Journal of Theoretical and Applied Information Technology
30th September 2025. Vol.103. No.18

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

UTILIZING FUZZY-IDENTITY-BASED ENCRYPTION WITH PROXY-RE-ENCRYPTION FOR DATA SHARING

JIBIN JOY[1], DR. S. DEVARAJU[2], DR. J. RAMKUMAR[3]

[1.] Research Scholar (Ph.D.), Department of Computer Science, Sri Krishna Arts and Science College, Coimbatore, Tamil Nadu, India
[2.] Senior Assistant Professor, VIT Bhopal University, Bhopal, Madhya Pradesh, India
[3.] Assistant Professor, Department of Computer Science, Sri Krishna Arts and Science College, Coimbatore, Tamil Nadu, India
jibinjoysamuel@gmail.com[1], devamcet@gmail.com[2], ramkumarj@skasc.ac.in[3]

ABSTRACT

Replication of information also means that efficiency of storing cost is assured since only a copy of information is kept according to the different types of variations. This has been necessitated even further by the fact that, the world information has increased at a greater pace. The sharing of data in the cloud is assessed using Fuzzy-Identity Based-Encryption with Proxy-Re-Encryption (FuzzyIBE PRE) in the new research. The team of researchers is interested in identifying the answers to the question of discovering the effectual mechanism of sharing applied by users of cloud by embracing the benefits of PRE FuzzyIBE. FuzzyIBE PRE proves that it can use open access control scheme by maintaining the privacy of the information. In order to realize this research paper, the research shall provide a critical narration of all the available literatures on the attribute-based encryption and the proxy re encryption in specific with regard to the fuzzy identity description. This will be followed by the running of the FuzzyIBE PRE on real life assessments to determine the degree of effectiveness FuzzyIBE is going to have when it comes to actual implementation of the application cloud sharing data. The study objective will be to get an understanding of the secure privacy based data exchange functions in clouds.

Keywords: *Fuzzy-Identity-Based-Encryption with Proxy-Re-Encryption (FuzzyIBE-PRE), Fuzzy-Identity-Based-Encryption (FIBE), Media-Access-Control (MAC), Information-Management-Table (IMT), Non-Volatile memory (NVM)*

1. INTRODUCTION

The cloud computing is the technology that allows the organisation or people to access the computing resources, that can be, servers, storage, databases, networking, software and analytics, without the need of maintaining it on a computer or a physical server to access them. As compared to the plan of acquiring and integrating physical hardware and software, the users are able to rent out the computing capability, along with the storage space in cloud service providers, such as Amazon Web Services (AWS), Microsoft Azure or Google Cloud Platform (GCP) on a pay-as-you-go platform.The reduction of storage costs becomes efficient under deduplication protocols because they maintain only one data copy despite its multiple minor variations. The urgency of this requirement rises because global data growth has become sudden and rapid. The framework creation for cloud data sharing uses FuzzyIBE PRE as its base to construct the system. The investigation will create reliable sharing methods for data within cloud environments by incorporating FuzzyIBE PRE functionality. FuzzyIBE PRE functions to deliver adaptive control solutions which safeguard data private information as its main operational purpose. The research seeks achievement of its target through comprehensive evaluation of attribute based encryption and proxy re encryption methods with emphasis on fuzzy identity attribute management techniques. The work concludes by conducting practical testing of FuzzyIBE PRE to assess its execution in cloud data sharing situations. This research work aims to disclose privacy-conscious and secure methods for exchanging data in cloud platforms. The research uses Fuzzy Identity Based Encryption with Proxy Re Encryption (FUZZYIBE PRE) as its replacement for current data security systems. FuzzyIBE and PRE establish important theoretical connections that guide FUZZYIBE PRE toward becoming a method which both strengthens privacy features along with key

management systems and delivers flexible authorization rules for cloud system security. Remote encryption technology successfully addresses cloud security issues through its integration with fuzzy identity systems and encryption proxy solution. The document teaches readers how to deploy FUZZYIBE PRE through detailed instructions and includes methods for encryption together with re-encryption and key generation processes and authorization controls. The examination includes an evaluation of security characteristics for this method. The research evidence in FUZZYIBE PRE demonstrates real-world implementation of its functionality for cloud-data-sharing that satisfies current cryptographic security needs of modern cloud platforms. The simplified management framework of sensitive data through the scheme demonstrates usefulness in solving cloud technology problems.

2. LITERATURE REVIEW

The paper by Bosman and colleagues [1] showed that dedupilation risks expose vulnerabilities through which attackers with advanced methods could use basic system functions for attack purposes. The researchers established how deduplication primitives function when exploited because this showed that advanced attackers could extract sensitive information from deduplicated systems. UWare middleware was developed by Cui and his team [3] to minimize encrypted cloud storage data transfers as they sought solutions for client security concerns about side-channel attacks while continuing deduplication functionality benefits. System performance was balanced with deduplication efficiency through the Proof-of-Work (PoW) protocol and similarity attributes exploitation by their team. Efforts to improve deduplication efficiency were presented by Garg et al. [5] through their utilization of graphics processing units. Through their Catalyst method they shifted deduplication tasks to GPUs that detected suitable deduplication pages efficiently thus outperforming standard approaches in memory data sharing speed. Data deduplication received study from Kaur and colleagues [9] because they recognized its efficiency in cloud computing to minimize storage costs and network traffic while reducing energy consumption through innovative deduplication techniques that boost large storage systems. The group-based memory deduplication strategy developed by Ning and his team [11] functions as a new approach for covert channel defense in multi-tenant cloud environments. VMs became protected from side-channel threats because this approach maintained group-level isolation with shared secrets inside each group. The PageCmp program created by Raoufi et al. [13] used DRAM bulk bitwise operations to minimize deduplication data transfer via the DRAM charge-sharing effect and still maintained acceptable execution times and power usage with lower bandwidth requirements. Vano Garcia and Marco Gisbert [15] conducted research on kernel randomization impact on memory deduplication optimization within hypervisors. This analysis focused on showing that kernel randomization generates additional memory requirements and makes it challenging to implement security solutions into cloud environments. The researchers Wang and colleagues [17] developed NV-Dedup designed for file-systems operating on non volatile memory (NVM). Workload adaptive fingerprinting integrated with a metadata table allows inline deduplication to function across CPU and NVM environments by cutting down resource demanding procedures. Evidence obtained from their assessment showed that NV-Dedup effectively minimized the inefficiencies in NVM storage space. Zuo et al. developed DeWrite as a method for encrypted non volatile memory (NVMM) write deduplication which aimed to extend live expectancy and speed up performance results. The researchers managed to merge deduplication with NVMM encryption while executing inline deduplication on secure NVMM which yielded enhanced memory performance and decreased power usage in experimental tests.

3. EXISTING METHODOLOGY

Gupta I. et al. (2019) Demonstrated a complete security framework to enhance cloud environment data security and privacy specific for data sensitivity protection. A multi layer security system implemented in this model relieves cloud service providers from carrying the full security responsibility. This research succeeds in managing data utility and security through dedicated security protocols which match the different sensitivity and operational requirements at separate levels. The system implements unique techniques involving hash functions beside encryption and watermarking to achieve the best possible balance between data protection and user accessibility throughout all system layers. The security platform delivers its highest value when organizations discover unauthorized access of top secret or classified information. The system features an auditing function that tracks leaks through

comparing IMT unique identifiers with embedded document IDs to permit data owners for revoking access from the specific individual who caused the breach. Fu A. et al. (2017) published a study about public auditing techniques which establish multi-level privacy protection for shared cloud data that supports multiple administrator types. This auditing methodology protects group member identity because the Third Party Auditor (TPA) remains unable to know who signed the documents. The Non Frameability Public auditing (NPP) model requires support from at least 't' group managers to uncover any illicit behavior by users while also stopping unauthorized authority misuse from a single manager. Through this method group members can access an undisputed accurate data version after corruption events by using the designated binary tree to track modifications.

4. PROPOSED METHODOLOGY

The main objective focuses on understanding how cryptographic methods enhance adaptable access control systems. The study focuses on preserving data confidentiality amongst users and groups operating in cloud environments. The research evaluates multiple cryptologic approaches with the purpose of uncovering adaptable access strategies which protect data during secure collaborative activities.

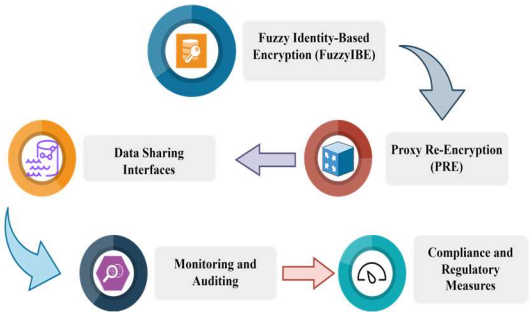

Fig 4.1: Proposed Methodology

Following this, the practical application and rigorous testing of the FuzzyIBE-PRE system will be carried out to assess its efficiency in actual cloud data sharing situations. The study is designed to meticulously gather and analyze data, aiming to enhance the understanding of how to securely and discretely share data on cloud platforms, especially when dealing with the intricate issues related to fuzzy identity attributes and proxy re-encryption mechanisms.

4.1 Infrastructure- Cloud Storage

The four-tier hierarchical structure of the cloud storage platform delivers convenient operation to all storage elements. The cloud storage system requires this four-tier architecture for maintaining cloud data storage which aligns with the following layers:

4.1.1 Data Storage-Layer

Cloud storage resources and services are located at the fundamental layer provided by the cloud provider. A systematic approach exists for the perfect organization which enables uninterrupted service operations. The data storage layer implemented a distributed system based on service-oriented storage which detects storage device conditions while providing scalability features. The storage performance receives enhancements through technological methods involving virtualization and clustering techniques at this layer. Cloud infrastructure resource optimization depends on the allocation of virtual machines (VMs) together with clustering technology.

4.1.2 Data Management-Layer

The data management-layer conducts various essential operations including profile management and security preservation and data distribution procedures. The user interface uses the capabilities of multiple storage devices from the data storage layer to achieve high-speed collaboration functions. Parts of the distributed file system data management layer participate in operational activities and maintenance to maintain data safety and reliability and protection features. The data management layer performs both encryption and replication operations in addition to its other functions. The main task of this layer entails backup management because backups serve as the foundation for disaster recovery procedures.

4.1.2 Application Interface Layer

Through the application interface layer users access services delivered through the internet as part of their data interaction. The interface layer functions as the main connection point between users and cloud storage storage facilities that their provider operates. The layer not only manages user authentication as well as authorization but additionally provides access control functionality. Through an integration of storage device file systems with API the system reaches versatility in cloud storage operation.

4.1.3 User Access Layer

This topmost layer is where users directly interface with the cloud storage system. It provides the means for users to access, manage, and utilize the data stored in the cloud. The user access layer is designed to be user-friendly and accessible from various devices, ensuring that users have a seamless experience when interacting with their stored data in the cloud.

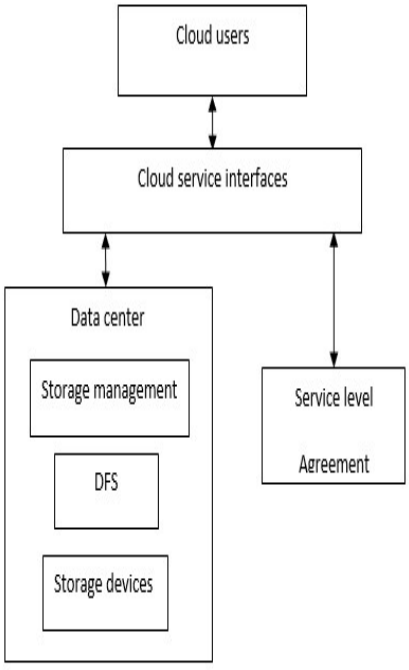

Fig 4.2: Architecture for Cloud Computing Privacy Preserving

4.2 Cloud Storage Concerns on Privacy

Because of its unique architecture cloud storage systems face major data privacy challenges. Maintaining the confidentiality and control of sensitive information becomes challenging in shared and distributed system infrastructures. The main issues that affect data privacy protection include the following concerns.

Lack of User Control

The process of uploading data to cloud servers causes organizations and individuals to relinquish their authority to manage and control such data specifically. Current problems arise from totally losing control of data ownership when transferring data to cloud servers.

Data owners face challenges in understanding the actual storage and processing sites of their data which makes it difficult to follow different laws across international borders.

A high number of governing areas involved in data storage creates intense challenges regarding following legal requirements and operational procedures.

Service providers typically avoid disclosing privacy breaches to their users due to reputational concerns so the data owners stay unaware of the incidents.

Data that exists throughout different locations creates challenges for meeting organizational compliance requirements.

The necessity of reviewing regulatory compliance becomes ongoing since different border laws make data management complicated.

Multiple geographical storage of data improves reliability yet attracts complexities in managing centralized data management.

Data Privacy and Dynamic Provisioning

Data privacy risks occur because the growing amount of data accompanied by its flexible distribution methods present major privacy concerns.

Data transfers across countries become vulnerable to privacy dangers because nation-state privacy regulations differ from one another.

Data Outsourcing generates problems because third-party data management systems that do not maintain rigorous privacy standards.

Public Cloud Privacy Breaches

Public cloud platforms encounter data breaches because their system policies are insufficient and their user expectations differ from what their providers offer.

Employed policies remain ineffective because of weak police enforcement which results in poor system defenses against attacks.

Data understanding suffers when providers implement different rules than users anticipate for the use of their information.

The implementation of insufficient confidentiality and integrity measures through poor security management practices enables unauthorized access together with malware attacks.

Lack of Availability

Data privacy risks occur because the growing amount of data accompanied by its flexible distribution methods present major privacy concerns.

Data transfers across countries become vulnerable to privacy dangers because nation-state privacy regulations differ from one another.

Data Outsourcing generates problems because third-party data management systems that do not maintain rigorous privacy standards.

Public Cloud Privacy Breaches

Public cloud platforms encounter data breaches because their system policies are insufficient and their user expectations differ from what their providers offer. Employed policies remain ineffective because of weak police enforcement which results in poor system defenses against attacks. Data understanding suffers when providers implement different rules than users anticipate for the use of their information. The implementation of insufficient confidentiality and integrity measures through poor security management practices enables unauthorized access together with malware attacks.

4.3 Cloud Computing Privacy safeguarding

Cloud data requires a solid privacy regulation system to prevent unapproved access to stored information. The privacy regulations achieve critical importance when providers move data between each other because users must verify that data exchanges conform to the privacy guidelines they have set. The transmission process depends on user selection and compliance with current laws to protect personal data confidentiality. Every data transfer must start with providers checking whether the receiving system has implemented proper policies. The rule engine converts user-established preferences into operational security rules through which internal threats along with external risks receive protection. Data protection through encryption occurs as a method to boost privacy before storage in cloud systems. The exchange between service providers and users depends on specific security credentials that function separately. While user privacy policies exist in formats understandable by computers they present issues due to the need for effective encryption during machine-readability conversion. Decision points in policy systems enable decision management and enforcement points serve to execute the policies that have been decided. Providers that show proven reliability may make it unnecessary to encrypt data that is outsourced to them. The Extensible Markup Language (XML) serves two data security functions by converting plaintext to machine-readable content. Through XML encryption systems allow users to create secure documents by protecting full texts or individual sections within them. XML signatures function as digital signatures through the security protocol to enhance encryption of files. The XML based Access Control Language (XMLACL) serves as the platform to guarantee that cloud users have correct permission levels assigned. Data protection within the cloud platform requires encryption to remain a central security element.

4.4 Privacy Preserving at the User's End

Secure transactions in cloud storage systems occur through networks using cryptographic methods. When users store data on the system they use encryption protocols which protect their sensitive and confidential information. The encryption system called homomorphic encryption enhances privacy protection inside cloud storage systems. Security measures are strengthened through the inclusion of a bilinear aggregate signature in this research.

Two categories of privacy preservation measures exist which protect personal data either before instances occur or afterward through specific responses. The implementation of encryption techniques makes data secure before cloud storage uploads take place. The noise obfuscation technique belongs to reactive methods which protect sensitive information by applying additional random noise to prevent unauthorized disclosure. The method ensures information confidentiality and simultaneously lowers costs due to its implementation. The reactive information protection method known as noise obfuscation helps prevent data exposure after an upload operation has been completed.

5. IMPLEMENTATION

The proposed identity-based encryption method is designed to enhance cloud data security and follows a structured approach. During the initial setup phase, the Private Key Generator (PKG) handles encryption by selecting two cyclic groups, G1 and G2. Group G1 is additive and includes a generator P, while the bilinear mapping is defined as (e: G_1 \times G_2 \rightarrow G_2). The PKG computes (P, sP, tP,) and (P_{pub} = tP), keeping (s) and (t) confidential and sharing them with the Cloud Service Provider (CSP). The research also defines three hash functions: (H_0) and (H_i), both mapping to (G_1), (H_j), mapping to (G_2

), and (H_k), which maps to (Z_p). Finally, the public parameters, (PP = (G_1, G_2, p, P_{pub}, e, H_i, H_k)), are published to complete the setup. This stage forms the foundation for secure data encryption and management in cloud environments.

5.1 For Encryption and Decryption Process:

In cryptographic systems RSA stands as the central method that uses asymmetric keys. The factorization law establishes a secure computational base because it increases the difficulty of number factoring. The extensive research points to a requirement of approximately seventy years for someone to find 100-digit keys indicating the high security level of RSA. The IIBES creation process employs this algorithm to determine encryption speed and key length and determine secure protection against breaching and compute efficiently.

RSA algorithm achieves its operations through diverse sequential procedures. The algorithm begins with selecting two big prime numbers A and B which we will use later in the procedure. instantiation follows by finding their product N and multiplying A by B and then generating variable Z by multiplying A-1 against B-1. Users need to select a public Encryption key E that has no factors in common with Z. The decision of what private key to use for decryption lies with D while (D*E) mod (A-1)(B-1) =1 is achieved. The encryption process begins by computing CT=PT^E mod N before decrypting data by means of PT =CT^D mod N. This procedure provides an encrypted-decryption system to protect private information securely.

5.2 .Fuzzy-Identity-Based Encryption-with-Proxy Re-Encryption (FIBE-PRE)

Fuzzy Identity Based Encryption with Proxy Re-Encryption (FIBE-PRE) integrates the group-level encryption of Fuzzy Identity Based Encryption (FIBE) along with Proxy Re-Encryption (PRE) data sharing capabilities. Within the FIBE-PRE framework the encryption system incorporates fuzzy public keys that operate at an attribute group level instead of working specifically with identities which makes the framework beneficial towards access control administration. Secure data delegation through PRE proves useful for collaboration environments which need complex access control policies in healthcare systems. Adjustments need to be made to transform fuzzy characteristics and surrogates together with cryptographic keys into practical forms.

5.2.1 Performance-Enhancement

Mambo and Okamoto presented a system for assigning decryption privileges to boost performance over typical decrypt-then-encrypt procedures.

5.2.2 Challenges & Solutions

Mambo and Okamoto suggested a system authorization mechanism for decryption authorization which gives superior performance compared to traditional decrypt-then-encrypt structures. The authors Blaze, Bleumer and Strauss generated "atomic proxy cryptography" which enables cryptographic transformation by decoding without proxy access to plaintext. The authors created two-way secret key exchange protocols for Elgamal RSA and IBE scheme by removing the capability of proxies to delegate additional permissions than they possessed. Enhanced and homomorphic cloud delegation schemes together with threshold proxy re-encryption methods were developed to secure the delegation of sensitive cloud data that is growing in volume.

5.2.3 Homomorphic-Encryption

The ability to run operations on encrypted messages through homomorphic encryption improves cloud data storage safety by offering confidentiality protection.

Users benefit from secure fine-grained access management and enhanced data protection through FIBE-PRE and the homomorphic encryption system during cloud owner requests for any kind of data access. The system operates differently than RSA along with generic access control systems and traditional cryptographic protocols.

5.3 Algorithm

The proposed method uses PK, SK, t, E(PK, m1), E(PK, m2), \ldots, E(PK, mk) and proxy server and key server as its titular input elements. The encryption creates combined codeword symbols by multiplying message values (E(PK, m_i)) with values (g_i) before using (E(PK, \prod_{i=1}^k (m_i g_i))). The proxy server receives encrypted messages in combination with their corresponding secret key for decryption procedures. The proxy server performs threshold value (t) verification while obtaining parts of the secret share from the key server. With the received shares the sender applies the formula (D(SK, E(PK, \prod_{i=1}^k (m_i g_i)))) to decrypt the combined message then separates it into (m1, m2, \ldots, mk).

Cloud storage maintains encrypted messages but the key server stores both the secret key together with threshold value and partial secret shares. The cloud storage system implements protected methods which enable users to receive and decrypt stored data. The output from this system yields decrypted messages (m1, m2, \ldots, mk) through a secure procedure for data management.

6. PERFORMANCE EVALUATION

Companies depend on performance evaluation tools to measure employee work quality and achievements. Organizations evaluate employee work performance in order to consider both strong points and areas needing improvement before setting up development targets for the future. Both organizations and personnel receive benefits from performance evaluations through workplace progress development and improved production while employees work toward organizational targets.

File Size (KB)	Encryption Time		
	IBE	Proxy Re-Encryption	FuzzyIBE-PRE
1	0.8	0.9	0.4
2	0.23	0.37	1.15
4	1.59	1.25	1.06
8	2.15	1.6	0.94

Table 6.1 Encryption time comparison table

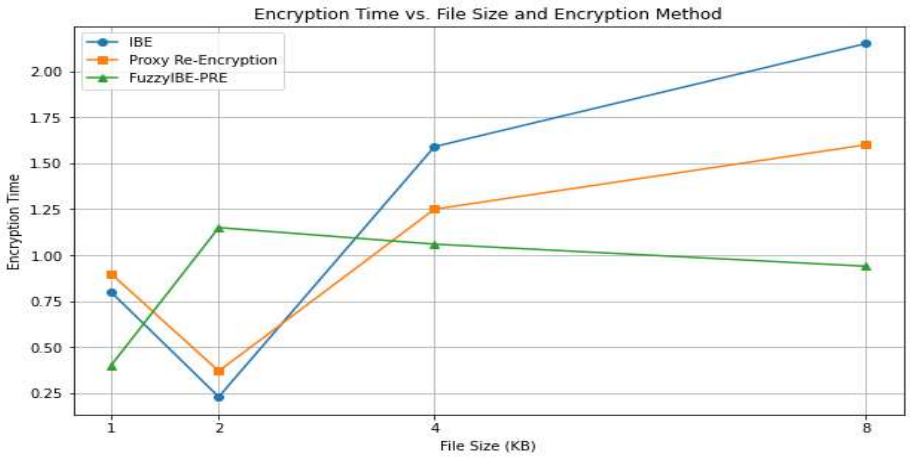

Figure 6.1: Encryption comparison chart

The encryption time examination of diversity file sizes proves Proxy Re-Encryption and Identity-Based Encryption (IBE) and Fuzzy Identity-Based Encryption with Proxy Re-Encryption (FuzzyIBE-PRE) are the most efficient techniques. Different file sizes (in kilobytes) were used for measuring encryption times in seconds through the data shown in **Table 6.1 and Figure 6.1** to depict performance differences. The encryption duration for small files of 1KB measured 0.8 seconds for IBE yet both Proxy Re-Encryption and FuzzyIBE-PRE required 0.9 seconds and 0.4 seconds respectively. FuzzyIBE-PRE proved itself to be the fastest encryption tool through its shorter encryption durations than other methods. The encryption process of all algorithms took extended time periods when files grew larger from 2KB to 4KB to 8KB. The encryption times of FuzzyIBE-PRE remained the briefest among the techniques both at 1KB file size and through the period when the file sizes continuously increased. The encryption time of FuzzyIBE-PRE slightly increased when processing larger files but still maintained efficient processing of expanded data volumes. The encryption time results for Proxy Re-Encryption grew substantially indicating potential issues with its ability to scale

up when processing larger files. The study demonstrates how FuzzyIBE-PRE enables high-speed encryption of data which creates a leading framework for handling encrypted content of various sizes.

File Size (KB)	Decryption Time		
	IBE	Proxy Re-Encryption	FuzzyIBE-PRE
1	0.1241	0.0213	0.0158
2	0.0388	0.0298	0.0254
4	0.0524	0.0433	0.0239
8	0.0943	0.0839	0.0570

Table 6.2: Decryption time comparison table

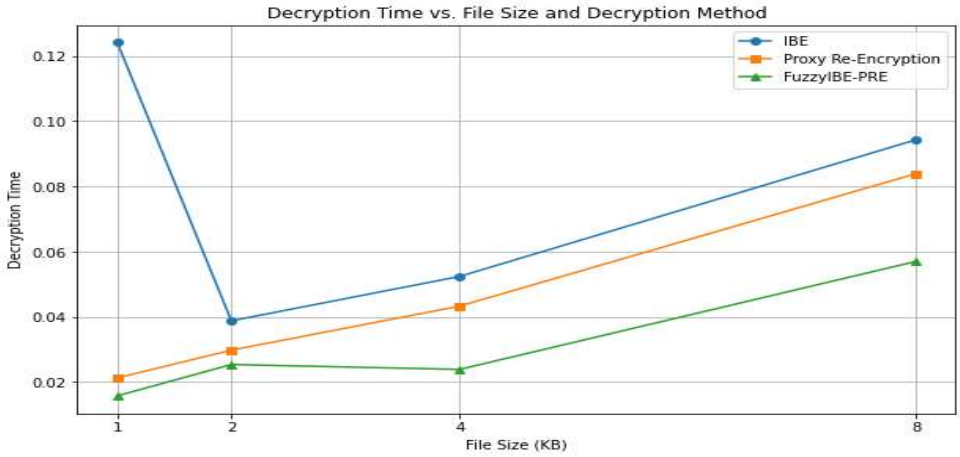

Figure 6.2: Decryption comparison chart

The decryption performance evaluation discusses the performance variation between Identity-Based Encryption (IBE) and Proxy Re-Encryption and Fuzzy Identity-Based Encryption with Proxy Re-Encryption (FuzzyIBE-PRE). **Table 6.2** together with **Figure 6.2** provide information about decryption times for different file sizes to evaluate the efficiency differences between these methods.

File sizes of 1KB display extreme variations between decryption methods. The decryption process of IBE took 0.1241 seconds thus demonstrating it had the slowest processing speed. Proxy Re-Encryption processed files at 0.0213 seconds. FuzzyIBE-PRE proved itself superior since it finished decryption within 0.0158 seconds. The small-scale encryption operations of the FuzzyIBE-PRE method demonstrate superior processing speed than its counterparts.

The increase in file dimensions from 2KB to 4KB and 8KB resulted in equivalent proportionate growth of decryption times for all three methods. The decryption performance of FuzzyIBE-PRE proved to be the quickest among all file sizes thus establishing its position as the fastest encryption technique. The decryption process under Proxy Re-Encryption needed more time than IBE but less than all other methods to secure second position in efficiency statistics. The encryption process duration between FuzzyIBE-PRE and Proxy Re-Encryption decreased over time as file dimensions grew larger. Under large data volume conditions Proxy Re-Encryption outperforms FuzzyIBE-PRE in terms of efficiency yet

FuzzyIBE-PRE proves most efficient in comprehensive analysis.

The data shows essential value in situations requiring fast data recovery procedures and encryption operations. The peculiar system configuration of FuzzyIBE-PRE makes it superior for programs that need immediate responsiveness because it reaches maximum operational efficiency in both performance-bound systems and time-critical real-time situations. Security solutions of the modern age should employ FuzzyIBE-PRE due to its steady premium decryption performance during small file operations. Proxy Re-Encryption maintains dependable file processing capabilities but delivers it through a slower speed management system. IBE demonstrates better suitability compared to other alternatives for security-sensitive operations focused on ease of decryption instead of speedy decryption procedures. A proper decryption method selection follows the principle of aligning specific performance requirements with particular data operational needs.

7. CONCLUSION AND FUTURE SCOPE

Blockchain technology improves data governance through its ability to enable transparent and accountable cloud transactions that are fully traceable. Artificial intelligence emerges as a revolutionary instrument to enhance cloud operations. Intelligent decision-making systems that automate processes to achieve enhanced operational efficiency become empowered by these technologies. The study emphasizes the need to tackle ethical considerations together with regulatory compliance obstacles in cloud practices to promote responsible and sustainable progress. The study of hybrid and multi-cloud frameworks remains essential because it aims to establish seamless cross-cloud communication while optimizing resource use across diverse cloud platforms. The implementation of these architectural solutions boosts cloud systems' scalability and adaptability to address organizational needs. Contemporary experimental methodologies in research are establishing foundational changes in cloud infrastructure systems. The enhancement of deduplication techniques combined with cryptographic advancements allows for the fortification of security protocols. AI-driven optimization solutions combined with blockchain applications will boost operational performance while guaranteeing regulatory compliance. The evolution of cloud computing demands addressing ethical issues during hybrid cloud deployment to achieve interoperability standards. In today's digital environment collaborative initiatives strengthen cloud security platforms while functioning as effective tools for developing operational data governance strategies.

Acknowledgment

JIBIN JOY acknowledges the writing assistance provided by Sri Krishna Arts and Science College, Coimbatore, Tamil Nadu, India. Additionally, Jibin Joy declares a non-financial association with Sri Krishna Arts and Science College, Coimbatore, Tamil Nadu, India.

Conflicts of interest

The authors have no conflicts of interest to declare.

Data availability

The data may be provided by the corresponding author upon reasonable request.

Authors contribution statement

JIBIN JOY acknowledges the writing assistance provided by Sri Krishna Arts and Science College, Coimbatore, Tamil Nadu, India. Additionally, Jibin Joy declares a non-financial association with Sri Krishna Arts and Science College, Coimbatore, Tamil Nadu, India.Co-Authors: Dr. S. Devaraju, Senior Assistant Professor, VIT Bhopal University, Bhopal, Madhya Pradesh, India. Declare that they have no known competing financial interests or personal relationships that could have influenced the work reported in this paper.

REFEERENCES

[1] Bosman, E., Razavi, K., Bos, H., & Giuffrida, C. (2016). Dedup Est Machina: Memory Deduplication as an Advanced Exploitation Vector. 2016 IEEE Symposium on Security and Privacy (SP). doi:10.1109/sp.2016.63

[2] Cui, H., Duan, H., Qin, Z., Wang, C., & Zhou, Y. (2019). SPEED: Accelerating Enclave Applications Via Secure Deduplication. 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS). doi:10.1109/icdcs.2019.00110

[3] Cui, H., Wang, C., Hua, Y., Du, Y., & Yuan, X. (2018). A Bandwidth-Efficient Middleware for Encrypted Deduplication. 2018 IEEE Conference on Dependable and Secure Computing (DSC). doi:10.1109/desec.2018.8625127

[4] Fu, Y., Xiao, N., Jiang, H., Hu, G., & Chen, W. (2017). Application-Aware Big Data Deduplication in Cloud Environment. IEEE Transactions on Cloud Computing, 1–1. doi:10.1109/tcc.2017.2710043

[5] Garg, A., Mishra, D., & Kulkarni, P. (2017). Catalyst. Proceedings of the 13th ACM SIGPLAN/SIGOPS International Conference on Virtual Execution Environments - VEE '17. doi:10.1145/3050748.3050760

[6] Huang, H., Yan, C., Liu, B., & Chen, L. (2017). A survey of memory deduplication approaches for intelligent urban computing. Machine Vision and Applications, 28(7), 705–714. doi:10.1007/s00138-017-0834-6

[7] Jagadeeswari, N., & Mohanraj, V. (2017). A survey on memory deduplication employed in cloud computing. 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS). doi:10.1109/icecds.2017.8390074

[8] Jia, S., Wu, C., & Li, J. (2017). Loc-K: A Spatial Locality-Based Memory Deduplication Scheme with Prediction on K-Step Locations. 2017 IEEE 23rd International Conference on Parallel and Distributed Systems (ICPADS). doi:10.1109/icpads.2017.00049

[9] Kaur, R., Chana, I., & Bhattacharya, J. (2017). Data deduplication techniques for efficient cloud storage management: a systematic review. The Journal of Supercomputing, 74(5), 2035–2085. doi:10.1007/s11227-017-2210-8

[10] Kim, D., Song, S., & Choi, B.-Y. (2016). Existing Deduplication Techniques. Data Deduplication for Data Optimization for Storage and Network Systems, 23–76. doi:10.1007/978-3-319-42280-0_2

[11] Ning, F., Zhu, M., You, R., Shi, G., & Meng, D. (2016). Group-Based Memory Deduplication against Covert Channel Attacks in Virtualized Environments. 2016 IEEE Trustcom/BigDataSE/ISPA. doi:10.1109/trustcom.2016.0063

[12] Niu, Y., Liu, W., Xiang, F., & Wang, L. (2015). Fast Memory Deduplication of Disk Cache Pages in Virtual Environments. 2015 IEEE Fifth International Conference on Big Data and Cloud Computing. doi:10.1109/bdcloud.2015.50

[13] Raoufi, M., Deng, Q., Zhang, Y., & Yang, J. (2019). PageCmp: Bandwidth Efficient Page Deduplication through In-memory Page Comparison. 2019 IEEE Computer Society Annual Symposium on VLSI (ISVLSI). doi:10.1109/isvlsi.2019.00023

[14] Saharan, S., Somani, G., Gupta, G., Verma, R., Gaur, M. S., & Buyya, R. (2020). QuickDedup: Efficient VM deduplication in cloud computing environments. Journal of Parallel and Distributed Computing. doi:10.1016/j.jpdc.2020.01.002

[15] Vano-Garcia, F., & Marco-Gisbert, H. (2018). How Kernel Randomization is Canceling Memory Deduplication in Cloud Computing Systems. 2018 IEEE 17th International Symposium on Network Computing and Applications (NCA). doi:10.1109/nca.2018.8548338

[16] Veni, T., & Bhanu, S. M. S. (2014). MDedup++: Exploiting Temporal and Spatial Page-Sharing Behaviors for Memory Deduplication Enhancement. The Computer Journal, 59(3), 353–370. doi:10.1093/comjnl/bxu149

[17] Wang, C., Wei, Q., Yang, J., Chen, C., Yang, Y., & Xue, M. (2018). NV-Dedup: High-Performance Inline Deduplication for Non-Volatile Memory. IEEE Transactions on Computers, 67(5), 658–671. doi:10.1109/tc.2017.2774270

[18] Wu, J., Hua, Y., Zuo, P., & Sun, Y. (2018). Improving Restore Performance in Deduplication Systems via a Cost-efficient Rewriting Scheme. IEEE Transactions on Parallel and Distributed Systems, 1–1. doi:10.1109/tpds.2018.2852642

[19] Jibin Joy, S. Devaraju (2024) Novelic Approach For Enhancing Storage Efficiency With Block Size Memory Deduplication. Frontiers in Health Informatics, 13 (3), 9714-9727

[20] Xia, W., Jiang, H., Feng, D., Douglis, F., Shilane, P., Hua, Y., … Zhou, Y. (2016). A Comprehensive Study of the Past, Present, and Future of Data Deduplication. Proceedings of the IEEE, 104(9), 1681–1710. doi:10.1109/jproc.2016.2571298

[20] Zuo, P., Hua, Y., Zhao, M., Zhou, W., & Guo, Y. (2018). Improving the Performance and Endurance of Encrypted Non-Volatile Main Memory through Deduplicating Writes. 2018 51st Annual IEEE/ACM International Symposium on Microarchitecture (MICRO). doi:10.1109/micro.2018.00043

[21] Jibin Joy, S. Devaraju (2024) Ensuring Secure Cloud Data Sharing Through Blockchain-Based Auditing For Authentication And Fuzzy Identity-Based Proxy Re-Encryption For Access Control. Library Progress International, 44(1s), 134-146.