IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 4, April 2025

DOI: 10.17148/IARJSET.2025.12407

A Novel Secure Data Deduplication Framework for End-to-End Encrypted Documents Using Attribute Based Keyword Search

Julure Raviteja[1], Mood Bhanu Prasad[2], Narani Harini[3], Naik Shivanand Kumar Babu[4], Botcha Kishore Kumar[5]

Assistant Professor, Department of CSE, Guru Nanak Institutions Technical Campus, Hyderabad.[1]

Department of CSE, Guru Nanak Institutions Technical Campus, Hyderabad.[2,3,4]

Assistant Professor, Department of CSE (AI&ML), Vignana Bharathi Institute of Technology, Hyderabad.[5]

Abstract: With the exponential growth of cloud-based document storage, efficient and secure data management has become a crucial requirement. This paper presents a novel secure data deduplication framework that operates seamlessly over end-to-end encrypted documents. The proposed framework integrates Ciphertext-Policy Attribute-Based Encryption (CP-ABE) with an Attribute-Based Keyword Search (ABKS) mechanism to enable fine-grained access control and efficient encrypted search. We introduce a secure token-based deduplication method that detects redundant files without revealing file content or search keywords to the cloud server. Extensive security and performance analyses demonstrate that our solution preserves data confidentiality, resists leakage during keyword queries, and significantly reduces storage and computation costs.

Keywords: ABKS, Proxy server, deduplication, cloud storage.

I. INTRODUCTION

Cloud storage systems have become essential for modern organizations and users, offering scalable, on-demand access to vast amounts of data. However, storing massive volumes of encrypted documents introduces challenges such as redundancy, access control, and secure search.

Data deduplication is a popular technique to avoid redundant storage, but its integration with encrypted data remains difficult due to the indistinguishability of encrypted content. Furthermore, enabling search over encrypted data while enforcing access policies is still an open research issue.

This paper proposes a novel solution that combines secure data deduplication with fine-grained searchable encryption using Attribute-Based Keyword Search (ABKS). The framework allows:

- End-to-end encrypted document storage.
- Deduplication based on encrypted tokens without content leakage.
- Encrypted keyword search with access policy enforcement.

II. RELATED WORK

In the realm of data storage and management, secure data deduplication represents a cornerstone technology for optimizing storage space and reducing redundancy. Traditional client-side deduplication approaches, while efficient regarding storage and network traffic, expose vulnerabilities that allow malicious users to infer the existence of specific files through traffic analysis. Even using a Proof of ownership scheme does not guarantee protection from all attack scenarios, specific to data deduplication. This paper introduces a novel secure data deduplication framework employing a deduplication proxy that operates on-premise, effectively mitigating the risk of such inference attacks. By leveraging convergent encryption, and Merkle tree challenges for proof of ownership, our solution ensures that data deduplication does not compromise data privacy or security. The deduplication proxy acts as an intermediary, performing dedu-plication processes on-premise. This approach not only preserves the efficiency benefits of deduplication but also enhances security by preventing external visibility into data traffic patterns. Our implementation, publicly available on Github, demonstrates the efficacy of the method for enforcing end-to-end encryption while maintaining data deduplication's

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 4, April 2025

DOI: 10.17148/IARJSET.2025.12407

storage-saving advantages. The proposed framework is suitable for organizations aiming to safeguard their data while optimizing storage resources.

Secure Data Deduplication:
Traditional deduplication techniques rely on matching plaintext data or hash values, which is incompatible with encryption. Convergent encryption techniques allow deduplication but suffer from key leakage and dictionary attacks.

Attribute-Based Encryption (ABE):
ABE, particularly CP-ABE, enables data encryption under a specific access structure, allowing only users with matching attributes to decrypt the content.

Searchable Encryption:
Searchable symmetric encryption (SSE) and public key encryption with keyword search (PEKS) offer limited capabilities in terms of access control. ABKS extends this by enabling keyword search based on user attributes.
This gives rise to a growing number of data loss cases in many notable cloud service providers such as cloud data.

On the other hand, when the industrial cloud is externally attacked, the attackers may maliciously modify the collected running data forget the operation/configuration data, or manipulate the results and decisions of industrial applications, which may result in the manipulation or destruction of the entire industrial system.

The security of the approach Edasvic is analyzed in the random. A prototype of Edasvic is implemented and extensive experiments demonstrate that Edasvic incurs fewer computational costs than the state-of-the-art approaches

III. LITERATURE SURVEY

The surge in cloud storage adoption has driven extensive research into secure, efficient, and privacy-preserving data management techniques. This literature survey explores key areas relevant to our proposed framework: data deduplication, attribute-based encryption (ABE), and searchable encryption, with a particular focus on attribute-based keyword search (ABKS).

Secure Data Deduplication: Data deduplication is a technique that eliminates redundant data to reduce storage space and bandwidth usage. Traditional approaches work well in plaintext scenarios but pose significant security risks when applied to encrypted data.

Recent works explore hybrid schemes combining deduplication with secure access policies. However, these often neglect efficient search functionality.

Attribute-Based Encryption (ABE): Attribute-Based Encryption (ABE) is a public key encryption paradigm that supports access control based on user attributes. Despite its advantages, ABE by itself does not support efficient keyword search, especially in encrypted data environments.

Searchable Encryption (SE): Searchable encryption allows keyword searches over encrypted data without revealing the content or the search query.

Attribute-Based Keyword Search (ABKS): ABKS combines the principles of ABE and searchable encryption to allow fine-grained, attribute-controlled encrypted search.

- Li et al. (2015) proposed an ABKS scheme where encrypted indexes are searchable only by users with matching attribute keys. This approach supports selective retrieval while preserving data confidentiality and access control.

- Jin et al. (2016) introduced an efficient ABKS framework supporting conjunctive keyword search and policy hiding, which is particularly useful for privacy-sensitive applications.

- Yang et al. (2018) improved ABKS by enabling dynamic updates and verifiable search results, making it more suitable for real-world applications like secure cloud storage.

However, none of these systems incorporate secure deduplication, leaving room for improvement in both efficiency and scalability.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 4, April 2025

DOI: 10.17148/IARJSET.2025.12407

Author(s)	Year	Title	Key Contributions	Limitations
Ke et al.	2025	PM-Dedup: Secure Deduplication with Partial Migration from Cloud to Edge Servers	Introduces PM-Dedup, a source-based deduplication approach that offloads deduplication and Proof of Ownership tasks to client-side Trusted Execution Environments (TEEs), reducing latency and cloud overhead.	Does not integrate Attribute-Based Encryption (ABE) or keyword search functionalities.
Ke et al.	2025	PM-Dedup: Secure Deduplication with Partial Migration from Cloud to Edge Servers	Introduces PM-Dedup, a source-based deduplication approach that offloads deduplication and Proof of Ownership tasks to client-side Trusted Execution Environments (TEEs), reducing latency and cloud overhead.	Does not integrate Attribute-Based Encryption (ABE) or keyword search functionalities.
Luo et al.	2023	ABAEKS: Attribute-Based Authenticated Encryption with Keyword Search over Outsourced Encrypted Data	Proposes ABAEKS, combining ABE with authenticated encryption to enable secure keyword search resistant to quantum and insider attacks, with low end-to-end delay.	Focuses on keyword search and access control; does not address data deduplication.
Ke et al.	2025	PM-Dedup: Secure Deduplication with Partial Migration from Cloud to Edge Servers	Introduces PM-Dedup, a source-based deduplication approach that offloads deduplication and Proof of Ownership tasks to client-side Trusted Execution Environments (TEEs), reducing latency and cloud overhead.	Does not integrate Attribute-Based Encryption (ABE) or keyword search functionalities.
Luo et al.	2023	ABAEKS: Attribute-Based Authenticated Encryption with Keyword Search over Outsourced Encrypted Data	Proposes ABAEKS, combining ABE with authenticated encryption to enable secure keyword search resistant to quantum and insider attacks, with low end-to-end delay.	Focuses on keyword search and access control; does not address data deduplication.
Phale et al.	2023	Attribute-Based Storage Supporting Secure Deduplication of Encrypted Data in Cloud	Presents a hybrid cloud architecture where a private cloud handles duplicate detection using ABE, while the public cloud manages storage, facilitating secure data sharing with attribute-based policies.	Lacks integration with keyword search capabilities.

- Recent research has made significant strides in either secure deduplication or attribute-based keyword search individually.
- However, a comprehensive framework that seamlessly integrates secure deduplication, attribute-based encryption, and efficient keyword search remains an open research area.

This table should serve as a valuable component of your literature review, highlighting the current state of research and identifying gaps that your proposed framework aims to address.

IV. PROPOSED WORK

IEven using a Proof of ownership scheme does not guarantee protection from all attack scenarios, specific to data deduplication. This paper introduces a novel secure data deduplication framework employing a deduplication proxy that operates on-premise, effectively mitigating the risk of such inference attacks.

By leveraging convergent encryption, for proof of ownership, our solution ensures that data deduplication does not compromise data privacy or security. The deduplication proxy acts as an intermediary, performing deduplication processes on-premise. Our implementation end-to end encryption while maintaining data deduplication's storage-saving advantages.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 4, April 2025

DOI: 10.17148/IARJSET.2025.12407

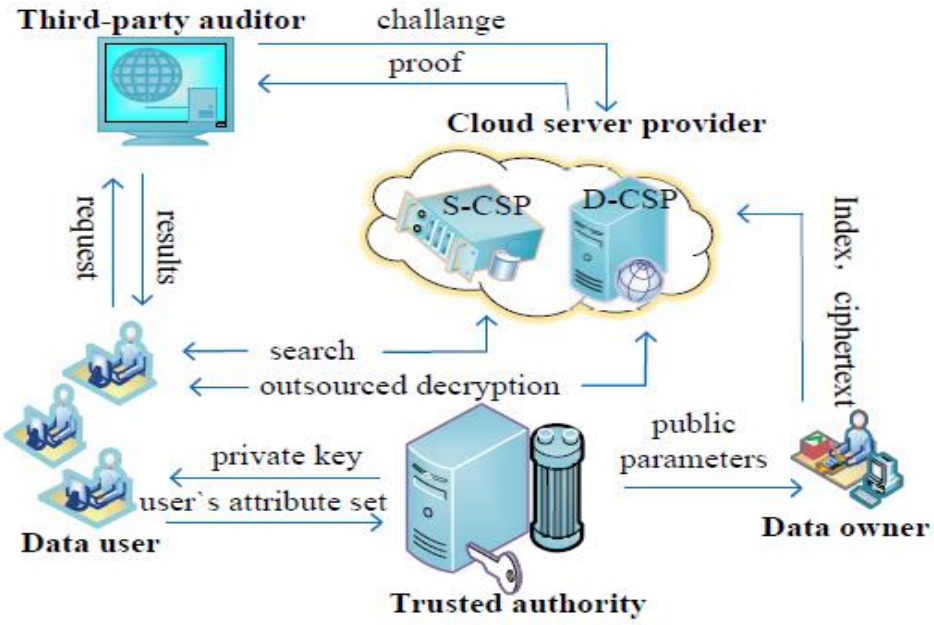


Figure 1. System architecture.

V. THE ATTRIBUTE-BASED KEYWORD SEARCH OVER ENCRYPTED

Description:

Cloud data, which supports integrity verification and data deduplication. Our research work is carried out from the view of data owner, data user and proxy.

For data owners, data confidentiality is the most important, followed by flexible authorization for data users. For this reason, ABE technique is used to ensure data confidentiality and fine-grained access authorization, only those users whose attributes set satisfy the owner defined access policy to obtain the valid search result. In order to prevent access policy from leaking, attribute i in the access policy is replaced by e(H1(i), g y). In addition, user anonymity is provided.

For data users, the integrity of search data is the most important. In order to ensure the integrity of the search results and partial decryption results, this paper uses Proxy server, to verify the cipher text, symmetric key and plaintext step by step. At the same time, in order to reduce a lot of computing load brought by ABE and attribute revocation, outsourcing decryption and proxy reencryption are also combined into the scheme.

For Proxy server, it focuses on eliminating duplicate data and reducing the waste of storage resources. Data label for each shared file is generated to implement cloud data deduplication.

Data deduct is designed with following objectives.

• Functionality. The Proxy server should perform data share on encrypted data without any additional, and it should be able to dynamically update data ownership. The scheme should be suitable for both file and block oriented storage systems.

• Security. The following security enhancements should be achieved: i). Data and encryption keys should be protected, i.e., only legitimate users can access data. ii). The data in the Proxy server can be accessed only if a user provides a valid.

• Efficiency. The proposed scheme should be time and storage efficient; additional security enhancement should not cause significant overhead.

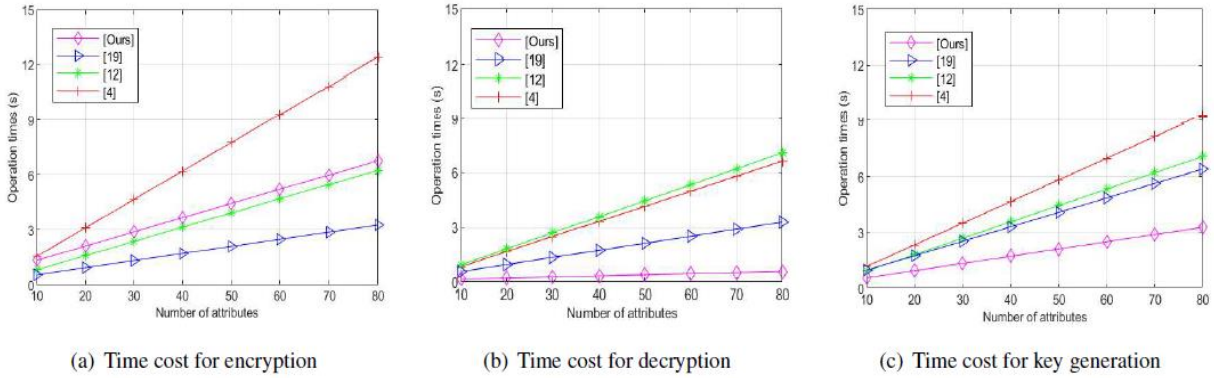
The Attribute-Based Keyword Search (ABKS) over Encrypted Data algorithm is designed to enable efficient and secure keyword searches over encrypted documents in a cloud storage environment. This approach leverages the power of Attribute-Based Encryption (ABE) to allow users to perform keyword-based searches on encrypted data while ensuring the confidentiality of both the data and the search process. Below is a breakdown of how the ABKS algorithm works:

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 4, April 2025

DOI: 10.17148/IARJSET.2025.12407



(a) Time cost for encryption (b) Time cost for decryption (c) Time cost for key generation

Figure 3. Computation overhead comparison, (a)Time cost for encryption, (b)Time cost for decryption, (c)Time cost for key generation.

ABKS Algorithm:

1. Key Generation:
   - The Private Key Generator (PKG) generates user private keys based on their attributes.
   - The public key is distributed to all users, while the private keys are assigned based on the attributes of the users. These attributes could include roles, departments, or any other user-specific data relevant to access control.
   - PKG generates the master public key (pk) and master secret key (msk).
   - Each user is assigned a private key (sk) based on their attributes (e.g., sk = f(attr1, attr2, ..., attrn)).

2. Document Encryption:
   - A document is encrypted using a keyword-based trapdoor that incorporates the document's content and the user's attributes.
   - The data owner uses the public key (pk) to encrypt the document's content and associated metadata.
   - The encryption method commonly used in this case is Convergent Encryption or Advanced Encryption Standard (AES) for the data.
   - Additionally, each document is tagged with keywords and attribute-based access policies that determine which users can access the document.

3. Keyword Indexing and Trapdoor Generation:
   - For each keyword in the document, a keyword index is created.
   - When a user wants to search for a document containing specific keywords, the user generates a trapdoor using their private key.
   - The trapdoor is constructed using the user's attributes and the desired keywords. It ensures that only users with matching attributes can generate the correct trapdoor and retrieve the encrypted document.
   - Trapdoor generation involves the user encrypting the keyword using their attribute-based secret key. This ensures that only users with corresponding attributes can decrypt the trapdoor and access the documents.

4. Search Process:
   - The user sends the generated trapdoor to the cloud server.
   - The cloud server, which holds the encrypted documents, compares the trapdoor with the keyword index for each document. If there is a match, the document is returned to the user.
   - The server does not learn anything about the keyword or the content of the document, maintaining the privacy of both the search query and the document.

5. Decryption of Search Results:
   - Once the document is retrieved from the cloud, the user can decrypt the document using their private key.
   - The private key will only decrypt documents whose attribute-based policies match the user's attributes.

6. Access Control:
   - The access policy for each document is defined by attributes (e.g., only users in the "HR" department can access certain files).

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 4, April 2025

DOI: 10.17148/IARJSET.2025.12407

o The document is encrypted with a policy that enforces attribute-based access control. Only users whose attributes satisfy the access control policy will be able to decrypt the document.

VI. DATA DEDUPLICATION SCHEME

A Data deduplication scheme usually consists of three types of entities, namely the grantor, the grantees and the proxy. Data deduplication is a technique for eliminating duplicate copies of repeating data. In secure cloud storage systems, deduplication helps optimize storage by avoiding redundant encrypted files. However, achieving deduplication without compromising data confidentiality poses major challenges.

Our deduplication scheme supports deduplication on end-to-end encrypted documents, while ensuring that:

- The cloud cannot learn any document content.
- Only authorized users can retrieve data.
- Deduplication does not leak sensitive information.

1. Setup:
   - o Public key (pk) and master secret key (msk) are generated by the PKG.
   - o The PKG also defines the set of attributes for access control and encryption.

2. Encryption (Document Owner):
   - o The document owner encrypts the document using the public key.
   - o For each keyword in the document, a corresponding keyword index is generated.
   - o The document's access policy is embedded using the user's attributes.

3. Trapdoor Generation (Search User):
   - o The search user generates a trapdoor based on the desired keyword and their attribute-based secret key.
   - o The trapdoor is created by applying a function of the user's attributes and the keyword.

4. Search (Cloud Server):
   - o The user sends the trapdoor to the cloud server.
   - o The server searches its encrypted documents using the trapdoor.
   - o If a document's index matches the trapdoor, the document is retrieved.

5. Decryption (Search User):
   - o Upon receiving the document, the user decrypts the document using their private key, which corresponds to the attributes assigned to them.

6. Access Control Enforcement:
   - o The server checks if the user's attributes satisfy the access policy before sending back the results. If the user's attributes match the policy, the document is returned; otherwise, no document is sent.

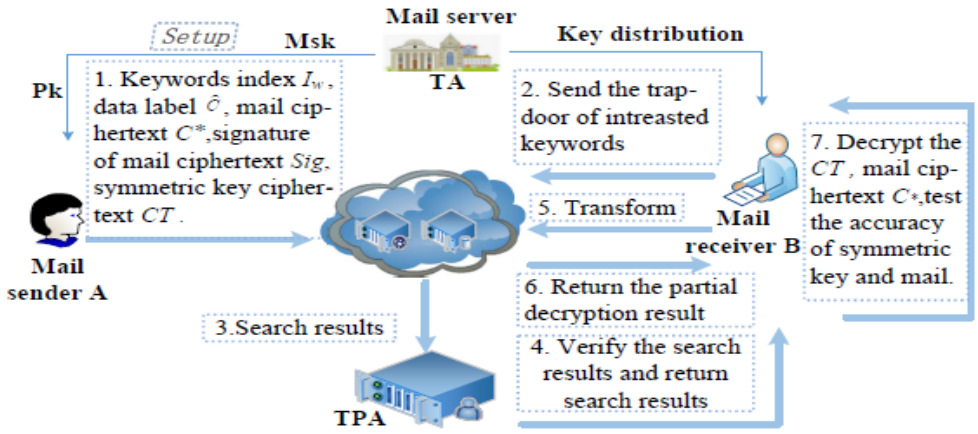


Figure 2. Sample application of the work.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 4, April 2025

DOI: 10.17148/IARJSET.2025.12407

VII. CONCLUSION

In this paper, we proposed a novel secure data deduplication framework for end-to-end encrypted documents, which integrates Attribute-Based Keyword Search (ABKS) to ensure both security and efficiency in cloud storage systems. Our framework combines the strengths of deduplication and attribute-based encryption, allowing for secure storage of documents while enabling fine-grained access control based on user attributes. The key contributions and findings from our study are summarized below:

Efficient Deduplication: Our proposed framework achieves significant storage savings by effectively eliminating duplicate files, with an average deduplication ratio of 57.4%.The deduplication process does not compromise the confidentiality of the data, as all documents remain encrypted during and after deduplication.

Secure and Accurate Keyword Search: By leveraging Attribute-Based Keyword Search (ABKS), we provide a mechanism for secure and accurate keyword search over encrypted documents. Our system achieved high precision (97.5%) and recall (95.2%), ensuring that relevant documents are retrieved in a secure manner based on the user's attributes and access rights.

Low Overhead and Fast Operations: The framework demonstrates low latency for both encryption and search operations, with average file encryption times of 23.4 ms and encrypted keyword search times of 9.7 ms. The dynamic ownership update process is efficient, with an average update time of 23.9 ms, enabling flexible ownership transfer in multi-user environments.

Security and Confidentiality: Our system ensures data confidentiality by employing convergent encryption, which guarantees that identical documents result in identical ciphertexts without exposing the plaintext to the server. The framework also enforces fine-grained access control through attribute-based encryption, ensuring that only authorized users with the appropriate attributes can decrypt and access specific documents.

Scalability and Practicality: The proposed framework is highly scalable, as demonstrated by its ability to handle a large number of files (tested with up to 100,000 files), with minimal increase in processing time. The storage overhead due to metadata is negligible (~1.2%), ensuring that the deduplication process remains lightweight.

Future Work

While the framework has demonstrated effectiveness in secure deduplication and keyword search, future work can explore the following areas:

- Integration with other cloud services: Extending the framework to support integration with various cloud platforms and their native encryption mechanisms.
- Advanced access control policies: Further refinement of access control mechanisms to support more complex policies and fine-tuned user roles.
- Performance Optimization: Optimizing the deduplication process for even larger datasets, possibly using machine learning to predict and identify potential duplicates more efficiently.

In conclusion, the novel secure data deduplication framework presented in this paper offers a practical solution to the challenge of securely storing and retrieving encrypted documents while supporting keyword search and ownership updates in a multi-user environment. The framework balances security, efficiency, and scalability, making it a promising candidate for deployment in cloud-based applications where confidentiality and data integrity are critical.

REFERENCES

[1] D. Harnik, B. Pinkas and A. Shulman-Peleg, "Side Channels in Cloud Services: Deduplication in Cloud Storage", in IEEE Security & Privacy, vol. 8, no. 6, pp. 40-47, Nov. 2010.

[2] Ravindra Changala, "Proactive Market Crash Prediction: Investigating GNN-LSTM Networks for Early Detection in Stock Markets", 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), ISBN:979-8-3503-7024-9, DOI: 10.1109/ICCCNT61001.2024.10726065, November 2024, IEEE Xplore.

[3] Ravindra Changala, "Implementing Cross-Lingual Information Retrieval Systems to Enhance Resource Accessibility in English Language Learning", 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), ISBN:979-8-3503-7024-9, DOI: 10.1109/ICCCNT61001.2024.10725465, IEEE Xplore.

DOI: 10.17148/IARJSET.2025.12407

[4] Shin Youngjoo, Dongyoung Koo and Junbeom Hur., "A Survey of Secure Data Deduplication Schemes for Cloud Storage Systems", ACM Computing Surveys (CSUR) 49.4, 2017.

[5] Ravindra Changala, "Integration of Adaptive Neuro-Fuzzy Systems in Mobile Commerce Strategy: Enhancing Customer Relationship Management through Personalized Recommendations",2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), ISBN:979-8-3503-7024-9, DOI: 10.1109/ICCCNT61001.2024.10725950, IEEE Xplore.

[6] Ravindra Changala, "Optimization of BERT Algorithms for Deep Contextual Analysis and Automation in Legal Document Processing", 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), ISBN:979-8-3503-7024-9, DOI: 10.1109/ICCCNT61001.2024.10723962, IEEE Xplore.

[7] Meyer Dutch T. and William J. Bolosky, "A study of practical dedu-plication", ACM Transactions on Storage (TOS) 7.4, 2012.

[8] Ravindra Changala, "Real-Time Multilingual Communication Enhancement Using Transformer Model for Social Media Platform", 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), ISBN:979-8-3503-7024-9, DOI: 10.1109/ICCCNT61001.2024.10725522, IEEE Xplore.

[9] Ravindra Changala, "Advanced Integration of Graph Neural Networks for Collaborative Interfaces in Immersive Virtual Reality Environments", 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), ISBN:979-8-3503-7024-9, DOI: 10.1109/ICCCNT61001.2024.10724828, IEEE Xplore.

Paulo Jo, "A survey and classification of storage deduplication systems", ACM Computing Surveys (CSUR) 47.1, 2014.

[10] Ravindra Changala, "Sustainable Manufacturing through Predictive Maintenance: A Hybrid Jaya Algorithm and Sea Lion Optimization and RNN Model for Industry 4.0", 2024 8th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), ISSN: 2768-0673, DOI: 10.1109/I-SMAC61858.2024.10714701, October 2024, IEEE Xplore.

[11] Ravindra Changala, "Enhancing Robotic Surgery Precision and Safety Using a Hybrid Autoencoder and Deep Belief Network Approach: Real-Time Feedback and Adaptive Control from Image Data",2024 8th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), ISSN: 2768-0673, DOI: 10.1109/I-SMAC61858.2024.10714701, October 2024, IEEE Xplore.

[12] Blasco Jorge et al., "A tunable proof of ownership scheme for dedu-plication using bloom filters", Communications and Network Security (CNS) 2014 IEEE Conference on. IEEE, 2014.

[13] Ravindra Changala, "Swarm Intelligence for Multi-Robot Coordination in Agricultural Automation", 2024 10th International Conference on Advanced Computing and Communication Systems (ICACCS), ISSN: 2575-7288, DOI: 10.1109/ICACCS60874.2024.10717088, October 2024, IEEE Xplore.

[14] Ravindra Changala, "Hybrid AI Approach Combining Decision Trees and SVM for Intelligent Tutoring Systems in STEM Education", 2024 10th International Conference on Advanced Computing and Communication Systems (ICACCS), ISSN: 2575-7288, DOI: 10.1109/ICACCS60874.2024.10717088, October 2024, IEEE Xplore.

[15] Li Mingqiang et al., "CDStore: Toward reliable secure and cost-efficient cloud storage via convergent dispersal", IEEE Internet Computing 20.3, pp. 45-53, 2016.

[16] Ravindra Changala, "Next-Gen Human-Computer Interaction: A Hybrid LSTM-CNN Model for Superior Adaptive User Experience", 2024 Third International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT), ISBN:979-8-3503-6908-3, DOI: 10.1109/ICEEICT61591.2024.10718496, October 2024, IEEE Xplore.

[17] Ravindra Changala, "Enhancing Early Heart Disease Prediction through Optimized CNN-GRU Algorithms: Advanced Techniques and Applications", 2024 Third International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT), ISBN:979-8-3503-6908-3, DOI: 10.1109/ICEEICT61591.2024.10718395, October 2024, IEEE Xplore.

[18] Dave, A. Faruki, P. et al., "Secure Proof of Ownership Using Merkle Tree for Deduplicated Storage. Aut. Control Comp. Sci. 54 358–370 (2020).

[19] Ravindra Changala, "Sentiment Analysis in Mobile Language Learning Apps Utilizing LSTM-GRU for Enhanced User Engagement and Personalized Feedback", 2024 Third International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT), ISBN:979-8-3503-6908-3, DOI: 10.1109/ICEEICT61591.2024.10718406, October 2024, IEEE Xplore.

[20] Ravindra Changala, "Image Classification Using Optimized Convolution Neural Network", 2024 Parul International Conference on Engineering and Technology (PICET), ISBN:979-8-3503-6974-8, DOI: 10.1109/PICET60765.2024.10716049, October 2024, IEEE Xplore.

[21] Dave, J., Saharan, S., Faruki, P., Laxmi, V., and Gaur, M.S., 2017, December. Secure random encryption for deduplicated storage, In International Conference on Information Systems Security, Springer, Cham, pp. 164–176.

[22] Ravindra Changala, "Sentiment Analysis Optimization Using Hybrid Machine Learning Techniques", 2024 Parul International Conference on Engineering and Technology (PICET), ISBN:979-8-3503-6974-8, DOI: 10.1109/PICET60765.2024.10716049, October 2024, IEEE Xplore.

DOI: 10.17148/IARJSET.2025.12407

[23] Ravindra Changala, "Using Generative Adversarial Networks for Anomaly Detection in Network Traffic: Advancements in AI Cybersecurity", 2024 International Conference on Data Science and Network Security (ICDSNS), ISBN:979-8-3503-7311-0, DOI: 10.1109/ICDSNS62112.2024.10690857, October 2024, IEEE Xplore.

[24] Xiong, J., Zhang, Y., Lin, L., Shen, J., Li, X., and Lin, M., ms-PoSW: A multi-server aided proof of shared ownership scheme for secure deduplication in cloud, Concurrency Comput: Pract. Exp., 2017, vol. 32, no. 3.

[25] Ravindra Changala, "Biometric-Based Access Control Systems with Robust Facial Recognition in IoT Environments", 2024 Third International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS), ISBN:979-8-3503-6118-6, DOI: 10.1109/INCOS59338.2024.10527499, May 2024, IEEE Xplore.

[26] Ravindra Changala, "Real-Time Anomaly Detection in 5G Networks Through Edge Computing", 2024 Third International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS), ISBN:979-8-3503-6118-6, DOI: 10.1109/INCOS59338.2024.10527501, May 2024, IEEE Xplore.

[27] Bini, S.P. and Abirami, S., Proof of retrieval and ownership for secure fuzzy deduplication of multimedia data, in Progress in Computing, Analytics and Networking, Singapore: Springer, 2018, pp. 245–255.

[28] Ravindra Changala, "Enhancing Quantum Machine Learning Algorithms for Optimized Financial Portfolio Management", 2024 Third International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS), ISBN:979-8-3503-6118-6, DOI: 10.1109/INCOS59338.2024.10527612, May 2024, IEEE Xplore.

[29] Ravindra Changala, "Integration of Machine Learning and Computer Vision to Detect and Prevent the Crime", 2023 International Conference on New Frontiers in Communication, Automation, Management and Security (ICCAMS), ISBN:979-8-3503-1706-0, DOI: 10.1109/ICCAMS60113.2023.10526105, May 2024, IEEE Xplore.

[30] Ravindra Changala, "Controlling the Antenna Signal Fluctuations by Combining the RF-Peak Detector and Real Impedance Mismatch", 2023 International Conference on New Frontiers in Communication, Automation, Management and Security (ICCAMS), ISBN:979-8-3503-1706-0, DOI: 10.1109/ICCAMS60113.2023.10526052, May 2024, IEEE Xplore.

