IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.12406

Optimizing Cloud Computing Performance through Scalable Hybrid Process Modelling

B Sharath raj[1], Dr Murugan R[2]

Student, Department of Computer Science and IT Jain (Deemed to be) University

Karnataka -560041, Bengaluru, India[1]

MCA, Computer Science and IT Jain (Deemed to be) University

Karnataka -560041, Bengaluru, India[2]

Abstract: A smart health system that benefits both patients and doctors is a personal health record (PHR) system. Typically, a PHR is managed and kept on the cloud by a semi-reliable cloud service provider. Nonetheless, there is still a chance that untrusted people and semi trusted parties could see confidential health information. In this article, a patient-centric PHR sharing structure is suggested in order to safeguard patients' privacy and guarantee that they have control over their PHRs. This framework eliminates the key hosting issue and achieves fine-grained access control to PHRs by encrypting all PHRs with multiauthority attribute-based encryption prior to outsourcing. In order to guarantee data integrity on the cloud and protect the user's identity during authentication, an anonymous authentication between the cloud and the user is also suggested. The new online-offline attribute-based signature that the proposed authentication is based on is issued. It can strengthen patients' control over their PHRs by making the encrypted PHRs resistant to collusion attempts and preventing forgery during the sharing time. Decryption that is done online-offline and through outsourcing also lowers computation costs and boosts productivity. Lastly, comparisons based on numerical trials are shown.

Keywords: Process discovery; hybrid process model; event log; big data; service computing; cloud computing

I. INTRODUCTION

1.1 General Introduction

ECC, an alternative technique to RSA, is a powerful cryptography approach. It generates security between key pairs for public key encryption by using the mathematics of elliptic curves.

RSA does something similar with prime numbers instead of elliptic curves, but ECC has gradually been growing in popularity recently due to its smaller key size and ability to maintain security. This trend will probably continue as the demand on devices to remain secure increases due to the size of keys growing, drawing on scarce mobile resources. This is why it is so important to understand elliptic curve cryptography in context.

In contrast to RSA, ECC bases its approach to public key cryptographic systems on how elliptic curves are structured algebraically over finite fields. Therefore, ECC creates keys that are more difficult, mathematically, to crack. For this reason, ECC is considered to be the next generation implementation of public key cryptography and more secure than RSA.

It also makes sense to adopt ECC to maintain high levels of both performance and security. That’s because ECC is increasingly in wider use as websites strive for greater online security in customer data and greater mobile optimization, simultaneously. More sites using ECC to secure data means a greater need for this kind of quick guide to elliptic curve cryptography.

An elliptic curve for current ECC purposes is a plane curve over a finite field which is made up of the points satisfying the equation:
$y^2=x^3 + ax + b$.

In this elliptic curve cryptography example, any point on the curve can be mirrored over the x-axis and the curve will stay the same. Any non-vertical line will intersect the curve in three places With the improvement of cloud services, data proprietors are getting motivated in outsourcing their data into the cloud server to achieve better access and storage facility at a low cost. Encrypting the data before outsourcing into the cloud is considered as a general approach for protecting data privacy. Even though encryption protects the data against unauthorized access, but at the same time, it also activates *inconvenience for the authorized users* in accessing the encrypted data at large.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 4, April 2023
DOI: 10.17148/IJARCCE.2023.12406

As a result, much research is being carried out so as to quickly retrieve the information from the huge pool of data using some **keyword-based search techniques**. It has become a challenge for the researchers to give an efficient multi-keyword search model. Privacy-preserving conjunctive keyword search system over encrypted cloud data cares the update operations dynamically. The index structure is constructed on the basis of **Multi-Attribute Tree (MAT)** and an effective search procedure which is known as search MAT algorithm is introduced. In order to enhance the efficiency of the text searching the index structure based on the **Hierarchical Agglomerative Clustering tree index (HAC-tree)** is proposed. To encrypt the index of HAC tree and query vector, this method uses the secure inner product algorithm. In this, Non-candidate Pruning Depth First Algorithm is used to search the corresponding file in the tree which prunes the sub-tree which does not contain any search result to increase the relevance of the searched keyword to the cloud file, the coordinate matching along with inner product similarity is introduced. Reverse data structure to permit users to accomplish dynamic operations on document collection is proposed, which perform either inserting or deleting. The sparse matrix is used to encrypt the index matrix and query vector to enhance efficiency to provide privacy for both cloud service providers as well as data users, the new **Oblivious Multiple Keyword Search (OMKS)** is proposed.

The proposed protocol support multiple keyword searches such as conjunctive keyword search and disjunctive keyword search. In the disjunctive keyword search, it apprehends in a simple way that it sends the values of the keyword to the server in the query. In the conjunctive keyword search, the addition of all keywords values is used as the fresh keywords values involved in the calculation. By using these two searches this method achieves efficient search and matched cipher text the multi-keyword tree-based search scheme is proposed to provide security to the sensitive information of the data owners. The document collection in the cloud environment is achieved through the hierarchical clustering method. To generate an encrypted index as well as query vectors, the vector space model is used and to achieve efficient search, DFS algorithm is used. The secure proposed algorithm is used to encrypt the query vectors.

The clustering of documents is performed using bisecting k-means clustering. Context-aware search is introduced to make semantic search smart. The proposed method first introduces the **Semantic Compound Keyword Search (SCKS)** as a knowledge representation tool. Two schemes are proposed based on CG. This method converts original CG into their corresponding linear form with few modifications and it matches them to numerical vectors. Ranked multi keyword search over encrypted data in the cloud is introduced on the basis of two threat models. To resolve the problem in the privacy-preserving smart semantic search based on CGs, the proposed scheme uses PRSCG and PRSCG-TF schemes. The compound concept semantic similarity evaluation method is projected to quantify the similarity between the compound concepts. This method integrates both secure K nearest neighbour scheme and CCSS with Locality Sensitive Hashing Function, thus proposing the **Semantic Compound Keyword Search (SCKS)**. The goal of secure this scheme is to steadily recognize the K-Nearest points in the encrypted databank to a provided encrypted query. This proposed method not only achieves semantic-based search but at the same time also performs a multi-keyword search and ranks the searched result

1.2 OBJECTIVE:

The main objective is,

- To performance Blockchain
- To perform the, Encryption and Decryption with less data loss.
- To implement the hybrid AES and ECC learning algorithm.
- To enhance the performance analysis.

1.3 PROBLEM STATEMENT

- To perform the, Encryption and Decryption with less data loss.
- Although this method is straightforward and user, it has some severe limitations.
- Time taken to done the Encryption and decryption is very low, when compared with the other techniques

II. SYSTEM PROPOSAL

2.1 EXISTING SYSTEM

- The use of a proxy server in a **Cloud Service Provider (CSP)** reduces search time and increases search efficiency by utilizing a **Boolean search** in the proxy server.
- Main server supports multiple users at a time with the help of Deep learning based Neural Network, which provides an accurate result.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.12406

- Trusted Authority is employed to provide secure document retrieval for authorized user. TA manages dual security processes as key management and Security Device Issuing.
- Secure top k ranking is achieved using Euclidean distance calculation and accuracy of document retrieval is improved.

2.1.1 DISADVANTAGE

- Encryption and decryption file on time high
- Along with that, data loss is more when compared with the other conventional methods.

2.2 PROPOSED SYSTEM

- Cloud services have increased the number of data owners it has been store their encrypted data in the cloud, while an equal or greater number of data users based in data retrieval.

- It is based on Blockchain
- **Hybrid ECC and AES Algorithm** using the Encrypted and Decrypted the dataset
- Encrypted File will be Stored in Cloud Server and User based on Keyword Searching for Algorithm.
- User based Enter the keyword that also Encrypted Query After that Searching Encrypted Cloud Server
- Finally, Retrieval process is done to fetch the encrypted file, which is Related to the Query data.
- User based enter the Particular key user decrypts File the better performance better performance in terms of recall, ranking privacy, precision, searching time.

2.2.1 ADVANTAGE:

- Time taken to done the Encryption and decryption is very low, when compared with the other techniques.
- Easy to retrieve the data from the cloud.
- Data loss is low, in the receiver side during the decryption process

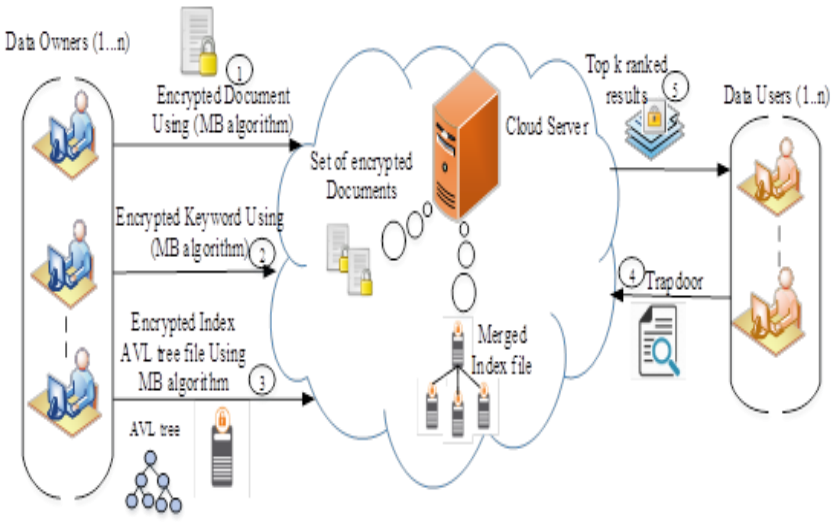

Fig 1. Proposed architectural design

3.2 **Key Generation**: Hybrid AES and ECC based on 128 bits key Generated For Encrypted data Wise. A encryption system is designed by combining the characteristics of the AES and ECC Which Can solve Security Problem itself Efficiently realize the information, data encryption, signature, and
identity verification.

3.2 **Classification:** Machine learning is a method of data analysis that automates analytical model building. It is a branch of artificial intelligence based on the idea that systems can learn from data, identify patterns and make decisions with minimal human intervention.

3.2.1 Random forest algorithm creates decision trees on data samples and then gets the prediction from each of them and finally selects the best solution by means of voting.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 4, April 2023
DOI: 10.17148/IJARCCE.2023.12406

3.2.2 Decision Tree Simple to understand and to interpret. Trees can be visualised. Requires little data preparation. k-nearest neighbours (KNN) algorithm is a simple, supervised machine learning algorithm that can be used to solve both classification and regression problems

4.2 **Generation:** Accuracy , precision Recall,f1-score

III. CONCLUSION

In this scheme, the identity and attributes of the user are hidden and known only to the trusted central authority. To prevent cloud server from tampering with cipher text or spoofing end users, an anonymous authentication based on attribute-based signature is proposed. In the whole access-control process, only authorized users can access and obtain messages. For achieving lightweight computation, online and offline technique and outsourcing operations are used. Compared with the existing works, the proposed scheme not only keeps the encrypted PHRs to resist collusion attacks and not to be attack

REFERENCES

[1] L. Zhang, Y. Zhang and H. Ma, "Privacy-Preserving and Dynamic Multi-Attribute Conjunctive Keyword Search Over Encrypted Cloud Data", IEEE Access, vol. 6, pp. 34214-34225, 2018.
[2] Z. Xiangyang, D. Hua, Y. Xun, Y. Geng, and L. Xiao, "MUSE: An Efficient and Accurate Verifiable Privacy-Preserving Multi-keyword Text Search over Encrypted Cloud Data", Security and Communication Networks, vol. 2017, pp. 1-17, 2017.
[3] L. Chen, L. Qiu, K-C. Li, W. Shi, and N. Zhang, "DMRS: an efficient dynamic multi-keyword ranked search over encrypted cloud data", Soft Computing, vol. 21(16), pp. 4829–4841, 2017.
[4] R. Zhang, R. Xue, L. Liu, and L. Zheng, "Oblivious Multi-Keyword Search for Secure Cloud Storage Service", 2017 IEEE 24th International Conference on Web Services, pp. 269-276, 2017.
[5] P. K. Samantaray, N. K. Randhawa, and S. L. Pati, "An Efficient Multi-keyword Text Search Over Outsourced Encrypted Cloud Data with Ranked Results", Computational Intelligence in Data Mining, pp. 31-40, 2018.
[6] Z. Fu, F. Huang, K. Ren, J. Weng, and C. Wang, "Privacy-Preserving Smart Semantic Search Based on Conceptual Graphs Over Encrypted Outsourced Data", IEEE Transactions On Information Forensics And Security, vol. 12(8), pp. 1874-1884, 2017.
[7] B. Lang, J. Wang, M. Li, and Y. Liu, "Semantic-based Compound Keyword Search over Encrypted Cloud Data", IEEE Transactions On Services Computing, 2018.
[8] Z. Fu, L. Xia, X. Sun, A. X. Liu, and G. Xie, "Semantic-aware Searching over Encrypted Data for Cloud Computing", IEEE Transactions on Information Forensics and Security, vol. 13(9), pp. 2359-2371, 2018.
[9] Z. Wu, and K. Li, "VBTree: forward secure conjunctive queries over encrypted data for cloud computing", The VLDB Journal, pp. 1–22, 2018.
[10] Y. Yang, X. Liu, and R. H. Deng, "Multi-user Multi-Keyword Rank Search over Encrypted Data in Arbitrary Language", IEEE Transactions on Dependable and Secure Computing, 2018.
[11] X. Ding, P. Liu, and H. Jin, "Privacy-Preserving Multi-keyword Top-k Similarity Search Over Encrypted Data", IEEE Transactions on Dependable and Secure Computing, 2018.
[12] Y. Li, F. Zhou, Y. Qin, M. Lin, and Z. Xu, "Integrity-verifiable conjunctive keyword searchable encryption in cloud storage", International Journal of Information Security, vol. 17(5), pp. 549–568, 2018.
[13] C. Guo, X. Chen, Y. Jie, Z. Fu, M. Li, and B. Feng, "Dynamic Multi-phrase Ranked Search over Encrypted Data with Symmetric Searchable Encryption", IEEE Transactions On Services Computing, 2018.
[14] Raghavendra S, Girish S, Geeta C. M., R. Buyya, Venugopal K. R., S. S. Iyengar, and L. M. Patnaik, "Split keyword fuzzy and synonym search over encrypted cloud data", Multimedia Tools and Applications, vol. 77(8), pp. 10135–10156, 2018.
[15] A. V. Vora, and S. Hegde, "Keyword-based private searching on cloud data along with keyword association and dissociation using cuckoo filter", International Journal of Information Security, pp. 1–15, 2018.
[16] H. Wang, X. Dong, and Z. Cao, "Secure and efficient encrypted keyword search for multi-user setting in cloud computing", Peer-to-Peer Networking and Applications, pp. 1–11, 2018.
[17] Z. Shen, J. Shu, and W. Xue, "Keyword Search with Access Control over Encrypted Cloud Data", IEEE Sensors Journal, vol. 17(3), pp. 858-868, 2017.
[18] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-Preserving Multi-Keyword Ranked Search overEncrypted Cloud Data," Proc. IEEE INFOCOM, pp. 829-837, Apr,2014.
[19] Jiadi Yu, Peng Lu, Yanmin Zhu, Guangtao Xue, Member, IEEE Computer Society, and Minglu Li, "Toward Secure Multikeyword Top k Retrieval over Encrypted Cloud Data", IEEE Transactions, July 2013.

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.12406

[20] Ming Li et al.," Authorized Private Keyword Search over Encrypted Data in Cloud Computing, IEEE proc. International conference on distributed computing systems, June 2011, pages 383-392.

[21] J. Li et al., "Fuzzy Keyword Search Over Encrypted Data in Cloud Computing," Proc. IEEE INFOCOM, 2010, pp. 441–45.

[22] Ming Li et al., "Toward Privacy-Assured and Searchable Cloud Data Storage Services", IEEE Transactions on Network, volume 27, Issue 4, July/August2013.

[23] D. Boneh, G.D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public Key Encryption with Keyword Search," Proc. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), 2004.

[24] Zhou et al., "K-Gram Based Fuzzy Keyword Search over Encrypted Cloud Computing "Journal of Software Engineering and Applications, Scientific Research , Issue 6, Volume 29-32,January2013.

[25] E.-J. Goh, "Secure Indexes," Cryptology ePrint Archive, http://eprint.iacr.org/2003/216.2003.

[26] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized Private Keyword Search over Encrypted Data in Cloud Computing," Proc. 31st Int'l Conf. Distributed Computing Systems (ICDCS '10), pp. 383-392, June 2011.

[27] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure Ranked Keyword Search over Encrypted Cloud Data," Proc. IEEE 30th Int'l Conf. Distributed Computing Systems (ICDCS'10), 2010.