ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Protection and Systematic Serving in Public Data Investigate In Poverty Cloud Computing

Gundabattula Saikumar
M.Tech Student
Sri Vatsavayi Krishnam Raju College of Engineering & Technology
Bhimavaram, AP.

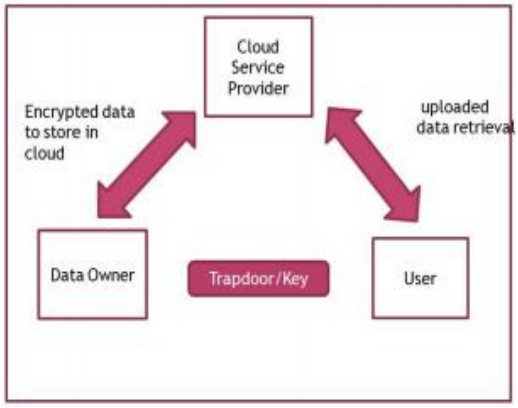
Dr.Penmetsa Vamsi Krishna Raja, M.Tech
Principal
Sri Vatsavayi Krishnam Raju College of Engineering & Technology
Bhimavaram, AP.

Abstract:
Users in a particular group need to compute signatures on the blocks in shared data so that the shared data integrity can be confirmed publicly Various blocks in shared data are usually Enabling complete user control over his data, anonym sing security the sensitive data in outsourcing, finding the data owner take data access the serve take helping in the progress of strengthening the security and efficient model in Cloud Computing number of models is Homomorphism Authenticable Ring Signature (HARS) security and efficient public auditing System for data storage security is discussed Public key cryptosystem the MD5 Message-Digest Algorithm is depicted. Proof Irretrievability Markel Hash Tree (MHT) for the block tag security message is discussed the semi trusted cloud can resign the blocks that were previously signed by the revoked user with the valid proxy re-signatures, when a user in the group is revoked.

Index Terms: ***Public auditing, privacy-preserving, shared data, Digital Signature, DPDP, PDP, Cloud Computing.***

1. INTRODUCTION

Cloud computing is the useful techniques in the a network of remote manage and process data number of times a local server is a personal computer The security preserving supports the public[1] auditing without the retrieval access of entire data blocks. The security preserving public auditing is used to integrate the homomorphism authenticated with random masking technique proof-of-irretrievability system is used for public verifiability Preserving the privacy of user, his identity and data in the cloud is very mandatory. With the rise in growth of cloud computing, the concerns about privacy preserving are also getting increased [11, 14]. But reaching the peak in providing and assuring privacy-preserved data access in cloud is yet in progress and still needs much attention to attain the goal. The tied in issues of privacy which acts as the barrier are listed in Table 1. Addressing all these issues and designing a system which could not be compromised by the intruders or attackers would mark the success of Cloud Computing [2]



ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

In the model data is divided into number of small blocks each block is independently signed the owner and a random communications of all the blocks instead in the total data is access in the integrity checking A public user could be a data user who would like to utilize the owners data via the cloud or a third-party auditor (TPA) is provide expert integrity checking services.[3] Existing public auditing model is actually be extended to verify distubuted data integrity and data freshness , a new significant security model introduced in the case of shared data with the use of backend model is the leakage of identity security to public verifiers To protect the confidential data is essential and critical top reserve identity security from public verifiers during public auditing [4]

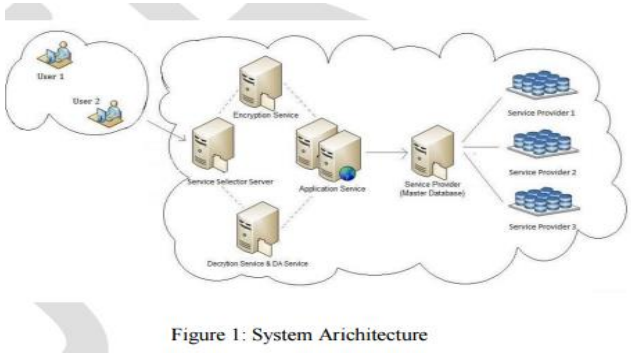
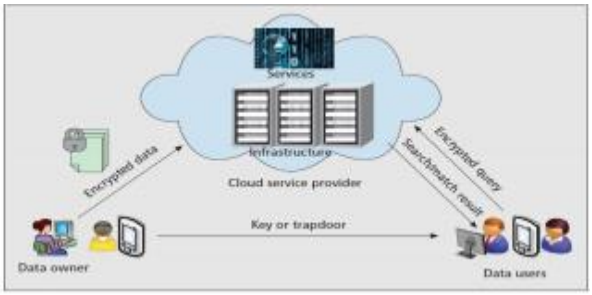


Figure 1: System Arichitecture

2. RELATED WORK:

M. Bellare stated that different signature models enables a group of signers to produce a compact joint signature on a common document, and has many potential uses[7]. Privies model is impose key setup requirements that make them impractical, such as take a dedicated, distributed key generation protocol number of potential signers different strong concurrent zero knowledge id of knowledge of secret keys done to the CA at key registration number of requestments s limit the use of the schemes We provide a new models is proven secure in the plain public-key model[5]meaning requires different each signer has a public key. Furthermore the important simplification in key management achieved is not at the cost of efficiency our scheme matches Lemma that may independent [6] interest's C.Merkle stated that new Cryptographic protocols which take full advantage of the unique properties of public key cryptosystems evolving. Different protocols for public key sharing [8]



3. EXISTING SYSTEM:

Using the cryptographic techniques for ensuring data security care should be taken for storing encryption and decryption keys. Rigorous methods should be adopted to prevent insiders and privileged user from gaining access to the encrypted data and decryption key simultaneously. Thus, the importance of SLAs is recognized in this context. The policies responsible for user data protection must be clearly mentioned in the provider's contract[9]. After reviewing the data security requirements following recommendations have been included in multiparty SLA suggested at the end to ensure data security in cloud:

1. Encrypted data and decryption key must not be stored at the same place
2. Access control techniques should be applicable for malicious insiders and privileged users
3. Independent audits must be conducted to access the effectiveness of techniques employed for data storage
4. Service providers must abide the ethics and legal laws and should be responsible for discrepancies if any
5. Backup and reset methods against system crash and failures[10]

1. Ring Signatures:

The concept of ring signatures is first proposed by Rivest et al. in 2001 With ring signatures, a verifier is convinced that a signature is computed using one of group members private keys, but the verifier is not able to determine which one. This property can be used to preserve the identity of the signer from a verifier [13]

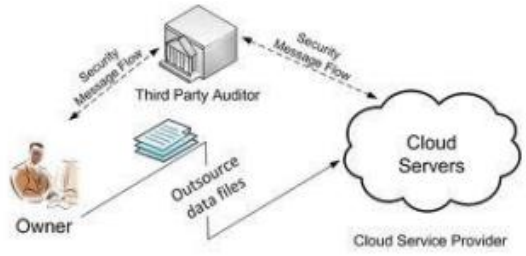
ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

2. Integrity Threats:

Two kinds of threats related to the integrity of shared data are possible an adversary may try to corrupt the integrity of shared data and prevent users from using data correctly the cloud service provider may inadvertently corrupt data in its storage due to hardware failures and human errors [11]

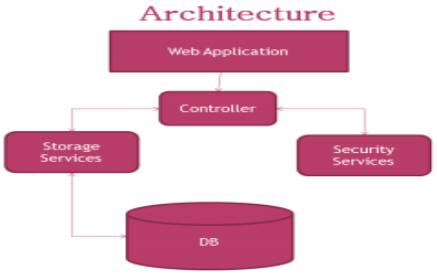
3. Privacy Threats:

The identity of the signer on each block in shared data is private and confidential to the group. During the process of auditing, a semi trusted TPA try to reveal the identity of the signer on each block in shared data based on verification information once the TPA reveals the identity of the signer on each block. [12]



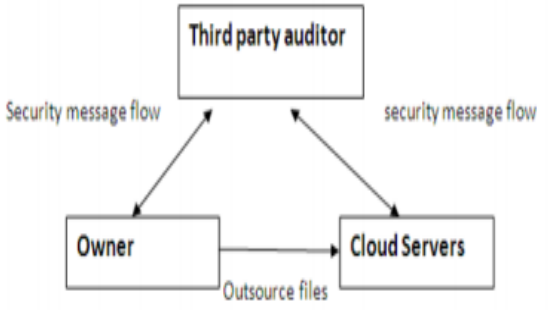
4. Proposed System

The cloud computing explained in hardware point of view and software point of view.The advantages of SAAS in cloud is also explained The authors listed the various Conditions that influence the organizations to become the cloud computing providers. The location for the data centers need to be selected properly in order to reduce the electricity cost. Many new types of applications have been developed[13] with the help of cloud computing. The obstacles and opportunities for the cloud computing is been explained. The bottle necks are used in cloud. The software like application software, hardware systems are been explained [2]



A.HOMOMORPHIC AUTHENTICATORS IN CLOUD PRIVACY

The first privacy preserving public auditing mechanism to audit the shared data in cloud Ring signature are been Used to construct the homomorphism authenticators. The Third Party Auditor (TPA) can audit but do not know the user on each block. Batch auditing can be used to audit multiple task The Ring Signature used in the construction of ORUTA will increase the size of storage space Homomorphism Authenticable Ring Signature (HARS) a novel idea is used in this paper. The HARS is been extended from the classic ring signature scheme [1] The new paradigm for cloud computing. Data protection as a service is the paradigm designed in this paper. The authors also used two different approaches to data privacy they are full-disk encryption and computation on encrypted data. In the full-disk encryption (FDE) the entire physical disks are encrypted for the simplicity and speed. The fully homomorphism encryption (FHE) is used for computation on cipher texts [14] They proposed this scheme as setup phase and audit phase. The public auditing scheme has four algorithms they are KeyGen, SigGen, GenProof, VerifyProof. The privacy preserving public auditing supports for batch auditing. Third Party Auditor (TPA) can handle multiple auditing delegations between different users request. But the individual auditing is very difficult in TPA. So the author deals that we can use TPA to perform the multiple auditing tasks in a batch process concurrently. The auditing system in the cloud server is been illustrated in fig 1.The block of message is sent to the auditor for checking integrity [4]

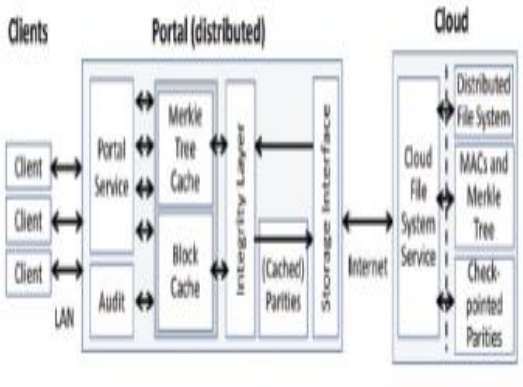


ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The scheme proof-of irretrievability system The author used BLS signatures and secure in the random oracle model to build the first scheme. This scheme is used to let on public verifiability. [15] The second scheme frames on the pseudo random functions (PRFs), this is used only for private verification. The proof-of-storage scheme is used to boost the response length of the simple MAC-based scheme using homomorphism authenticators. In this paper the author built two contributions. The first one is on the PRFs. The second one is based on the BLS signatures. In the first scheme the user breaks the erasure encoded file. In the second scheme it is publicly verifiable. This uses BLS signatures to authenticate values that can be publicly verifiable [16]

B.THE MD5 ALGORITHM AND LT CODES

The MD5 Message-Digest Algorithm describes that algorithm takes the input as message of arbitrary length and produces output as 128-bit "finger print" or "message digest" of the given input. This algorithm can be used for digital signature applications. So that large type of files can be "compressed" in a secure way before the encryption can be made with private key under the public key cryptosystem for example RSA[17]. There are five steps to compute the message digest of the message. The message is extended so that the bit length is congruent to 448, modulo 512. A 64-bit representation is made with B and the result is added with the previous step. The algorithm consists of four word buffer to compute the message digest. The four auxiliary functions need to be defined first. It takes input as three 32-bit words and produce output as one 32-bit word. The message digest produce output as A,B,C,D. Starts with low-order byte A and end with high-order of byte D [7]. The designed LT codes based cloud storage service (LTCS). The author has examined the problem of secure and reliable cloud storage. The author has used low complexity LT codes to empower efficient decoding for data users in the data retrieval process. The fast belief propagation decoding algorithm is been used for the adequate data retrieval. The LTCS has less storage cost and faster data retrieval than network coding-based storage services. The future work of this paper is to detect the decidability. The LT codes generate vast number of encoded packets by performing bitwise XOR algorithm on a subset of original packets [13]



C. Privacy Preserving Methods

Several methods have been put forward to tackle this issue of privacy preserving. This work studies some of those approaches and provides a brief overview. It is important [18] This layer has an associated Unique User Cloud Identity Generator. Hence, this layer preserves the privacy of users' sensitive information by implementing the Privacy check mechanism. This mechanism enables the user to specify the access control and the amount of data transparency in the cloud. If a particular Personal Data Attribute (PDA) of a user has to be specified with the transparency level, then a Boolean function of the attribute is to be carried out, which is named as Transparency Purpose in Cloud (TPC). Thus, PccP forecloses both the access of user identification and data content [19]

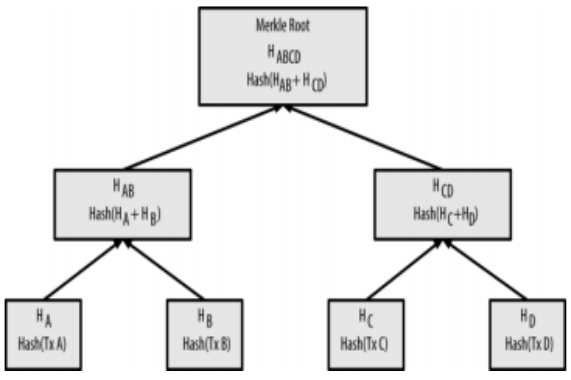
D. Dynamic Metadata Reconstruction

Adela Wear [7] focused on the possibility of metadata exploitation in the cloud. By gaining knowledge of the metadata, the attacker could compromise users' privacy. As a solution, a framework is proposed to preserve the data privacy. First, the metadata that has to be put in cloud's database are segregated. The segregated attributes are then grouped as exclusively private, partially private and no private depending on the sensitivity of data. Following this data

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

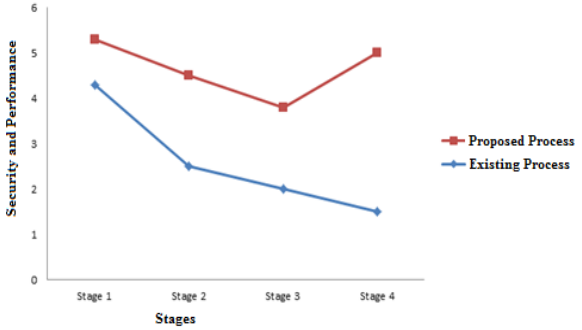
classification, the next phase called table splitting comes up, where the database tables are divided both horizontally and vertically. The splitting of the database table ensures the database normalization. Next is to perform metadata reconstruction as and when required by the cloud [20] This phase is called ephemeral referential consonance. This phase guarantees that data is not leaked from the cloud database both before and after splitting. These steps are illustrated by considering the possible attacks on metadata kept in Eucalyptus database files and ensuring the prevention of attacks by the proposed framework. Thus, the method proves to be efficient

The DPDP scheme is very much useful in distributed applications [9] The classic Merkle Hash Tree (MHT) construction for the block tag authentication This scheme provides wide range of security and the performance analysis. The bilinear map is a map e it is commutable, bilinear and non degenerate The MHT is a authentication structure that is used to prove that the set of elements are unimpaired and unchanged. The author have used BLS signature as a support. The direct addition of PDP or POR schemes to pillar data dynamics have security problems The experiments display that the scheme is capable in aiding data dynamics with provable verification. The Merkle Hash Tree is been illustrated. Leaves are hashes of the data blocks. Nodes are hashes of their children [10]



5. RESULTS:

In results we will be showing how there will be significant difference between the methods that are previously and also the improved method.[21]



Graph showing the existing and proposed

In the above graph we will be observing there is a significant difference between both the methods and we can clearly understand which can yield more result when methods are compared. Proposed approach will be giving more security as well as performance in the system. And we also observe that our native approach[22] will be giving less security. There will be number of stages that will showing the whole process we will be showing all the process in just 4 stages as by that we can observe the difference.

6. CONCLUSION

The security aspect in cloud is major concern thus we have proposed novel system which can process the request in grouping or batch manner which can enhance performance and efficiency of data transfer/system The algorithm clearly shows improvements to its predecessor in various fashions like security, transfer of data, scalability and Privacy preserving is discussed in this paper. This paper deals with certificate less public auditing mechanisms for confirming the data integrity in the cloud. Remote Data Checking (RDC) an avoidance Tool is discussed in detail. Public key cryptosystem the MD5 Message-Digest Algorithm are discussed LT codes based cloud storage service (LTCS) are studied in detail. Certificate less public auditing mechanisms are depicter some approaches utilized traditional cryptographic methods to achieve privacy, some other approaches kept them away and focused on alternate methodologies in achieving privacy. Also, approaches to preserve privacy at the time of public auditing are

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

also discussed. Thus, to conclude it is necessary that every cloud user must be guaranteed that his data is stored, processed, accessed and audited in a secured manner at any time

7. Further Work:

The user must be given complete access control over the published data. Also, powerful security mechanisms must always supplement every cloud application. Attaining all these would end up in achieving the long dreamt vision of secured Cloud Computing in the nearest future In this paper author has extend their result to implement TPA to perform audits for several end users concurrently. By using this technique the performance and security both are very efficient

8. REFERENCES

[1] 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.

[2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song," Provable Data Possession at Untrusted Stores, in Proc. ACM Conference on Computer and Communications Security (CCS)", 2007, pp. 598610.

[3] C.Wang, Q.Wang, K. Ren, andW. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing, in Proc. IEEE International Conference on Computer Communications (INFOCOM)", 2010, pp.525533.

[4] R. L. Rivest, A. Shamir, and Y. Tauman,"How to Leak a Secret, in Proc. International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT)". SpringerVerlag, 2001, pp. 552565.

[5] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps, in Proc. International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)". Springer-Verlag, 2003, pp. 416432.

[6] H. Shacham and B. Waters, "Compact Proofs of Retrievability,in Proc. International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT)". SpringerVerlag, 2008, pp. 90107.

[7] 7. M. Blaze, G. Bleumer, and M. Strauss, "Divertible Protocolsand Atomic Proxy Cryptography, inthe Proceedings of EUROCRYPT 98".Springer-Verlag, 1998, pp. 127144.

[8] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S.Yau, "Dynamic Audit Services for Integrity Verification of Outsourced Storage in Clouds, in Proc. ACM Symposium on Applied Computing (SAC)", 2011, pp.15501557

[9] Wang C, Chow S S M et al. (2013). Privacy-Preserving Public Auditing for Secure Cloud Storage, IEEE Transactions on Computers, vol 62(2), 362–375.

[10]. Wang B, Li B et al. (2012). Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud, IEEE Fifth International Conference on Cloud Computing, 295–302.

[11]. Gellman R (2009). WPF REPORT: Privacy in the clouds: Risks to privacy and confidentiality from cloud computing.

[12]. Rong C, Nguyen S T et al. (2013). Beyond lightning: A survey on security challenges in cloud computing , Computers & Electrical Engineering, vol 39(1), 47–54.

[13]. Takabi H (2010). Security and Privacy Challenges in Cloud Computing Environments, IEEE Security & Privacy, vol 8(6), 24–31.

[14]. Xiao Z, and Xiao Y. Security and Privacy in Cloud Computing, IEEE Communications Surveys & Tutorials, vol PP(99), 1–17.

[15] 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.

[16] 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.

[17] D. Song, E. Shi, I. Fischer, and U. Shankar, "Cloud Data Protection for the Masses,"Computer, vol. 45, no. 1, pp. 39-45, 2012.

[18] 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.

[19] B. Wang, M. Li, S.S. Chow, and H. Li, "Computing EncryptedCloud Data Efficiently under Multiple Keys,"Proc. IEEE Conf. Comm. and Network Security (CNS '13), pp. 90-99, 2013.

[20] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems,"Comm. ACM,vol. 21, no. 2, pp. 120-126, 1978.

[21] The MD5 Message-Digest Algorithm (RFC1321). https://tools.ietf.org/html/rfc1321, 2014.

[22] H. Shacham and B. Waters, "Compact Proofs of Retrievability,"Proc. 14th Int'l Conf. Theory and Application of Cryptology and Infor

Author Details

Gundabattula Saikumar is one of the author received B.Tech (CSE) Degree from JNTU Kakinada in 2013. He is studying M.Tech in Sri Vatsavayi Krishnam Raju College of Engineering & Technology, Bhimavaram, AP.

Dr.Penmetsa Vamsi Raja, He did his PhD from JNTU Kakinada AP. He received M.Tech Post Graduation degree in C.S.T department from Andhra University, Visakhapatnam, A.P. He is presently working as Principal in Sri Vatsavayi Krishnam Raju College of Engineering & Technology Bhimavaram AP. He has authored more than 20 relevant publications in journals and Conferences. His Research areas include Computer Networks, Network Security, Cloud Computing, Big Data, Data Mining and Software Engineering.