JES
Journal of Engineering Sciences

Vol 13, Issue 03, MARCH /2022

ISSN NO:0377-9254

Secure Keyword Search and Secure Data Sharing Mechanism Using Re-encryption

Nagaraju Shanmukh Poojith[1], A S S K Sreeharsha[2], Balina Vinay Kumar[3], Kattirapalli Sai Teja[4], Sai Pratheek Chalamalasetty[5]

#1,#2,#3,##4 Student, Department of CSE, Gitam University, Gitam University,Gand hi nagar Rushikonda Visakhapatnam530045 Andhra Pradesh, INDIA.

#5 Assistant Professor, Department of CSE, Gitam University, Gitam University,Gand hi nagar Rushikonda Visakhapatnam530045 Andhra Pradesh, INDIA.

Abstract_ The emergence of cloud infrastructure has considerably decreased the fees of hardware and software program sources in computing infrastructure. To make sure security, the facts is generally encrypted earlier than it is outsourced to the cloud. Unlike looking out and sharing the simple data, it is difficult to search and share the facts after encryption. Nevertheless, it is a necessary challenge for the cloud carrier issuer as the customers assume the cloud to behavior a rapid search and return the end result barring dropping facts confidentiality. To overcome these problems, we advise a ciphertext-policy attribute-based mechanism with key-word search and facts sharing (CPAB-KSDS) for encrypted cloud data. The proposed answer now not solely helps attribute-based key-word search however additionally permits attribute-based information sharing at the identical time, which is in distinction to the present options that solely guide both one of two features. Additionally, the key-word in our scheme can be up to date all through the sharing segment besides interacting with the PKG. In this article, we describe the idea of CPAB-KSDS as nicely as its protection model. Besides, we advise a concrete scheme and show that it is in opposition to chosen ciphertext assault and chosen key-word assault invulnerable in the random oracle model. Finally, the proposed development is confirmed sensible and environment friendly in the overall performance and property comparison.

Index Terms—Cloud Data Sharing, Searchable Attribute-based 25 Encryption, Attribute-based Proxy Re-encryption, Keyword Up26 date

1.INTRODUCTION

Distributed computing has been the solution for the issue of individual information the board and upkeep because of the development of individual electronic gadgets. It is on the grounds that clients can re-appropriate their information to the cloud effortlessly and minimal expense. The development of distributed computing has additionally affected and overwhelmed Information Technology ventures. It is unavoidable that distributed computing likewise experiences security and protection challenges Encryption is the fundamental strategy for empowering information classification and trait based encryption is a conspicuous delegate because of its expressiveness in client's character and information [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.Hence, it doesn't uphold looking and sharing. Assume in a Person Health Record (PHR) framework [5]–[7], a gathering of patients store their encoded individual wellbeing reports Enc(D1; P1;KW1); ;Enc(Dn; Pn;KWn) in the cloud, where Enc(Di; Pi;KWi) is a characteristic based encryption of the

wellbeing report Di under an entrance strategy Pi and a catchphrase KWi. Specialists fulfilling the approach Pi can recuperate the record Di. Be that as it may, they couldn't recover the particular record by basically composing the catchphrase. All things being equal, a specialist Alice needs to initially download and unscramble the encoded records. After unscrambling, she can utilize the watchword to look through the particular one from a lot of the decoded wellbeing records. Another badly arranged situation is that Alice endeavors to impart a record to her associate, for the situation like she wants to counsel the report with a subject matter expert. In the present circumstance, she should download the scrambled records, then, at that point, unscramble them. Then, at that point, after she has procured the basic record, she scrambles the record utilizing the arrangement of the subject matter expert. Accordingly, this framework is extremely wasteful as far as looking and sharing. Also, the customary quality based encryption (ABE) innovation utilized in the current PHR frameworks may cause one more issue for watchword upkeep in light of the fact that the ABE calculation couldn't scale well for catchphrase refreshes 65 once the quantity of the records altogether increments. For instance, subsequent to checking on a wellbeing report with the patient self stamped "infectious" tag, Alice from emergency clinic An affirmed it isn't the infectious condition and revised the tag to "non-infectious". With the end goal for Alice to share a wellbeing report that is scrambled with a tag "infectious" with one more specialist from emergency clinic B, she really wants to change the tag as "non-infectious" without decoding the report. As the customary characteristic based encryption with watchword search can't uphold catchphrase refreshing, Alice needs to create another tag for all common ciphertexts to keep the security of the catchphrase. From above situations, the customary characteristic based encryption isn't adaptable for information looking and sharing. Moreover, characteristic based encryption isn't all around scaled when there is an update solicitation to the catchphrase. To look and share a particular record, Alice downloads and unscrambles the ciphertexts. Nonetheless, this interaction is unrealistic to Alice particularly when there is countless ciphertexts. The more awful circumstance is the information proprietor Alice should remain online all the time since Alice needs to give her private key to the information decoding. Accordingly, ABE arrangement doesn't take the upsides of cloud computing.An elective technique is to appoint an outsider to do the inquiry, re-encode and watchword update work rather than Alice. Alice can store her private key in the outsider's stockpiling, and along these lines the outsider can do the weighty occupation for Alice. In such a methodology, notwithstanding, we want to completely believe the outsider since it can admittance to Alice's private key. If the outsider is compromised, all the client information including delicate protection will be spilled also.

2.LITERATURE SURVEY

2.1) DaSCE: Data Security for Cloud Environment with Semi-Trusted Third Party

AUTHORS: Ali, M., Malik, S. and Khan, S.,

Off-site information storage is an utility of cloud that relieves the clients from focusing on records storage system. However, outsourcing records to a third-party administrative manipulate entails serious safety concerns. Data leakage may additionally appear due to assaults by means of different customers and machines in the cloud. Wholesale of statistics through cloud carrier issuer is but any other trouble that is confronted in the cloud environment. Consequently, high-level of protection measures is required. In

this paper, we advocate Data Security for Cloud Environment with Semi-Trusted Third Party (DaSCE), a records safety machine that presents (a) key administration (b) get entry to control, and (c) file certain deletion. The DaSCE makes use of Shamir's (k, n) threshold scheme to manipulate the keys, the place okay out of n shares are required to generate the key. We use a couple of key managers, every web hosting one share of key. Multiple key managers keep away from single factor of failure for the cryptographic keys. We (a) put into effect a working prototype of DaSCE and consider its overall performance based totally on the time fed on in the course of more than a few operations, (b) formally mannequin and analyze the working of DaSCE the usage of High Level Petri nets (HLPN), and (c) affirm the working of DaSCE the usage of Satisfiability Modulo Theories Library (SMT-Lib) and Z3 solver. The outcomes disclose that DaSCE can be successfully used for safety of outsourced statistics with the aid of using key management, get right of entry to control, and file certain deletion.

2.2) Control Cloud Data Access Privilege and Anonymity With Fully Anonymous Attribute-Based Encryption

AUTHORS: Jung, T., Li, X. Y., Wan, Z. and Wan, M

Cloud computing is a innovative computing paradigm which allows flexible, on-demand and affordable utilization of computing resources, however the records is outsourced to some cloud servers, and a variety of privateness issues emerge from it. Various schemes based totally on the Attribute-Based Encryption have been proposed to tightly closed the cloud storage. However, most work focuses on the facts contents privateness and the get admission to control, whilst much less interest is paid to the privilege manage and the identification privacy. In this paper, we current a semi-anonymous privilege manipulate scheme AnonyControl to tackle no longer solely the information privateness however additionally the consumer identification privateness in current get entry to manipulate schemes. AnonyControl decentralizes the central authority to restriction the identification leakage and as a result achieves semi-anonymity. Besides, it additionally generalizes the file get admission to manage to the privilege control, via which privileges of all operations on the cloud records can be managed in a fine-grained manner. Subsequently, we current the AnonyControlF which wholly prevents the identification leakage and obtain the full anonymity. Our safety evaluation indicates that each AnonyControl and AnonyControl-F are impervious underneath the DBDH assumption, and our overall performance comparison well-knownshows the feasibility of our schemes.

2.3) Fine-Grained Two-Factor Access Control for Web-Based Cloud Computing Services

AUTHORS: Liu, J. K., Au, M. H., Huang, X., Lu, R., and Li, J

In this paper, we introduce a new fine-grained two-factor authentication (2FA) get entry to manipulate device for web-based cloud computing services. Specifically, in our proposed 2FA get right of entry to manipulate system, an attribute-based get admission to manage mechanism is applied with the necessity of each a person secret key and a light-weight safety device. As a consumer can't get right of entry to the gadget if they do no longer maintain both, the mechanism can beautify the safety of the system, specially in these situations the place many customers share the identical laptop for web-based cloud services. In addition, attribute-based manipulate in the gadget additionally permits the cloud server to preclude the get

admission to to these customers with the equal set of attributes whilst maintaining person privacy, i.e., the cloud server solely is aware of that the consumer fulfills the required predicate, however has no thought on the specific identification of the user. Finally, we additionally elevate out a simulation to display the practicability of our proposed 2FA system.

3.PROPOSED SYSTEM

Prior work did now not show that the present attribute-based mechanisms should both help key-word search and statistics sharing in one scheme besides resorting to PKG. Therefore, a new attribute-based mechanism is wished to reap the intention for the above PHR scenario. One might also argue that the trouble can be trivially solved by means of combining an AB-PRE scheme and attribute-based key-word search scheme (AB-KS).However, the mixture should end result in two predominant issues: 1) the mixed scheme is now not CCA secure, 2) it is prone to collusion attack

Therefore, a impervious scheme is favored to totally assist key-word searching, records sharing as nicely as the safety of the privateness of keyword. All of these worries inspire us to graph a mechanism that:

1) approves the records proprietor to search and share the encrypted fitness file barring the needless decryption process.

2) helps key-word updating for the duration of the statistics sharing phase.

3) greater importantly, does no longer want the exist of the PKG, both in the segment of facts sharing or key-word updating.

4) the information proprietor can totally figure out who should get entry to the records he encrypted.

3.1 IMPLEMENTATION

The CPAB-KSDS system, consists of 5 entities: the PKG, the cloud server (act as the proxy), the fitness file owner, the delegator (recipient of the unique ciphertext) and the delegatee (recipient of the re-encrypted ciphertext). The workflow for the device is described as follows.

System Initialization: This segment is achieved through the PKG. The PKG generates the device public parameters that are publicly handy for all the members of the machine and the grasp secret key which is stored personal by using the PKG.

Registration: The registration segment is finished through the PKG. When every person problems a registration request to the PKG,the PKG generates a non-public corresponds to his attribute set.

Ciphertext Upload: The private fitness report proprietor encrypts his file with the unique recipient's coverage and the keyword, and then add the encrypted document to the cloud server.

Ciphertext Search: The recipient generates a search token and problems a search request consists of the search token to the cloud server. The cloud server searches the ciphertext by way of the Test algorithm and returns the search end result to the recipient.

Re-encryption: The delegator generates a re-encryption key and troubles a re-encryption request consists of the re-encryption key to the cloud server. The cloud server converts the authentic encrypted document to a re-encrypted ciphertext underneath a new get entry to policy. Decryption: The recipient (a delegatee or a delegator) requests a re-encrypted (or an original) ciphertext from the cloud server and then decrypts the ciphertext with his very own personal key to get the underlying record. Note that, a delegatee may additionally act as a delegator for different participants.

Journal of Engineering Sciences

Vol 13, Issue 03, MARCH /2022

ISSN NO:0377-9254

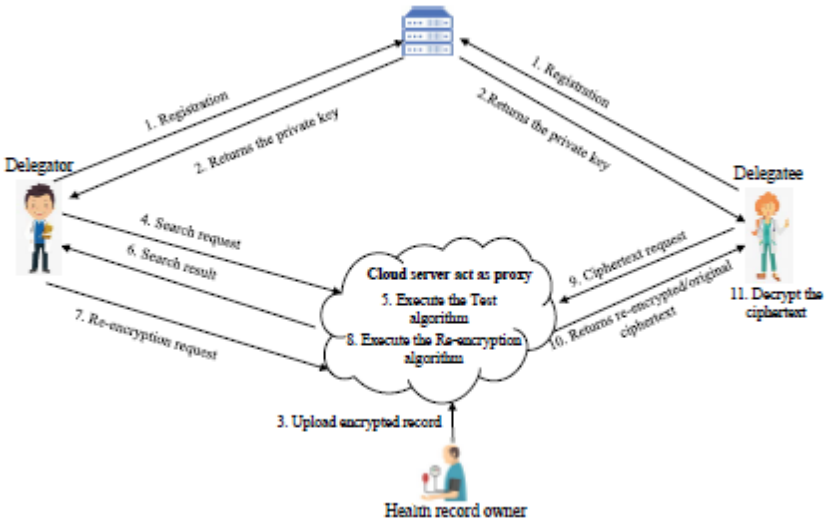

Fig 1:Architecture

4.RESULTS AND DISCUSSIONS

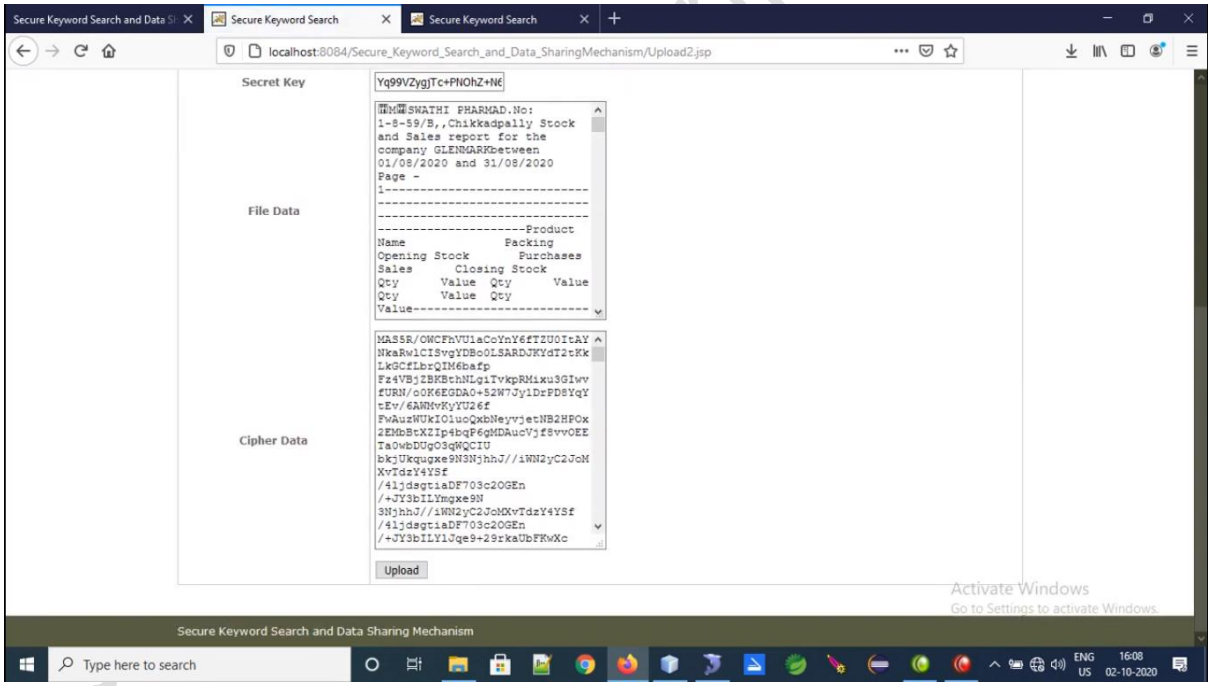

Fig 4.1 Encrypted Data

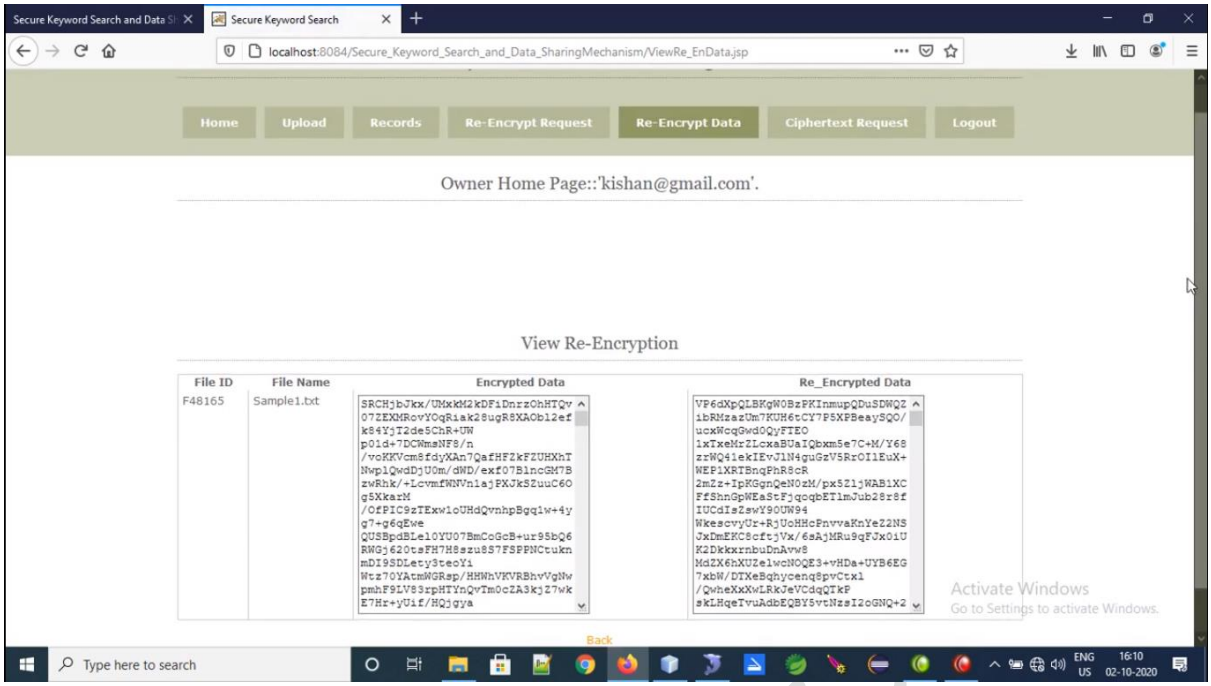

Fig 4.2 Re-encrypted data

5.CONCLUSION

In this work, another thought of ciphertext-strategy property based instrument (CPAB-KSDS) is acquainted with help catchphrase 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. The proposed plot is shown productive and useful in the exhibition and property examination. This paper gives a confirmed response to the open testing issue brought up in the earlier work [36], which is to plan a property based encryption with watchword looking and information sharing without the PKG during the sharing stage.

FUTURE ENHANCEMENT

Furthermore, our work motivates interesting open problems as well including designing CPAB-KSDS scheme without random oracles or proposing a new scheme to support more expressive keyword search.

REFERENCES

[1] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 457–473, Springer, 2005.

[2] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proceedings of the 13th ACM conference on Computer and communications security, 986 pp. 89–98, Acm, 2006.

[3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute988 based encryption," in Security and Privacy, 2007. SP'07. IEEE Sympo989 sium on, pp. 321–334, IEEE, 2007.

[4] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in International Workshop on Public Key Cryptography, pp. 53–70, Springer, 2011.

[5] H. Qian, J. Li, Y. Zhang, and J. Han, "Privacy-preserving personal health record using multi-authority attribute-based encryption with revocation," International

Journal of Information Security, vol. 14, no. 6, pp. 487–497, 2015.

[6] J. Liu, X. Huang, and J. K. Liu, "Secure sharing of personal health records in cloud computing: Ciphertext-policy attribute-based signcryp999 tion," Future Generation Computer Systems, vol. 52, pp. 67–76, 2015.

[7] L. Fang, W. Susilo, C. Ge, and J. Wang, "Interactive conditional proxy re-encryption with fine grain policy," Journal of 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-policy attribute-based encryption scheme with constant ci1005 phertext length," in International Conference on Information Security 1006 Practice and Experience, pp. 13–23, Springer, 2009.

[9] S. Hohenberger and B. Waters, "Attribute-based encryption with fast 1008 decryption," in Public-Key Cryptography–PKC 2013, pp. 162–179, 1009 Springer, 2013.

[10] A. Lewko and B. Waters, "New proof methods for attribute-based 1011 encryption: Achieving full security through selective techniques," in 1012 Advances 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 sharing of personal health records in cloud computing using attribute1015 based encryption," IEEE transactions on parallel and distributed sys1016 tems, vol. 24, no. 1, pp. 131–143, 2012.

[12] L. Zhang, G. Hu, Y. Mu, and F. Rezaeibagha, "Hidden ciphertext policy 1018 attribute-based encryption with fast decryption for personal health record 1019 system," IEEE Access, vol. 7, pp. 33202–33213, 2019.

[13] M. Green, S. Hohenberger, B.Waters, et al., "Outsourcing the decryption 1021 of abe ciphertexts.," in USENIX Security Symposium, vol. 2011, 2011.

[14] J. Lai, R. H. Deng, C. Guan, and J. Weng, "Attribute-based encryption 1023 with verifiable outsourced decryption," IEEE Transactions on informa1024 tion forensics and security, vol. 8, no. 8, pp. 1343–1354, 2013.

[15] J. Li, X. Huang, J. Li, X. Chen, and Y. Xiang, "Securely outsourcing 1026 attribute-based encryption with checkability," IEEE Transactions on 1027 Parallel and Distributed Systems, vol. 25, no. 8, pp. 2201–2210, 2013.

[16] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic 1028 proxy cryptography," in International Conference on the Theory and 1029 Applications of Cryptographic Techniques, pp. 127–144, Springer, 1998.

Author's Profile

Nagaraju Shanmukh Poojith,Student, Department of CSE, Gitam University, Gitam University,Gand hi nagar Rushikonda Visakhapatnam530045 Andhra Pradesh, INDIA.

Vol 13, Issue 03, MARCH /2022

ISSN NO:0377-9254

A S S K Sreeharsha, Student, Department of CSE, Gitam University, Gitam University,Gand hi nagar Rushikonda Visakhapatnam530045 Andhra Pradesh, INDIA

Balina Vinay Kumar, Student, Department of CSE, Gitam University, Gitam University,Gand hi nagar Rushikonda Visakhapatnam530045 Andhra Pradesh, INDIA

Kattirapalli Sai Teja, Student, Department of CSE, Gitam University, Gitam University,Gand hi nagar Rushikonda Visakhapatnam530045 Andhra Pradesh, INDIA

Sai Pratheek Chalamalasetty

Assistant Professor , Department of CSE, Gitam University, Gitam University,Gand hi nagar Rushikonda Visakhapatnam530045 Andhra Pradesh, INDIA