Volume No:2, Issue No:12 (May-2017)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Key-Clump Searchable Coding (KCSC) For Cluster Information Sharing Via Cloud Storage

Jawad Yahya Kadhim
University POLITEHNICA of Bucharest,
Faculty of (FILS) Department of Engineering in Foreign Languages,
Engineer, Ministry of water resources /Iraq.
Email: yahya.joad@gmail.com

ABSTRACT:
The ability of by determination imparting encoded information to totally unique clients by means of open distributed storage may significantly ease security contemplations over unintended learning spills inside the cloud. A key test to concocting such coding plans exists in the efficient administration of coding keys. The required adaptability of imparting any group of choose archives to any bunch of clients requests totally extraordinary coding keys to be utilized for different records. Be that as it may, this furthermore infers the necessity of immovably conveying to clients an outsized scope of keys for each coding and inquiry, and individuals clients enough to solidly store the got keys, relate degreed present a similarly sizable measure of catchphrase/trapdoors to the cloud to perform seek over the common information.

The inexplicit need for secure correspondence, stockpiling, and multifaceted nature unmistakably renders the approach illogical. amid this paper, we tend to address this sensible drawback, that is essentially dismissed inside the writing, by proposing the novel considered key-clump searchable coding (KCSC) and instantiating the thoroughly considered a solid KCSC topic, amid which a data proprietor exclusively needs to convey one key to a client for sharing an outsized scope of reports, and along these lines the client exclusively needs to submit one trapdoor to the cloud for questioning the mutual archives. The wellbeing investigation and execution examination each guarantee that our anticipated plans are undeniably secure and much sparing.

Keywords:
Key-clump searchable coding (KCSC).

INTRODUCTION:

Cloud Storage has gotten the unmistakable quality as of later. In big business settings, we witness the climb looked for after for data outsourcing, which assists with the key organization of corporate information. It is likewise utilized as a center development behind various online organizations for individual applications. Nowadays, it is definitely not hard to apply with the desire of complimentary records for electronic mail, photo accumulation, archive sharing and/or remote access, with a limit measure more than 25GB (or several dollars for more than 1TB). Working together with the present remote advancement, customers can get to the bigger part of their records and messages with a cell phone in any side of the universe [1]. Considering information security, a conventional approach to manage objective without question, it is to depend on upon the server to support the way control after confirmation, which proposes any unforeseen favorable position expanding velocity will uncover all information. In a shared residency disseminated figuring environment, things end up being significantly more serious. Information from different clients can be encouraged on segregated virtual machines (VMs) be that as it may, harp on a singular physical machine. Information in an objective VM could be stolen by instantiating another VM co-possess with the objective one. A secure server in addition to giving an ensured establishment to facilitating your Web applications, and Web server design assumes a basic character in your Web

Volume No:2, Issue No:12 (May-2017)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

application's security. A server can prompt unapproved access. Ignored client records can allow an attacker to hack your data without notice. Seeing the risks to your Web server and having the ability to recognize appropriate countermeasures licenses you to presume various ambushes and surprise the routinely creating amounts of aggressors. This structure gives bidirectional encryption of correspondences between a customer and server, which guarantees against listening stealthily and upsetting or potentially producing the substance of the correspondence. Much talking, this gives a sense surety that one is relating with unequivocally. The circumstance that I purposed to talk with and furthermore ensuring that the substance of understandings between the customer and the site can't be scrutinized or produced by any outcast. Secure Server Plus application has essentially twofold login security. That is, in the wake of marking into the application customer gets a shrouded key on his enlisted gmail id. This private key must be inclosed in the fly up box appeared in the wake of marking into SSP Application.

This application has two functionalities, Encryption and Decryption. Encoding is the convenience in which the report to be organized over the mail in initially isolated in 4 an adjust of in byte setup and a while later encoded using particular encryption computations [2]. After Encryption records would be sent to the recipient through Gmail At the recipient end, He will download the archives and using SSP Application data as a piece of reports would be unscrambled and mixed. After Encryption records would be sent to the recipient through Gmail At the recipient end, He will download the reports and using SSP Application data as a piece of archives would be unscrambled and mixed. Customer security is moreover required in cloud. By using insurance the cloud or distinctive customers don't have the foggiest thought regarding the uniqueness of the other customer. Client security is likewise required in cloud. By utilizing protection the cloud or different clients don't have the foggiest idea about the individuality of the other client.

The swarm can hold the client represents the data in the cloud, and in like manner, to give benefits the cloud itself is responsible. The validity of the customer who stores the data is additionally affirmed. In that regard is additionally a need for law approval isolated from the specific responses for certification security and assurance. Various encryption frameworks have been rehearsed to secure data on cloud to examine the information while doing estimations on the data. By using Attribute based encryption plot, the cloud gets figure substance of the data and performs figurings on the figure substance and passes the encoded estimation of the last outcome to the customer then the customer can decipher the result, in spite of the way that the cloud does not appreciate what data it has worked. Different methods have been proposed to ensure the information substance protection by means of user control.

Identity based encryption(IBE) was at first introduced by Shamir, in which the sender of a message can show a character to such an extent that only a recipient with organizing character can unscramble it. A twosome of years sometime later, Fuzzy Identity-Based Encryption are proposed, which is generally called Attribute-Based Encryption (ABE).In such encryption plot, a personality is seen as a course of action of clear qualities, and translating is possible if a decrypter's character has a couple covers with the one characterized in the ciphertext. A little while later, more wide tree-based ABE arranges, Key-Policy Attribute-Based Encryption (KP-ABE) and Ciphertext-Policy Attribute-Based Encryption (CP-ABE), are acquainted with express more wide condition than direct 'cover'.A little while later, more expansive tree-based ABE arranges, Key-Policy Attribute-Based Encryption (KP-ABE) and Ciphertext-Policy Attribute-Based Encryption (CP-ABE), are acquainted with express more wide condition than direct 'cover'. They are mates to each different as in the decision of encryption technique (who can or can't disentangle the message) is set by different get-togethers [3].

Volume No:2, Issue No:12 (May-2017)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

In the KP-ABE, a ciphertext is related with a strategy of characteristics, and a private key is related with a monotonic get to structure like a tree, which portrays this present client's personality (e.g. IIT AND (Ph.D OR Master)).They are spouses to each other as in the choice of encryption strategy (who can or can't decode the message) is set by various gatherings [3]. In the KP-ABE, a ciphertext is associated with a course of action of qualities, and a private key is associated with a monotonic access structure like a tree, which describes this present customer's identity (e.g. IIT AND (Ph.D OR Master)). A customer can unscramble the ciphertext if and only if the passageway tree in his private key is satisfied with the references in the ciphertext. In any case, the encoding scheme is depicted in the keys, so the Encrypter does not possess total mastery over the encoding approach. It needs to believe that the key generators issue keys with the right structures to the right clients.

Plus, when a re-encryption happens, most of the nodes in the same organization must hold their individual keys, re-issued keeping in mind the end goal to blend to the re-encoded discs, and this technique causes huge issues in the execution. Of course, those issues and operating expense are all rated in the CP-ABE. In the CP-ABE, ciphertexts are made with a passage structure, which indicates the encryption methodology, and private keys are created by qualities. A customer can disentangle the ciphertext if and only if his attributes in the private key satisfy the passage tree demonstrated in the ciphertext. In this way, the Encrypter holds a complete force about the encoding system. Furthermore, the starting now issued private keys will never be modified unless the whole system reboots [4]. Dissimilar to the information secrecy, less effort is paid to ensure clients' identity protection amid those intelligent conventions. Clients' identities, which are described with their properties, are by and large unveiled two key guarantors, and the backers issue private keys as indicated by their traits.

In any case, it comes out to be characteristic that clients are willing to keep their identity mystery while despite everything they get their private keys. Therefore, we propose Anony Control and Anony Control-F to permit cloud servers to control clients' entrance benefits without knowing their character data. Concerning of records, there is a movement of cryptographic arrangements which work comparably as allowing an outside analyst to decide the availability of content documents in light of a legitimate concern for the data proprietor without spilling anything about the data, or without exchanging ceaselessly the data proprietors anonymity. So also, cloud customers undoubtedly won't have the firm conviction that the cloud server is profiting an occupation to the extent camouflage. A cryptographic course of action, with showed security re-laid on number-theoretic assumptions are all the more bewildering, at whatever point the customer is not flawlessly content with believing the security of the VM or the dependability of the particular staff.

These clients are induced to put together their data with their own specific keys before exchanging them to the waiter. Information sharing is a fundamental handiness in circulated stockpiling. For instance, bloggers can turn over their colleagues an opportunity to see a subset of their private pictures; an exertion may give her agents access to a touch of fragile data. The testing issue is the way to sufficiently share mixed data. Clearly, customers can download the encoded data from the limit, translate them, then ship them to others for sharing, be that as it may it loses the thought of disseminated memory. Customers should have the mental capacity to assign the passage benefits of the offering data to others to the objective that they can get to this data from the server direct. In any case, finding an able and safe way to deal with offer midway data in circulated stockpiling is not irrelevant. Underneath we will take Dropbox1 as a case for diagram [5]. Expect that Alice puts all her private photos on Dropbox, and she wouldn't wish to open her photos to everyone.

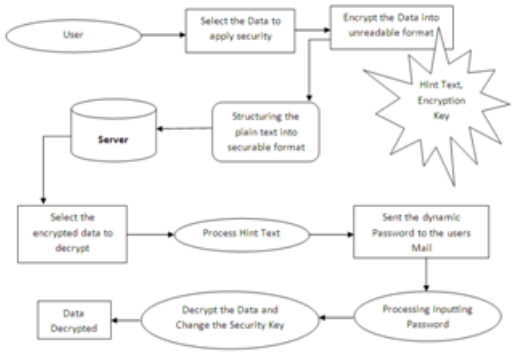
Volume No:2, Issue No:12 (May-2017)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Because of different information spillage probability Alice can't feel relieved by basically depending upon the security protection portions gave by Dropbox, so she encodes every one of the photographs utilizing her own particular keys before trading. Single day, Alice's amigo, Bob, requests that she partakes in the photographs expected control over every one of these years which Bob showed up in. Alice can then utilize the offer furthest reaches of Dropbox, however the point now is the route by which to dole out the unscrambling rights for these photographs to Bob. A conceivable choice Alice can pick is to safely send Bob the bewilder keys included. Concurrent encryption has been purported to authorize information con-fidentiality while making duplication possible. It entombs/unscrambles an information duplicate with a concurrent key, which is acquired by registering the cryptographic hash estimation of the meaning of the information duplicate. Later a key era and data encryption, clients obtain the keys and send the ciphertext to the swarm.

Since the encryption operation is deterministic and is taken from the information content, identical information duplicates will create the same focalized key and henceforth the same ciphertext. To keep away from unapproved get to, a protected affirmation of the proprietorship tradition is also required to pass the check that the client in actuality claims a similar plate when a transcript is found. After the proof, ensuing customers with a similar archive will be given a pointer from the server without hoping to change a similar platter. A client can download the encoded record with the pointer from the server, which must be unscrambled by the contrasting data proprietors and their simultaneous keys. Subsequently, simultaneous encryption allows the cloud to perform deduplication on the ciphertexts and the confirmation of proprietorship keeps the unapproved customer to go to the papers [6]. Regardless, past deduplication structures can't bolster differential endorsement duplicate check, which is huge in various applications.

In such an endorsed deduplication structure, each client is issued a usage of system. Each record exchanged to the cloud is in like manner controlled by a game plan of advantages to show which kind of customers are allowed to do the duplicate check and bring to the archives. Before giving his duplicate check interest for some record, the client needs to get this archive and his own specific advantages as sources of info. The customer can find a duplicate of this archive if and just if there is a rehash of this record and a planned advantage set away in a swarm. For instance, in an association, an extensive variety of advantages will be doled out to performing artists. Thus as to extra cost and beneficially organization, the data will be moved to the limit server provider (S-CSP) in the all inclusive community cloud with demonstrated advantages and the deduplication technique will be associated with store one and just copy of a similar book [7].

As a outcome of security considerations, a few records will be scrambled and permitted the copy check by representatives with indicated benefits to understand the entry control. Conventional deduplication frameworks in view of concurrent encryption, albeit ace voiding privacy to some degree, don't back up the copy check with different benefits. At the close of the day, no differential benefits have been seen in the deduplication in light of the vocalized encryption method. It is by all accounts repudiated on the off chance that we demand to acknowledge both duplication and differential approval copy check in the meanwhile.



Flow Diagram of the Proposed System Design

Volume No:2, Issue No:12 (May-2017)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

SYSTEM ANALYSIS

EXISTING SYSTEM:

There may be a rich composition on searchable puzzle creating, and furthermore compass point arrangements and PEKS arranges. In refinement to those present work, inside the setting of circulated stockpiling, catchphrase look for underneath the multi-residency setting may be an additional general circumstance. In such a circumstance, the information proprietor may really need to confer a chronicle to a gathering of approved customers, and every customer WHO has the get the opportunity to right will give a trapdoor to play out the catchphrase investigate the normal record, to be particular, the "multi-customer searchable encryption" (MUSE) circumstance. Some current work center to such a MUSE situation, however every one of them receive single-key consolidated with get to administration to accomplish the objective. In MUSE plots square measure made by sharing the report's searchable mystery composing key with all clients WHO will get to it, and communicate mystery composing is utilized to accomplish coarse-grained get to administration. In quality basically based mystery composing (ABE) is connected to accomplish fine-grained get to administration mindful watchword seek. Accordingly, in MUSE, the most disadvantage is the best approach to administration that clients will get to that records, while the best approach to downsize the amount of shared keys and trapdoors isn't considered.

DISADVANTAGES OF EXISTING SYSTEM:

- Unexpected benefit increment can uncover all
- It is not temperate.
- Shared data won't be secure.

PROPOSED SYSTEM:

In this paper, we tend to address this test by proposing the novel develop of key-cluster searchable composition (KCSC), and instantiating the build through a solid KCSC topic. The arranged KCSC topic applies to any distributed storage that backings the searchable group data sharing common sense, which proposes any client could by choice impart a cluster of choose records to a pack of choose clients, while allowing the last to perform watchword seek over the past. To bolster searchable group data sharing the most necessities for prudent key administration are twofold. Initial, an information proprietor exclusively should circulate one cluster key (rather than a pack of keys) to a client for sharing any assortment of documents. Second, the client exclusively should submit one cluster trapdoor (rather than a bundle of trapdoors) to the cloud for acting watchword seek over any assortment of shared records. We introductory layout a general system of key bunch searchable written work (KCSC) made out of seven polynomial calculations for security parameter setup, key era, encryption, key extraction, trapdoor era, trapdoor conformity, and trapdoor testing.

We keep an eye on then depict each intentional and security necessities for arranging a sound KCSC subject. We then instantiate the KCSC structure by arranging a solid KCSC subject. When giving expounded developments to the seven calculations, we have a tendency to break down the intensity of the subject, and set up its security through explained investigation. We talk about various sensible issues in building Associate in Nursing real group data sharing framework upheld the arranged KCSC topic, and judge its execution. The examination affirms our framework will meet the execution necessities of sensible applications.

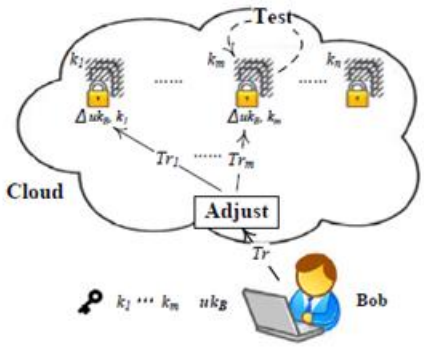
ADVANTAGES OF PROPOSED SYSTEM:

- It is more secure.
- Decryption key should be sent by means of a safe channel and unbroken mystery.
- It is relate efficient open key cryptography topic that backings flexible appointment.

To the least difficult of our information, the KCSC topic arranged amid this paper is that the underlying best-

Volume No:2, Issue No:12 (May-2017)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

SYSTEM ARCHITECTURE:



INPUT DESIGN:

The info configuration is the connection between the data framework and the client. It involves the creating determination and strategies for information planning and those means are important to put exchange information into a usable shape for preparing can be accomplished by examining the PC to peruse information from a composed or printed record or it can happen by having individuals entering the information straightforwardly into the framework. The outline of info concentrates on controlling the measure of information required, controlling the blunders, evading delay, staying away from additional means and keeping the procedure basic. The info is composed in such a route along these lines, to the point that it gives security and convenience with holding the protection. Input Design considered the accompanying things:

- What information ought to be given as info?
- How the information ought to be masterminded or coded?
- The discourse to direct the working staff in giving info.
- Methods for planning input approvals and ventures to take after when blunder happen.

OBJECTIVES:

1. Input Design is the way toward changing over a client situated portrayal of the contribution to a PC based framework. This arrangement is basic to keep up a key separation from bumbles in the data input handle and exhibit the correct bearing to the organization for getting right information from the automated structure.
2. It is accomplished by making easy to understand screens for the information passage to deal with vast volume of information. The objective of planning info is to make information passage less demanding and to be free from mistakes. The information passage screen is outlined such that every one of the information controls can be performed. It likewise gives record seeing offices.
3. Right when the information is entered it will check for its realness. Information can be entered with the assistance of screens. True blue messages are given as when required so that the client won't be in maize of minute. Thusly the objective of data design is to make a data configuration that is definitely not hard to take after

OUTPUT DESIGN

A quality yield is one, which meets the necessities of the end client and presents the data obviously. In any system eventual outcomes of taking care of are bestowed to the customers and to other structure through yields. In yield arrange it is settled how the information is to be evacuated for snappy need and besides the printed duplicate yield. It is the most basic and direct source information to the customer. Proficient and smart yield configuration enhances the framework's relationship to help client basic leadership.

1. Laying out PC yield should proceed in a sorted out, well altogether considered way; the right yield must be made while ensuring that each yield segment is created with the objective that people will find the structure can use easily and effectively. At the point when investigation plan PC yield, they ought to Identify the particular yield that is expected to meet the prerequisites.
2. Select strategies for displaying data.
3. Create record, report, or different organizations that contain data created by the framework.

Volume No:2, Issue No:12 (May-2017)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

The yield kind of an information system should accomplish no less than one of the going with targets.

- Convey data about past exercises, current status or projections of the Future.
- Signal imperative occasions, openings, issues, or notices.
- Trigger an activity.
- Confirm an activity.

IMPLEMENTATION

MODULES:

1. Data Owner
2. Network Storage
3. Encrypted Aggregate Key and Searchable Encryption Key Transfer
4. Trapdoor Generation
5. File User

MODULES DESCRIPTION:

Data Owner:

In this module we tend to dead by the data proprietor to setup a record on an untrusted server. On info a security level parameter 1λ and furthermore the assortment of figure content classes n (i.e., classification record should be an entire number limited by one and n), it yields the overall population framework parameter param, that is precluded from the contribution of the inverse calculations for curtness.

Network Storage (Drop box):

With our answer, Alice will just send Bob one blend key by means of a protected email. Bounce will exchange the encoded photographs from Alice's dropbox range so utilize this blend key to revise these scrambled photographs. Amid this Network Storage is untrusted outsider server or dropbox.

Encrypted Aggregate Key and Searchable Encrypted key Transfer:

The information proprietor sets up the overall population framework parameter by means of Setup and creates an open/ace mystery key consolidate by means of KeyGen. Messages are encoded by means of figure by anybody United Nations office also chooses what figure content class is related with the plaintext message to be scrambled. The data proprietor will utilize the ace mystery to get relate in nursing bunch mystery composing key for a gathering of figure content classes by means of Extract. The created keys is passed to delegates solidly (by means of secure messages or secure gadgets) at last; Associate in Nursing client with a cluster key will modify any figure message the length of the figure content's class is contained inside the bunch key by means of rework

Trapdoor generation:

Trapdoor era calculation is controlled by the client who has the bunch key to play out a pursuit. It takes as info the bunch searchable coding key kcc and a watchword w, then yields just a single trapdoor Tr.

File User:

The created keys is passed to delegates solidly (by means of secure messages or secure gadgets) at long last; any client with the Trapdoor watchword era technique will disentangle any figure message on condition that the figure content's class is contained inside the Encrypted cluster key and Searchable Encrypted key by means of decode.

CONCLUSION:

Considering the sensible disadvantage of security monitoring learning sharing framework upheld open distributed storage which needs a data proprietor to appropriate an outsized scope of keys to clients to adjust them to get to his/her reports, we tend to for the essential time propose the origination of key-cluster searchable mystery composing (KCSC) and develop a solid KCSC subject. Every investigation and examination comes about guarantee that our work will offer an effective response to amassing sensible information sharing framework upheld open distributed storage. in an exceedingly KCSC subject, the proprietor exclusively should appropriate one key to a client once offering incomprehensible records to

Volume No:2, Issue No:12 (May-2017)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

the client and in this manner the client exclusively should submit one trapdoor once he questions over all archives shared by consistent proprietor. Be that as it may, if a client needs to address over records shared by various property holders, he ought to create numerous trapdoors to the cloud. an approach to decrease the measure of trapdoors underneath multi-proprietors setting could be a future work. In addition, joined mists have pulled in stores of consideration nowadays however our KCSC can't be connected amid this case specifically. It's also a future work to supply the response for KCSC inside the instance of joined mists.

Future Work ability:

Each analysis and analysis results ensure that our work will offer an efficient answer to assembling sensible knowledge sharing system supported public cloud storage. in an exceedingly KCSC theme, the owner solely must distribute one key to a user once sharing immeasurable documents with the user and therefore the user solely must submit one trapdoor once he queries over all documents shared by constant owner. However, if a user needs to question over documents shared by multiple homeowners, he should generate multiple trapdoors to the cloud. a way to cut back the amount of trapdoors below multi-owners setting could be a future work. Moreover, united clouds have attracted heaps of attention these days however our KCSC cannot be applied during this case directly. It's additionally a future work to supply the answer for KCSC within the case of united clouds.

REFERENCES:

[1] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing", Proc. IEEE INFOCOM, pp. 534-542, 2010.

[2] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing", Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.

[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.

Volume No:2, Issue No:12 (May-2017)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

[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.