International Journal on Applications in Information and Communication Engineering
Volume 2: Issue 2: Feburary 2016, pp 36-39. www.aetsjournal.com ISSN (Online) : 2394-6237

Achieving Cloud Data Sharing Using Key Aggregate Searchable Encryption

K. Rajasrika , P.S. Smitha

Abstract— In Cloud Storage there is an important functionality called Data Sharing. But the query always present in every one's mind is how to securely, efficiently, and flexibly share data with others in cloud storage. The preferred suppleness of distribution any collection of chosen credentials with any assembly of user's difficulties poles apart encryption keys to be used for dissimilar credentials. On the other hand, this also involve the obligation of steadily distribute to users a outsized amount of keys for both encryption and rummage around, and those users will have to securely store the traditional keys, and put forward an equally hefty number of keyword trapdoors to the cloud in order to perform search over the shared data. A new public-key cryptosystem is introduced to produce a constant size cipher texts called KASE. Advanced Key sharing system based on hint text methodology is formed to share the data safely. Once the data sharing is completed then the key aggregate differs from its actual form. So the user cannot guess the key aggregate cryptosystem and this process provides efficient solution than the existing ones.

Index Terms — Data Security, Cloud, Integrity, Bulk Request, Bulk Response, Dynamic Keys.

I. INTRODUCTION

Cloud storage space has come out as a talented resolution for as long as ever-present, expedient and on insists right of entry to outsized amounts of information shared over the Internet. Nowadays, millions of users are distribution individual information, such as photos and videos, with their friend's from side to side social network submissions based on cloud storeroom on every day foundation. Business users are also life form paying attention by cloud storeroom due to its frequent benefits, counting subordinate price, superior nimbleness and improved reserve operation.

On the other hand, while take pleasure in the expediency of distribution information via cloud storeroom, users are also more and more worried about unintentional information seep out in the cloud. Such data leaks, caused by a malicious adversary or a misbehaving cloud machinist can more often than not guide to solemn contravenes of individual solitude or business clandestine [Ex: the current far above the ground profile occurrence of famous person photos being seep out in iCloud].

Ms. K. Rajasrika is a Student in the Department of Computer Science and Engineering in Velammal Engineering College, Chennai, Tamil Nadu, and India.

Ms. P.S. Smitha, Assistant Professor, Department of Computer Science and Engineering in Velammal Engineering College, Chennai, Tamil Nadu, India.

To speak to user's apprehension in excess of possible information pour out in obscure storage space, an ordinary move toward is for the information proprietor to encrypt all the information previous to uploading them to the cloud, such that afterward the encrypted information may be get back and decrypted by those who have the decryption keys. Such cloud storeroom is frequently called the cryptographic cloud storeroom [1]. On the other hand, the encryption of information makes it demanding for users to search and then selectively get back only the information enclosing known keywords.

A general explanation is to make use of a searchable encryption (SE) scheme in which the information possessor is compulsory to encrypt possible keywords and upload them to the cloud jointly with encrypted information, such that, for get back data corresponding a keyword, the user will propel the equivalent keyword trapdoor to the cloud for performing arts search over the encrypted information. Even though come together a searchable encryption method with cryptographic obscure storeroom can complete the fundamental safety measures necessities of a cloud storage space, put into operation such a organization for great size submissions connecting millions of users and billions of files may still be caught up by no-nonsense subjects concerning the well-organized administration of encryption keys, which, to the most excellent of our knowledge, are for the most part unobserved in the journalism.

Original of all, the require for selectively distribution encrypted information with dissimilar users [Ex: distribution a photo with persuaded friends in a social network demand, or distribution a business article with convinced generation on a cloud constrain] more often than not anxiety dissimilar encryption keys to be used for poles apart files. On the other hand, this involves the numeral of keys that require to be disseminated to users, both for them to investigate over the encrypted files and to decrypt the files, will be relative to the number of such files. Such a great amount of keys have got to not only be disseminated to users via protected channels, but also be steadily stored and administered by the users in their campaigns.

In adding up, an outsized quantity of trapdoors have got to be produced by users and put forward to the cloud in arrange to carry out a keyword investigate in excess of many documentations. The indirect necessitate for protected announcement, storage space, and computational complication may cause to be such a scheme incompetent and not practical. In this paper, we speak to this confront by propose the novel

concept of Key Aggregate Searchable Encryption [KASE], and instantiating the concept through a tangible KASE method. The planned KASE proposal is relevant to any cloud storeroom that ropes the searchable collection information distribution functionality, which means any user can selectively go halves a assembly of elected files with a assemblage of preferred users, while consent to the latter to carry out keyword investigate over the previous.

To hold up searchable collection information allocation the main requirements for well-organized key administration are double. Foremost, a information proprietor only requirements to deal out a on its own aggregate input [in its place of a assembly of keys] to a user for distribution any amount of documentations. Subsequent, the user only desires to put forward a solitary collective trapdoor [as an alternative of a cluster of trapdoors] to the cloud for the theater keyword rummage around over several quantities of communal documentations. To the most excellent of our information, the KASE method projected in this paper is the primary known proposal that can make happy together necessities [the key collective cryptosystem [2], which has stimulated our effort, can gratify the first prerequisite but not the succeeding].

Challenges and Issues

In past systems, user faces lots of challenges and issues while using cloud based key aggregation Systems. Some of them are listed below:

(i) Hard to maintain the set of keys to maintain the privacy.

(ii) Difficult to handle this type of system for large data usage scenarios.

(iii) Cost efficient process.

(iv) Each and every file or data should be processed individually, difficult to suite for multiple data management.

(v) Confusion occurs while handling with set of data at same time.

II. CONTRIBUTIONS

Additionally, our major donations are as follows.

(a) We primary describe a universal arrangement of key aggregate searchable encryption [KASE] collected of seven polynomial algorithms for safety stricture setup, key cohort, encryption, key taking out, trapdoor cohort, trapdoor modification, and trapdoor difficult. We then explain both purposeful and safety measures necessities for manipulative a convincing KASE proposal.

(b) We then instantiate the KASE construction by conniving a tangible KASE method. Subsequent to as long as comprehensive manufacturing for the seven algorithms, we investigate the good organization of the proposal and institute its safety measures through comprehensive psychotherapy.

(c) We thrash out an assortment of no-nonsense questions in construction an concrete assemblage information allocation arrangement based on the projected KASE method and appraise its presentation. The assessment corroborates our classification can get together the presentation necessities of no-nonsense submissions.

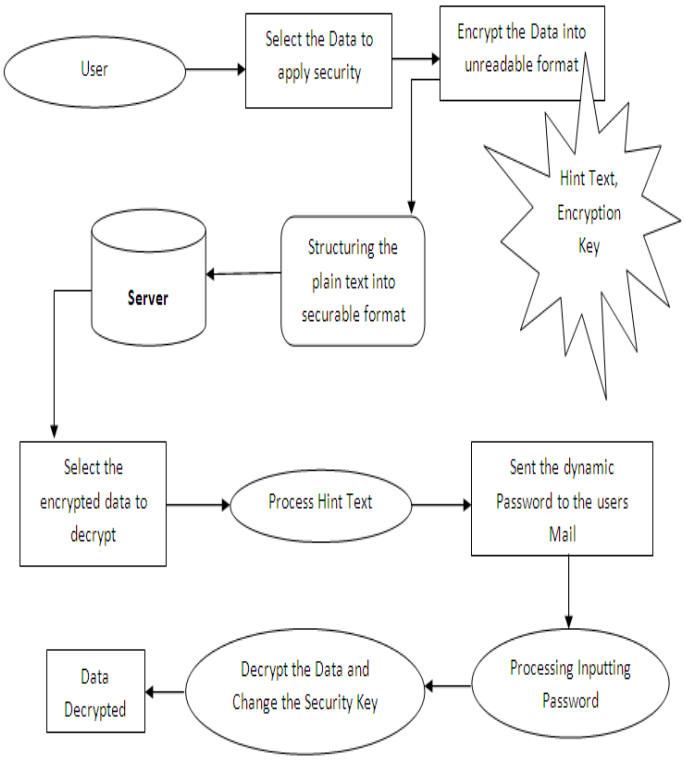

Fig.1. Flow Diagram of the Proposed System Design

Procedure: EncryptString ()

1) Create Function called " EncryptString ()"

2) Make Exceptional Try...Catch block

3) Dimensionate the variables up to n depends on your needs.

4) Assign the value to the declarations.

5) Dimensionate unstring as String

6) Write Clear () function to clear all the items available in the Unique Item List

7) Add the first index item into List

8) Create Looping Statements for identifying unique items

Ex:

```
Dim RijndaelCipher As New RijndaelManaged()
Dim PlainText As Byte() = System. Text.Encoding. Unicode.GetBytes(InputText)
Dim Salt As Byte() = Encoding.ASCII. GetBytes (Password.Length.ToString())
Dim SecretKey As New PasswordDeriveBytes (Password, Salt)
Dim Encryptor As ICryptoTransform = Rijndael Cipher.CreateEncryptor(SecretKey.GetBytes(16), SecretKey.GetBytes(16))
Dim memoryStream As New IO.MemoryStream()
Dim cryptoStream As New CryptoStream (memoryStream,Encryptor, CryptoStream Mode. Write)
cryptoStream.Write(PlainText, 0, PlainText.Length)
cryptoStream.FlushFinalBlock()
Dim CipherBytes As Byte() = memory Stream.To Array()
memoryStream.Close()
```

cryptoStream.Close()
Dim EncryptedData As String = Convert.ToBase64 String (CipherBytes)
Return EncryptedData

Procedure: DecryptString ()

1) Create Function called "DecryptString ()"
2) Make Exceptional Try...Catch block
3) Dimensionate the variables up to n depends on your needs.
4) Assign the value to the declarations.
5) Dimensionate unstring as String
6) Write Clear () function to clear all the items available in the Unique Item List
7) Add the first index item into List
8) Create Looping Statements for identifying unique items

Ex:
Try
Dim RijndaelCipher As New RijndaelManaged()
Dim EncryptedData As Byte() = Convert.From Base64 String(InputText)
Dim Salt As Byte() = Encoding.ASCII. GetBytes (Password.Length.ToString())
Dim SecretKey As New PasswordDerive Bytes (Password, Salt)
Dim Decryptor As ICryptoTransform = Rijndael Cipher.Create Decryptor(SecretKey.GetBytes(16), SecretKey.GetBytes(16))
Dim memoryStream As New IO.Memory Stream (EncryptedData)
Dim cryptoStream As New CryptoStream(memoryStream,Decryptor, Crypto Stream Mode.Read)
Dim PlainText As Byte() = New Byte (Encrypted Data.Length - 1) {}
Dim DecryptedCount As Integer = crypto Stream. Read (PlainText, 0, PlainText.Length)
memoryStream.Close()
cryptoStream.Close()
Dim DecryptedData As String = Encoding.Unicode.GetString (PlainText, 0, DecryptedCount)
Return DecryptedData
Catch exception As Exception
Return (exception.Message)
End Try

III. SURVEY

A sequence of searchable symmetric encryption proposal has been projected to facilitate search on cipher text. Long-established proposals make possible users to steadily repossess the cipher text, excluding these proposals shore up only Boolean keyword search, that is, whether a key exists in a system or not, without considering the difference of relevance with the queried keys of these encrypted data in the result. Preventing the security from involving in ranking and entrusting work to the user is a natural way to avoid information leakage. However, the limited computational power on the user side and the high computational overhead against information security.

Limitations in Past Work

- To improve security without sacrificing efficiency, schemes presented in show that they support top-k single key retrieval under various scenarios.
- Authors made attempts to solve the problem of top-k multi-keys over encrypted data. These schemes, however, suffer from two problems – Boolean representation and how to strike a balance between security and efficiency.
- In the former, data are ranked only by the number of retrieved keys, which impairs search accuracy. In the latter, security is implicitly compromised to tradeoff for efficiency, which is particularly undesirable in cloud based security oriented applications.

IV. PROPOSED APPROACH

Our work is flexible in the sense that this constraint is eliminated, that is, no special relation is required between the classes. The technique of bilinear aggregate signature is used to achieve key auditing. Key auditing reduces the computation overhead. Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient. We introduce the concepts of similarity relevance and scheme robustness to formulate the privacy issues in encryption schemes, and then solve the insecurity problem by proposing a random key encryption scheme. Novel technologies in the cryptography community and information retrieval community are employed.

Merits of Proposed System

- To achieve better robustness and improve efficiency.
- This scheme fulfills the secure multi-keyword top-k retrieval over encrypted data.
- Specifically, for the first time we employ relevance score to support multi-keyword top-k retrieval.
- Thorough analysis on security demonstrates the proposed scheme guarantees high data privacy. Furthermore, performance analysis and experimental results show that our scheme is efficient for practical utilization.

V. CONCLUSION

Bearing in mind the matter-of-fact difficulty of privacy preserving information distribution organization based on public cloud storeroom which necessitates an information proprietor to share out a bulky numeral of keys to users to facilitate them to right of entry his or her credentials, we for the foremost time recommend the perception of key aggregate searchable encryption [KASE] and put up a tangible KASE proposal. In cooperation psychoanalysis and assessment results corroborate that our occupation can make available an effectual explanation to construction no-nonsense information

distribution organization based on public cloud storeroom. In a KASE method, the proprietor only needs to hand out a on its own key to a user when allocation lots of credentials with the user, and the user only needs to put forward a single trapdoor when he queries over all credentials mutual by the same owner.

On the other hand, if a user wants to inquiry over credentials communal by numerous proprietors, he be obliged to produce manifold trapdoors to the cloud. How to decrease the amount of trapdoors under multi proprietor's surroundings is a prospect vocation. Furthermore joined together clouds have paying attention a group of concentration these days, but our KASE cannot be functional in this case in a straight line. It is also a prospect vocation to make available the explanation for KASE in the case of amalgamated clouds.

REFERENCES

[1] R. Curtmola, J. Garay, S. Kamara, R. Ostrovsky. "Searchable symmetric encryption: improved definitions and efficient constructions", In: Proceedings of the 13th ACM conference on Computer and Communications Security, ACM Press, pp. 79-88, 2006.

[2] C. Chu, S. Chow, W. Tzeng, et al. "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage", IEEE Transactions on Parallel and Distributed Systems, 2014, 25(2): 468-477.

[3] X. Liu, Y. Zhang, B. Wang, and J. Yan. "Mona: secure multiowner data sharing for dynamic groups in the cloud", IEEE Transactions on Parallel and Distributed Systems, 2013, 24(6): 1182-1191.

[4] C. Chu, S. Chow, W. Tzeng, et al. "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage", IEEE Transactions on Parallel and Distributed Systems, 2014, 25(2): 468-477.

[5] X. Song, D.Wagner, A. Perrig. "Practical techniques for searches on encrypted data", IEEE Symposium on Security and Privacy, IEEE Press, pp. 44C55, 2000.

[6] R. Curtmola, J. Garay, S. Kamara, R. Ostrovsky. "Searchable symmetric encryption: improved definitions and efficient constructions", In: Proceedings of the 13th ACM conference on Computer and Communications Security, ACM Press, pp. 79-88, 2006.

[7] P. Van,S. Sedghi, JM. Doumen. "Computationally efficient searchable symmetric encryption", Secure Data Management, pp. 87-100, 2010.

[8] S. Kamara, C. Papamanthou, T. Roeder. "Dynamic searchable symmetric encryption", Proceedings of the 2012 ACM conference on Computer and communications security (CCS), ACM, pp. 965-976, 2012.

[9] D. Boneh, C. G, R. Ostrovsky, G. Persiano. "Public Key Encryption with Keyword Search", EUROCRYPT 2004, pp. 506C522, 2004.

[10] Y. Hwang,P. Lee. "Public Key Encryption with Conjunctive Keyword Search and Its Extension to a Multi-user System", In: Pairing-Based Cryptography C Pairing 2007, LNCS, pp. 2-22, 2007.

[11] J. Li, Q. Wang, C. Wang. "Fuzzy keyword search over encrypted data in cloud computing", Proc. IEEE INFOCOM, pp. 1-5, 2010.

[12] C. Bosch, R. Brinkma,P. Hartel. "Conjunctive wildcard search over encrypted data", Secure Data Management. LNCS, pp. 114-127, 2011.

[13] C. Dong, G. Russello, N. Dulay. "Shared and searchable encrypted data for untrusted servers", Journal of Computer Security, pp. 367-397, 2011.

[14] F. Zhao, T. Nishide, K. Sakurai. Multi-User Keyword Search Scheme for Secure Data Sharing with Fine-Grained Access Control. Information Security and Cryptology, LNCS, pp. 406-418, 2012.

[15] J. W. Li, J. Li, X. F. Chen, et al. "Efficient Keyword Search over Encrypted Data with Fine-Grained Access Control in Hybrid Cloud", In: Network and System Security 2012, LNCS, pp. 490-502, 2012.