A Secure Access and Sharing Of Data in Cloud with Time Bound Decryption

P.Lavanya,

M.E (Computer Science and Engineering) Final year, Mahendra Engineering College. Namakkal, Tamilnadu.

Dr. M.Kannan B.E.,M.S.,Ph.D.,

Professor and HOD, Department of Computer Science Engineering, Mahendra Engineering College.

Namakkal. Tamilnadu

ABSTRACT:

Cloud computing is widely utilized in various fields due to its applications and advantages. The major issue focused is security, because cloud is Honest but curious. Most of research works were focused on transmission of file from a sender to receiver however if a sender wants to send a particular file to n number of users then encrypting the file every time will leads to overhead. Therefore group sharing concept was introduced which reduces overhead and time consumption for processing. In our proposed work, in group sharing to achieve conditional dissemination of data between sender and receiver is proposed. It does not focus dissemination of data alone with condition in addition secure sharing of data among a group based on attribute verification is implemented. Similarly there is possibility of data leakage when more number of users upload their file with same file name. To overcome this issue temporary keyword search is implemented which ensures availability of data for a particular period of time and if user does not download the file within time it will expires and again request from user is required. Hence we conclude that our proposed method achieved better security and efficient group sharing process without data leakage compared to other existing methods.

Keywords: group sharing, conditional based dissemination, temporary keyword search, security and ABE.

I.INTRODUCTION

Cloud computing is the way toward getting to the administrations without knowing the specific area of the information. Distributed computing is called as an utility registering since it utilizes pay per use worldview. Clients need to pay for the uses. With the innovation of distributed computing, clients can get to an assortment of assets like projects, stockpiling and application improvement stages. Cloud is the augmentation of item situated programming and it utilizes the idea of reflection. With the assistance of incredible server farms it is workable for cloud specialist organizations (CSP) to pass on different administrations to cloud clients on request. Be that as it may, this information application in the distributed storage is preoccupied by some security issue, for example, data spillage since cloud specialist organizations are not totally trusted [1]. A fundamental arrangement gave by existing framework to keep touchy client information classified against un-believed server is scrambling the information documents, before transferring into the cloud server. Be that as it may, tragically structuring a protected and effective cloud information sharing plan for dynamic gatherings in the cloud isn't basic undertaking in view of the some troublesome issues.

Multi owner process:

Multiple-owner manner is more adaptable than single proprietor way on the grounds that different proprietor habits permit each part in the gathering ought to have the option to adjust their own information for example Each part ready to peruse the information as well as alter his piece of information in the whole information record, while single proprietor way permit just Group Admin to store and change information in the cloud and individuals can just peruse the information [2].

Results of dynamic groups:

The regular varieties of enrollment make effective and make sure about information partaking in Cloud exceptionally confounded and hard because of the accompanying two essential reasons: First, new conceded clients are not permitted to get familiar with the substance of information documents put away before their investment by the unknown framework, since it outlandish for new allowed clients to legitimately contact with information proprietors and get the relating unscrambling keys [3]. Second, to decrease the intricacy of key administration it is important to get an effective participation denial instrument without refreshing the private keys of the rest of the clients.

Significance of group data sharing

A group is characterized as a set or assortment of information proprietors (clients) allocated to a lot of authorizations. Gatherings are basically centered around client's personalities [10]. Information partaking in the gathering has accomplished more noteworthy significance in numerous spaces, for example, organizations, governments and associations in reality.

Contribution of the paper:

1) The data owner should define who get to access the data within a group or list of users.

2) In a group, a user should get the permission from data owner to access data.

3) In a cloud, the group members and data owner should have authorization to store data

4) The data owner should have powers to restrict access to users in a group

LITERATURE SURVEY

Sathishkumar Easwaramoorthy et.al (2018), presents a few existing strategies were inspected and ordered dependent on three classifications: key administration and encryption draws near, looking over scrambled information and access control plans. From the order, it was inferred that there is a need to upgrade security, and security and furthermore need to give as solid as-conceivable insurance systems, without computational overheads from cloud information proprietor. Additionally, the arrangements should mull over the presentation and focus on

the speed of looking and unscrambling since the measure of information in the cloud is enormous, though the method will be wasteful in the event that it requires some investment to recover information for clients. At long last, the restrictions and difficulties that require future scientists to deal with them are talked about.

Shobha D. Pati et.al(2013), presents the fundamental help gave by the Cloud is Data Storage. Notwithstanding, it is a troublesome assignment for sharing information in multi-proprietor way where bunch administrator and all gathering individuals can store and alter information while saving information and personality protection from an untrusted cloud worker, because of the continuous difference in the enrollment. Hence secure multi-proprietor information sharing plan for dynamic gatherings in the distributed computing have been proposed which include combination of gathering mark and broadcast encryption methods. However, this framework likewise recognized a few constraints regarding productivity and security. The touchy data put away may abused by specialist organizations. To keep up cloud record's security and protection customary evacuation of undesirable documents is required. To determine this downside we propose new structure for MONA that eliminate undesirable documents naturally when the predefined timespan for sharing indicated by information proprietor has been lapsed which improve execution of the framework regarding security and effectiveness.

N.Mounika et.al (2015), describes a tricky task for sharing information in multi-proprietor way anyplace bunch administrator and all gathering individuals can store and modify information while shielding information and character protection from an untrusted cloud server, because of the incessant difference in the enrollment. so secure multi-proprietor information sharing plan for dynamic gatherings in the distributed computing have been anticipated which ingest expansion of gathering mark and communicate encryption procedures. Anyway this framework likewise perceived a few limits as far as skill and security. since multi-proprietor information putting away and partaking in a unique environmental factors dumps gigantic measure of information records in the cloud, which scraps in cloud for loose timeframe. The private data put away may changed by specialist co-ops. To keep up cloud document's security and protection standard disposal of undesirable records is required. To decide this disadvantage we propose new structure which is Reliable and Scalable Secure Method to Store and Share Secrete Data for bunches in Cloud i.e MONA that evacuate superfluous records naturally when the predefined timespan for sharing indicated by information proprietor has been run out which improve execution of the framework as far as security and proficiency.

Deepa P L et.al (2012), describes another style of registering where the assets are given online through the web. It gives stockpiling just as administration. It utilizes the strategy of virtualization. Virtualization gives the deliberation of information. Enormous measure of information can store in the cloud. Cloud supplier scrambles the touchy information and stores it in the cloud with the goal that lone the validated clients can get to the information. In this way the catchphrase security is kept up. Looking is exceptionally troublesome in encoded information. Right now center around various looking through systems and toward the end a superior arrangement is distinguished.

Mr.Ar.Arunachalam et.al (2015), presents a nice conveniences for the clients to get joy from the on-request cloud applications while not thinking about the local foundation constraints. All through the data getting to, totally various clients is additionally in an agreeable relationship, thus information sharing gets imperative to accomplish gainful edges. the overarching security arrangements essentially focus on the validation to comprehend

that a client's privative information can\'t be unapproved gotten to, anyway disregard a fragile protection issue all through a client troublesome the cloud server to demand elective clients for information sharing. The tested access demand itself could uncover the client's security whether or not or not or not it will obtain the data get to authorizations. Numerous plans utilizing quality based cryptography (ABE) are anticipated for get to the board of redistributed information in distributed computing.

Abhinay B.Angadi et.al (2013), describes security issues and potential issues in distributed computing. So as to keep the cloud secure, these security dangers should be controlled. Besides information living in the cloud is additionally inclined to various dangers and different issues like security issues, openness issues, secrecy, and trustworthiness of information. Both the cloud specialist co-op and the client should ensure that the cloud is protected enough from all the outer dangers, so there will be a solid and shared comprehension between the client and the cloud specialist co-op. Moreover, cloud specialist co-ops must guarantee that all the SLA's are met and human mistakes on their part ought to be limited, empowering smooth working. Right now security concerns identified with the three fundamental administrations gave by a Cloud processing condition are considered and the answers for forestall them have been talked about.

Qinlong Huang (2016), states the key issue is the means by which to bear the cost of secure compose procedure on ciphertext cooperatively, and different issues remember trouble for key administration and overwhelming calculation overhead on client since helpful clients may peruse and compose information utilizing any gadget. Right now, propose a safe and proficient information cooperation conspire, in which fine-grained get to control of ciphertext and make sure about information composing activity can be managed dependent on trait based encryption (ABE) and quality based mark (ABS) separately. So as to mitigate the trait authority from overwhelming key administration trouble, our plan utilizes a full designation instrument dependent on various leveled characteristic based encryption (HABE).

Wei Teng et.al (2017), instructs to accomplish practicable access control of scrambled information in an untrusted domain is a dire issue that should be fathomed. Trait based encryption (ABE) is a promising plan reasonable for access control in distributed storage frameworks. This paper proposes a various leveled characteristic based admittance control plot with consistent size ciphertext. The plan is proficient on the grounds that the length of ciphertext and the quantity of bilinear matching assessments to a consistent are fixed. Its calculation cost in encryption and decoding calculations is low. In addition, the progressive approval structure of our plan diminishes the weight and danger of a solitary power situation. We demonstrate the plan is of CCA2 security under the decisional q-Bilinear Diffie-Hellman Exponent suspicion. What's more, we actualize our plan and break down its exhibition.

Qinlong Huang et.al (2018), describes a personality based information bunch sharing and spread plan out in the open cloud, where information proprietor could communicate encoded information to a gathering of collectors one after another by indicating these recipients characters in a helpful and secure manner. So as to accomplish secure and adaptable information bunch dispersal, we embrace trait based and coordinated delivery restrictive intermediary re-encryption to ensure that solitary information disseminators whose characteristics fulfill the entrance strategy of scrambled information can scatter it to different gatherings after the delivering time by appointing a re-

encryption key to cloud worker. The re-encryption conditions are related with characteristics and delivering time, which permits information proprietor to implement fine-grained and coordinated delivery access power over scattered ciphertexts.

III.METHODOLGOY

ABE based encryption has been used to encrypt user data and stored in cloud with access control list. This access control benefits will forestall our information unapproved client get to. Anyway once a client share their information with different clients with set of properties in the event that any benefit alteration is finished by co-client, at that point information ought to be re-scrambled by his/her characteristics. This is prepared as a substitute re-encryption plan and it is utilized to accomplish secure information dispersal in distributed computing by appointing a re-encryption key related with the new recipients to the CSP. The issue behind this current framework is once client achieves specific key of the particular report there is an opportunity of re-getting to the document without client information. Consequently in our proposed ABE encryption is executed to scramble the information.

When record is encoded and put away in cloud with catchphrase. On the off chance that client needs specific report he/she will look through it utilizing watchword. To upgrade security the scanned information will be accessible for a specific time else it will be terminated thusly it ought to be looked once more. On the off chance that the record doesn't unscramble inside the specific time it will be terminated on the other hand the client needs to send solicitation to the information proprietor and new key will be created. Thus it will guarantee client protection from with no spillage.

The user role has been arranged into the accompanying classifications: information proprietor, information co-proprietor, information disseminator and information accessor. The information proprietor can pick an arrangement accumulation procedure and characterize an entrance approach to implement spread conditions. At that point he scrambles information for a lot of beneficiaries, and re-appropriates the figure content to CSP for sharing and scattering. The information co-proprietors labeled by information proprietor can attach get to approaches to the encoded information with CSP and produce the reestablished figure content. The information disseminator can get to the information and furthermore create the re-encryption key to spread information proprietor's information to other people on the off chance that he fulfills enough access arrangements in the figure content. The information accessor can unscramble the underlying, restored and re-encoded figure content with her or his private key. The client can enroll and verify if the client exists. The approved clients can transfer the record to the server. The server consequently creates a private key through encryption calculation; the record is encoded and put away on the servers. Any client can demand to download a document at first by checking the accessibility of record and assets, and afterward the approved client can download document by giving his private key.

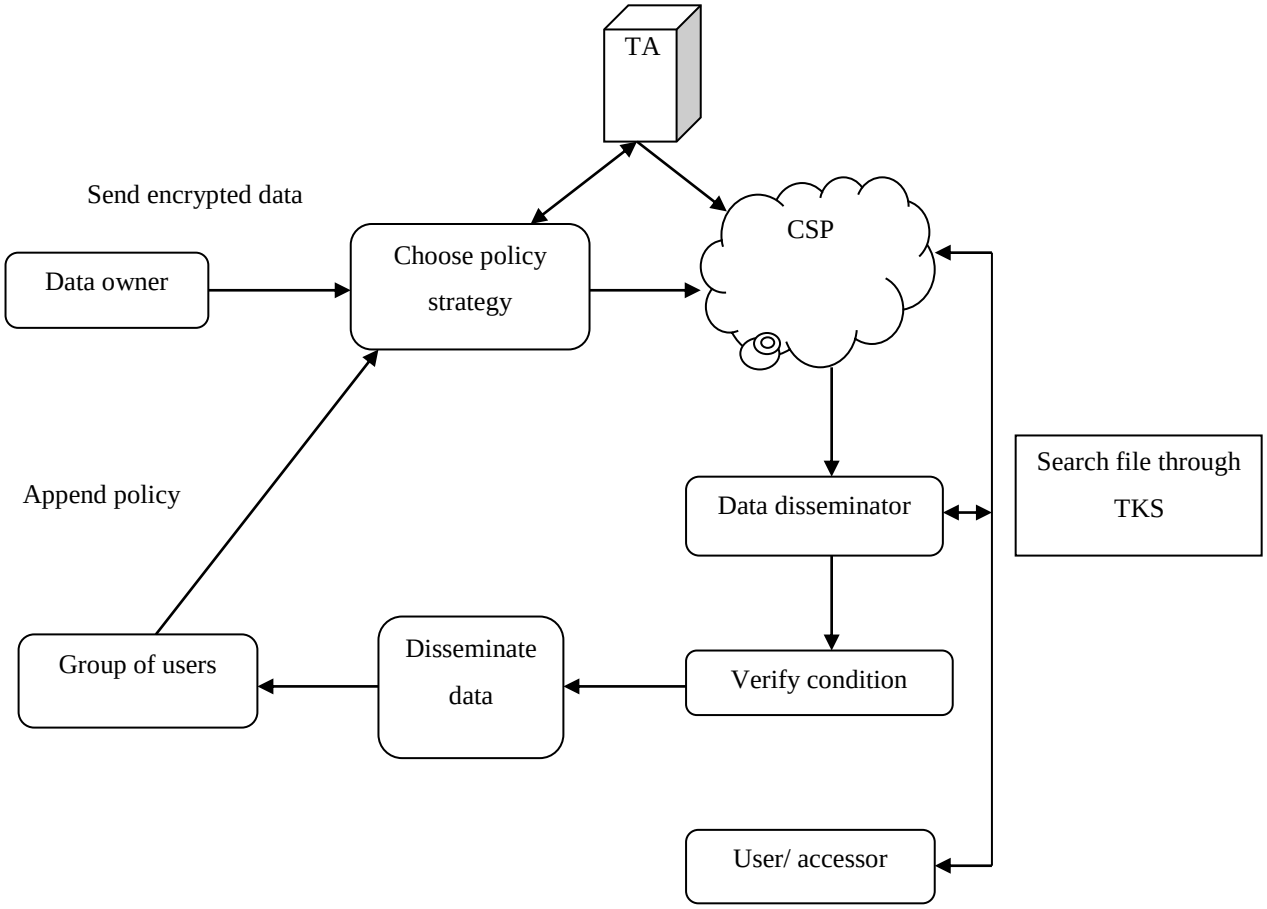

Figure 1: Working Of Proposed System

ABE: Attribute-Based Encryption:

Setup: This algorithm takes as an input security parameter k, and returns public key PK which is used for encryption by sender and secret master key MK which is used by TA to generate user secret keys. It takes security parameters as input and outputs public parameters and master secret key.

Encrypt: This algorithm takes as information PK, M and T; and yields ciphertext CT. The encryption calculation takes as info the open boundaries PK, a message M, and an entrance structure An over the universe of characteristics. The calculation will scramble M and produce a ciphertext CT with the end goal that solitary a client that has a lot of traits that fulfills the entrance structure will have the option to decode the message. We will accept that the ciphertext certainly contains A.

Key Generation: It takes as an info γ related with client and MK. It yields SK used to decode message encoded under T if and just if γ matches T. The key age calculation takes as information the ace key MK and a lot of qualities S that depict the key. It yields a private key SK.

Decrypt: It takes as input CT`, SK for γ. It yields M if and just if γ fulfills access structure related with CT. The decoding calculation takes as info the open boundaries PK, a ciphertext CT, which contains an entrance strategy An, and a private key SK, which is a private key for a set S of traits. On the off chance that the set S of properties fulfills the entrance structure A, at that point the calculation will unscramble the ciphertext and return a message M.

Trusted authority:

The believed authority is a completely confided to some degree that instates the framework open key, and creates private keys just as characteristic keys for clients. For instance, it tends to be acted by the chairman of the association or government disability organization. These substances perform information open inspecting and record confirmation before send to the client. Re-encryption performs for information sharing between numerous clients.

Encryption with timing:

In this module, proprietors transfer the information to cloud. Here information proprietor relegates get to rights for document and dole out co-proprietors of information and transfer it. The principle objective for these models is to give security and access control. The principle perspectives are to give adaptability, versatility and fine grained get to control. In old style model, this can be accomplished just when client and server are in a confided in space. In ABE plot both the client mystery key and the ciphertext are related with a lot of traits. A client can unscramble the figure content if and just if in any event a limit number of properties cover between the figure content and client mystery key. Unique in relation to customary open key cryptography, for example, Identity-Based Encryption, ABE is actualized for one-to numerous encryption in which figure writings are not really encoded to one specific client, it might be for more than one number of clients.

Policy aggregation strategy:

1) Full permit: All proprietors (counting information proprietor and information co-proprietors) have a similar option to choose the spread states of information. The information disseminator ought to fulfill all the entrance arrangements characterized by these proprietors.

2) Owner priority: The information proprietor's choice has high need, however he labels the co-proprietors. The information disseminator can disperse the information just when he fulfills the entrance strategy of information proprietor or all the entrance strategies of information co-proprietors.

3) Majority permit: The information proprietor initially picks a limit esteem, and the information can be scattered if and just if the aggregate of access arrangements fulfilled by disseminator's traits is more prominent than or equivalent to this fixed edge.

IV.RESULT AND DISCUSSION

Enabling secure data access in group sharing by conditional dissemination factor in efficient way. Security against different encryption method and our proposed method has been shown in below graph and data integrity.

MD5 attains higher data integrity compared to security and AES data integrity respectively. But in AES it gains more security than data integrity. Comparing these two algorithms our algorithm attains higher security and data integrity.

Data integrity is the maintenance of and the assurance of the accuracy and consistency of data over its entire life-cycle, and is a critical aspect to the design, implementation and usage of any system which stores, processes, or retrieves data.

Data security refers to the process of protecting data from unauthorized access and data corruption throughout its lifecycle. Data security includes data encryption, hashing, tokenization, and key management practices that protect data across all applications and platforms.

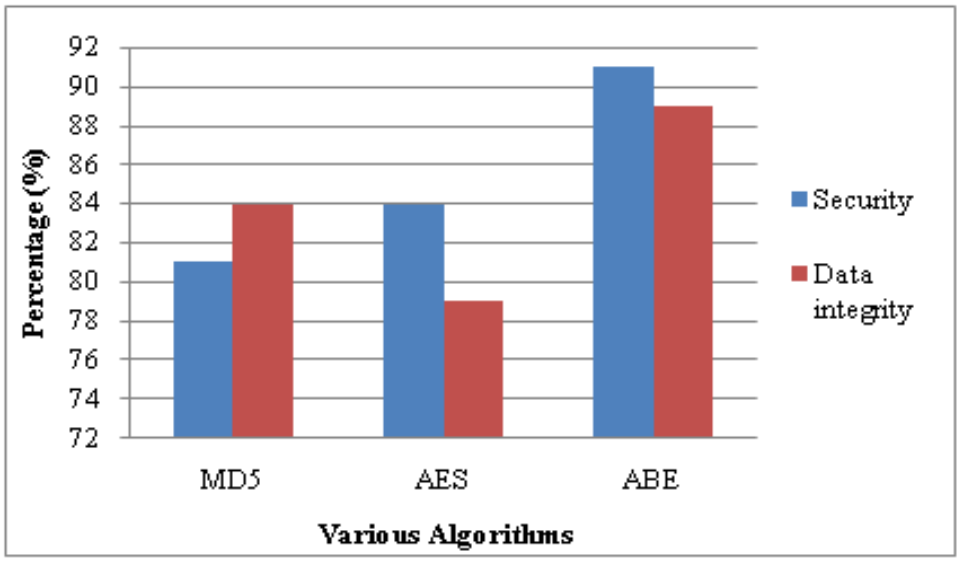

Figure 2: comparison graph of security and data integrity

Data leakage is the unauthorized transmission of data from within an organization to an external destination or recipient. It needs to safeguard the security and durability of service based on the demand of users.

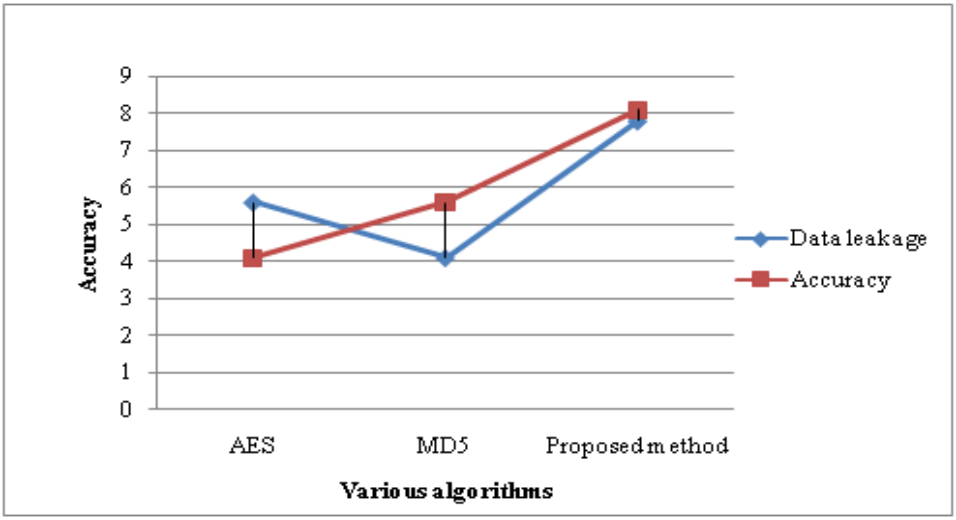

Figure 3: Accuracy level of data retrieval and data leakage comparison

In above graph data leakage and data extraction has been described. Compared to existing algorithms our proposed method retrieves most accurate data with respect to keyword and it reduces data leakage through temporary keyword search.

CONCLUSION:

In cloud computing, enabling security is major issue. This has been taken as issue and focused in our work and propose solution for it. In general obtaining security in cloud during transmission data from particular sender to receiver was done by cryptography approach. However single data sharing leads to overhead of key maintenance, encryption and decryption for a particular file. This can be overcome by group sharing and it had been implemented earlier. However in a group if a owner wants to achieve his/her privacy is sharing file is not possible. This was implemented and achieved in our work. Through ABE and based on priority sharing a data owner can share their file with condition in a group. Similarly there is chance for data leakage while searching file in cloud through a particular keyword. Temporary keyword search has been implemented it enables time availability for a particular file if user does not retrieves data within time it will be unavailable for particular user therefore again new request should be generated to owner of the file.

REFERENCES:

[1] Sathishkumar Easwaramoorthy, Chunduru Anilkumar, Usha Moorthy, Sravankumar, "Review on dynamic group data sharing in cloud environment" International Journal of Engineering & Technology, volume 7, issue 2, 19 May 2018.

[2] Shobha D. Patil, Dr. Sulochana B. Sonkamble, "A Dynamic Secure Group Sharing in Cloud Computing" International Journal of Science and Research (IJSR) Volume 4 Issue 8, August 2015.

[3] N.Mounika, N.Parushuram, R.Anil Kumar, "A Dynamic Secure Group Sharing Framework in Public Cloud Computing" International Journal of Computer Engineering In Research Trends Volume 2, Issue 12, December-2015.

[4] Deepa P L, S Vinoth Kumar, Dr S Karthik, "Searching Techniques In Encrypted Cloud Data" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 1, Issue 8, October 2012.

[5] Mr.Ar.Arunachalam, Deepak Kumar, Atul Ranjan, "Shared Authority Based Privacy-preserving Authentication Protocol in Cloud Computing" An international journal of advanced computer technology, 4 (4), April-2015 (Volume-IV, Issue-IV).

[6] Abhinay B.Angadi, Akshata B.Angadi, Karuna C.Gull, "Security Issues with Possible Solutions in Cloud Computing-A Survey" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 2, February 2013.

[7] Qinlong Huang, Yixian Yang and Mansuo Shen, "Secure and efficient data collaboration with hierarchical attribute-based encryption in cloud computing"

[8] W. Teng, G. Yang, Y. Xiang, T. Zhang, and D. Wang, "Attributebased access control with constant-size ciphertext in cloud computing," IEEE Transactions on Cloud Computing, vol. 5, no. 4, pp. 617-627, 2017.

[9] Q. Huang, Y. Yang, and J. Fu, "Secure data group sharing and dissemination with attribute and time conditions in Public Clouds," IEEE Transactions on Services Computing, Volume 09, Special Issue 4, May 2019, Page 264-274.

[10] N. Paladi, C. Gehrmann, and A. Michalas, "Providing user security guarantees in public infrastructure clouds," IEEE Transactions on Cloud Computing, vol. 5, no. 3, pp. 405-419, 2017.