Cloud Data Storage Using Attribute based Encryption with Verifiable Outsourcing Auditor Security Schemes

A.S. Syed Fiaz, Balabhadruni Rahul, Janapareddy Rupendra, K. Nitesh

Abstract--- ***Cloud storage services turned out to be continuously elegant. Owing to the implication of security, a few cloud storage secret composing schemes are anticipated to monitor data from those that don't approach. Every single such plan accepted that cloud storage providers region unit safe and can't be hacked; at the same time, in pursue, a few experts may drive cloud storage providers to uncover client insider facts or confidential data on the cloud, hence by and large going around storage mystery composing schemes. Amid this paper, we tend to bless our style for a pristine cloud storage mystery composing subject that permits cloud storage providers to make persuading false client privileged insights to protect client security. Since coercers can't reveal whenever acquired insider facts zone unit genuine or not, the cloud storage providers ensure that client security keeps on being immovably secured. The vast majority of the anticipated schemes expect cloud storage service providers or dependable outsiders taking care of key administration square measure solid and can't be hacked; nonetheless, in pursue, a few substances would conceivably capture interchanges among clients and cloud storage providers at that point urge storage providers to unfasten client privileged insights by misuse government control or diverse proposes that. All through this case, scrambled information square measure thought to be known and storage provider's square measure asked for to unfasten client insider facts***

Keywords--- ***Cloud Storage, Secure Information Retrieval, Access Control, Attribute based Encryption (ABE), Deniable Encryption.***

I. INTRODUCTION

Cloud computing [11] worldview has seen a gigantic move towards its reception and it has turned into a pattern in the data innovation space as it guarantees critical cost decreases and new business potential to its uses and suppliers. Cloud computing, as another innovation worldview with promising further, is winding up increasingly more well-known these days. It can give clients boundless computing asset. Undertakings and individuals can redistribute tedious calculation remaining tasks at hand to cloud without spending the additional capital on sending and keeping up equipment and programming. Lately, re-appropriating calculation has pulled in much consideration and been inquired about generally. It has been considered in numerous applications including logical calculations. Nonetheless, it needs to fulfill a few new prerequisites to accomplish this objective. Right off the bat, the genuine customer's mystery keys for cloud storage auditing ought not to be known by the approved party who performs re-appropriating calculation for key updates. Else, it will bring the new security danger. So the approved party should just hold an encoded form of the client's mystery key for cloud storage auditing. Besides, on the grounds that the approved party performing redistributing calculation just realizes the scrambled mystery keys, key updates ought to be finished under the encoded state. A focal security highlight of Attribute-Based Encryption is conspiracy obstruction. A plot safe encryption calculation is the one in which two data sources don't hash to a similar yield. These schemes accept that the cloud suppliers don't unveil the cloud client's data and mysteries, which isn't the reality dependably. For instance, in 2010, without telling its clients, Google discharged client records to the FBI subsequent to getting a court order [2]. In 2014, Edward Snowden unveiled the presence of worldwide observation programs that gather such cloud data as messages, messages, and voice messages from some innovation organizations [3], [4]. In some cases unapproved client may likewise endeavor to get to the data wrongfully. So as to control unlawful access to cloud data, there is a requirement for deniable encryption service that denies illicit access to real data. This procedure was first proposed by R. Canetti et. Al [5]. This encryption plot is based on polynomial deniability and produces a phony client data if the client is observed to be unapproved. The general thought of this deniable encryption plot is to persuade the unapproved client by giving the phony data with the goal that the client does not attempt to get to the data once more. Deniable encryption schemes don't model endeavor cloud data get to great as far as client reaction time on the grounds that the plan does not address reaction time prerequisites of clients of such frameworks. Along these lines a deniable encryption plot is proposed in this examination that tends to security and reaction time necessities of clients.

II. RELATED WORK

ABE a helpful instrument for cloud storage services since data sharing is a vital element for such services. There are such a large number of cloud storage clients that it is unfeasible for data proprietors to encode their data by pairwise keys.

Manuscript received September 16, 2019.

A.S. Syed Fiaz, Assistant Professor, Department of Computer Science and Engineering, Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, Chennai, T.N, India.

Balabhadruni Rahul, B.Tech Scholar, Department of Computer Science and Engineering, Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, Chennai, T.N, India.

Janapareddy Rupendra, B.Tech Scholar, Department of Computer Science and Engineering, Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, Chennai, T.N, India.

K. Nitesh, B.Tech Scholar, Department of Computer Science and Engineering, Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, Chennai, T.N, India.

Besides, it is likewise an unreasonable to encode data commonly for such a large number of individuals. With ABE, data proprietors choose just which sort of clients can get to their scrambled data. Clients who can fulfill the conditions can decode the scrambled data. There are two sorts of ABE, CP-ABE and Key-Policy ABE (KPABE). The contrast between these two lies in approach checking. KP-ABE is an ABE in which the strategy is inserted in the client mystery key and the attribute set is implanted in the altered or mystery or figure content. On the other hand, CP-ABE installs the arrangement into the ciphertext and the client mystery has the attribute set. Goyal et al. proposed the first KPABE in they developed an expressive method to relate any monotonic recipe as the approach for client mystery keys. Bethen court et al. proposed the first CP-ABE in This plan utilized a tree get to structure to express any monotonic equation over attributes as the approach in the ciphertext. The first completely expressive CP-ABE was proposed by Waters in, which utilized Linear Secret Sharing Schemes (LSSS) to fabricate a ciphertext strategy. Lewko et al. improved the Waters plan to a fullysecure CP-ABE, however with some productivity misfortune, in [13]. Recently, Attrapadung et al. built a CP-ABE with a steady size ciphertext in and Tysowski et al. designed their CP-ABE conspire for asset obliged clients in. SQL implantation is the web attack instruments used to take data from cloud by developers. It is a technique which tries to pass SQL Commands to connect with back end database. Generally it is used to relax the web security up cloud at login page where customer name and watchword will be seen by the SQL Injection. XML signature portrays XML language structure for modernized mark which is a wrapping attack; it is used by various web developments, for instance, SOAP, SAML and others [4]. The attack is done in the midst of the understanding of Simple Object Access Protocol (SOAP) message between a true blue customer and the web server which licenses programs that continue running on unique working systems to confer Hyper Text Transfer Protocol (HTTP) and its Extensible Mark-up Language (XML). The attack is done by duplicating the customer's record and mystery word in the login period, the software engineer embeds a trick part (the wrapper) into the message structure, and moves message with pernicious code and after that sends the message to the server. Since the primary body is up 'til now real, the server will be cheated into affirming the message that has truly been changed. Appropriately, the software engineer can increment unapproved access to verified resources and procedure the arranged tasks. The noteworthy security risks gone up against by web applications in cloud computing are [5] • Injection imperfections like SQL, OS and LDAP mixture • Cross-site scripting • Broken Authentication and session organization • Insecure direct inquiry references • Cross-page request creation • Security misconfiguration • Insecure cryptographic storage • Failure to keep URL get to • Insufficient transport layer protection • Invalidated redirects and advances An Information system security course of action watches out for the essential Issues in light of CIA Triad that is Confidentiality, Integrity and Availability while AAA thought issues are Authentication and Identification, Authorization and Auditing. Protection of data in cloud storage is keeping the un-endorsed presentation of data extremely still or travel. The key obligations of the Integrity are affirming the data initiation, Detecting the adjustment of data, choosing if the data beginning stage is changed and Recovery from recognizable botches and data mishaps. Openness is stressed over denying silly access to preparing resources and maintaining a strategic distance from external perils, risks and attacks. Affirmation is the methodology of unmistakable evidence it says u's identity and the Authorization is the path toward checking, it says what you agrees to use utilities are. Assessing is a survey, check or purposeful examination as for limit in cloud computing.

III. METHODOLOGY

Most deniable open key plans are bitwise, which implies these plans can process one piece a period. Henceforth, bitwise deniable encryption plans are bumbling for genuine use, particularly in the distributed storage administration case. To determine this issue, considered a half breed encryption plot that simultaneously utilizes symmetric and deviated encryption they utilize a deniably encoded arrangement ahead symmetric information encryption key, while genuine information are scrambled by a symmetric key encryption instrument. Chiefly deniable encryption plans have unscrambling mistake issues. These mistakes originate from the thought about unscrambling instruments. Utilizations the subset choice component for decoding the beneficiary chooses the unscrambled message as indicated by the subset choice outcome. On the off chance that the sender wants a component from the all inclusive set yet unfortunately the component is situated in the particular subset, at that point a blunder happens. The indistinguishable mistake happens in all straight forward set-based deniable encryption plans. Degree the arrangement of a document may be unused to under the solicitation by the client, while closing the season of the understanding or thoroughly move the records beginning with one cloud [12] then onto the following cloud nature's area. The position when any of the above criteria exists the arrangement will dismiss and the key executive will thoroughly pull back from the open key of the related record. So nobody can get the control key of a disavowed record in future. Because of this reason we can say the record is unquestionably eradicated. To get well the document, the client must request the key controller to manufacture the open key. For that the client must be checked. The key arrangement trait based encryption standard is used for document get to which is affirmed by methods for a property associated with the record.

Deniable Encryption process

Deniable encryption includes senders and collectors making acceptable phony verification of phony information in figure messages with the end goal that outside coercers are satisfied. Note that deniability originates from reality that coercers can't affirm the proposed actualities is wrong and thus no motivation to decrease the given proof.

This methodology attempts to generally square intimidation endeavors since coercers realize that their endeavors will be pointless. We utilize this thought with the end goal that distributed storage suppliers can give review free stockpiling administrations. In the distributed storage circumstance, information proprietors who store their information on the cloud are much the same as senders in the deniable encryption conspire. The individuals who can get to the scrambled information assume the job of recipient in the deniable encryption conspire, including the distributed storage suppliers themselves, who have framework wide insider facts and must most likely unscramble all encoded information. We utilize ABE attributes for verifying put away information with a fine-grained get to control component and deniable encryption to forestall outside evaluating.

Composite order Bilinear Group

Structure a deniable CPABE conspire with Composite request bilinear gatherings for structure review free distributed storage administrations. Composite request bilinear gatherings contain two appealing properties, to be specific anticipating and dropping. We utilize the dropping property for structure a predictable domain; then again, Freeman likewise brought up the vital issue of computational expense as to the Composite request bilinear gathering. The bilinear guide activity of a Composite request bilinear gathering is much slower than the task of a prime request bilinear gathering with a similar security level. That is, in this plan, a client will pay out a lot of time in unscrambling while getting to documents from the cloud. To make Composite request bilinear gathering plans increasingly practical, into prime request plans. Both anticipating and dropping can't be all the while accomplished in prime request bunches in. For a similar reason, we utilize a recreating instrument anticipated to change over our Composite request bilinear gathering plan to a prime request bilinear gathering plan. This apparatus depends on double orthonormal bases and the subspace supposition. Not at all like subgroups are reenacted as various orthonormal bases and in this way, by the symmetrical property, the bilinear activity will be dropped between various subgroups. Our formal deniable CP-ABE development strategy utilizes just the dropping property of the Composite request gathering.

Attribute-Based Encryption

Distributed storage administrations have quickly turned out to be progressively famous. Clients can store their information on the cloud and access their information anyplace whenever. For the reason of client security, the information put away on the cloud is regularly encoded and shielded from access by different clients. Thinking about the common property of the cloud information, attribute based encryption (ABE) is viewed as a standout amongst the most reasonable encryption plans for distributed storage. There are a few ABE plans that have been proposed, including. A large portion of the proposed plans accept distributed storage specialist co-ops or believed outsiders overseeing key administration are trusted and can't be hacked; yet, practically speaking, a few substances may cut off interchanges among clients and distributed storage suppliers and afterward constrain capacity suppliers to discharge client insider facts by utilizing government control or different methods. For this situation, scrambled information is comprehended to be known and capacity suppliers are mentioned to discharge client privileged insights.

Cloud Storage

Distributed storage administrations have developed famously. For the reason of the significance of security, many distributed storage encryption plans have been anticipated to shield information from the individuals who don't approach. Every single such plan accepted that distributed storage suppliers are sheltered and can't be hacked. In any case, practically speaking, a few experts (i.e., coercers) may constrain distributed storage suppliers to uncover client privileged insights or private information on the cloud, in this manner altogether going around capacity encryption plans. Here we present a plan for another distributed storage encryption plot that empowers distributed storage suppliers to produce sensible phony client privileged insights to ensure client protection. As should be obvious whenever acquired privileged insights are right or not, the distributed storage suppliers ensure that client security is still solidly ensured. The vast majority of the anticipated plans surmise distributed storage specialist co-ops or believed outsiders overseeing key administration are trusted and can't be hacked;

Distributed Key Policy Attribute Based Encryption

KP-ABE is an open key cryptography crude for one-to many correspondences. In KP-ABE, data is related with properties for every one of which an open key part is portrayed. The encode or colleagues the arrangement of credits to the message by scrambling it with the looking at open key parts. Every customer is doled out an entrance game plan which is typically portrayed as an entrance tree over data qualities. Customer mystery key is portrayed to replicate the entrance structure so the customer has the aptitude to disentangle a figure content if and just if the data traits satisfy his entrance structure.

IV. THREAT MODEL

A. Integrity Threats

There are two kinds of threats related to the integrity of shared data. In first threat, an adversary may try to corrupt the integrity of shared data. In second threat, the cloud service provider may inadvertently corrupt (or even remove) data in its storage due to hardware failures and human errors. In worse case the cloud service provider is economically motivated, which means it may be reluctant to inform users about such corruption of data in order to save its reputation and avoid losing profits of its services.

B. Privacy Threats

The identity of the signer on each block in shared data is private and confidential to the group.

In the process of auditing, a public verifier, who is only allowed to verify the correctness of shared data integrity, may try to reveal the identity of the signer on each block in shared data based on verification metadata. Once the public verifier reveals the identity of the signer on each block, it can easily distinguish a high-value target from others.

V. SECURITY ISSUES IN CLOUD

The security will be analyzed in terms of two aspects, that is, the confidentiality of data and the authorization of duplicate check [13]. We suppose that all the files are sensitive and needed to be fully protected against both public cloud and private cloud. Under this assumption, two kinds of adversaries are considered, that is, adversaries who aim to extract secret information as much as possible from both public cloud and private cloud, and internal adversaries who aim to obtain more information on the file from the public cloud and duplicate-check token information from the private cloud outside of their scopes. The data will be encrypted in our deduplication system before outsourcing to the storage cloud to maintain the confidentiality of data. The data is encrypted with the traditional encryption scheme and the data encrypted with such encryption method which guarantees the security of data. System address the problem of privacy preserving deduplication in cloud computing and propose a new deduplication system supporting for Differential Authorization and Authorized Duplicate Check. Each authorized user is able to get his/her individual token of his file to perform duplicate check based on his privileges. Under this assumption, any unauthorized user cannot generate a token for duplicate check out of his privileges or without the aid from the private cloud server. Authorized user is able to use his/her individual private keys to generate query for certain file and the privileges he/she owned with the help of private cloud, while the public cloud performs the duplicate check directly and tells the user if there is any duplicate. The security requirements considered in two folds, including the security of data files and security of file token. For the security of file token. Unauthorized users without appropriate privileges or file prevented from getting or generating the file tokens for duplicate check of any file stored at the Storage cloud. The users are not allowed to collude with the public cloud server. It requires that any user without querying the private cloud server for some file token, he cannot able to get any useful information from the token, which includes the privilege or the file information and to maintain the data confidentiality unauthorized users without appropriate privileges or files, prevented from access to the underlying plaintext stored at Storage cloud.

VI. THIRD PARTY AUDITOR

The review in distributed computing is extensively characterized into three, they are first gathering examiner or inner inspector where the cloud client association reviews by its own, it is a self-appraisal method for interruption discovery and aversion framework. Second gathering evaluator is a Cloud Service Provider who has huge assets and specialists in structure and overseeing circulated distributed storage servers, possesses and works where an outside examining system is utilized for information security and quality administration in cloud administrations. The Cloud information stockpiling design comprises of three performing artists, the cloud client who has vast measure of information to be put away and recovered according to the prerequisite in the cloud. The cloud specialist organization who keeps up the distributed storage benefits and gives cloud information stockpiling. To empower security saving open inspecting for cloud information stockpiling appeared in the model, the convention we planned ought to accomplish the accompanying counteractive action, insurance and execution ensures;

1. **Storage accuracy**: To ensure that the users data are indeed stored appropriately and kept all the time in cloud.
2. **Reliable Security:** To ensure that the TPA cannot gain users data from the information collected during the auditing process.
3. **Group auditing**: To enable TPA provide secure and efficient auditing to possible large number of different users simultaneously
4. **Detection and Prevention:** To allow TPA to provide auditing with minimum communication.

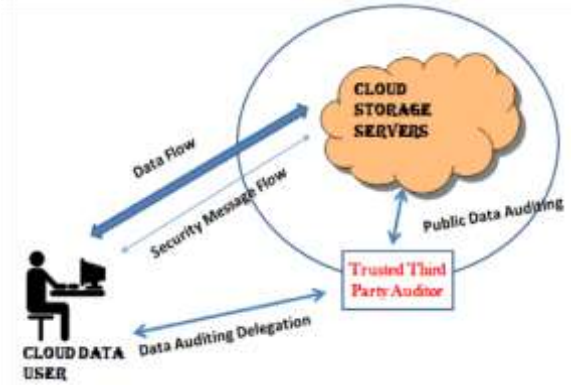

Figure 1: The Architecture of Cloud Data Storage Services

The Trusted Third Party (TTP) is an audit based organization which facilitates secure interactions between two parties that is cloud user and cloud provider, where both of them trust this third party. The Third Party Auditor (TPA) registered security service provider allocated by the cloud service provider with strong Authentication and Authorization. The TPA can perform Multiple Auditing Tasks for single or multiple clouds in branch manner for better efficiency and security [6].Public audit-ability: to allow TPA to verify the correctness of the cloud data on demand without retrieving a copy of the whole data or introducing additional online burden to the cloud users.

VII. HOMOMORPHIC AUTHENTICATORS

Homomorphic authenticators (likewise called homomorphic evident labels) are fundamental apparatuses to build open examining components. The unforgeability, a homomorphic authenticable mark conspire, which signifies a homomorphic authenticator dependent on marks, ought to likewise fulfill the accompanying properties.

A. Square less evidence

It enables a verifier to review the rightness of information put away in the cloud server with an exceptional square, which is a direct blend of the considerable number of squares in information. In the event that the respectability of the joined square is right, at that point the verifier trusts that the uprightness of the whole information is right. Along these lines, the verifier does not have to download every one of the squares to check the honesty of information.

B. Non-pliability

It shows that a foe can't create substantial marks on self-assertive squares by directly joining existing marks.

VIII. PROPOSED SYSTEM ARCHITECTURE & RESULTS

This paper includes three gatherings: the cloud server, the outsider inspector and clients is appeared in Figure 3. There are two sorts of clients in a gathering: the first client and various gathering clients. The first client and gathering clients are the two individuals from the gathering. Gathering individuals are permitted to get to and change shared information made by the first client dependent on access control polices. Shared information and its check data are both put away in the cloud server. The outsider reviewer can check the honesty of shared information in the cloud server in the interest of gathering individuals.

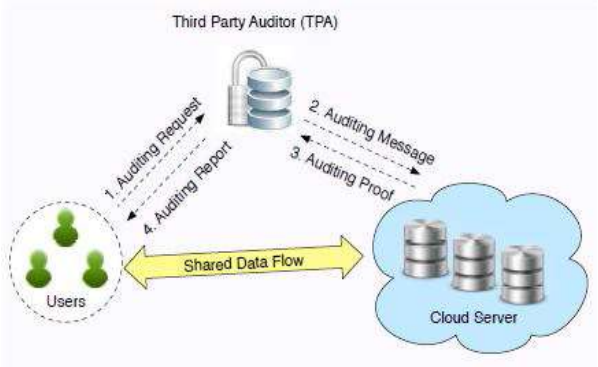

Figure 2: System model includes User, Cloud Server and TPA

In this paper, we just think about how to review the trustworthiness of imparted information in the cloud to static gatherings. It implies the gathering is pre-characterized before shared information is made in the cloud and the enrollment of clients in the gathering isn't changed amid information sharing. The first client is in charge of choosing who can share her information before redistributing information to the cloud. At the point when a client (either the first client or a gathering client) wishes to check the respectability of shared information, she initially sends an evaluating solicitation to the TPA. Subsequent to getting the examining demand, the TPA produces an evaluating message to the cloud server, and recovers a reviewing evidence of shared information from the cloud server. At that point the TPA confirms the accuracy of the reviewing evidence. At long last, the TPA sends a reviewing report to the client dependent on the consequence of the check.

Proposed Algorithm

Confirmation, Authorization and Auditing for secure distributed storage is executed based on the accompanying key focuses

- Our System Supports an External examiner to review clients re-appropriated information in the cloud without learning information on the information content.
- The TPA underpins adaptable on solicitation by cloud specialist organization for proficient open examining in the distributed computing
- Auditing is the procedures which is accomplished for the cloud to accomplish clump inspecting where numerous designated examining errands from various clients can be performed at the same time by the TPA
- The examining is the insight based Dynamic information process for the information and data security in distributed computing
- data respectability calculation, for example, Message Authentication Code (MAC code) by methods for Hash Based Message Authentication Code (HMAC code) to check the honesty of the information being put away in the cloud.
- By methods for MAC code, we upgrade the information uprightness of the cloud information.

Stage 1: Start of an Algorithm

Stage 2: Key Generation by Advanced Encryption Standard (AES) Algorithm 16-bit Hexa Decimal keys are created

Stage 3: Map the Key to the documents

Stage 4: Divide the documents into the squares

Stage 5: Each Encrypted Block is Associated with Key

Stage 6: Store the information squares to the Cloud Storage Server

Stage 7: Simultaneously Intelligent framework sends a duplicate of keys to TPA

Stage 8: On solicitation of Cloud Service Provider (CSP) the Auditing forms with be finished by TPA

Stage 9: Validate the information by marks and information respectability proofs

Stage 10: Successful approval, confirmation will be accomplished for dynamic evaluating by TPA End of Algorithm.

IX. CONCLUSION

Cloud information security is a vital viewpoint for the customer while utilizing cloud administrations. Outside Auditor can be utilized to guarantee the security and respectability of information. Outsider evaluator can be a believed outsider to determine the contentions between the cloud specialist co-op and the customer. Different plans are proposed by creators throughout the years to give a confided in condition to cloud administrations. Encryption and Decryption calculations are utilized to give the security to client while utilizing outsider examiner.

This paper gives a conceptual perspective on various plans proposed in later past for cloud information security utilizing outsider inspector. The majority of the creators have proposed plans which depend on encoding the information utilizing some encryption calculation and make outsider inspector store a message digest or scrambled duplicate of similar information that is put away with the specialist organization. The outsider is utilized to determine any sort of contentions between specialist co-op and customer.

REFERENCES

1. C. Wang, S.S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," IEEE Trans. Computers, vol. 62, no. 2, pp. 362-375, Feb. 2013.
2. D. Song, E. Shi, I. Fischer, and U. Shankar, "Cloud Data Protection for the Masses," Computer, vol. 45, no. 1, pp. 39-45, 2012.
3. N. Cao, S. Yu, Z. Yang, W. Lou, and Y.T. Hou, "LT Codes-Based Secure and Reliable Cloud Storage Service," Proc. IEEE INFO-COM, 2012.
4. B. Wang, B. Li, and H. Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud," Proc. IEEE Fifth Int'l Conf. Cloud Computing, pp. 295-302, 2012.
5. Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S.S Yau," Dynamic Audit Services for Integrity Verification of Outsourced Storages in Clouds,"Proc. ACM Symp. Applied Computing (SAC'11), pp. 1550-1557, 2011.
6. B. Chen, R. Curtmola, G. Ateniese, and R. Burns, "Remote Data Checking for Network Coding-Based Distributed Storage Systems," Proc. ACM Workshop Cloud Computing Security Workshop (CCSW'10), pp. 31-42, 2010.
7. M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A.Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing,"Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010.
8. C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," Proc. IEEE INFOCOM, pp. 525-533, 2010.
9. C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, "Dynamic Provable Data Possession," Proc. 16th ACM Conf. Com-puter and Comm. Security (CCS'09), pp. 213-222, 2009.
10. Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamic for Storage Security in Cloud Computing," Proc. 14th European Conf. Research in Computer Security (ESORICS'09), pp. 355-370, 2009.
11. Syed Fiaz. A.S, S. Sankar "Iaas: Qos based Automated User Requirement Identification for Optimal Resource Allocation in Multi Cloud", International Journal of Engineering & Technology (UAE), Vol 7, No 3.34, pp.210 – 212, ISSN: 2227-524X, 2018
12. Syed Fiaz.A.S, "Prediction of best cloud service provider using the QoS ranking framework", International Journal of Engineering & Technology (UAE), Vol 7, No 1.1, pp.486-488, ISSN: 2227-524X, 2018
13. Syed Fiaz A S, N Asha, D Sumathi, Syed Navaz A S, "Data Visualization: Enhancing Big Data More Adaptable and Valuable", International Journal of Applied Engineering Research, Volume 11, Number 4, pp.2801-2804, ISSN 0973-4562, Feb 2016.