Shodhasamhita : Journal of Fundamental & Comparative Research
Vol. VIII, No. 1(X) : 2021
ISSN: 2277-7067

ANALYSIS OF A SECURED KEY SEARCH AND DATA SHARING MECHANISM FOR CLOUD COMPUTING BASED ON RE-ENCRYPTION

[1]I. Shalini, [2]T. Raja Mohan Reddy, [3]Sd. Afrin, [4]P.Malyadri
[1,2,3]Dept of Computer Science and Engineering, Sree Venkateswara College Of Engineering, Nellore (Dt), Andhra Pradesh, India.
[4]Dept of Electronics and Communication Engineering, Sree Venkateswara College Of Engineering, Nellore (Dt), Andhra Pradesh, India.

ABSTRACT
With the growth of cloud infrastructure, the cost of hardware and software resources in computer infrastructure has greatly decreased. To maintain security, the data is frequently encrypted before being delivered to the cloud. After encryption, finding and transferring information is more difficult than finding and transmitting simple data. However, it poses a serious challenge for cloud service providers because customers want the cloud to perform a speedy search and deliver the results without revealing private data. We suggest a cipher text-policy attribute-based technique with key-word search and information sharing (CPAB-KSDS) for encrypted cloud data in order to address these issues. The proposed approach now not only provides attribute-based key-word search but also permits attribute-based information exchange at the same time, in contrast to the current solutions, which only support one of the two qualities.
Keywords: Attribute based proxy encryption, cloud data sharing.

INTRODUCTION

Distributed computing has emerged as the solution to the issue of managing and maintaining personal information as a result of the proliferation of personal electronic devices. It is predicated on the notion that users may quickly and affordably upload their data to the cloud. Information Technology ventures have also been impacted and overtaken by the growth of distributed computing. Distributed computing will inevitably run into problems with security and protection. Trait-based encryption is a prominent delegate because to its expressiveness in client's character and information, and encryption is the main technique for enabling information categorization [1]–[4].After the property based encoded information is transferred in the cloud, approved clients face two essential activities: information looking and information sharing. Shockingly, conventional quality based encryption simply guarantees the classification of data. As a result, it opposes looking and sharing. Imagine that a group of patients uses a Person Health Record (PHR) framework [5]–[7] to store their encoded individual health reports in the cloud, where Enc(Di; Pi;KWi) is a feature-based encryption of the health report Di under an entrance strategy Pi and a catchphrase KWi. The record Di may be recovered by experts using the method Pi. However, they were unable to locate the specific record by just writing the catchphrase. All things being equal, a specialist Aliceneedstoinitiallydownloadandunscrambletheencodedrecords.After unscrambling,shecanutilizethewatchword to look through the particularone from a lot of the decoded wellbeingrecords.Anotherbadly arranged situationisthatAliceendeavorstoimpartarecordto her associate, for the situation like shewants to counsel the report with a subjectmatter expert. In the present circumstance,sheshoulddownloadthescrambledrecords,then,atthatpoint,unscramblethem.Then,atthatpoint,afte rshehasprocured the basic record, she scramblesthe record utilizing the arrangement of thesubjectmatterexpert.Accordingly,thisframework is extremely wasteful as far aslooking and sharing. Also, the customaryquality based encryption (ABE) innovationutilizedinthecurrentPHRframeworksmay cause one more issue for watchwordupkeep in light of the fact that the ABEcalculationcouldn'tscalewellforcatchphrase refreshes 65 once the quantityof the records altogether increments. For instance, Alice from emergency clinic A confirmed it isn't the infectious ailment and changed the tag to "non-infectious" after reviewing a health report with the patient's self-stamped "infectious" tag. Alice truly wants to modify the tag from "infectious" to "non- infectious" without decoding the report in order to share a health report with another specialist from

emergency clinic B. Alice must develop a new tag for all common ciphertexts in order to maintain the security of the catchphrase because the conventional characteristic-based encryption with watchword search cannot support catchphrase renewing. According to the aforementioned scenarios, characteristic-based encryption isn't suitable for information exchange and searching. Moreover,characteristicbasedencryptionisn'tallaroundscaledwhenthereisanupdatesolicitationtothecatchphrase . Alice downloads and deciphers the ciphertexts in order to look at and share a specific record. However, given the abundance of ciphertexts, Alice finds this interaction to be implausible. The worse situation is that Alice, the owner of the information, must always be online since she must provide her private key for information decoding. As a result, the ABE setup ignores the benefits of cloud computing. Someone alternative method is to assign someone outsider to perform the research, re-encoding, and watchword updating tasks in place of Alice. Alice can keep her private key in the outsider's stash, and in this way, the outsider can carry out Alice's laborious task. Despite this, we want to fully believe the outsider in such a process since it has access to Alice's private key. All customer information, particularly sensitive information under delicate security, will be leaked if the outsider is penetrated.

LITERATURE REVIEW

Authors: Ali, Malik, and Khan for DaSCE: Data Security for Cloud Environment with Semi-Trusted Third Party Off-site information storage is a cloud service that frees clients from having to concentrate on their record-keeping infrastructure. However, there are significant safety risks when outsourcing records to a third-party administrative system. Additionally, data leaking may occur as a result of attacks by other cloud users and computers. We (a) put into effect a working prototypeofDaSCEandconsideritsoverallperformance based totally on the time fedoninthecourseofmorethanafewoperations.

Using fully anonymous attribute-based encryption, you may manage the access privileges and anonymity for cloud data. Authors: Jung, T., Li, X. Y., Wan, Z., and Wan, M. "Cloud computing is a cutting-edge computing paradigm that enables flexible, on-demand, and economical utilisation of computer resources. However, a lot of privacy issues arise as a result of the data being outsourced to specific cloud servers. Several Attribute-Based Encryption-based methods have been proposed to fully secure cloud storage. However, the majority of effort is concentrated on access control and data content privacy, with privilege control and identity privacy receiving far less attention.

Huang, X., Lu, R., and Li, J.; Liu, J. K.; Au, M. H.; and n this study, we provide a brand-new fine-grained two-factor authentication (2FA) access control system for web-based cloud computing services. A personal secret key and a portable security device are required for the attribute-based access control technique used in our recommended 2FA access control solution. Because a user cannot access the device if they don't maintain both, the method can increase system security, especially in situations where numerous users use the same computer for web-based cloud services.

PROPOSED SYSTEM

Previous studies failed to show that attribute-based strategies should be able to combine data sharing and key-word search without resorting to PKG. Therefore, in order to accomplish the objective for the PHR scenario described above, a new attribute-based strategy is required. Alternately, it might be argued that the problem can be easily solved by combining an AB-PRE scheme and an attribute-based key-word search approach (AB-KS). However, the combination should ultimately lead to two major problems: 1) The mixed system is no longer CCA secure, and 2) collusion attacks are possible.

In order to fully support keyword searching, information exchange, and the security of keyword privacy, an impermeable system is preferred. These concerns motivate us to design a method that:

1. Permits the records owner, subject to the unnecessary decryption process, to search and distribute the encrypted fitness file.helpskey-wordupdatingforthedurationofthestatisticssharingphase.
2. More significantly, does not want the PKG to continue to exist, either in the information sharing or keyword update segments.

3. The owner of the information may fully determine who should have access to the information that he has encrypted.

IMPLEMENTATION

The five elements that make up the CPAB-KSDS system are the PKG, the cloud server (which acts as a proxy), the owner of the fitness file, the delegator (who receives the original ciphertext), and the delegatee (who receives the re-encrypted ciphertext). The following is a description of the device's process.

Initialization of the system: The PKG is used to accomplish this phase. The PKG creates the machine's public parameters, which are accessible to all users, and the grasp secret key, which is saved privately via the PKG.

Registration: The PKG is used to complete the registration portion. When a person submits a registration request to the PKG, the PKG creates a user account that matches his set of attributes.

Ciphertext Upload: The owner of the personal fitness report encrypts his file using the keyword and the specific recipient's policy before uploading it to the cloud server.

Ciphertext Search: After creating a search token, the user asks the cloud server to do a search using the search token. The results of the cloud server's examination of the ciphertext using the Test algorithm are sent to the recipient.

Re-encryption: The delegator generates a re-encryption key and transmits the key and the re-encryption request to the cloud server. The cloud server converts the original encrypted document into a re-encrypted ciphertext in accordance with a new access policy. Decryption: The recipient (a delegatee or a delegator) asks the cloud server for a freshly encrypted (or an original) ciphertext in order to access the underlying record. He then uses the ciphertext's original encryption to decode it using his very own private key. Keep in mind that a delegatee might also serve as a delegator for other participants.

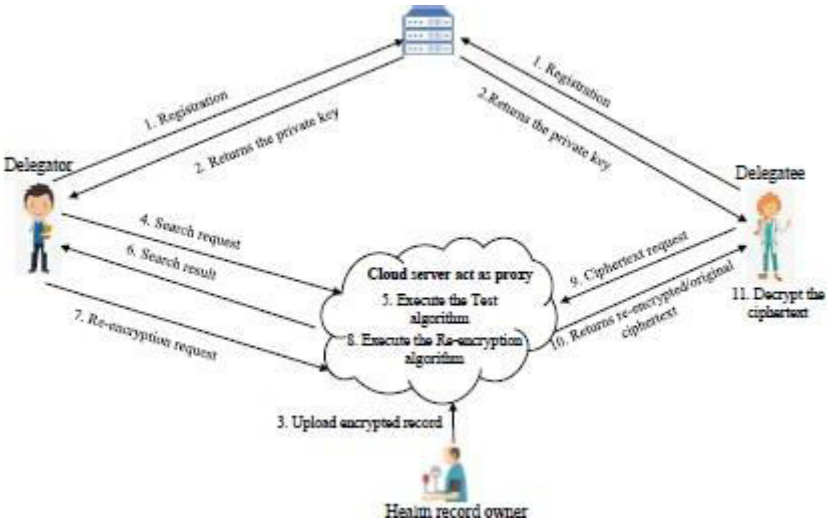

Fig1: Architecture

RESULTS AND DISCUSSIONS

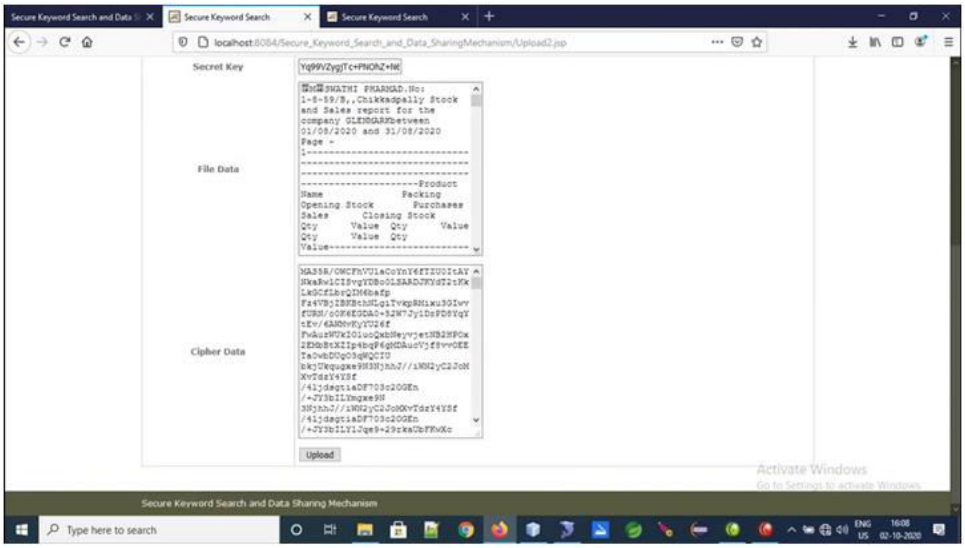

Fig.2.Encrypted Data

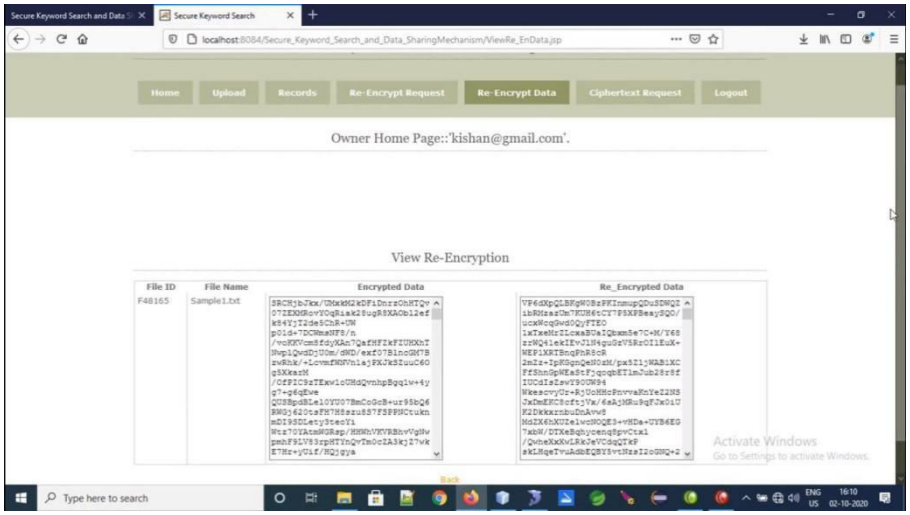

Fig.2.Re-encrypted data

CONCLUSION

In this work, another thought of cipher text- strategy property based instrument (CPAB-KSDS) is acquainted with help catch phrase looking and information sharing. A substantial CPAB-KSDS plot has been built in this paper and we demonstrate its CCA security in the arbitrary prophet model. In the display and property inspection, the suggested plot is demonstrated to be productive and beneficial. The preceding work raised an open testing challenge, which is to plan a property-based encryption with password searching and information sharing without the PKG at the sharing stage. This article provides a proven answer to that issue.

FUTURE ENHANCEMENT

Our approach also inspires intriguing open tasks, such as developing a CPAB-KSDS scheme without random oracles or putting forth a new framework to facilitate more expressive keyword search.

REFERENCES

1. A.SahaiandB.Waters,"Fuzzyidentity-basedencryption,"inAnnualInternationalConferenceontheTheoryandApplicationsofCryptographicTechniques,pp.457–473,Springer,2005.
2. V. Goyal, O. Pandey, A. Sahai, and B.Waters,"Attribute-basedencryptionforfine-grainedaccesscontrolofencrypteddata,"inProceedingsofthe13thACM conference on Computer

andcommunicationssecurity,986pp.89–98, Acm,2006.

3. J.Bethencourt,A.Sahai,andB.Waters,"Ciphertext-policyattribute988basedencryption,"inSecurityandPrivacy,2007.SP'07.IEEESympo989siumon, pp. 321–334,IEEE, 2007.
4. B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient,andprovablysecurerealization,"inInternationalWorkshoponPublicKeyCryptography,pp.53–70,Springer,2011.
5. H. Qian, J. Li, Y. Zhang, and J. Han,"Privacy-preserving personal health recordusingmulti-authorityattribute-basedencryption with revocation," InternationalJournal of Information Security, vol. 14,no.6, pp. 487–497, 2015.
6. J.Liu,X.Huang,andJ.K.Liu,"Secure sharing of personal health recordsincloudcomputing:Ciphertext-policyattribute-basedsigncryp999tion,"FutureGeneration Computer Systems, vol. 52, pp.67–76, 2015.
7. L.Fang,W.Susilo,C.Ge,andJ.Wang,"Interactiveconditionalproxy re-encryption with fine grain policy," Journalof Systems and Software, 1002 vol. 84, no.12,pp. 2293–2302, 2011.
8. K. Emura, A. Miyaji, A. Nomura, K.Omote, and M. Soshi, "A ciphertext-policyattribute-basedencryptionschemewithconstantci1005phertextlength,"inInternationalConferenceonInformation Security 1006 Practice and Experience, pp.13–23,Springer, 2009.
9. S.HohenbergerandB.Waters,"Attribute-based encryption with fast 1008decryption," in Public-Key Cryptography–PKC 2013, pp. 162–179, 1009 Springer,2013.
10. A. Lewko and B. Waters, "New proofmethodsforattribute-based1011encryption:Achievingfullsecuritythroughselectivetechniques,"in1012Advances in Cryptology–CRYPTO 2012,pp.180–198, Springer, 2012.
11. M.Li,S.Yu,Y.Zheng,K.Ren,and W. Lou, "Scalable and secure 1014 sharingofpersonalhealthrecordsincloudcomputingusingattribute1015basedencryption," IEEE transactions on paralleland distributed sys1016 tems, vol. 24, no.1, pp. 131–143, 2012.
12. L.Zhang,G.Hu,Y.Mu,andF.Rezaeibagha,"Hiddenciphertextpolicy1018 attribute-based encryption with fastdecryption for personal health record 1019system," IEEE Access, vol. 7, pp. 33202–33213, 2019.
13. M. Green, S. Hohenberger, B.Waters,et al., "Outsourcing the decryption 1021 ofabeciphertexts.,"inUSENIXSecuritySymposium,vol. 2011, 2011.
14. J. Lai, R. H. Deng, C. Guan, and J.Weng,"Attribute-basedencryption1023withverifiableoutsourceddecryption,"IEEETransactionsoninforma1024tionforensics and security,vol. 8, no. 8, pp.1343–1354,2013.
15. J.Li,X.Huang,J.Li,X.Chen,and Y.Xiang,"Securelyoutsourcing1026attribute-based encryption withcheck ability," IEEE Transactions on 1027Parallel and Distributed Systems, vol. 25,no.8, pp. 2201–2210, 2013.
16. M.Blaze,G.Bleumer,andM.Strauss, "Divertible protocols and atomic1028 proxy cryptography," in InternationalConferenceontheTheoryand1029Applications of Cryptographic Techniques,pp.127–144, Springer, 1998.