Library Progress International *Print version ISSN 0970 1052*
Vol.44, No.1s, January-June 2024: P.134-146

Original Article *Available online at www.bpasjournals.com*

Ensuring Secure Cloud Data Sharing Through Blockchain-Based Auditing For Authentication And Fuzzy Identity-Based Proxy Re-Encryption For Access Control

Jibin Joy[1], Dr. S. Devaraju[2]

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

How to cite this article: 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.

Abstract
In today's data-driven digital landscape, ensuring data integrity and transparency is crucial for businesses, governments, and organizations. Traditional auditing methods struggle with real-time, verifiable, and tamper-proof data transaction records. Blockchain technology emerges as a solution, offering immutability, transparency, and decentralization, which enhance auditing processes. Initially popular for cryptocurrencies like Bitcoin, blockchain is now a versatile tool for creating transparent, secure audit trails, allowing stakeholders to verify data authenticity without centralized authorities. Coupled with digital signatures, blockchain-based auditing ensures public auditability, making audit records publicly accessible yet tamper-proof. This research explores blockchain-based auditing for data public auditability, focusing on integrating digital signatures to bolster security and trust. It examines blockchain and digital signature principles, their synergy, and their potential to revolutionize auditing. The study also discusses the benefits, challenges, and future developments of this approach, highlighting its role in ensuring data integrity and accountability amid rapid data proliferation and cyber threats. Additionally, the research investigates cloud data sharing using Fuzzy Identity-Based Encryption with Proxy Re-Encryption (FuzzyIBE-PRE), aiming to develop robust, efficient data-sharing mechanisms. By leveraging FuzzyIBE-PRE, the study facilitates flexible access control and data privacy, addressing security and performance challenges in cloud computing.

Keywords: Information Management Table (IMT), Fuzzy Identity-Based Encryption with Proxy Re-Encryption (FuzzyIBE-PRE), Fuzzy Identity-Based Encryption (FIBE), media access control (MAC), Proxy Re-Encryption (PRE)

1. INTRODUCTION

In the current digital landscape, cloud computing has become a cornerstone technology, revolutionizing data storage, processing, and distribution. However, ensuring the security and confidentiality of data on cloud platforms remains a paramount concern. Standard encryption methods, while robust, often lack the flexibility needed for dynamically adjusting access permissions. Emerging cryptographic solutions like Fuzzy Identity-Based Encryption (FuzzyIBE) and Proxy Re-Encryption (PRE) offer innovative approaches to address these limitations. FuzzyIBE introduces a more

adaptable form of access control by linking data to 'fuzzy identities,' which are sets of attributes. This allows for nuanced access policies, granting decryption rights to users with attribute sets that closely match the encryption identity, even if they aren't an exact match. Proxy Re-Encryption enables secure data sharing by authorizing a trusted intermediary to convert ciphertexts encrypted with one key into a form that can be decrypted with another key, without exposing the original plaintext.

This study presents a cutting-edge cryptographic methodology, Fuzzy Identity-Based Encryption with Proxy Re-Encryption (FuzzyIBE-PRE), merging the capabilities of FuzzyIBE and PRE. This composite scheme leverages the advantages of both fuzzy identities and proxy re-encryption to enhance privacy, streamline key management, and facilitate dynamic access controls in cloud environments. We explore the intricacies of the FuzzyIBE-PRE framework, including its structural design, encryption and re-encryption protocols, key generation processes, and access control mechanisms. Additionally, the paper provides a thorough security assessment of the scheme. Practical implementations and the benefits of using FuzzyIBE-PRE for cloud data sharing are discussed, highlighting its ability to meet the complex security and privacy demands of modern cloud infrastructures.

Simultaneously, ensuring the integrity and transparency of data is crucial for businesses, governments, and organizations across various sectors. Traditional auditing methods often face challenges in providing real-time, verifiable, and tamper-proof records of data transactions. This has led to the emergence of blockchain technology as a promising solution to enhance auditing processes through its inherent characteristics of immutability, transparency, and decentralization. Blockchain, initially popularized as the underlying technology for cryptocurrencies like Bitcoin, has evolved into a versatile tool with applications beyond finance. Its decentralized and distributed nature makes it ideal for creating transparent and secure audit trails, enabling stakeholders to verify the authenticity and accuracy of data without relying on centralized authorities.

Coupled with digital signatures, blockchain-based auditing ensures public auditability, making audit records publicly accessible yet tamper-proof. This research explores blockchain-based auditing for data public auditability, focusing on integrating digital signatures to bolster security and trust. It examines blockchain and digital signature principles, their synergy, and their potential to revolutionize auditing. The study also discusses the benefits, challenges, and future developments of this approach, highlighting its role in ensuring data integrity and accountability amid rapid data proliferation and cyber threats.

By combining these innovative approaches, the research aims to address the dual challenges of secure data sharing and robust data auditing in cloud environments. FuzzyIBE-PRE offers a flexible and efficient solution for cloud data sharing, while blockchain-based auditing provides a transparent and immutable record-keeping system. Together, these technologies represent a significant advancement in data security and management, ensuring that data remains both accessible and protected in the digital age. The combined study delves into the theoretical foundations, practical applications, and security implications of these technologies, offering valuable insights into their potential to transform cloud computing and data auditing practices. Through this comprehensive exploration, the research contributes to the development of advanced cryptographic techniques and auditing frameworks that meet the evolving needs of modern digital infrastructures.

2. RELATED WORKS

Bosman and colleagues [1] highlighted potential risks associated with memory deduplication, demonstrating how seemingly benign features can be exploited by sophisticated attackers. Their work showed that deduplication-based primitives could be manipulated to extract sensitive information, underscoring the need for robust security measures in deduplication methods. Cui and his team [3] introduced UWare, a middleware designed to reduce data transfer for encrypted cloud storage. UWare aimed to address client concerns about side-channel attacks while maintaining the benefits of deduplication. By leveraging similarity attributes and incorporating the Proof-of-Work (PoW) protocol, they balanced deduplication efficiency with system performance.

Garg et al. [5] tackled the challenge of enhancing deduplication efficiency by utilizing graphics processing units (GPUs). Their approach, named Catalyst, offloaded the deduplication workload to GPUs, effectively identifying pages for deduplication and significantly increasing memory data sharing speed compared to traditional methods. Kaur and

colleagues [9] examined data deduplication in the context of cloud computing, recognizing its role in reducing storage costs, network traffic, and energy consumption. They called for innovative deduplication techniques to improve the efficiency of large storage systems. Ning and his team [11] proposed a group-based memory deduplication strategy as a novel defense against covert channel attacks in multi-tenant cloud environments. This method ensured group-level isolation, protecting virtual machines (VMs) from side-channel threats through shared secrets within the group. Raoufi et al. [13] presented PageCmp, a memory-based page comparison tool that minimized data transfer during deduplication by leveraging the charge-sharing effect in DRAM bulk bitwise operations. This significantly reduced bandwidth needs while maintaining reasonable execution time and power usage.

Vano-Garcia and Marco-Gisbert [15] explored the impact of kernel randomization on optimizing memory deduplication in hypervisors. They revealed the memory overhead caused by kernel randomization and the challenges of integrating security solutions with cloud computing. Wang and associates [17] proposed NV-Dedup for NVM-centric file systems, an inline deduplication strategy using a CPU and NVM-friendly metadata table and workload-adaptive fingerprinting to minimize resource-intensive processes. Their evaluation confirmed that NV-Dedup effectively reduced NVM space wastage. Finally, Zuo et al. [20] developed DeWrite, a technique to deduplicate writes in encrypted non-volatile memory (NVMM) to extend its lifespan and enhance performance. They addressed the challenges of integrating deduplication with NVMM encryption and performing in-line deduplication on secure NVMM. Their experiments showed substantial improvements in memory performance and reductions in energy consumption. In summary, this body of work highlights the diverse approaches and innovations in memory deduplication and secure cloud data management. Bosman and colleagues [1] illuminated the security risks inherent in deduplication methods, while Cui et al. [3] and Garg et al. [5] focused on enhancing deduplication efficiency and security. Kaur et al. [9] underscored the importance of deduplication in cloud computing for cost and energy savings. Ning and his team [11] introduced strategies to protect against covert channel attacks, and Raoufi et al. [13] presented tools to optimize deduplication processes. Vano-Garcia and Marco-Gisbert [15] explored the balance between security and efficiency in memory deduplication, while Wang et al. [17] and Zuo et al. [20] developed advanced techniques for NVMM systems, enhancing performance and reducing wastage. Together, these studies contribute to the evolving landscape of secure and efficient data management in modern computing environments.

3. MATERIALS AND METHODS

This study investigates secure data-sharing methods within cloud services, focusing on Fuzzy Identity-Based Encryption combined with Proxy Re-Encryption (FuzzyIBE-PRE). The objective is to explore how this cryptographic approach can provide flexible access management while ensuring data confidentiality among cloud users or groups. The research begins with an extensive review of existing literature on attribute-based encryption and proxy re-encryption, emphasizing the management of imprecise identity attributes. **Figure 1** provides a detailed description of the overall implementation methodology. Simultaneously, the paper explores the integration of blockchain technology and digital signatures to enhance the auditing process for ensuring data public auditability. In today's data-centric environment, maintaining the integrity and transparency of data transactions is crucial for various stakeholders. Traditional auditing methods often struggle to provide real-time, verifiable, and tamper-proof records of data exchanges. Blockchain technology, renowned for its decentralized and immutable nature, offers a promising solution to these challenges. By leveraging blockchain's inherent characteristics and integrating digital signatures, this study proposes a robust framework for conducting audits that are both transparent and secure. **Figure 2** delves into the fundamental concepts of blockchain technology, digital signatures, and their combined application in revolutionizing auditing practices.

The integration of FuzzyIBE-PRE and blockchain-based auditing aims to address the dual challenges of secure data sharing and robust data auditing in cloud environments. FuzzyIBE-PRE offers a flexible and efficient solution for cloud data sharing, allowing nuanced access policies and secure data exchange through trusted intermediaries. Concurrently, blockchain-based auditing provides a transparent and immutable record-keeping system, enabling stakeholders to verify the authenticity and accuracy of data without relying on centralized authorities. This combined approach represents a significant advancement in data security and management. By exploring the theoretical foundations, practical applications, and security implications of these technologies, this research contributes to the development of advanced cryptographic techniques and auditing frameworks. These innovations are designed to meet the evolving

needs of modern digital infrastructures, ensuring that data remains both accessible and protected in the digital age. Through this comprehensive exploration, the study aims to offer valuable insights into secure and efficient data management practices, enhancing the overall security posture of cloud computing environments.

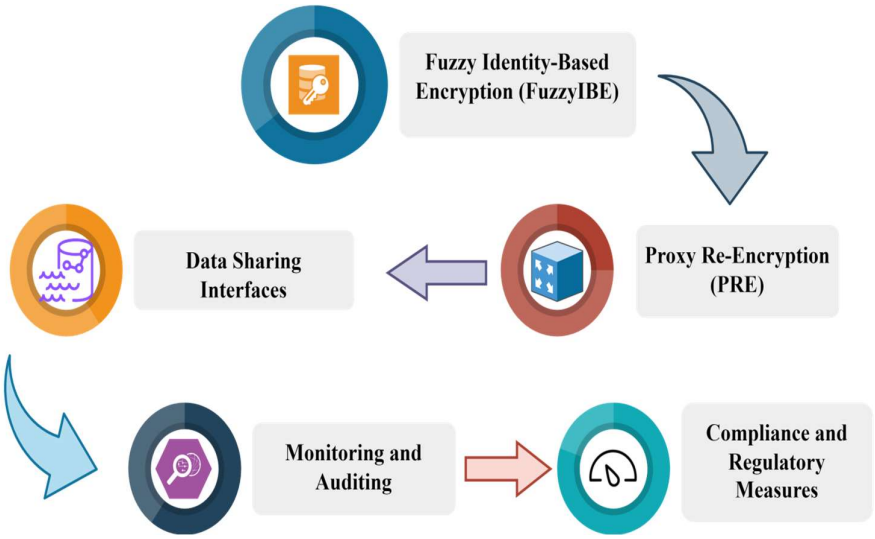

Figure 1: Proposed FuzzyIBE-PRE

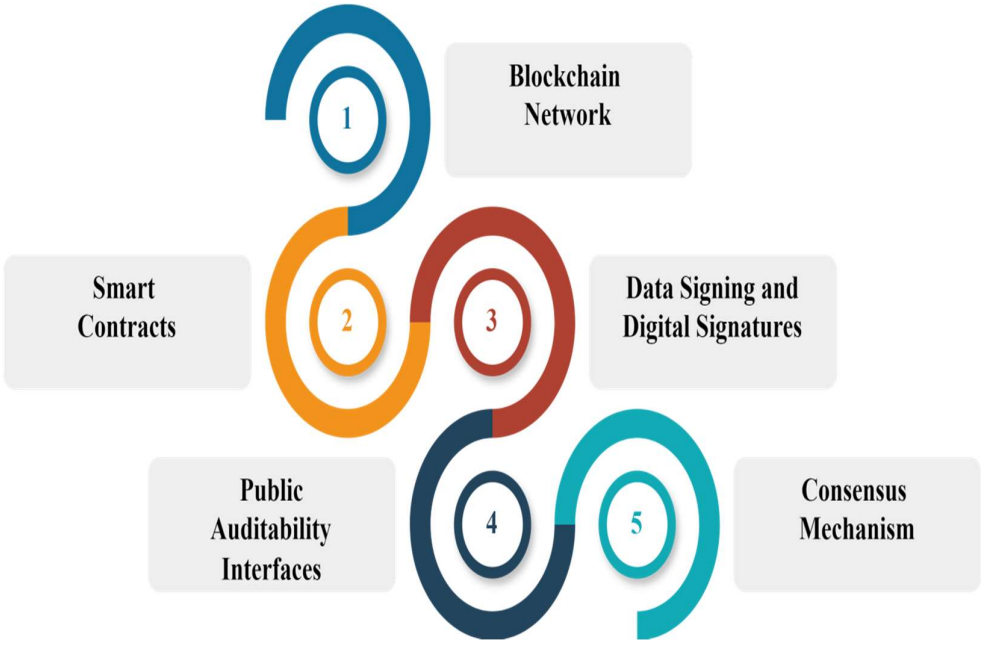

Figure 2: Proposed Block chain technology

3.1 Preserving Privacy in Cloud Computing

A structured set of privacy regulations is essential for preventing unauthorized data access in cloud storage. These regulations become particularly important when data is transferred between providers, ensuring that the exchange complies with established privacy policies. User preferences and relevant legal requirements are critical for maintaining the confidentiality of personal data. Before any data exchange occurs, providers must verify that the receiving party has implemented the necessary privacy policies. This verification process ensures that data handling aligns with both user-defined preferences and legal standards. A rule engine plays a key role in this process by converting user preferences into actionable rules that protect against internal and external threats. Additionally, to enhance privacy, data within the cloud is encrypted. This encryption adds an extra layer of security, protecting data both during storage and transmission. **Figure 3** illustrates this encryption process, highlighting its importance in safeguarding data.

By implementing these structured privacy regulations, cloud providers can create a secure environment that meets user expectations and legal requirements. This approach ensures the integrity and confidentiality of personal data throughout its lifecycle, from storage to transfer. The combination of privacy policies, user preferences, legal compliance, and encryption forms a comprehensive strategy to protect sensitive information in cloud computing environments.

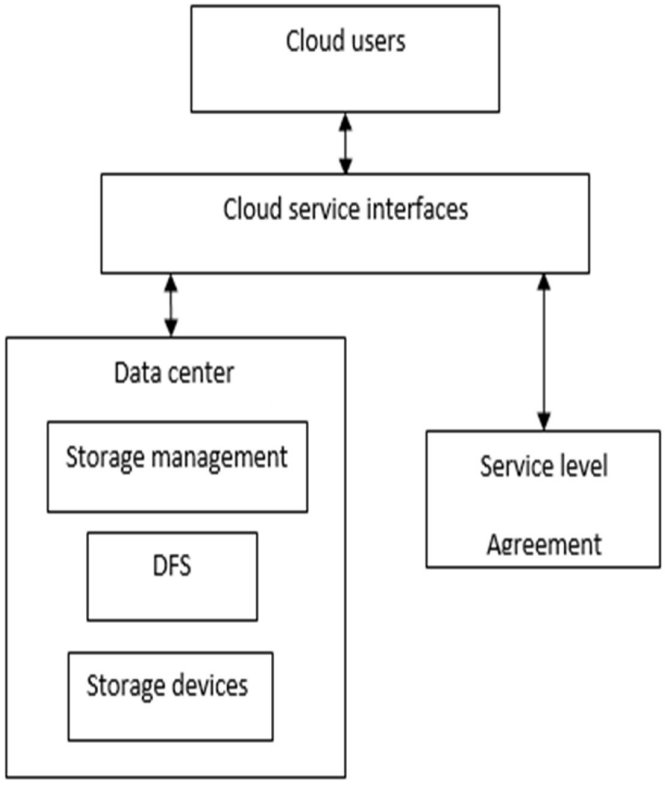

Figure 3: Architecture for Preserving Privacy in Cloud Computing

3.2 Security Credentials and Policy Management

Each user request and service provider response is accompanied by unique security credentials. Individuals' privacy policies are stored in a computer-interpretable format, though translating these rules into machine-readable formats can be challenging, despite efficient encryption handling. Policy decision points are used for decision-making

processes, while policy enforcement points apply these policies. If a cloud provider is deemed trustworthy, encrypting outsourced data may not always be necessary.

3.3 Utilizing XML for Machine Readability and Data Security

Extensible Markup Language (XML) is used to convert plaintext into a machine-readable format. XML-based encryption can encrypt entire documents or specific sections. To enhance security, these encrypted files are signed with XML signatures, serving as digital signatures. XML-based Access Control Language (XMLACL) ensures proper permission levels for cloud users. Encryption keys are exchanged through a protected channel to maintain data security within the cloud infrastructure. The cloud provider manages data and offers extensive storage capabilities. When cloud storage data is encrypted, the provider's control over the data is effectively nullified, enhancing privacy and confidentiality. Analyzing metadata allows for the tracking of transactions and potential attacks. An encryption proxy enables secure data retrieval by users from the cloud. Upon receiving a request, the rule engine assesses user credentials, and if these credentials meet the set criteria, access is granted, recognizing the individual as an authorized user. This system not only maintains data privacy but also ensures robust data confidentiality and security. By combining security credentials, XML-based data handling, and encrypted cloud storage, this comprehensive system ensures data protection, privacy, and efficient management of user access and permissions in the cloud environment.

3.4 Preserving Privacy on the User's End

In cloud storage systems, secure transactions are ensured through the use of cryptographic methods over a network. On the user side, protocols encrypt data to protect sensitive and confidential information when it is stored. Homomorphic encryption is employed to significantly enhance privacy within cloud storage frameworks. Additionally, the research incorporates bilinear aggregate signatures to further bolster security measures. To protect personal data, both proactive and reactive privacy preservation techniques are utilized. Proactive methods, such as encryption, secure data before it is uploaded to the cloud. Reactive methods, like noise obfuscation, add noise to sensitive data to obscure it from unauthorized access. This dual approach not only maintains the confidentiality of crucial information but also reduces costs. Noise obfuscation, as a reactive method, mitigates the risk of information leakage after data has been uploaded.

By integrating these proactive and reactive privacy techniques, cloud storage systems can provide robust security and privacy protection. Homomorphic encryption allows for computations on encrypted data without exposing the actual data, thereby enhancing privacy. Bilinear aggregate signatures ensure data integrity and authenticity during transactions. Together, these advanced cryptographic methods, along with traditional encryption and noise obfuscation, create a comprehensive framework for secure and private data storage in cloud environments. This approach effectively preserves data confidentiality and offers efficient, cost-effective protection against potential security threats.

3.5 Using Digital Signature with trusted application

Digital signatures and handwritten signatures differ primarily in that the former, being digital, cannot be physically seen by the recipient upon signing. The digital signature algorithm employs a private key to generate a secure encrypted hash code for user applications.

If an intruder compromises a node, they can impersonate a genuine user, intercept communications, and deceive others by presenting fraudulent documents. To prevent such compromises, a robust authentication procedure must be implemented between the user's applications (like word processors or email) and the digital signature application. This procedure ensures the verification of user credentials within their respective nodes before digitally signing any communication. In these scenarios, the signing application may require all requests across the system to undergo digital signing to enhance security measures.

4. IMPLEMENTATION

The proposed identity-based encryption technique aims to enhance the security of cloud data. The research plan consists of several stages:

4.1 Set Up

During this phase, the Private Key Generator (PKG) executes the encryption process. It chooses two cyclic groups, G1 and G2, where G1 is additive and has the generator P. A bilinear mapping is defined as \(e: G_1 \times G_1 \rightarrow G_2 \). Then, it calculates \(P_s = sP \) and \(P_t = tP \), ensuring the confidentiality of both \(s \) and \(t \) while transmitting them to the CSP. Furthermore, the research introduces three hash functions as described below:

- H_0:{0,1}^*→G_1,H_i:{0,1}^*→G_1H_j:G_2→{0,1}^*
- H_k:{0,1}^* X{0,1}^*→Z_p

Finally, it publishes the public parameters PP=(G_1,G_2,p,P_pub,e,H_i,H_k)

4.2 Encryption and Decryption Process:

RSA Cryptographic Technique

RSA, a widely adopted asymmetric key cryptographic technique, leverages the mathematical challenge of integer factorization. Based on mathematical research, breaking RSA keys with 100 digits would require approximately 70 years for an attacker. When designing IIBES, the RSA algorithm is evaluated across multiple factors including computational speed, key length, encryption efficiency, and resilience against security threats.

4.2.1 Phases of the RSA Algorithm

Step 1: Select two large prime numbers, A and B.
Step 2: Compute N = A * B and Z = (A-1) * (B-1).
Step 3: Choose a public key for encryption (E) such that it is relatively prime with Z.
Step 4: Choose a private key for decryption (D) such that it satisfies the equation (DE)mod(A-1)(B-1) = 1.
Step 5: To encrypt the plaintext, use the equation CT = 〖PT〗^E mod N.
Step 6: To decrypt the ciphertext, use the equation PT = 〖CT〗^D mod N.

4.3 Blockchain-Based Auditing for Data Security (BCADS)

Blockchain-Based Auditing for Data Security (BCADS) utilizes blockchain technology to transform auditing practices, ensuring data security, integrity, and transparency. By recording each data event as an immutable block on a decentralized blockchain network, BCADS eliminates vulnerabilities associated with centralized control. This approach fosters transparency among stakeholders and guarantees the integrity of the entire audit trail. The blockchain's immutability ensures that once data is recorded, it remains unchanged, providing a dependable record of all activities. This decentralized model enhances security by mitigating single points of failure and enables real-time auditing and continuous monitoring.

BCADS is applicable across diverse industries such as finance, healthcare, supply chain management, and government. It offers auditors a robust framework to independently verify data integrity, thereby fostering trust and accountability in digital transactions. Successful implementation of BCADS requires addressing considerations like regulatory compliance, data privacy, scalability, and interoperability with existing systems to fully capitalize on its benefits.

In contrast, traditional ink signatures can be easily replicated by copying or digitally reproducing them. In contrast, digital signatures are cryptographically protected, making them highly secure and trustworthy when sending messages. Paper-based contracts can be susceptible to tampering, whereas digital signatures ensure the integrity of the entire document, including its final page, through cryptographic protection.

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

Fuzzy Identity-Based Encryption with Proxy Re-Encryption (FIBE-PRE) merges the flexibility of Fuzzy Identity-Based Encryption (FIBE) with the data sharing functionalities of Proxy Re-Encryption (PRE). In FIBE-PRE, encryption utilizes fuzzy public keys associated with attribute sets rather than exact identities, enabling sophisticated access control. Proxy Re-Encryption enables safe data delegation, facilitating secure collaborations and precise access policies in domains such as healthcare systems. Skillful administration of fuzzy attributes, proxies, and cryptographic keys is pivotal for maximizing its practical utility.

4.4.1 Performance Enhancement

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

4.4.2 Challenges and Solutions

Blaze, Bleumer, and Strauss introduced the concept of "atomic proxy cryptography," allowing a semi-trusted proxy to decrypt and transform messages without access to the original plaintext. Dodis and Ivan implemented a two-way secret key exchange mechanism for Elgamal, RSA, and an IBE scheme, resolving issues related to proxy's ability to provide more delegation permissions on its own. Concerns about the security of sensitive data stored in the cloud have led to the development of enhanced and homomorphic cloud-based delegation techniques and a threshold proxy re-encryption strategy.

4.4.3 Homomorphic Encryption

Homomorphic encryption allows operating on encrypted messages without decrypting them, providing enhanced security for cloud-based data storage and retrieval. The RSA algorithm and Fuzzy Identity-Based Encryption with Proxy Re-Encryption offer secure and fine-grained access control, while homomorphic encryption provides enhanced security for cloud-based data storage and retrieval.

4.5 Algorithm

4.5.1 Input:

- Public Key (PK)
- Secret Key (SK)
- Threshold value (t)
- Encrypted messages (E(PK, m1), E(PK, m2), ..., E(PK, mk))
- Proxy server
- Key server

4.5.2 Encryption Process:

- Generate an encoded code word symbol for each message: E(PK,m_i) g_i where g_i represents the coefficient for message m_i.
- Compute E(PK,∏i=1k(migi)) to obtain the code word symbol for the combined message.

4.5.3 Decryption Process:

- Send the encrypted messages and corresponding secret key to the proxy server.
- The proxy server verifies the threshold value (t) and retrieves partial secret shares from the key server.
- Compute D(SK,E(PK,∏i=1k(migi))) using the received partial secret shares to decrypt the combined message.
- Separate the combined message back into individual decrypted messages: m1, m2,...,mk.

4.5.4 Blockchain-Based Auditing for Data Security (BCADS)

In the case of aggregate signature schemes, aggregation is supported such that if there are 'n' signatures on 'n' messages from 'n' users, all these signatures can be combined into a single aggregated signature with a constant size relative to the number of users. This aggregated signature can then be verified to confirm that all 'n' users are indeed associated with their respective original messages. Digital signatures are typically transmitted securely and are resistant to imitation or tampering by unauthorized users, partly due to automatic timestamping. Consequently, once a sender has digitally signed a message and sent it, they cannot easily disown or repudiate the signature later, as the authenticity of the originally signed message remains intact after transmission.

Key Generation

a. Choose an elliptic curve \(E \) and select a base point \(G \) on that curve.

b. Select a private key \(d \) randomly from the interval [1, n-1], where \(n \) is the order of the base point \(G \).

c. Compute the corresponding public key \(Q = dG \).

Signature Generation:

a. Compute the hash value \(H(M) \) of the message \(M \) to obtain a digest.

b. Choose a random integer \(k \) from [1, n-1].

c. Calculate the point \(R = kG \) on the elliptic curve.

d. Compute \(s = (k^{-1} \cdot (H(M) + d \cdot R_x)) \mod n \), where \(R_x \) is the x-coordinate of \(R \).

e. The signature is represented as \((R, s) \).

Signature Verification:

a. Verify that \(R \) is a valid point on the elliptic curve and \(s \) lies within the range [1, n-1].

b. Compute the hash value \(H(M) \) from the received message \(M \).

c. Compute \(w = s^{-1} \mod n \) and \(u1 = (H(M) \cdot w) \mod n \), \(u2 = (R \cdot w) \mod n \).

d. Calculate the point \(P = u1G + u2Q \).

e. If \(P \) equals the x-coordinate of \(R \) (i.e., \(P_x = R_x \)), then the signature is valid; otherwise, it is invalid.

4.5.5 Storage and Retrieval:

- Encrypt messages and store them on the cloud storage server.
- Store the secret key, threshold value, and partial secret shares on the key server.
- Employ secure methods for retrieving and decrypting data from the cloud storage system.

Output:

- Decrypted messages (m1, m2, ..., mk)

5. RESULTS AND DISCUSSION

Performance evaluations are essential tools used by companies to assess the effectiveness and contributions of their employees. These evaluations typically involve reviewing an employee's work performance, identifying strengths, pinpointing areas for improvement, and setting future development goals. They benefit both employees and employers by fostering growth, enhancing productivity, and aligning individual efforts with organizational objectives. Similarly, any digital signature can be applied to any type of message, ensuring that the receiver can verify the sender's identity and ensuring the integrity of the message. Digital certificates also play a critical role, as they include the issuer's digital signature, allowing authorities to authenticate the certificate's validity.

Table 1: Encryption time comparison table I

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

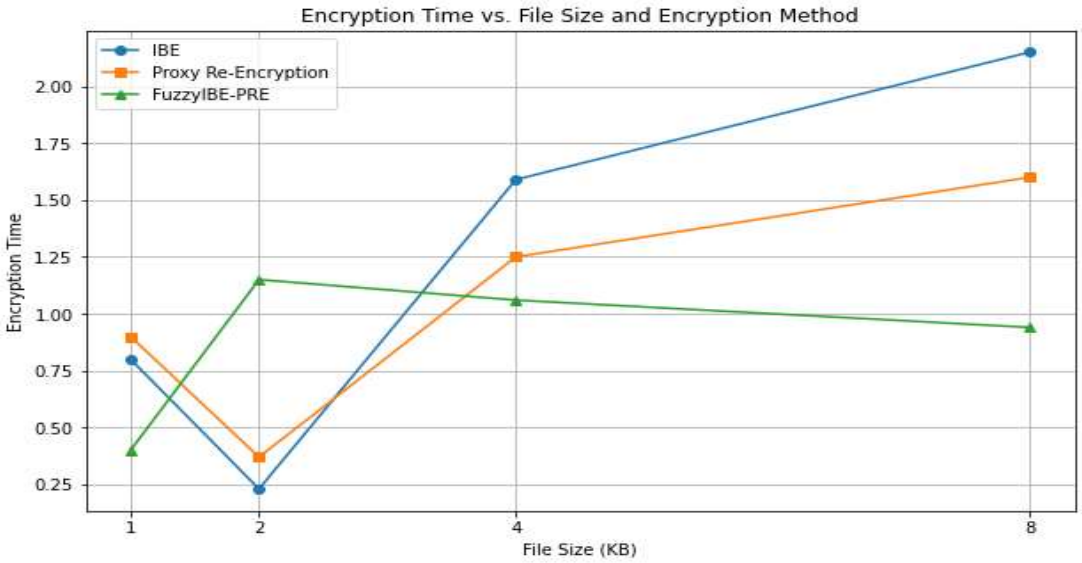

Figure 4: Encryption comparison chart I

The data presented in **Table 1 and Figure 4** illustrates the encryption times, measured in seconds, for different file sizes (in kilobytes) using three distinct encryption techniques: Identity-Based Encryption (IBE), Proxy Re-Encryption, and Fuzzy Identity-Based Encryption with Proxy Re-Encryption (FuzzyIBE-PRE).

- For files of 1KB:
  - IBE: 0.8 seconds
  - Proxy Re-Encryption: 0.9 seconds
  - FuzzyIBE-PRE: 0.4 seconds
- -As file sizes increased to 2KB, 4KB, and 8KB, encryption times increased uniformly across all methods. Notably, FuzzyIBE-PRE consistently exhibited the shortest encryption times, followed by IBE and Proxy Re-Encryption.
- FuzzyIBE-PRE showed a marginal increase in encryption times with larger file sizes, whereas Proxy Re-Encryption experienced a more pronounced increase.
- The findings indicate that FuzzyIBE-PRE offers efficient encryption, striking a balance between speed and security. This makes it a viable option for applications where fast encryption is critical.

Table 2: Encryption time comparison table II

File Size (KB)	Encryption Time

	Blockchain	Digital Signatures	BCADS
1	0.6	0.7	0.3
2	0.21	0.33	1.11
4	1.57	1.22	1.01
8	2.14	1.4	0.92

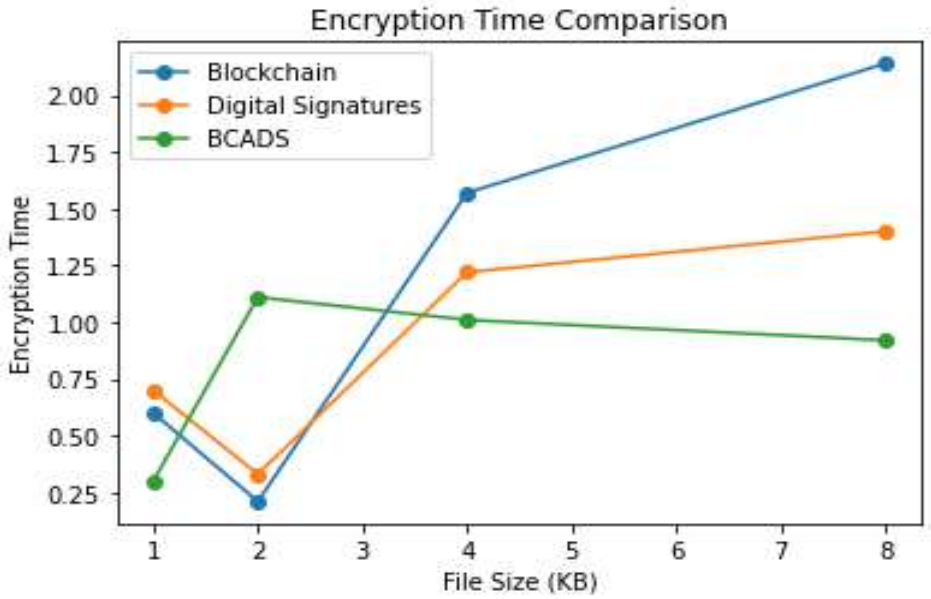

Figure 5: Encryption comparison chart II

The data presented in **Table 2 and Figure** 5 illustrates the encryption times in seconds for different file sizes (measured in kilobytes) using three methods: Blockchain, Digital Signatures, and BCADS (Blockchain-Based Auditing with Digital Signatures). For 1 KB files, BCADS demonstrates the shortest encryption time at 0.3 seconds, followed by Blockchain at 0.6 seconds and Digital Signatures at 0.7 seconds. However, as file sizes increase to 2 KB, BCADS shows a notable increase in encryption time to 1.11 seconds, surpassing both Blockchain (0.21 seconds) and Digital Signatures (0.33 seconds). Notably, for larger file sizes of 4 KB and 8 KB, BCADS maintains relatively lower encryption times compared to Blockchain and Digital Signatures, recording times of 1.01 seconds and 0.92 seconds, respectively. In contrast, Blockchain experiences a significant rise in encryption time as file sizes increase, reaching 1.57 seconds for 4 KB and 2.14 seconds for 8 KB files. Similarly, Digital Signatures also demonstrate increased encryption times with larger files, recording times of 1.22 seconds and 1.4 seconds for 4 KB and 8 KB files, respectively. Overall, BCADS proves to be competitive in terms of encryption time across various file sizes, highlighting its efficiency in handling larger data volumes while maintaining relatively low encryption overhead.

Table 3: Decryption time comparison table I

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

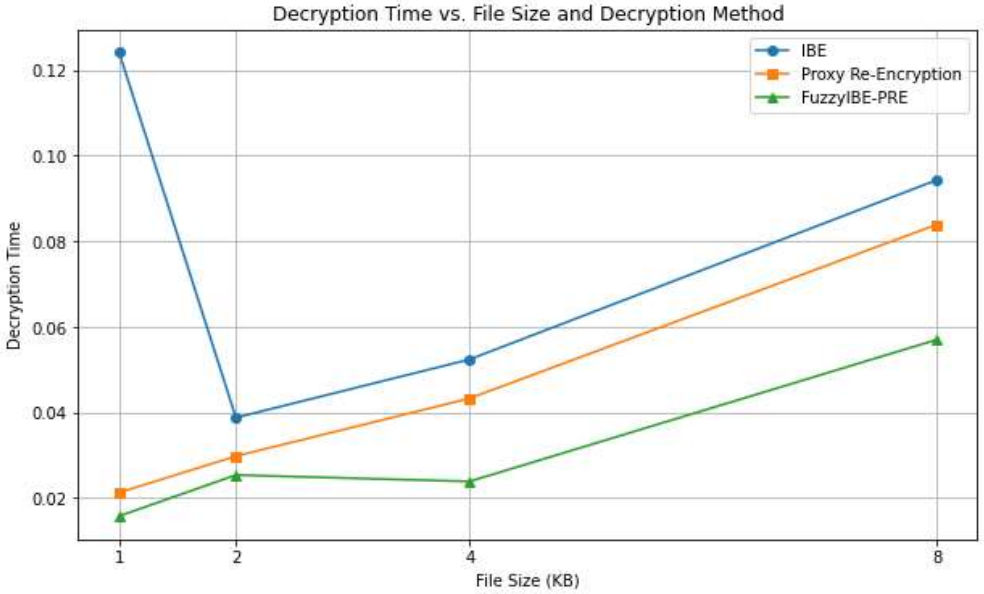

Figure 6: Decryption comparison chart I

The data presented in **Table 3 and Figure 6** Decryption times for various file sizes using Identity-Based Encryption (IBE), Proxy Re-Encryption, and Fuzzy Identity-Based Encryption with Proxy Re-Encryption (FuzzyIBE-PRE) are detailed in table 2 and figure 6. Key findings include:

- For 1KB files:
  - IBE decryption time: 0.1241 seconds
  - Proxy Re-Encryption decryption time: 0.0213 seconds
- FuzzyIBE-PRE decryption time: 0.0158 seconds

- As file sizes increased (2KB, 4KB, 8KB), decryption times rose uniformly across all methods. Notably:
- FuzzyIBE-PRE consistently showed the shortest decryption times.
- Proxy Re-Encryption followed with slightly longer decryption times.
- IBE consistently had the longest decryption times.

Comparatively, as file sizes grew, the difference in decryption times between FuzzyIBE-PRE and Proxy Re-Encryption decreased, indicating Proxy Re-Encryption's efficiency relative to FuzzyIBE-PRE improves with larger files. FuzzyIBE-PRE proves effective for fast decryption, particularly with smaller file sizes, making it ideal for scenarios requiring swift data access.

Table 4: Decryption time comparison table II

File Size (KB)	**Decryption Time**		
	Blockchain	Digital Signatures	BCADS
1	0.1251	0.0203	0.0148

2	0.0398	0.0288	0.0244
4	0.0514	0.0423	0.0229
8	0.0923	0.0829	0.0560

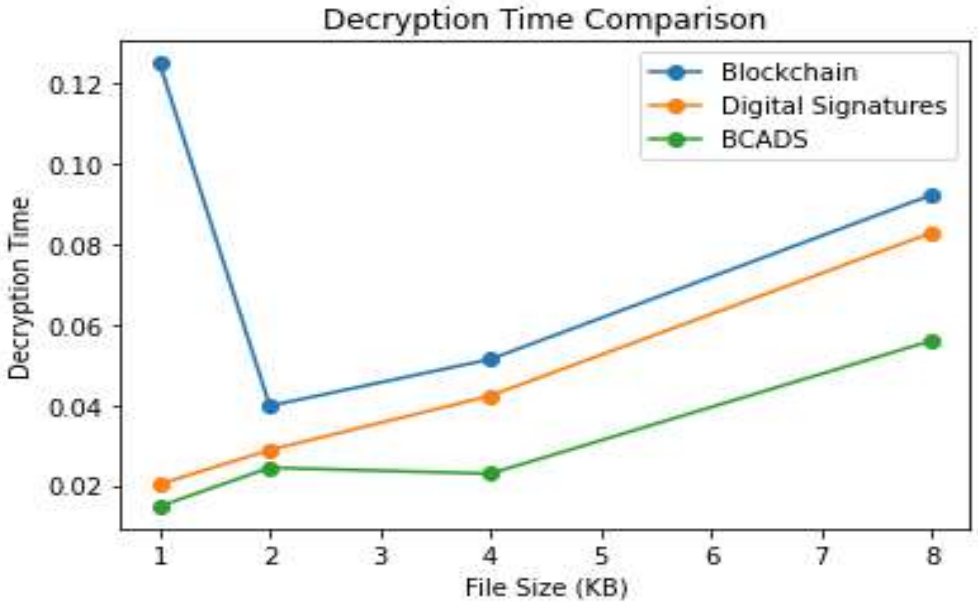

Figure 7: Decryption time comparison chart II

The data presented in **Table 4 and Figure 7** present data on decryption times in seconds for different file sizes (in kilobytes) using three methods: Blockchain, Digital Signatures, and BCADS (Blockchain-Based Auditing with Digital Signatures). For 1 KB files, BCADS shows the quickest decryption time at 0.0148 seconds, followed by Digital Signatures at 0.0203 seconds and Blockchain at 0.1251 seconds. As file sizes increase to 2 KB, BCADS maintains efficiency with a decryption time of 0.0244 seconds, outperforming Blockchain (0.0398 seconds) and Digital Signatures (0.0288 seconds). This trend continues for larger sizes (4 KB and 8 KB), with BCADS demonstrating times of 0.0229 seconds and 0.0560 seconds, respectively. In contrast, Blockchain and Digital Signatures exhibit increased decryption times as file sizes grow, reaching 0.0923 seconds and 0.0829 seconds for 8 KB files, respectively. Overall, BCADS consistently delivers faster decryption times across various file sizes, highlighting its efficiency and suitability for efficient decryption tasks.

6. CONCLUSION AND FUTURE SCOPE

This study explores the application of Fuzzy Identity-Based Encryption with Proxy Re-Encryption (FuzzyIBE-PRE) to enhance secure data sharing in cloud environments, focusing on flexible access control and privacy protection. The research methodology includes conducting a comprehensive literature review, implementing FuzzyIBE-PRE, and performing testing to evaluate its practical effectiveness. The primary objective is to provide valuable insights into secure and privacy-preserving data sharing in the cloud, with particular emphasis on utilizing fuzzy identity attributes and proxy re-encryption techniques.

Additionally, the research project lays a foundation for future advancements in cloud computing. It addresses current challenges and proposes solutions while outlining potential future research directions. These directions include exploring advanced deduplication techniques suitable for diverse data types, integrating quantum-resistant cryptographic protocols for heightened data security, developing dynamic access control mechanisms to facilitate

flexible data sharing, and leveraging blockchain technology for comprehensive data governance. Furthermore, the research advocates for the adoption of AI-driven optimization and automation to streamline cloud operations and emphasizes the importance of addressing ethical and regulatory considerations in cloud computing practices. The study also underscores the significance of hybrid and multi-cloud architectures to ensure interoperability and efficient resource utilization across diverse cloud environments.

In summary, embracing these future research directions promises to optimize cloud infrastructures, fortify security measures, enhance data governance practices, and promote responsible and efficient cloud computing practices in the foreseeable future. Additionally, the paper introduces blockchain-based auditing for data public auditability, using digital signatures to ensure transparent and tamper-proof verification of data integrity. This implementation enhances trust in cloud-based systems by providing a secure and verifiable method for validating data authenticity.

ABBREVIATIONS

FuzzyIBE-PRE - Fuzzy Identity-Based Encryption with Proxy Re-Encryption
IBE- Identity-Based Encryption
FIBE - Fuzzy Identity-Based Encryption
PRE – Pre-Encryption
ECC- Enhanced Elliptic Curve Cryptography

DECLARATION OF COMPETING INTEREST

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

CONFLICTS OF INTEREST

The authors have no conflicts of interest to declare.

ACKNOWLEDGMENT
None.

DATA AVAILABILITY
No data was used for the research described in the article. The implementation is mainly based on the hardware dependency so that execution of the work is mainly dependent on the time and data complexity.

AUTHOR CONTRIBUTIONS
Mr. Jibin Joy wrote the entire article and responsible for data pre-processing. Dr. Devaraju S read and approved the final manuscript.

AUTHORS' INFORMATION
Mr. Jibin Joy is a Research Scholar(Ph.D) in Sri Krishna Arts and Science College Coimbatore,India, His research area is cloud computing and published various Scopus and research papers.
Dr. S. Devaraju is Senior Assistant Professor, VIT Bhopal University, India. He has more than 15 years of teaching experience with various Scopus and WoS research papers and also have association with various funded projects.

FUNDING
None

ETHICS APPROVAL AND CONSENT TO PARTICIPATE

This article does not contain any studies with human participants or animals performed by any of the authors.

COMPETING INTERESTS

The authors declare that they have no conflict of interest

AUTHOR DETAILS

Jibin Joy, Research Scholar(Ph.D), Sri Krishna Arts and Science College, Coimbatore,India
Dr. S. Devaraju, Senior Assistant Professor, VIT Bhopal University, Bhopal, Madhya Pradesh, India

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. 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. Sumathi Gurusamy, Rajesh Selvaraj, Resource allocation with efficient task scheduling in cloud computing using hierarchical auto-associative polynomial convolutional neural network, Expert Systems with Applications, Volume 249, Part B, 2024, 123554, ISSN 0957-4174, https://doi.org/10.1016/j.eswa.2024.123554.

22. Xiyuan Xu, Shaobo Zang, Muhammad Bilal, Xiaolong Xu, Wanchun Dou, Intelligent architecture and platforms for private edge cloud systems: A review, Future Generation Computer Systems, 2024, ISSN 0167-739X, https://doi.org/10.1016/j.future.2024.06.024

23. Patrick Langer, Stephan Altmüller, Elgar Fleisch, Filipe Barata, CLAID: Closing the Loop on AI & Data Collection — A cross-platform transparent computing middleware framework for smart edge-cloud and digital biomarker applications, Future Generation Computer Systems, Volume 159, 2024, Pages 505-521, ISSN 0167-739X, https://doi.org/10.1016/j.future.2024.05.026.

24. Abdeslam Rehaimi, Yassine Sadqi, Yassine Maleh, Gurjot Singh Gaba, Andrei Gurtov, Towards a federated and hybrid cloud computing environment for sustainable and effective provisioning of cyber security virtual laboratories, Expert Systems with Applications, Volume 252, Part B, 2024, 124267, ISSN 0957-4174, https://doi.org/10.1016/j.eswa.2024.124267.

25. Sheharyar Khan, Zheng Jiangbin, Muhammad Irfan, Farhan Ullah, Sohrab Khan, An expert system for hybrid edge to cloud computational offloading in heterogeneous MEC–MCC environments, Journal of Network and Computer Applications, Volume 225, 2024, 103867, ISSN 1084-8045, https://doi.org/10.1016/j.jnca.2024.103867.

26. J. Kok Konjaang, John Murphy, Liam Murphy, Energy-efficient virtual-machine mapping algorithm (EViMA) for workflow tasks with deadlines in a cloud environment, Journal of Network and Computer Applications, Volume 203, 2022, 103400, ISSN 1084-8045, https://doi.org/10.1016/j.jnca.2022.103400.

27. Ahmad Salah AlAhmad, Hasan Kahtan, Yehia Ibrahim Alzoubi, Omar Ali, Ashraf Jaradat, Mobile cloud computing models security issues: A systematic review, Journal of Network and Computer Applications, Volume 190, 2021, 103152, ISSN 1084-8045, https://doi.org/10.1016/j.jnca.2021.103152.