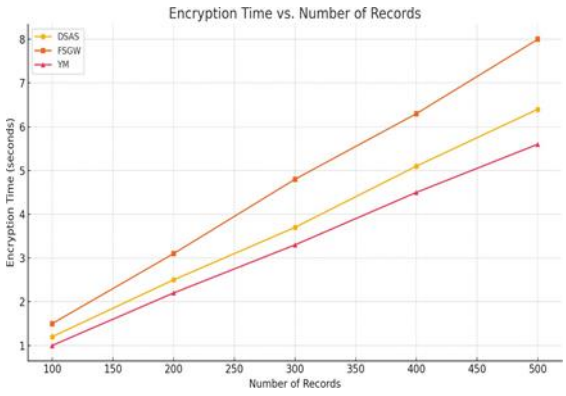

Figure 4 presents the encryption time as a function of the number of records for DSAS, FSGW, and YM. As the dataset size increases, DSAS consistently demonstrates lower encryption latency compared to FSGW and only slightly higher than YM. The nearly linear growth curve of DSAS highlights its scalability and efficiency in handling large volumes of encrypted Personal Healthcare Records (PHRs), confirming its applicability in real-world e-healthcare systems that demand both security and speed.

CONCLUSION

This study implemented the DSAS framework to enable secure and efficient sharing of encrypted Personal Healthcare Records (PHRs) in cloud-based e-healthcare systems. By combining searchable encryption with conditional proxy re-encryption, DSAS ensures fine-grained access control, keyword-based search, and data privacy. Experimental results confirm that DSAS offers lower computational overhead than existing schemes like FSGW and YM while providing enhanced security features such as proxy invisibility and condition hiding.

Future enhancements may include integrating blockchain for transparent access logging and attribute-based encryption for more flexible policy enforcement. The framework can also be extended to support edge computing in IoMT devices and optimized search performance using intelligent indexing mechanisms.

REFERENCES

[1] *D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Proc. EUROCRYPT, 2004, pp. 506–522.*

[2] *M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Paillier, and H. Shi, "Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions," in Proc. CRYPTO, 2005, pp. 205–222.*

[3] *J. Baek, R. Safavi-Naini, and W. Susilo, "Public key encryption with keyword search revisited," in Proc. Comput. Secur. ESORICS, 2008, pp. 124–139.*

[4] *K. Yang, X. Jia, and K. Ren, "Secure and verifiable policy update outsourcing for big data access control in the cloud," IEEE Trans. Parallel Distrib. Syst., vol. 26, no. 12, pp. 3461–3470, Dec. 2015.*

[5] *W. A. Yasnoff, "Privacy issues in shared electronic health records," Health Informatics J., vol. 11, no. 4, pp. 291–300, Dec. 2005.*

[6] *M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in Proc. EUROCRYPT, 1998, pp. 127–144.*

[7] *G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," ACM Trans. Inf. Syst. Secur., vol. 9, no. 1, pp. 1–30, Feb. 2006.*

[8] *M. Green and G. Ateniese, "Identity-based proxy re-encryption," in Proc. ACNS, 2007, pp. 288–306.*

[9] *S. Seo, M. Nabeel, S. Bertino, and H. Hong, "Privacy-preserving proxy re-encryption by partially hiding re-encryption policies," in Proc. ICDE, 2013, pp. 144–155.*

[10] *J. Fang, H. Liu, Y. Zhang, and H. Tian, "Fuzzy identity-based proxy re-encryption with keyword search," Soft Comput., vol. 20, no. 8, pp. 3135–3146, 2016.*

[11] *J. Fang, H. Liu, H. Tian, and L. Wang, "Anonymous conditional proxy re-encryption with keyword search," Soft Comput., vol. 18, no. 12, pp. 2481–2494, 2014.*

[12] *J. Yang and J. Ma, "Conditional proxy re-encryption with condition hiding for secure cloud storage," J. Cloud Comput., vol. 8, no. 1, p. 14, 2019.*

[13] *J. Shao and Z. Cao, "CCA-secure proxy re-encryption without pairings," in Proc. ESORICS, 2010, pp. 357–374.*

[14] *J. Weng, J. Liu, J. Ma, and W. Lou, "Conditional proxy re-encryption with keyword search," in Proc. ACISP, 2014, pp. 62–78.*

[15] *J. Weng, J. Ma, W. Lou, and J. Liu, "CPRE: Conditional proxy re-encryption for secure big data sharing in cloud environment," IEEE Trans. Inf. Forensics Security, vol. 12, no. 3, pp. 654–667, Mar. 2017.*

[16] *Z. Fu, F. Huang, K. Ren, J. Weng, and C. Wang, "Privacy-preserving smart semantic search based on conceptual graphs over encrypted outsourced data," IEEE Trans. Inf. Forensics Security, vol. 12, no. 8, pp. 1874–1884, Aug. 2017.*

[17] *M. Green, "Proxy re-encryption and its applications," Ph.D. dissertation, Johns Hopkins Univ., Baltimore, MD, USA, 2007.*

[18] *D. Bhatia and P. Chaudhary, "Certificateless proxy re-encryption for mobile cloud storage," Wireless Pers. Commun., vol. 101, no. 4, pp. 1751–1766, 2018.*

[19] *D. Bhatia and A. Thakur, "Enhanced certificateless proxy re-encryption scheme for mobile PHRs in cloud," Int. J. Inf. Secur., vol. 19, no. 3, pp. 277–290, 2020.*

[20] *Tarambale, M. ., Naik, K. ., Patil, R. M. ., Patil, R. V. ., Deore, S. S. ., & Bhowmik, M. . (2024), "Detecting Fraudulent Patterns: Real-Time Identification using Machine Learning", International Journal of Intelligent Systems and Applications in Engineering, 12(14s), 650, 2024*

[21] *Rajendra V. Patil, Dr. Renu Aggarwal "Comprehensive Review on Image Segmentation Applications", Sci.Int.(Lahore), 35(5), pp. 573-579, Sep. 2023*

[22] *Rajendra V. Patil., Dr. Renu Aggarwal, "Edge Information based Seed Placement Guidance to Single Seeded Region Growing Algorithm", International Journal of Intelligent Systems and Applications in Engineering, 12(12s), 753–759, 2024*

[23] *Rajendra V. Patil, Dr. Renu Aggarwal, Govind M. Poddar, M. Bhowmik. Manohar K. Patil, "Embedded Integration Strategy to Image Segmentation Using Canny Edge and K-Means Algorithm", International Journal of Intelligent Systems and Applications in Engineering, 12(13s), 01–08, 2024*

[24] *Govind M. Poddar, Rajendra V. Patill, Satish Kumar N, "Approaches to handle Data Imbalance Problem in Predictive Machine Learning Models: A Comprehensive Review", Int J Intell Syst Appl Eng, vol. 12, no. 21s, pp. 841–856, Mar. 2024.*

[25] *Sagar V. Joshi, Rajendra V. Patil, Manoj Tarambale, Balkrishna K Patil, Vinit Khetani, Yatin Gandhi, "Stochastic Processes in the Analysis of Electrical Load Forecasting", Advances in Nonlinear Variational Inequalities, 28(1), pp. 15-29, 2025.*

[26] *Suwarna J, Kirti N. Mahajan, Yogesh B. Pawar, Yogita D. Bhise, Bharti Jagdale, Rajendra V. Patil, "Plant Growth Analysis using IoT and Reinforcement Learning Techniques for Controlled Environment", Advances in Nonlinear Variational Inequalities, 27(3), pp. 706–715, 2024.*

[27] *Rajendra V. Patil, Indrabhan S. Borse, Manesh P. Patil, Abhijit H. Khadke, Govind M. Poddar, Shravani R. Patil, "Ensuring Trust in Blockchain Enabled Business Processes using Smart Contract Audits", 8th International Conference on Inventive Computation Technologies [ICICT 2025], April. 2025.*

[28] *D. D. Rao, V. Roy, K. Bhopte, K. Mukilan, P. K. Shukla and R. V. Patil, "Fuzzy-Based Cluster Head Management with Artificial Flora Optimization for Energy-Efficient and Secure Routing in Fog-Enabled Wireless Sensor Networks," 2024 IEEE 2nd International Conference on Innovations in High Speed Communication and Signal Processing (IHCSP), Bhopal, India, 2024,*

[29] *K. C. Jondhale , R. V. Patil, "Edge Based technique to estimate Number of clusters in K-means Color Image Segmentation", 3rd IEEE International Conference on Computer Science and Info Tech, Chegndu , China, 2010*