MJRET
Open Access
Multidisciplinary Journal of Research in Engineering and Technology
Journal homepage: www.mjret.in
ISSN:2348 - 6953

SECURING PUBLIC CLOUD USING MULTI-ATTRIBUTE, MULTI-AUTHORITY LAYER SCHEME WITH DATASET FRAGMENTS

Mr. Vipin, Dr. Pankaj Agarkar
Department of Computer Engineering
Dr. D. Y. Patil School of Engineering,
Pune, India

Abstract: *Ciphertext-policy Attribute-Based Encryption (CP-ABE) has been embraced as a promising method to give adaptable, fine-grained and protect information from unauthorized access for distributed storage with genuine yet inquisitive cloud servers. In any case, in the current CP-ABE designs, the single quality master must execute the monotonous customer realness check and secret key course, and hereafter it results in a lone point execution bottleneck when a CP-ABE plot is grasped in a far-reaching scale appropriated capacity system. Clients may think to use complex key and its access mechanism for that they can use extensive stretch to acquire their secrete keys, accordingly bringing about low-effectiveness of the framework. Even though multi specialist involved in the proposed security mechanism, these plans still can't defeat the disadvantages of single-point bottleneck and low productivity, because of the way that every one of the experts still autonomously deals with a unique property set. In this paper, we propose a novel heterogeneous framework to oust the issue of single-point execution bottleneck and give a more viable access control plot with an analyzing segment. clients might imagine using complicated key and it get right of entry to mechanism for that they can use big stretch to accumulate their secrete keys, as a result, bringing approximately low-effectiveness of the framework. even though multi expert worried within the proposed safety mechanism, these plans still cannot defeat the dangers of unmarried-point bottleneck and occasional productiveness, because of the manner that every one of the experts still autonomously deals with a completely unique assets set. on this paper, we propose a novel heterogeneous framework to oust the issue of single-point execution bottleneck and give an extra possible access manipulate plot with a studying section. Our framework uses various credit score*

government to share the pile of patron legitimacy check. in the interim, in our arrangement, a CA (important Authority) is acquainted with create mystery keys for realness affirmed customers. To remodel security, we moreover recommend an assessing phase to perceive which first-rate master has incorrectly or maliciously performed out the validness take a look at framework.

***Keywords**: Cloud Computing, Central Authority, Attribute-Based Encryption, Master Key*

1. INTRODUCTION

Cloud stockpiling is a promising and vital administration worldview in cloud figuring. Advantages of utilizing cloud stockpiling incorporate more prominent availability, higher dependability, quick sending and more grounded security, to give some examples [1]. Since cloud stockpiling is worked by cloud specialist co-ops, who are often outside the confided in area of information proprietors, the conventional access control strategies in the Client/Server display are not appropriate in cloud stockpiling condition. The data get the chance to control in cloud amassing condition has thus transformed into a testing issue. To address the issue of data, get the chance to control in cloud amassing, there have been numerous plans proposed, among which Cipher content Policy Attribute Based Encryption (CPABE) is seen as a champion among the most promising systems. A straight forward arrangement to clear the single point bottleneck is to empower distinctive specialists to commonly manage the general characteristic set, with the goal that each one of them can scatter puzzle keys to customers independently [2]. By grasping various pros to share the stack, the effect of the single point bottleneck can be decreased to a degree. Regardless, this game plan will convey risks on security issues. Since there are different essentially unclear masters playing out a comparative technique, it is slippery the careful master if messes up have been made or dangerous practices have been completed amid the time spent puzzle scratch the age and dispersion[5] A straight forward arrangement to empty the single point bottleneck is to empower diverse authorities to together manage the broad property set, so every one of them can flow secret keys to customers self-sufficiently.

By receiving several professionals to percentage, the heap, the effect of the single point bottleneck can be diminished to a selected diploma. Be that as it is able to, this arrangement will supply dangers on safety troubles [three]. when you consider that there are various practically indistinguishable specialists gambling out a similar methodology, it's far elusive the capable expert if botches had been made or vindictive practices were actualized at some stage in the time spent thriller key age and dissemination.

As an example, an expert can also erroneously convey thriller keys past patron's proper assets set. Such frail factor on security makes this straight forward thought difficult to satisfy the security necessity of get right of entry to manage for public cloud stockpiling. Our ongoing work, TMACS, is a side multi professional CPAB get to govern plot for public cloud stockpiling wherein numerous specialists collectively deal with a uniform trait set [1,2]. As a remember of truth, it tends to the single point bottleneck of execution and safety, but, presents a few greater overheads. in this manner, in this paper, we present a practical arrangement which advances effectiveness and strength, in addition to ensures that the brand-new association is as relaxed because the first single professional plans.

The primary contributions of this work may be summarized as follows.

- To deal with the unmarried-point execution bottleneck of key appropriation existed in the contemporary plans, we propose a robust and effective heterogeneous structure with single CA(imperative Authority) and numerous AAs (attribute specialists) for public cloud stockpiling. the overpowering heap of client authenticity affirmation is shared via severa AAs, every one in every of which offers with the all-inclusive belongings set and can freely overall the purchaser authenticity test, even as CA is in charge of computational undertakings. To the pleasant of our insight, that is the primary work that proposes the heterogeneous get right of entry to manage machine to address the low productiveness and single-factor execution bottleneck for cloud stockpiling.
- We reproduce the CP-ABE plan to deal with our proposed gadget and recommend a robust and high-proficient get admission to control conspire, in the period in-between the plan nevertheless jelly the excellent granularity, adaptability and safety highlights of CP-ABE.
- Our plan incorporates an examining gadget that makes a distinction the framework follows an AA's trouble making on client's authenticity confirmation.

2. LITERATURE REVIEWS

There are some varying systems which utilized as a bit of various examining structures. This range present some the systems like CPABE, RAAC and so forth which are utilized for different purposes like information endorsement, information decency in surveying courses of action on cloud.

Ciphertext-Policy Attribute-Based Encryption (CPABE): Even however the definitions and developments of various CPABE plans are not constantly precise, the employments of the entrance structure in Encrypt and Decrypt calculations are almost the equivalent. Here we receive the definition and development from [6, 10]. A CP-ABE plot comprises of four

calculations: Setup, Encrypt, Key Generation (KeyGen), and Decrypt. Setup(λ,U) → (PK,MSK). The setup calculation takes the security parameter λ and the characteristic universe depiction Uas the information. It yields the general population parameters PK and an ace mystery key MSK.

- Encrypt(PK,M,A) → CT. The encryption calculation takes the general population parameters PK, a message M, and an entrance structure An as info. The calculation will encode M and deliver a ciphertext CT with the end goal that just a client whose traits fulfills the entrance structure will be capable todecrypt the message. We will expect that the ciphertext certainly contains A. KeyGen(MSK, S) → SK. The key age calculation takes the ace mystery key MSK and an arrangement of qualities S as information. It yields a mystery key SK.
- Decrypt(PK,CT, SK)→M. The decoding calculation takes general society parameters PK, a ciphertext CT which contains an entrance strategy An, and a mystery key SK as info, where SK isa mystery key for a set S of qualities. In the event that the set S of traits fulfills the entrance structure A, the calculation will unscramble the ciphertext and restore a message M.

Robust and Auditable Access Control (RAAC) (RAAC): In this paper, roused by the heterogeneous design with single CA and different RAs, we propose a powerful and auditable access control plot (named RAAC) for open distributed storage to advance the execution while keeping the adaptability and fine granularity highlights of the current CP-ABE plans. In our plan, we separate the strategy of client authenticity check from the mystery key age and allocate these two sub methods to two various types of experts. There are numerous experts (named characteristic specialists, As), every one of which is responsible for the entire quality set and can direct client authenticity confirmation autonomously. In the meantime, there is just a single worldwide confided in authority (alluded as Central Authority, CA) accountable for mystery key age and circulation. Before playing out a mystery key age and dispersion process, one of the AAs is chosen to check the authenticity of the client's qualities and afterward it creates a middle of the road key to send to CA. CA creates the mystery key for the client based on the got middle of the road key, with no need of any more confirmation. Along these lines, numerous AAs can work in parallel to share the heap of the tedious authenticity check and reserve for one another in order to evacuate the single-point bottleneck on execution. In the interim, the chose AA doesn't assume the liability of producing last mystery keys to clients. Rather, it creates middle of the road keys that connect with clients' properties and verifiably connect with its own personality, and sends them to CA.

Attribute Based Access Control with Efficient Revocation: Cipher content approach property based encryption is a promising cryptographic answer for these issues for authorizing access control strategies characterized by an information proprietor on redistributed information a few difficulties as to the characteristic and client renouncement. Access control instrument utilizing figure content approach credit-based encryption to implement get to control strategies with proficient quality and client repudiation ability. The fine-grained get to control can be accomplished by double encryption component which exploits the property-based encryption and particular gathering key appropriation in each characteristic gathering

PRSE (Personalized multi-keyword Ranked Search over Encrypted data) Framework: In Cloud figuring accessible encryption is a testing undertaking. Nonetheless, most of the current works pursue the model of "one size fits all" and disregard customized look over outs sourced scrambled information. So PRSE structure takes care of the issue of customized multikey word positioned seek over encoded information by protecting security of the framework in distributed computing. This system assembles client intrigue display for each client with the assistance of semantic cosmology Word Net by investigation client's hunt history and by embracing a scoring component to express client premium adroitly.

Mehdi Sookhaka et al (2017): This paper gives an exhaustive study on trait-based access control plans and looks at each plan's usefulness and trademark. We likewise present a topical scientific classification of trait constructed approaches based with respect to critical parameters, for example, get to control mode, design, repudiation mode, renouncement strategy, denial issue, and disavowal controller. The paper audits the best in class ABE techniques and arranges them into three principle classes, for example, centralized, decentralized, and hierarchal, in light of their designs.

3. GENERAL DISCUSSION OF THE REVIEW WORK

Recently, we considered the single-point execution bottleneck of CP-ABE based plans and formulated a limit multi-authority CP-ABE get to control plot in another work [1]. Unique in relation to other multi-authority plans, in [1], numerous experts together deal with a uniform property set. Exploiting (t, n) edge mystery sharing, the ace mystery key can be shared among various specialists, and a legitimate client can create his/her mystery key by connecting with any t experts. This plan tended to the single-point bottleneck on both security and execution in CP-ABE based access control out in the open distributed storage. However, it is not efficient, because a user must interact with at least t authorities, and thus introduces higher interaction overhead.

The system model of our design is shown in Fig. 1, which involves five entities: a central authority (CA), multiple attribute authorities (AAs), many data owners (Owners), many data consumers (Users), and a cloud service provider with multiple cloud servers (here, we mention it as cloud server.).

- **The central authority (CA)** is the head of the whole framework. It is in charge of the framework development by setting up the framework parameters and producing public key for each attribute of the widespread attribute set. In the framework instatement stage, it allocates every client a one of a kind Uid and each attribute authority an extraordinary Aid. For a key demand from a client, CA oversees producing mystery keys for the client in light of the got middle of the road key related with the client's real attributes checked by an AA. As a director of the whole framework, CA can follow which AA has mistakenly or malignantly checked a client and has allowed ill-conceived attribute sets.

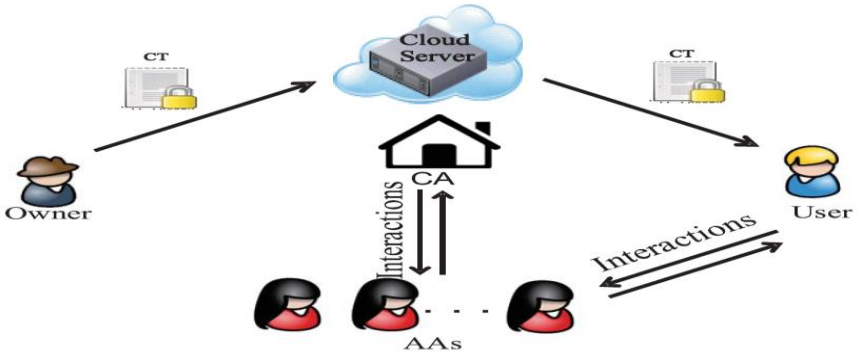


Fig. 1. System model [1].

- **The attribute authorities (AAs)** oversee performing client authenticity check and producing middle of the road keys for authenticity confirmed clients. Not at all like a large portion of the current multi-authority plans where every AA deal with a disjoint attribute set individually, our proposed plot includes different authorities to share the obligation of client authenticity check and every AA can play out this procedure for any client autonomously. At the point when an AA is chosen, it will check the clients' genuine attributes by physical work or validation conventions and produce a middle of the road key related with the attributes that it has authenticity confirmed. Middle of the road key is another idea to help CA to create keys.
- **The data (Owner)** characterizes the entrance arrangement about who can gain admittance to each record and encodes the document under the characterized approach. Above all else, every owner scrambles his/her data with a symmetric encryption calculation. At that point, the owner details get to arrangement over an

attribute set and scrambles the symmetric key under the strategy as indicated by public keys got from CA. From that point forward, the owner sends the entire scrambled data and the encoded symmetric key (meant as ciphertext CT) to the cloud server to be put away in the cloud.

- **The data consumer (User)** is allocated a worldwide client character Uid by CA. The client has an arrangement of attributes and is furnished with a mystery key related with his/her attribute set. The client can uninhibitedly get any intrigued scrambled data from the cloud server. Be that as it may, the client can decode the encoded data if and just if his/her attribute set fulfills the entrance arrangement inserted in the scrambled data.
- **The cloud server** provides a public platform for owners to store and share their encrypted data. The cloud server doesn't conduct data access control for owners. The encrypted data stored in the cloud server can be downloaded freely by any user.

4. PROBLEM DEFINITION

Data integrity is one of the essential troubles, as there's lack of identity privacy due to relinquish tendencies in cloud, in which the users are unacquainted with the auditor of the statistics, over geographically scattered data centers. this feature of cloud computing evolved various worries related to consumer's identity, statistics integrity and consumer's availability. ultimately this affect to advocate an stronger version on the way to audit the records integrity and preserving the identification of privacy with green person revocation even as sharing.

5. PROPOSED SYSTEM

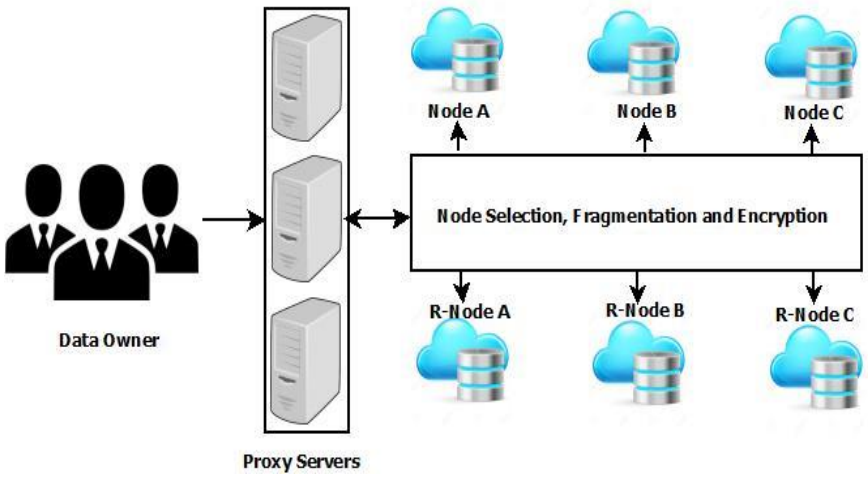


Fig. 2. System Architecture

In the proposed system, instead of transmitting the fragments of the file as it is, encryption technique is applied. Hence very high security is provided here. First user registration is

done. The file which user wants to replicate is fragmented into multiple parts. Key generation is done which we are going to apply on the fragments. By using key, these fragments are encrypted, and fragments are replicated to multiple nodes. For getting the original data, all the fragments are decrypted and merged.

6. MATHEMATICAL MODEL

A. Problem Design Using Set Theory

1. Let S= { } be as a secure Cloud System.
2. Obtain a set of shared keys' of Data Owner who upload file is ShK
   ShK1={ uid,dob,rP} ShK={ShK1,ShK2,ShK3}
   Where uid, dob are the Data Owner attributes &rP randomly choose odd big integer
   S={ShK }
3. Give input files upload to Cloud F F= {f1, f2,.....,fn}
   FR1,FR2, FR3
4. Decrypt(FR1, C)
5. Repeat step 3 for all fragments Merge all fragments Homomorphic
   Operations:
   Where f1is a plain text file
   S={ShK, F }
6. Create fragments of input file fX FR= {fR1, fR2, fR3}
   Where fXis a plain text file, FRis set of fragments S={ShK, F ,FR}
7. Perform encryption process on set of plain text fragments of afilefXis a En
   En= { FR, ShK}
   Where En process take input as set fragments of file and data owners shared key
   S={ShK, En ,FR}
8. Obtain a node_idto load file fragment of file uploaded by Data Consumer
   Nid= {FR, EXL}
   Where Nidnode id where fragment is loaded&EXLcurrent load of Nid
   S={ShK, En ,FR, Nid }
9. Obtain a replica_id to load file fragment of file uploaded by Data Consumer
   Rid = { FR, EXL }
   Where Ridnode id where fragment is replicated&EXLcurrent load of Rid
   S={ShK, En ,FR, Nid, Rid}
10. File accessor decryption process on set of cipher text fragments of a requestedfile

11. Dn= { ShK,FR, Nid}

    Where Dn process take input as set of fragments of file,data owners shared key and data node_idS={ShK, En ,FR, Nid, Rid,Dn }

12. Merge fragments Mrg Mrg = { fR1, fR2, fR3 }

    Where Mrg process take input as set of fragments of file and create single file S={ShK, En ,FR, Nid, Rid,Dn,Mrg }

13. Final Set

    S={ShK, En ,FR, Nid, Rid,Dn,Mrg }

B. Mathematical Model

KeyGen(p): The key is a random P-bit odd integer p.

Encrypt (p, m): To encrypt a bit m{0,1} , output the plain text c = m + p + r * p * q, where r is a random Rbitnumber and q is a contain Q-bit big integer.

Decrypt (p, c): Output (c mod p).

To decrypt bit m {0, 1}, output thecipher text c = m - p - r * p * q, where r is a random Rbitnumber and q is a contain Q-bit big integer.

Retrieval(c):

Take input file_id Fid,

Find locations of fragments of Fid which are FR1

Suppose there are two plaintext m1 and m2 under encryption. After encryption, the cipher text turns out to be c1 and c2 respectively.

c1 = m1 + p + r1 * p * q,

c2 = m2 + p + r2 * p * q…… (3)

Firstly, checking the additively homomorphic property of the proposed SDC scheme. Then

c3=c1 + c2= (m1 + m2) + (r1 + r2) * p * q + 2p.

…….(4)

And

m3 = c3 mod p = m1 + 2……(5)

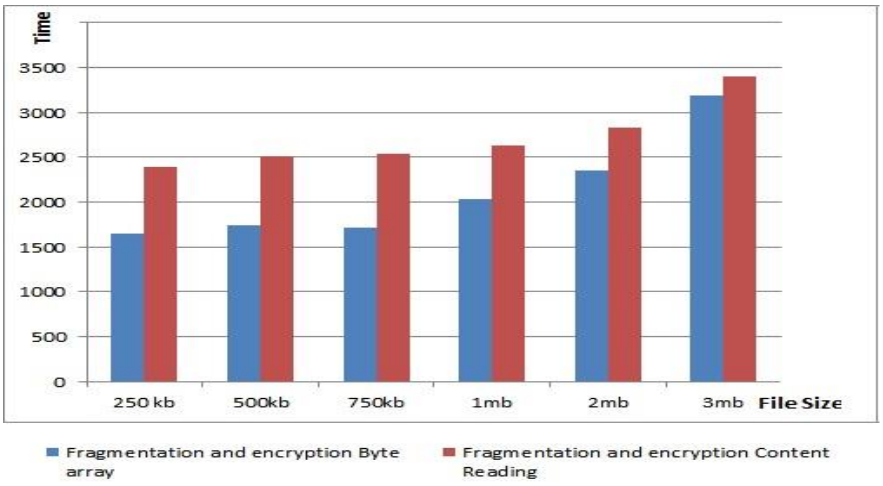
7. DATASET AND EXPECTED OUTCOMES

As over public cloud person uploads its non-public information inside the form of files and these documents having extraordinary formats like txt, document, pdf or it could incorporate pix, audio or video. earlier than data load to cloud garage it encrypted using real time encryption method. information tactics by means of gadget is a user input report and person authentication token retrieved at authentication method by way of server. File content

fragmentation is compared with byte array fragmentation with respect to file size where byte array fragmentation time is less than that of other.

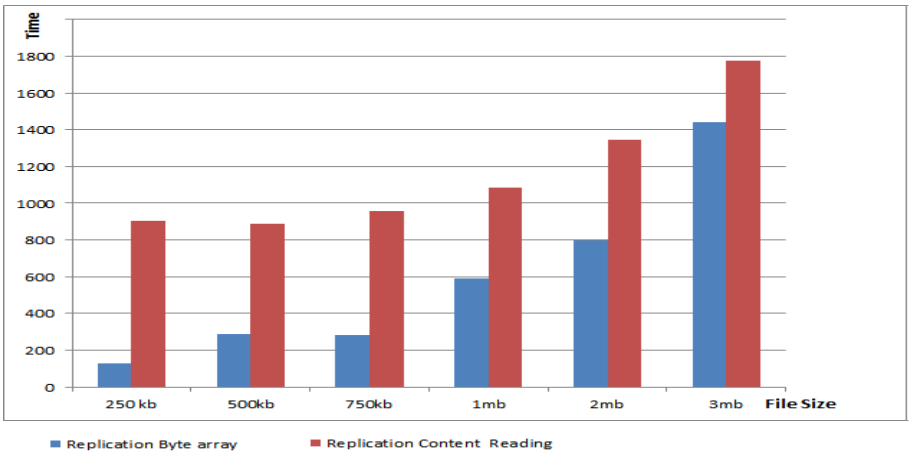
File size	Byte array		Content reading	
	Fragmentation and encryption time(milliseconds)	Replication time(milliseconds)	Fragmentation and encryption time(milliseconds)	Replication time(milliseconds)
250 kb	1645.7471	126.5909	2391.9457	903.8963
500kb	1713.6838	280.0631	2516.9615	885.7568
750kb	1746.1070	287.0199	2536.3845	956.5988
1mb	2033.7212	590.3808	2626.6444	1083.2420
2mb	2347.6645	799.8776	2832.9673	1343.9213
3mb	3190.6101	1439.1851	3398.3227	1774.8506

Table .1 Result analysis



Graph 1 Comparison of fragmentation and encryption time of byte array and file content

Above graph.1. shows the Comparison between fragmentation and encryption time of byte array and file content. Here fragmentation and encryption time of byte array is less than file content reading.



Graph 2 Comparison of replication time of byte array and file content

Above graph 2 shows the Comparison between replication time of byte array and file content. Here replication time of byte array is less than file content reading. Hence converting file content into byte array is beneficial.

8. CONCLUSION & FUTURE SCOPE

The statistics which consumer desires to add on the cloud. This information is first fragmented into distinct components. This record is available in byte array layout. On those fragments' encryption strategies are implemented to encrypt the data. After encryption the statistics get stored at the nodes and the replicated copy of that facts get replicated at the respective replication node. The records from that node may be brought in case of node failure. on every occasion original information is needed, the decryption of these fragments takes region and after merging all the decrypted fragments the authentic information may be derived.

Consequently, via encryption greater quantity of protection is supplied. as opposed to storing the fragments on sequential nodes, the records are saved on the random nodes in addition to encryption techniques are implemented so the higher security is supplied. right here fragmentation and encryption time for byte array is less than that of the content material array. additionally, replication time for byte array is much less than that of content material reading.

REFERENCES

[1] *Boyang Wang, IEEE, Baochun Li and Hui Li, "Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud", IEEE transactions on services computing, vol. 8, no. 1, january/february 2015*

[2] *C. Wang, Q. Wang, K. Ren, and W. Lou, "Towards Secure and Dependable Storage Services in Cloud Computing," IEEE Transactions on Services Computing, vol. 5, no. 2, pp. 220-232, 2011.*

[3] *Y. Zhu, G.-J. Ahn, H. Hu, S. S. Yau, H. G. An, and S. Chen, "Dynamic Audit Services for Outsourced Storage in Clouds," IEEE Transactions on Services Computing.*

[4] *S. Marium, Q. Nazir, A. Ahmed, S. Ahthasham and Aamir M. Mirza, "Implementation of EAP with RSA for Enhancing The Security of Cloud Computig", International Journal of Basic and Applied Science, vol 1, no. 3, pp. 177-183, 2012*

[5] *Balkrishnan. S, Saranya. G, Shobana. S and Karthikeyan.S, "Introducing Effective Third Party Auditing (TPA) for Data Storage Security in Cloud", International Journal of computer science and Technology, vol. 2, no. 2, ISSN 2229-4333 (Print) — ISSN: 0976- 8491(Online), June 2012.*

[6] *K. Kiran Kumar, K. Padmaja, P. Radha Krishna, "Automatic Protocol Blocker for Privacy-Preserving Public Auditing in Cloud Computing", International Journal of Com- puter science and Technology, vol. 3 pp, ISSN. 0976-8491(Online), pp. 936-940, ISSN: 2229-4333 (Print), March 2012.*

[7] *Jachak K. B., Korde S. K., Ghorpade P. P. and Gagare G. J.,"Homomorphic Authentication with Random Masking Technique Ensuring Privacy & Security in Cloud Computing",*

[8] *Bioinfo Security Informatics, vol. 2, no. 2, pp. 49-52, ISSN. 2249-9423, 12 April 2012.*

[9] *C. Wang, Q. Wang, K. Ren, and W. Lou, Towards Secure and Dependable Storage Services in Cloud Computing, IEEE Transactions on Services Computing, vol. 5, no. 2, pp. 220232, 2011.*

[10] *Y. Zhu, G.-J. Ahn, H. Hu, S. S. Yau, H. G. An, and S. Chen, Dynamic Audit Services for Outsourced Storage in Clouds, IEEE Transactions on Services Computing, accepted.*

[11] S. Marium, Q. Nazir, A. Ahmed, S. Ahthasham and Aamir M. Mirza, Implementation of EAP with RSA for Enhancing The Security of Cloud Computig, International Journal of Basic and Applied Science, vol 1, no. 3, pp. 177-183, 2012

[12] K. Kiran Kumar, K. Padmaja, P. Radha Krishna, Automatic Protocol Blocker for Privacy- Preserving Public Auditing in Cloud Computing, International Journal of Computer science and Technology, vol. 3 pp, ISSN. 0976-8491(Online), pp. 936-940, ISSN: 2229- 4333 (Print), March 2012

[13] J. Yuan and S. Yu, Proofs of Retrievability with Public Verifiability and Constant Communication Cost in Cloud, in Proceedings of ACM ASIACCS-SCC13, 2013