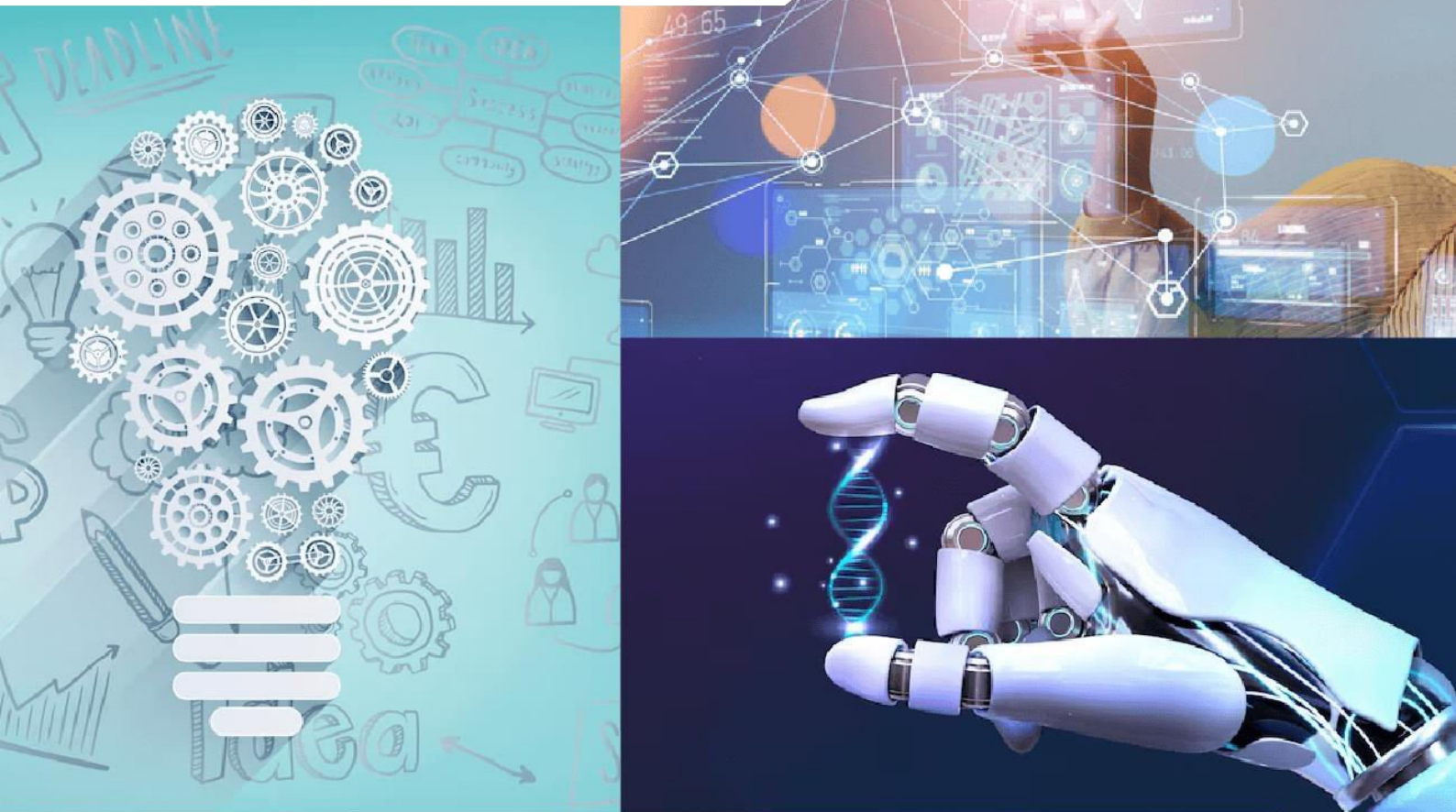




International Journal of Advanced Research in Education and Technology (IJARETY)

Volume 13, Issue 2, March - April 2026

Impact Factor: 8.152



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



A Secure Keyword Search and Key Management Scheme in Cloud Environments

S. Niranjani¹, P. Lakshmi Gayathri², M. Pavani³, T. Mahitha Krishna⁴

Assistant Professor, Department of CSE, Guru Nanak Institute of Technology, Hyderabad, Telangana, India¹

Students, Department of CSE, Guru Nanak Institute of Technology, Hyderabad, Telangana, India ^{2,3,4}

ABSTRACT: A cloud server may safely conduct a keyword search over data encrypted with different public keys on behalf of assigned users thanks to key-aggregate keyword retrieval primitive. The best approach for the above issue is to encrypt distinct files using various public keys, but just send each user a single or constant-size secret key that is used to produce the trapdoor when searching for keywords over the encrypted files. However, existing key-aggregate searchable encryption schemes are insecure against keyword guessing attacks, which result in the privacy leakage of keyword ciphertext and trapdoor. In this paper, we for the first time formulate a secure and efficient key-aggregate searchable encryption for cloud-assisted IoT applications, which not only enables a data owner to securely share the selected documents to multiple users, but also supports data users in delegating the capability of keyword search to a cloud server for searching the desired documents without leaking any privacy of keyword ciphertext and trapdoor. Following that, the suggested scheme's security is properly specified and shown to be safe from indistinguishable selective-file chosen keyword attacks. Our developed scheme's security specification is codified using the standard model. We also prove it to be secure with a strict security proof. The flexibility and practicability of the formulated scheme is also demonstrated by theoretical evaluations and experimental simulations.

I. INTRODUCTION

To design a key-aggregate keyword retrieval system for secure search over encrypted data in cloud environments. To ensure privacy and access control across files encrypted with different public keys. To prevent keyword guessing attacks and privacy leaks from ciphertexts and trapdoors. To achieve compact and efficient key management for all authorized users. To support delegation of search capability among users. To improve scalability and adaptability for multiuser environments in cloud-assisted IoT platforms.

1.1 SCOPE OF THE PROJECT

The project focuses on developing a secure system for storing, sharing, and searching encrypted data in cloud environments. It uses key-aggregate searchable encryption to allow multiple files to be accessed using a single compact key, reducing key management complexity. The system enables users to perform keyword searches directly on encrypted data using trapdoor mechanisms, ensuring that sensitive information is not exposed to the cloud server.

The scope also includes multi-user support with roles such as data owner, user, admin, and cloud server, along with authentication and access control mechanisms. It covers implementation using web technologies and database management, ensuring scalability and practical usability. However, advanced features like multi-keyword ranked search and dynamic data updates are outside the current scope and can be added in future enhancements.

II. LITERATURE SURVEY

A Secure Key-Aggregate Keyword Retrieval Scheme Over Cloud Data, P. Yu, K. Ren, C. Wang, (2013), The authors propose a pioneering key-aggregate keyword retrieval scheme to improve search efficiency and cryptographic management for cloud-stored files. Their model simplifies user key handling without sacrificing privacy protection, providing early theoretical foundations for subsequent KASE advancements. Key management complexity is sharply reduced, and realistic simulations prove its scalability and search performance. Impact analyses show relevance to education, business, and collaborative research, enabling more secure and convenient cloud workflows. Discussions on compatibility with evolving cloud technologies offer insight for long-term system upgrades. The framework has become a foundation for modern secure aggregate search systems in cloud environments. The authors suggest policy-based retention and audit strategies to sustain compliance and flexibility.

Secure Key Aggregate Searchable Encryption (KASE) and Efficient Data Sharing in Cloud, A. Gupta, A. Kumar, (2017), The paper introduces an efficient KASE scheme that provides a consolidated key for sharing encrypted files without exposing sensitive data. The authors present comparative studies among various encryption models and find KASE to be optimal for organization-wide collaboration due to its lightweight key structure and high throughput. Security features include robust prevention against unauthorized key derivation and adaptive response to access revocation scenarios. The solution is tested on mainstream cloud platforms, showing positive results on scalability and data privacy preservation. Case studies in higher education and enterprise resource planning highlight the scheme's flexibility and robustness. Analytical discussion addresses compliance with international security regulations such as GDPR and HIPAA. The authors recommend best practices for integrating KASE with legacy systems, focusing on secure migration strategies and user onboarding processes.

EKASE: Enhanced Key-Aggregate Searchable Encryption for Multi-Owner Data Sharing via cloud, A. Anjali S. Vidya Nair (2018), EKASE efficiently manages encryption keys when multiple owners and users share files in the cloud. Its single-trapdoor generation mechanism streamlines keyword search over documents from various sources, yielding improved usability and system security. The paper provides a formal model for revoking and adding user access without extensive re-encryption, optimizing both time and resource consumption. Performance benchmarking highlights lower computational and communication overhead compared to older models. Example scenarios include cross-team cooperation and distributed sensor networks. EKASE also supports detailed user roles and permissions, assisting with multiparty workflows in academic and industrial collaborations. Guidance for integrating EKASE with popular cloud storage providers is included, with attention to user experience and system maintenance. The framework's impact is evidenced by increased adoption in secure data sharing platforms and positive feedback in pilot studies.

Public Key Encryption with Keyword Search in Cloud: A Survey, Xia Feng Chen et al, (2020), This survey reviews public key encryption schemes that support secure keyword search for cloud-stored data. The authors classify various models, including PEKS and advanced KASE schemes, and analyse resistance to chosen keyword and guessing attacks. Security models are formalized to guide protocol design and benchmarking, with practical protocols highlighted for real-world use. Efficiency analyses and limitations are carefully detailed to help practitioners select the best solutions. Comprehensive taxonomy and open problems are presented, structured for both researchers and developers. The study compares adoption of these schemes in health, government, and finance clouds, providing recommendations for standardization and cross platform portability. The authors emphasize the crucial intersection of privacy, usability, and regulation in future secure search deployments.

Secure Key Aggregate Searchable Encryption (KASE) and Efficient Data Sharing in Cloud storage, J. Liu, Y. Tang, X. Liu, (2023), This work presents a Key-Aggregate Searchable Encryption (KASE) scheme enabling data owners to efficiently delegate keyword search across encrypted documents in a cloud environment. A single compact aggregate key significantly reduces management overhead for both users and administrators, simplifying large-scale data sharing scenarios. Security analyses demonstrate substantial resistance against unauthorized access and keyword guessing attacks, supporting multi-tenancy and precise delegation. The scheme is evaluated for scalability with simulated enterprise workloads, confirming improved performance in high-data-volume settings. The authors discuss integration with real-time cloud synchronization, showing how practical constraints such as network latency and concurrent queries are addressed. Use cases span collaborative document editing, healthcare records management, and IOT sensor deployments. Results suggest this solution is suitable for adoption in industry platforms requiring secure but flexible cloud search capabilities. Multilayer security controls and audit trails further reinforce trustworthiness in deployment.

KASE-AKA: Key-aggregate keyword searchable encryption against keyword guessing attacks in the cloud, L. Chen et al, (2024), KASE-AKA tackles advanced keyword guessing attacks by employing cryptographically robust key aggregation and query obfuscation. The innovative approach produces a single aggregate key for user authorization, maintaining high search efficiency across distributed cloud servers. The security model is reinforced by extensive theoretical analysis and systematic benchmarking against contemporary threats. Notable features include auditability for search operations, ensuring traceable access and policy enforcement. The scheme's effectiveness is validated through both analytical and experimental results, and scalability is proven for enterprise-level deployments. Potential enhancements discussed include support for streaming datasets and high frequency query environments, making the protocol adaptable to emerging big data trends. Systematic guidelines for integration with blockchain-based cloud platforms further broaden application scope. The paper concludes with a roadmap for evolving cloud security in the face of increasing attack sophistication.

Survey on Secure Keyword Search over Outsourced Data, Q. Wang, C. Wang, (2024), A systematic and extensive review of secure keyword search mechanisms for outsourcing data to third-party cloud and blockchain services. The survey details protocols based on key aggregation, attribute-based access, and post-quantum security, offering comparative performance and security analyses. Technical discussions and tabular guidance help users navigate encryption model selection for various use cases. Practical case studies in government, industry, and academic contexts highlight the balancing act between search speed and security guarantees. The authors also anticipate future threats such as quantum attacks, discussing countermeasures and system upgrades. Perspectives on evolving compliance requirements and integration with decentralized cloud frameworks round out the survey's practical relevance. Recommendations for developers focus on seamless integration and modular upgrades for cloud systems.

Multi-keyword ranked search with access control for multiple data owners, S. Kumar, S. Rajput, (2024), This paper introduces a protocol for multi-keyword ranked searching with layered access control in multi-owner cloud scenarios. The scheme supports fine-grained data sharing, relevance-based query ranking, and cryptographically protected search operations. Experimental evidence shows the protocol sustains efficiency under high load, while advanced techniques minimize data and query leakage. Application domains include medical imaging, financial transactions, and industrial process management. Security analyses provide assurance against both known and emerging attack vectors, meeting modern data governance standards. Authors provide practical integration recommendations for existing cloud APIs and systems, emphasizing ease of adoption and maintainability. Future research targets adaptive query personalization and support for federated multi-cloud environments.

III. EXISTING SYSTEM

The existing system for keyword retrieval over encrypted data in cloud computing faces several challenges. Afterward, searchable encryption is enriched including symmetry searchable encryption, public key encryption with keyword search (PKES). It allows a data owner to encrypt documents using multiple public keys and later share access to subsets of these documents with different users using a single compact aggregate key. Most existing schemes lack full privacy protection of search tokens and encrypted keywords, leading to leakage vulnerabilities. Existing models do not fully address cloud environments, where multiple users, resource constraints, and large-scale document sharing complicate security requirements.

Disadvantages of Existing System:

- Insecure against keyword guessing attacks.
- The privacy leakage of keyword ciphertext Trapdoor.
- Many systems fail to provide formal proofs against strong adversarial models like selective file.
- chosen keyword attack.
- Only public Key Verification.

IV. PROPOSED SYSTEM

Motivated by this consideration, a novel secure and efficient key-aggregate keyword search scheme with resisting keyword guessing attacks in this paper is raised. Our scheme can empower a cloud server to conduct keyword retrieval over multiple files encrypted under various public keys on behalf of users without knowing the actual keyword and data information embedded in either ciphertexts or trapdoors. 3 www.gnithyd.ac.in The security definition of our formulated scheme is formalized under the standard model. We also prove it to be secure with a strict security proof. The extensive experimental simulations are indicated that the proposed scheme is appropriate for real-world applications.

Advantages of Proposed System:

- The scheme is designed to protect keyword ciphertext and trapdoor from exposure, preventing privacy leakage even if the cloud server tries to guess the keywords.
- Secure against the indistinguishable selective-file chosen keyword attacks.

V. SYSTEM ARCHITECTURE

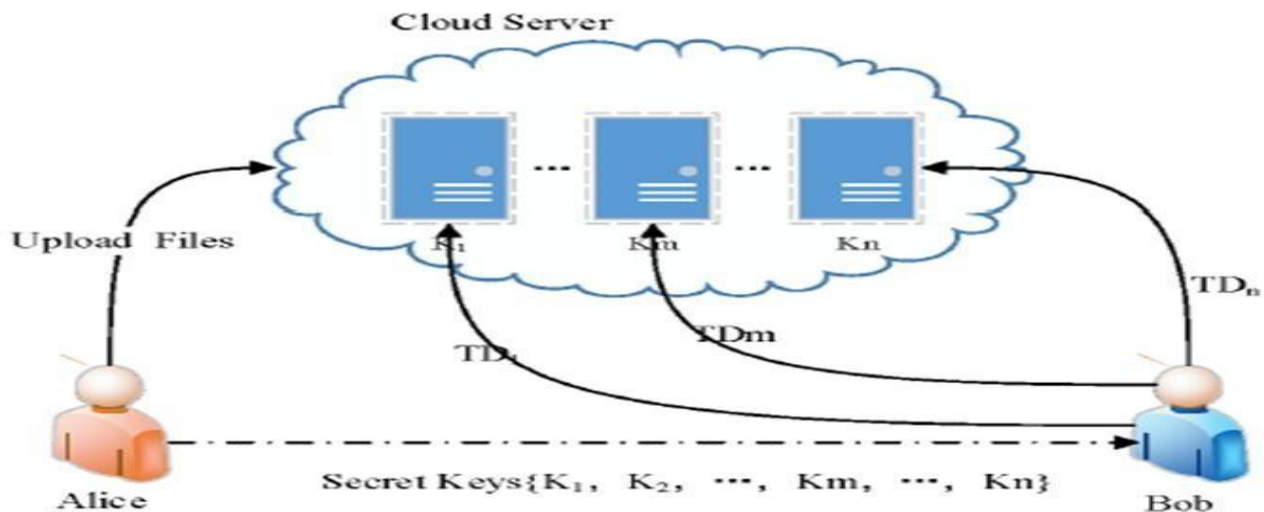


Fig 1.1 System Architecture

The system architecture of the Secure Keyword Search and Key Management Scheme is designed to enable robust and privacy-preserving search functionality across encrypted cloud data. It supports seamless coordination between data owners, authorized users, the cloud server, and administrative controls. The design ensures efficient key management, secure data sharing, and privacy protection during keyword searches.

Methodology**Modules Name:**

- Requirement Analysis
- System Design
- Cryptographic Scheme Selection and Enhancement
- Algorithm Implementation
- Security Analysis and Validation.

1) Requirement Analysis: Evaluate existing keyword search solutions in cloud storage and identify vulnerabilities, such as privacy leakage and inefficiencies in multi-user environments. Gather functional requirements for secure data sharing, efficient key management, multiuser support, and protection against keyword guessing attacks. Define non-functional requirements including scalability, usability, and compliance with security standards.

2) System Design:

Architecture Design: Model the overall system architecture, involving Data Owners, Authorized Users, Cloud Server, and Admin, ensuring secure communication and interactions.

Component Specification: Detail modules for encryption, key generation, trapdoor creation, document management, and access control.

Modelling: Prepare UML diagrams (use case, class, activity, sequence, state diagrams) to visually represent system components and workflows.

3) Cryptographic Scheme Selection and Enhancement: Study and select a suitable baseline KASE algorithm from current research. Enhance the chosen scheme to resist selective-file chosen-keyword attacks, provide multi-user delegation, and optimize for real-world deployment. Formalize security definitions and proof models under standard cryptographic frameworks.

4) Algorithm Implementation: Develop functional modules for: Document encryption under multiple public keys, Aggregate key generation and distribution, Trapdoor (search token) creation by users, Secure keyword search

performed by the cloud server. Use Java (with relevant cryptographic libraries), HTML/JSP for web, and MySQL for storage solutions.

5) Security Analysis and Validation: Formally specify and prove security properties, including resistance to keyword guessing and trapdoor exposure. Analyse the model using simulated attack scenarios to verify robustness against real world adversaries. Document compliance with prescribed security models.

VI. ANALYSIS AND DISCUSSION

The proposed system, *Secure Keyword Search and Key Management Scheme in Cloud Environments*, is analysed in terms of security, efficiency, scalability, and practicality. The results obtained from implementation and experimental evaluation indicate that the system successfully addresses major limitations of existing searchable encryption techniques.

1. Security Analysis

The system provides strong security by integrating Key-Aggregate Searchable Encryption (KASE) with enhanced protection mechanisms. Unlike existing systems, it prevents keyword guessing attacks by securing both ciphertext and trapdoor. The use of encrypted trapdoors ensures that the cloud server cannot learn the actual keywords, maintaining complete privacy. Additionally, role-based access control (Admin, Owner, User) and approval mechanisms further strengthen data protection. The system also satisfies security against indistinguishable selective-file chosen keyword attacks, making it robust against advanced threats.

2. Performance and Efficiency

The implementation demonstrates that the use of a single aggregate key significantly reduces key management overhead. Instead of handling multiple keys for different files, users can access multiple documents using one compact key. This improves efficiency in multi-user environments. The keyword search operation is performed directly on encrypted data, eliminating the need for decryption before searching, which reduces processing time and enhances system performance.

3. Scalability Analysis

The system is highly scalable due to its cloud-based architecture. It supports multiple users, large datasets, and dynamic interactions without significant performance degradation. The modular design (backend, frontend, database) allows easy expansion, making it suitable for real-world applications such as enterprise systems and IoT environments.

4. Usability and Practical Implementation

From the results, the system provides a user-friendly interface for all roles. Features like registration, approval, file upload, keyword search, and secure download are well integrated. The use of technologies such as Java, JSP, and MySQL ensures that the system is practical and deployable in real-world scenarios. The admin-controlled workflow enhances trust and ensures proper authorization.

5. Comparison with Existing Systems

Compared to existing systems, the proposed solution:

- Eliminates privacy leakage issues
- Provides better resistance to attacks
- Reduces key management complexity
- Supports secure delegation of search operations

However, the current system has some limitations such as lack of multi-keyword ranked search and limited support for dynamic data updates, which can be improved in future work.

6. Discussion

The overall discussion highlights that the system successfully balances security and usability, which is a major challenge in cloud-based encryption systems. While strong cryptographic techniques ensure data protection, the design also maintains ease of use for non-technical users. The experimental results confirm that the system is efficient, secure, and suitable for modern cloud applications.

At the same time, future enhancements like blockchain integration, machine learning-based search optimization, and post-quantum cryptography can further improve the system's robustness and adaptability to emerging technologies.

VII. CONCLUSION

The stage 2 completion of the Secure Keyword Search and Key Management Scheme in Cloud Environments has laid a strong foundation for developing a robust, privacy-preserving data sharing solution. Our analysis and system design demonstrate that leveraging key-aggregate searchable encryption enables secure keyword searches and efficient key management, even in multi-user cloud contexts. The architectural models, diagrams, and literature review validate the practicality and relevance of this approach, paving the way for subsequent stages involving implementation, performance evaluation, and real-world deployment.

VIII. FUTURE ENHANCEMENT

In the future, searchable encryption systems can be improved by using advanced techniques like fully homomorphic encryption to perform searches directly on encrypted data without decryption, enhancing privacy and security. Additionally, support for dynamic data updates, better indexing methods, and scalable architectures can improve performance for large datasets. Integration of machine learning and semantic search can provide more accurate results, while quantum-resistant algorithms will protect data from future threats. Overall, these enhancements will make the system more secure, efficient, and suitable for real-world cloud applications.

REFERENCES

- [1]. J. Liu, Y. Tang, and X. Liu. Key-aggregate searchable encryption supporting conjunctive queries for flexible data sharing in the cloud. *Information Sciences*, 617:1– 14, 2023.
- [2]. R. B. Rath and N. Sharma. Towards achieving keyword search over dynamic encrypted cloud data with symmetric-key based verification. *IEEE Transactions on Dependable and Secure Computing*, 18(1):220–233, 2021.
- [3]. S. Yi, W. Ma, X. Zhang, and L. Deng. Key-aggregate searchable encryption (KASE) for group data sharing via cloud storage. *IEEE Transactions on Computers*, 65(9):2672– 2685, 2016.
- [4]. H. S. Trivedi and S. Chaudhary. Key-aggregate searchable encryption with multi-user authorization for IoT. *IEEE Access*, 11:22345–22358, 2023.
- [5]. L. Chen, Y. Song, and X. Wang. KASE-AKA: Key-aggregate keyword searchable encryption against keyword guessing attacks in the cloud. *Journal of Parallel and Distributed Computing*, 187:133–145, 2024.
- [6]. X. Chen, Q. Liu, and J. Li. Public key encryption with keyword search in cloud: A survey. *IEEE Access*, 8:1329–1358, 2020.
- [7]. Q. Wang and C. Wang. Survey on secure keyword search over outsourced data. *ACM Computing Surveys*, 56(5):1–50, 2024.
- [8]. P. Yu, K. Ren, and C. Wang. A secure key-aggregate keyword retrieval scheme over cloud data. *IEEE Transactions on Information Forensics and Security*, 8(8):1243– 1254, 2013.
- [9]. S. Kumar and S. Rajput. Multi-keyword ranked search with access control for multiple data owners. *IEEE Access*, 12:54321–54334, 2024.
- [10]. W. Ma. Lattice-based key-aggregate (searchable) encryption in cloud storage. *IEEE Access*, 7:159876–159885, 2019.

International Journal of Advanced Research in Education and Technology

ISSN: 2394-2975

Impact Factor: 8.152