IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710


# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 4, April 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304263 |

# A Personal Privacy Data Protection Encryption and Revocation of High-Dimensional Attribute Domain

**Mrs. Meenakshi Simha, K. Srikanth, K. Shailaja, M. Sreshta**

Assistant Professor, Department of CSE, Anurag University, Hyderabad, India

Department of CSE, Anurag University, Hyderabad, India

**ABSTRACT**: It is more important than ever to discuss private data protection in light of the frequent occurrence of data breaches. Ciphertext-Policy Attribute-Based Encryption (CP-ABE) in conjunction with blockchain generally allows for safe data sharing and storage. Nevertheless, these approaches suffer from low data protection security, high computational overhead, and high attribute revocation costs in high dimensional attribute domains, i.e., big attribute counts. To solve these challenges, this study presents a technique for the encryption and revocation of high-dimensional attribute domains for personal privacy data protection. There are three parts to the suggested plan. First, to lower computational costs and increase data security, Fast High-dimensional Attribute Domain-based Message Encryption (HAD-FME) is suggested. Second, in conjunction with smart contracts, an attribute revocation mechanism based on sentry mode (SM-ARM) is designed. Finally, by fusing HAD-FME with SM-ARM, a Blockchain-based Model for Personal Privacy Data Protection (BC-PPDP) is put out. According to the security analysis results, the attribute revocation meets both forward and backward security, and the HAD-FME described in this research is secure under the DLIN assumption. Experiments demonstrate that smart contracts and blockchain function effectively, SM-ARM has a lower revocation cost than existing attribute revocation techniques, and HADFME has a higher computational efficiency than existing systems in the high-dimensional attribute domains.

**KEYWORDS**: personal privacy, data protection scheme, encryption, revocation, high-dimensional attribute domain.

## I. INTRODUCTION

In a time when data-driven decision-making and digital interactions rule, protecting individual privacy has become crucial. Robust data protection systems are needed due to the expansion of sensitive information in several fields such as healthcare, finance, and social media. However, established techniques to privacy preservation confront substantial hurdles as data grows more multidimensional and complicated.

Within this framework, the abstract presents a novel data security approach designed to manage and encrypt access to high-dimensional attribute domains while guaranteeing effective revocation procedures. High-dimensional attribute domains have special difficulties because of the complex needs for encryption and access control. Traditional approaches frequently find it difficult to adjust to the varied and dynamic characteristics linked to individual users' data.

The suggested plan seeks to overcome these obstacles by utilizing cutting-edge cryptographic approaches to protect individual privacy and facilitate efficient data use. The technique provides a sophisticated yet workable solution for secure data processing and fine-grained access control by combining homomorphic encryption and attribute-based encryption.

In addition, the plan includes a dynamic revocation mechanism that may be used to quickly remove access credentials when needed, reducing the possibility of unwanted data exposure. This guarantees that data is safe from unwanted access even in settings where access rights are regularly changed.

Scalability and efficiency are important features of the approach that tackle the real-world problems of handling attribute policies and encryption keys in high-dimensional domains. The scheme improves usability without sacrificing security by simplifying access control administration and integrating smoothly with current identity management frameworks.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304263 |

In summary, this introduction lays the groundwork for investigating a comprehensive data protection plan that is tailored to the changing requirements of high-dimensional attribute domain privacy preservation. With its combination of scalability, dynamic access control, and sophisticated cryptography, the method is a major step forward in protecting individual privacy in the face of increasingly complex modern data ecosystems.

## II. RELATED WORK

Within the larger subject of privacy-preserving approaches, research on encryption, revocation, and personal privacy data preservation in high-dimensional attribute domains is crucial. The following are some linked studies and methods:

Homomorphic Encryption: This type of encryption enables computations on encrypted material without the need to first decrypt it. To operate on high-dimensional attribute data while maintaining privacy, methods like fully homomorphic encryption (FHE) and partially homomorphic encryption (PHE) can be used.

Attribute-Based Encryption (ABE): This encryption technology enables the enforcement of access control based on user and data attributes. ABE can be used to simultaneously impose fine-grained access controls based on many attributes and encrypt data in high-dimensional attribute domains.

Differential privacy protects the privacy of individuals in datasets by ensuring that the inclusion or absence of an individual's data does not materially alter the computation's result. Strong privacy assurances can be obtained for high-dimensional attribute data by utilizing techniques like ε-differential privacy.

Secure Multi-Party Computation (SMPC): SMPC protects the privacy of inputs by enabling multiple participants to collaboratively compute a function over them. SMPC is a useful tool for performing computations on high-dimensional attribute data while maintaining the privacy of individual characteristics.

Proxy Re-Encryption: This technique enables a proxy entity to convert ciphertext that is encrypted with one key into another key-decryptable ciphertext. When access privileges need to be revoked dynamically in high-dimensional attribute domains, this might be helpful in revocation scenarios.

Secure Outsourced Computation: Data owners can assign computations on their high-dimensional attribute data to untrusted third-party servers while protecting their privacy by using techniques for secure outsourced computation. To do this, homomorphic encryption and secure multi-party computation are frequently combined.

Blockchain-Based Solutions: High-dimensional attribute domains can manage access control and revocation through decentralized, tamper-proof systems that are implemented using blockchain technology. Attribute-based access control and policy enforcement are two applications of smart contracts.

Machine learning techniques that protect privacy: Federated learning is one such technique that can be used to train models on high-dimensional attribute data without disclosing private information about individual characteristics.

## III. METHODOLOGY

.

Literature Review: To start, do a thorough analysis of the body of research on attribute-based access control, encryption methods, privacy-preserving data protection schemes, and revocation procedures. Determine the main issues, workable solutions, and areas of unmet research need in the field.

Requirement analysis: Determine the precise specifications and use cases for the data protection strategy by working with domain experts, privacy advocates, and possible users. Establish the categories of information that need to be secured, the characteristics of the users and the data, and the desired degree of privacy protection.

Cryptographic Techniques Selection: Choose the right cryptographic techniques for encryption and access control based on the requirements analysis and literature assessment. Take into account elements including each technique's security assurances, computational effectiveness, and suitability for high-dimensional attribute domains.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304263 |

Scheme Design: Create a logical structure for the data protection scheme by including a few chosen cryptographic algorithms. Describe attribute-based access control policies, revocation methods, and the data encryption process.

Prototype Implementation: To confirm the viability and efficacy of the data security plan, create a prototype implementation. To build encryption, access control, use cryptographic libraries and computer languages.

Evaluation: Use a number of simulations and experiments to assess the implementation of the prototype's security and performance. Measure elements including attack resistance, scalability, access control overhead, and encryption/decryption speed. Assess the scheme's practical applicability using real-world scenarios and benchmark datasets.

Refinement and Optimization: Make iterative changes to the design and implementation in response to stakeholder feedback and the findings of the evaluation. Adjust the plan to rectify any found inadequacies or shortcomings and maximize its functionality for practical implementation.

Integration and Deployment: Apply the improved data security plan to the platforms or data management systems that are already in place. Provide documentation and deployment recommendations so that businesses and individuals that care about privacy preservation can apply the scheme more easily.

Continuous Improvement: Set up procedures for continuing to keep an eye on, maintain, and enhance the implemented data protection plan. To make sure the plan is efficient and legal over time, keep up with new threats, developments in cryptography, and changing privacy laws.

## IV. SIMULATION RESULTS

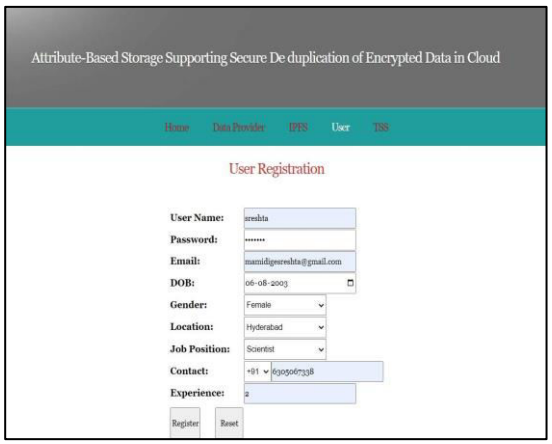



Figure 1: User registration

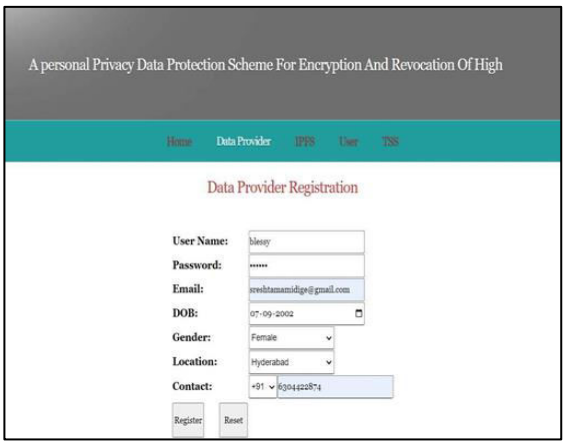



Figure 2: Data provider registration

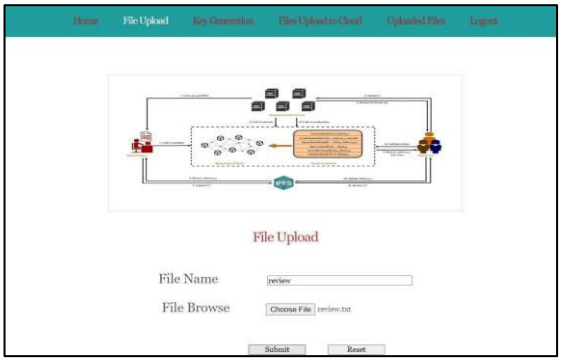



Figure 3: Uploading file

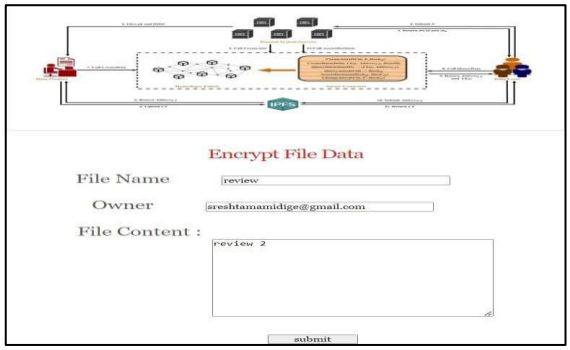



Figure 4: Encrypting Data File

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304263 |

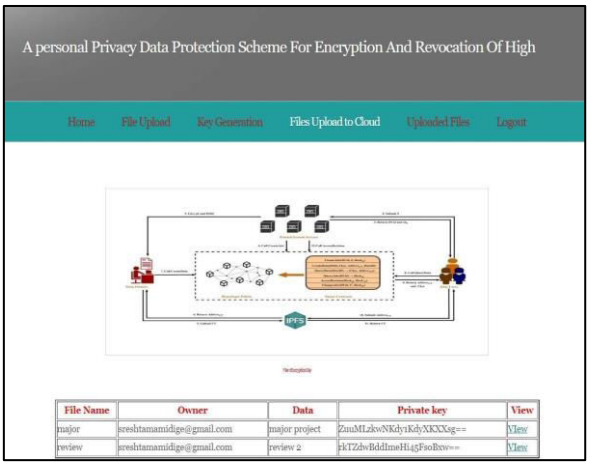



Figure 5: List of uploaded files

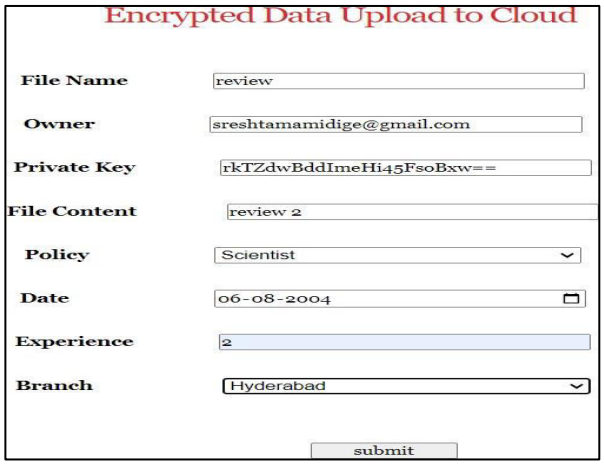
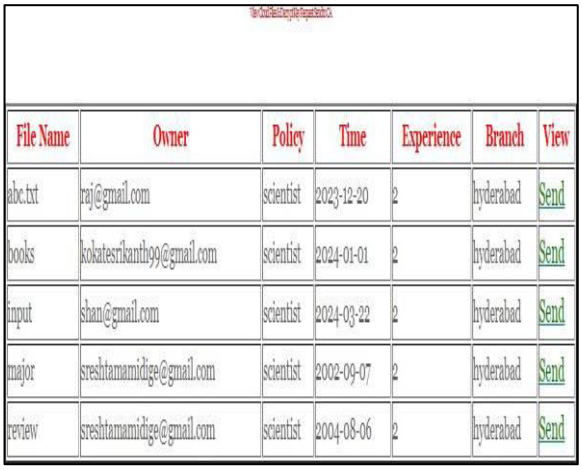
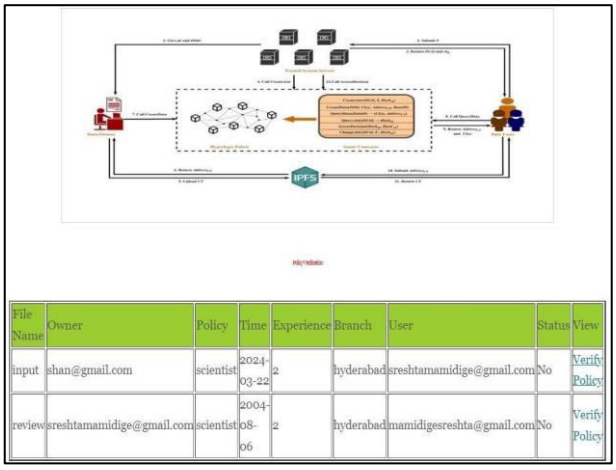



Figure 6: Generating secret key



| File Name | Owner | Policy | Time | Experience | Branch | View |
|---|---|---|---|---|---|---|
| abc.txt | raj@gmail.com | scientist | 2023-12-20 | 2 | hyderabad | Send |
| books | kokatesrikanth99@gmail.com | scientist | 2024-01-01 | 2 | hyderabad | Send |
| input | shan@gmail.com | scientist | 2024-03-22 | 2 | hyderabad | Send |
| major | sreshtamamidige@gmail.com | scientist | 2002-09-07 | 2 | hyderabad | Send |
| review | sreshtamamidige@gmail.com | scientist | 2004-08-06 | 2 | hyderabad | Send |

Figure 7: Files uploaded into cloud



| File Name | Owner | Policy | Time | Experience | Branch | User | Status | View |
|---|---|---|---|---|---|---|---|---|
| input | shan@gmail.com | scientist | 2024-03-22 | 2 | hyderabad | sreshtamamidige@gmail.com | No | Verify Policy |
| review | sreshtamamidige@gmail.com | scientist | 2004-08-06 | 2 | hyderabad | mamidigesreshta@gmail.com | No | Verify Policy |

Figure 8: Policy verification


Figure 9: Verification success

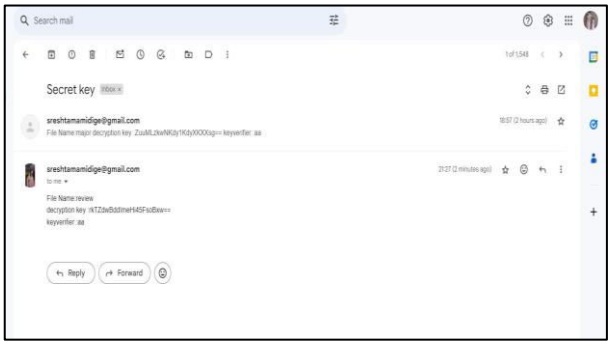



Figure 10: Secret key sent to m

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304263 |

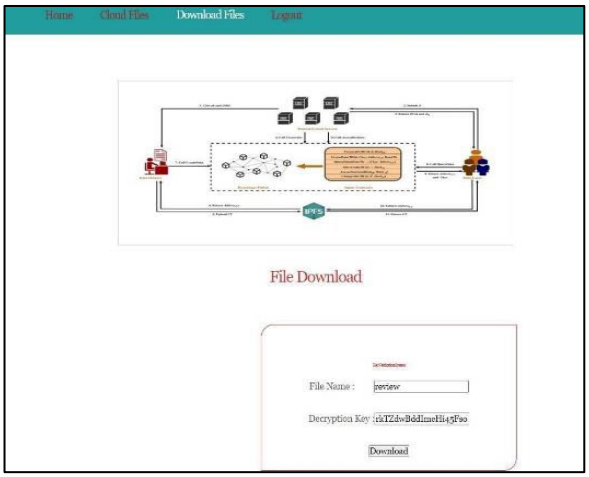



Figure 11: Downloading file using decryption key

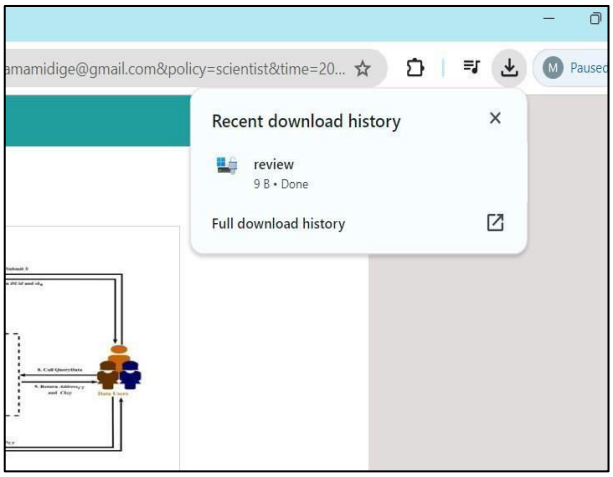



Figure 12: File successfully downloaded

## V. CONCLUSION AND FUTURE WORK

A Personal Privacy Data Protection Scheme for Encryption and Revocation of High-Dimensional Attribute Domains" offers a thorough method for protecting private data stored in intricate structures. High-dimensional attribute domains present distinct issues that the approach addresses by utilizing efficient revocation processes, fine-grained access control mechanisms, and advanced encryption techniques. Strong key management systems guarantee the integrity and confidentiality of encrypted data, while compliance tools make it easier to comply with legal obligations. Additionally, user-centric privacy technologies improve accountability and transparency by giving people the freedom to modify their data privacy preferences. In general, the program encourages user autonomy, security, and confidence in data handling procedures, setting the stage for responsible data stewardship across a range of application areas.

A thorough strategy for protecting private data, particularly in intricate data settings, is provided in "A Personal Privacy Data Protection Scheme for Encryption and Revocation of High Dimensional Attribute Domains." It has sophisticated techniques for jumbling data, meticulous access control, and astute methods for limiting access when required. Maintaining digital locks, or keys, is another important aspect of protecting and maintaining data security. The program assists companies in adhering to regulations regarding appropriate data handling. Furthermore, it allows individuals greater control over their personal data, allowing them to determine who can access it and how. All things considered, the system works well and gives everyone confidence that their information is being handled appropriately.

Integration of Machine Learning: Incorporating machine learning algorithms to dynamically adjust access control policies based on evolving data usage patterns and user behaviours, enhancing the adaptability and responsiveness of the scheme. Privacy-Preserving Data Analysis: Developing techniques for performing privacy preserving data analysis directly on encrypted data, enabling organizations to derive insights while preserving the confidentiality of sensitive information.

## REFERENCES

1. B. Waters, ‘‘Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization,’’ in Proc. Int. Workshop Public Key Cryptogr., 2011, pp. 53–70, doi: 10.1007/978-3-642-19379-8_4.
2. J. Chen, R. Gay, and H. Wee, ‘‘Improved dual system ABE in prime-order groups via predicate encodings,’’ in Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn., 2015, pp. 595–624, doi: 10.1007/978-3-662-468036_20.
3. Y. Zhang, D. He, and K.-K.-R. Choo, ‘‘BaDS: Blockchain-based architecture for data sharing with ABS and CP-ABE in IoT,’’ Wireless Commun. Mobile Comput., vol. 2018, pp. 1–9, Nov. 2018, doi: 10.1155/2018/2783658.
4. P. Sharma, R. Jindal, and M. D. Borah, ‘‘Blockchain-based decentralized architecture for cloud storage system,’’ J. Inf. Secur. Appl., vol. 62, Nov. 2021, Art. no. 102970, doi: 10.1016/j.jisa.2021.102970.
5. X. Lu and S. Fu, ‘‘A trusted data access control scheme combining attribute based encryption and blockchain,’’ Netinfo Secur., vol. 21, no. 3, pp. 7–8, 2021, doi: 10.3969/j.issn.1671-1122.2021.03.002.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304263 |

6. Z. Yang, S. Huang, and C. Y. Zheng, ‘‘Study on crowdsourced testing intellectual property protection technology based on blockchain and improved CP-ABE,’’ Comput. Sci., vol. 49, no. 5, pp. 325–332, 2022, doi: 10.11896/jsjkx.210900075.
7. P. Liu, Q. He, and W. Y. Liu, ‘‘CP-ABE scheme supporting attribute revocation and outsourcing decryption,’’ Netinfo Secur., vol. 20, no. 3, pp. 90–97, 2020, doi: 10.3969/j.issn.1671-1122.2020.03.012.
8. D. Zheng, B. Qin, Y. Li, and A. Tian, ‘‘Cloud-assisted attribute-based data sharing with efficient user revocation in the Internet of Things,’’ IEEE Wireless Commun., vol. 27, no. 3, pp. 18–23, Jun. 2020, doi: 10.1109/MWC.001.1900433.
9. F. Liu, W. Ji, L. Hu, J. Ding, S. Lv, A. Pyshkin, and R.-P. Weinmann, ‘‘Analysis of the SMS4 block cipher,’’ in Proc. 12th Australas. Conf. Inf. Secur. Privacy, 2007, pp. 158–170, doi: 10.1007/978-3-540-73458-1_13.
10. Y. Chen, S. Ding, Z. Xu, H. Zheng, and S. Yang, ‘‘Blockchain-based medical records secure storage and medical service framework,’’ J. Med. Syst., vol. 43, no. 1, Jan. 2019, Art. no. 5, doi: 10.1007/s10916-018-11214.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details