ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

A Survey on Public Auditing for Shared Data with Efficient User Revocation in the Cloud

Prof. Autade P.P[1], Prof.Gaikar M.R[2], Prof.Khairnar N.K.

Assistant Professor, Dept. of E&TC., Savitribai Phule Pune University, Maharashtra, India[1]

Assistant Professor, Dept. of E&TC., Savitribai Phule Pune University, Maharashtra, India[2]

Assistant Professor, Dept. of Civil Engineering, Savitribai Phule Pune University, Maharashtra, India[3]

ABSTRACT: Distributed computing has as of late developed as another worldview for facilitating and conveying administrations over the Internet. Distributed computing is appealing to entrepreneurs as it kills the prerequisite for clients to arrange ahead for provisioning, and permits undertakings to begin from the little and expansion assets just when there is an ascent in administration request. In any case, regardless of the way that distributed computing offers immense chances to the IT business, the improvement of distributed computing innovation is at present at its early stages, with numerous issues still to be tended to. With information stockpiling and sharing administrations in the cloud, clients can undoubtedly adjust and share information as a gathering. To guarantee shared information respectability can be checked freely, clients in the gathering need to register marks on every one of the pieces in shared information. Diverse squares in shared information are for the most part marked by various clients because of information changes performed by various clients. For security reasons, once a client is disavowed from the gathering, the squares which were already marked by this denied client must be re-marked by a current client. The straight forward system, which permits a current client to download the comparing a portion of shared information and re-sign it amid client disavowal, is wasteful because of the extensive size of shared information in the cloud. In this paper, we propose a novel open examining system for the uprightness of imparted information to proficient client renouncement personality a top priority. What's more, an open verifier is constantly ready to review the uprightness of shared information without recovering the whole information from the cloud, regardless of the possibility that some piece of shared information has been re-marked by the cloud.

KEYWORDS: Cloud computing, access control, dynamic Groups, and data sharing, Group signatures, revocation of group membership credentials, Cloud service providers, proxy re-signatures, and public verifier, resign blocks, and user revocation.

I. INTRODUCTION

Distributed computing is principally utilized for asset offering and to low-upkeep. The cloud administration suppliers (CSPs, for example, Amazon, can give a different administrations to cloud clients with the assistance of effective different server farms. Cloud Providers gives a major administration is information stockpiling (Storage as-an administration). An association permits its gathering individuals in the same gathering or office to store and share records in the cloud. By using the cloud, the gathering individuals can be totally discharged from its nearby information stockpiling and upkeep. A huge danger emerges in classification of those put away records. In this way, the clients are not completely believed the cloud servers worked by cloud supplier while delicate information put away in the cloud. In this paper, a novel open evaluating system for the trustworthiness of imparted information to proficient client disavowal in the cloud. Once a client in the gathering is renounced, the cloud can leave the pieces, which were marked by the repudiated client, with a re-marking key. Thus, the productivity of client disavowal can be altogether enhanced, and calculation and correspondence assets of existing clients can be effortlessly spared. Then, the cloud, which is not in the same trusted area with every client, is just ready to change over a mark of the denied client into a

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

mark of a current client on the same square, yet it can't sign self-assertive pieces in the interest of either the repudiated client or a current client.

To secure the respectability of information in the cloud, various components have been proposed [5][6] In these systems, a mark is connected to every square in information, and the uprightness of information depends on the accuracy of the considerable number of marks. [7] One of the most critical and normal components of these systems is to permit an open verifier to productively check information honesty in the cloud without downloading the whole information, alluded to as open examining this open verifier could be a customer who might want to use cloud information for specific purposes (e.g., look, calculation, information mining, and so on.) or an outsider inspector (TPA) [3] [8] why should capable give confirmation administrations on information trustworthiness to clients. The greater part of the past works concentrate on inspecting the trustworthiness of individual information. Not quite the same as these works, a few late works, [9] [10] concentrate on the most proficient method to save character security from open verifiers while inspecting the uprightness of shared information.

Sadly, nothing unless there are other options systems considers the effectiveness of client denial while examining the accuracy of shared information in the cloud. With shared information, once a client adjusts a piece, client additionally needs to figure another mark for the changed square. Because of the alterations from various clients, diverse pieces are marked by various clients. For security reasons, when a client leaves the gathering or gets out of hand, this client must be denied from the gathering. Thus, this denied client ought to never again have the capacity to get to and alter shared information, and the marks produced by this renounced client are no more legitimate to the gathering [10]. Hence, despite the fact that the substance of shared information is not changed amid client renouncement, the pieces, which were beforehand marked by the denied client, still should be re-marked by a current client in the gathering [11]. Subsequently, the respectability of the whole information can even now checked with general society keys of existing clients just. Such advancements are shaded and not all that centered.

II. RELATED WORK

[A] Techniques used in Public Auditing on Cloud There are some different techniques which used in different auditing mechanisms. This section introduce some the techniques like MAC, HLA etc. which are used for different purposes like data authentication, data integrity in auditing schemes on cloud.

1. MAC Based Solution

This technique used for data authentication. In this mechanism user upload data blocks with MAC and Cloud provider provides Secret key SK to TPA. Here TPA's task is to retrieve data blocks randomly and MAC uses SK to check correctness of data. Limitations of this technique are:

- Online burden to users due to limited use (i.e. Bounded usage) and stateful verification.
- Complexity in communication and computation
- Maintaining and updating TPA states is difficult.
- User need to download all the data to recomputed MAC and republish it on CS
- This technique only supports for static data.

2. HLA Based Solution

This method performs inspecting without recovering information piece. HLA is only remarkable check meta information that verify. It checks trustworthiness of information square by confirming it in straight mix of the individual pieces. This strategy permits proficient information evaluating and expending just consistent transfer speed, however its tedious as it uses straight blend for validation.

3. Using Virtual Machine

Abhishek Mohta proposed Virtual machines idea which use in the event of Software as a Service (SaaS) model of the distributed computing. In this instrument as appeared in Fig when client demand CSP for administration CSP verify the customer and give a virtual machine by method for Software as an administration. Virtual Machine (VM) utilizes RSA calculation for cryptography, where customer scramble and de-sepulcher the record. A SHA-512 calculation is likewise utilized for making the message process and check the uprightness of information. This likewise helps in maintaining a strategic distance from unapproved get to and giving protection and consistency. Impediment to this procedure is it is helpful just for SaaS model.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

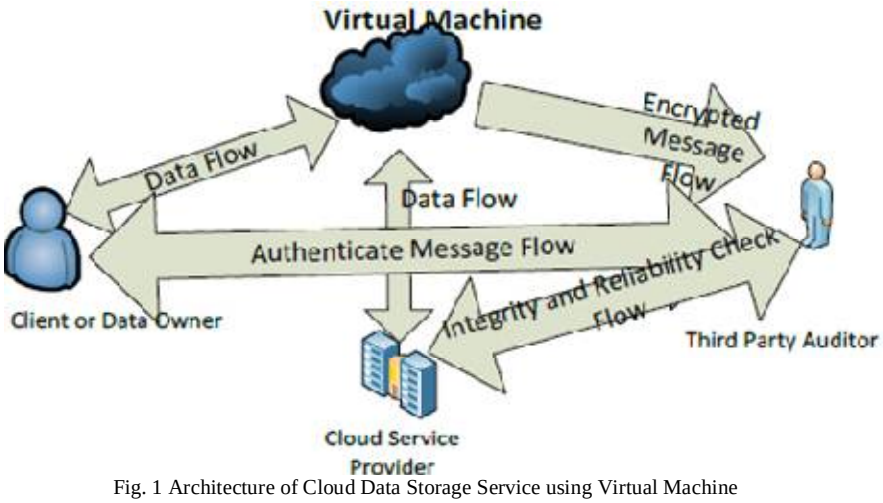

Fig. 1 Architecture of Cloud Data Storage Service using Virtual Machine

4. Using EAP

As said by S. Marium Extensible validation convention (EAP) can likewise use through three ways hand shake with RSA. Utilizing EAP they proposed character based signature for various levelled construction modelling. They give a verification convention to distributed computing (APCC) [4]. As contrast with SSL confirmation convention APCC is more lightweight and productive. It likewise utilized Challenge – handshake confirmation convention (CHAP) for validation.

The steps are as follows

1) When Client request for any service to cloud service provider, SPA send a CHAP request / challenge to the client.
2) The Client sends CHAP response/ challenges which is calculated by using a hash function to SPA
3) SPA checks the challenge value with its own calculated value. If they are matched then SPA sends CHAP success message to the client.

5. Using Automatic Protocol Blocker

Balkrishna proposed effective Automatic Protocol Blocker system for mistake remedy which checks information stockpiling accuracy [4].Kiran Kumar proposed programmed convention blocker to maintain a strategic distance from unapproved access [5]. At the point when an unapproved client access client information, a little application runs which screens client inputs, It coordinates the client info, on the off chance that it is coordinated then it permit client to get to the information else it will piece convention naturally. It contains five calculations as keygen, SinGen, GenProof, Verify Proof, Protocol Verifier. Convention Verifier is utilized by CS. It contains three stages as Setup, Audit and Block.

6. Random Masking Technique

BalJachak K. B. proposed security protecting Third gathering inspecting without information encryption. It utilizes a straight mix of examined square in the server's reaction is covered with haphazardly produced by a pseudo arbitrary capacity (PRF) [7].

[B] Different Public auditing mechanisms on Cloud

This section consist different mechanisms, different system proposed by authors which are used for auditing in cloud computing.

1. Compact Proofs of Retrievability

Hovav Shacham and Brent Watersy[9] proposed verification of-hopelessness framework. In this framework, information stockpiling focus must demonstrate to a verier that he is really putting away the greater part of a customer's information. They have proposed two homomorphism authenticators the initially, taking into account PRFs, gives a proof-of hopelessness plan secure in the standard model. The second, in light of BLS marks [8], gives a proof-of hopelessness plan with open variability secure in the irregular prophet model. Structures disclosed by them permit to contend about the frameworks unforgeability, extractability, and hopelessness with these three sections construct separately in light of cryptographic, combinatorial, and coding-hypothetical methods.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

2 Provable Data Possession at Untrusted Stores

Giuseppe Ateniese et all present a model which taking into account provable information ownership (PDP)[10]. This is utilized for confirming that server is handling the first information without recovering it. In this model probabilistic evidence of ownership is produced by examining arbitrary arrangements of pieces from the server. This serves to diminishes I/O cost.

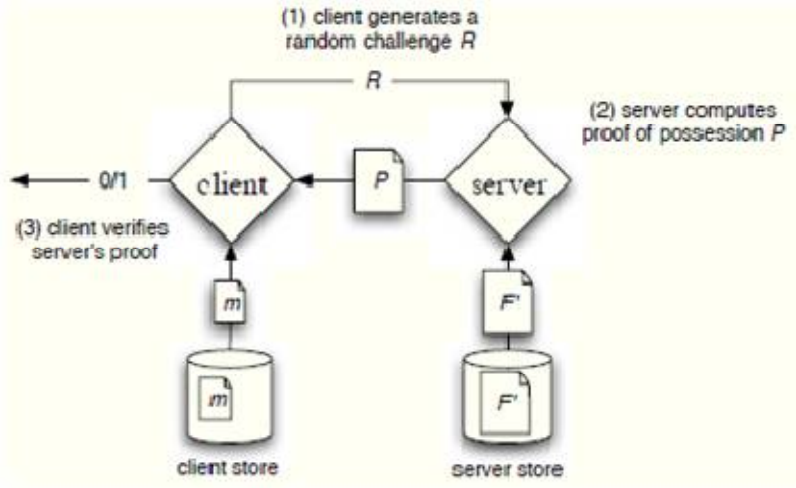

Fig.2 Provable Data Possession at Untrusted Stores

As shown in Fig.2 client maintains a constant amount of metadata to verify the proof. The challenge/response protocol transmits a small, constant amount of data, which minimizes network communication. DP model for remote data checking supports large data sets in widely-distributed storage systems. A key component of this mechanism is the homomorphism verifiable tags.

3. Privacy Preserving Public Auditing

Cong Wang Proposed Privacy Preserving Public Auditing method [11].In this strategy open evaluating permits TPA alongside client to check the honesty of the outsourced information put away on a cloud and Privacy Preserving permits TPA to do inspecting without asking for information. Here TPA can review the information by keeping up cloud information protection. They have utilized the homomorphism direct authenticator and arbitrary concealing to ensure that the TPA would not realize any information about the information content put away on the cloud server amid the productive inspecting process, which not just wipes out the weight of cloud client from the monotonous and potentially costly examining errand, additionally keep the clients from trepidation of the outsourced information spillage.

This mechanism is based on 4 algorithms:

- Keygen: It is a key generation algorithm for setup the scheme.
- Singen: It is used by the user to generate verification metadata which may consist of digital signature.
- GenProof: It is used by CS to generate a proof of data storage correctness.
- Verifyproof: Used by TPA to audit the proofs

4. LT Codes-based Secure and Reliable Cloud Storage Service

Ning Cao et all investigate the issue of secure and solid distributed storage with the effectiveness thought of both information repair and information recovery, and configuration a LT codes based distributed storage administration (LTCS)[12]. LTCS gives productive information recovery to information clients by using the quick Belief Propagation disentangling calculation, and discharges the information proprietor from the weight of enabling so as to be online open information respectability check and utilizing accurate repair. LTCS is much quicker information recovery than the deletion codes based arrangements. It presents less capacity cost, much speedier information recovery, and equivalent correspondence cost contrasting with system coding-based capacity administrations.

5. Oruta:

Boyang Wang et all proposed Oruta, the main protection safeguarding open inspecting instrument for shared information in the cloud in [13].They have utilized ring marks to build homomorphism authenticators, so the TPA can

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

review the uprightness of shared information, without recovering the whole information. They have utilized HARS and its properties for building Oruta.

III. PRELIMINAREE

In this section, we briefly introduce some cryptographic techniques we will use in this paper, including bilinear maps, homomorphic authenticators and proxy re-signatures.

A. Bilinear Maps

Let G1 and G2 be two multiplicative cyclic groups of prime order p, g be a generator of G1. Bilinear map e is a map e: G1 × G1 → G2 with the following properties:

1) Computability:
there exists an efficient algorithm for computing map e.
2) Bilinearity: for all u, v ∈G1 and a, b ∈Zp, e(ua, vb) = e(u, v)ab.
3) Non-degeneracy: e(g, g) 6= 1.

B. Complexity Assumptions

Definition *1:* Computational Diffie-Hellman (CDH)
Problem. For a, b ∈Zp, given g, ga, gb ∈G1 as input, output gab ∈G1.
The CDH assumption holds in G1 if it is computationally infeasible to solve the CDH problem in G1.
Definition *2:* Discrete Logarithm (DL) Problem. For a ∈Zp, given g, ga ∈G1 as input, output a.
The DL assumption holds in G1 if it is computationally infeasible to solve the DL problem in G1

C. Homomorphic Authenticators

Homomorphic authenticators [2], also called homomorphic verifiable tags, allow a public verifier to check the integrity of data stored in the cloud without downloading the entire data. They have been widely used in the previous public auditing mechanisms [2]–[9]. Besides *unforgeability* (only a user with a private key can generate valid signatures), a *homomorphic authenticable signature* scheme, which denotes a homomorphic uthenticator scheme based on signatures, should also satisfy the following properties:
Let (pk, sk) denote the signer's public/private key pair, σ1 denote the signature on block m1 ∈Zp, and σ2 denote the signature on block m2 ∈Zp.
• Blockless verifiability: Given σ1 and σ2, two random values α1, α2 in Zp and a block m′ = α1m1 + α2m2 ∈Zp, a verifier is able to check the correctness of block m′ without knowing m1 and m2. • Non-malleability: Given m1 and m2, σ1 and σ2, two random values α1, α2 in Zp and a block m′ = α1m1 + α2m2 ∈Zp, a user, who does not have private key sk, is not able to generate a valid signature σ′ on block m′ by combining σ1 and σ2. Blockless verifiability enables a verifier to audit the correctness of data in the cloud with only a linear combination of all the blocks, while the entire data does not need to be downloaded to the verifier. Non-malleability indicates that an untrusted party cannot generate valid signatures on combined blocks by combining existing signatures.

D. Proxy Re-signatures

Proxy re-signatures, first proposed by Blaze *et al*. [11], allow a *semi-trusted* proxy to act as a translator of signatures between two users, for example, Alice and Bob. More specifically, the proxy is able to convert a signature of Alice into a signature of Bob on the same block. Meanwhile, the proxy is not able to learn any private keys of the two users, which means it cannot sign any block on behalf of either Alice or Bob. In this paper, to improve the efficiency of user revocation, we propose to let the cloud to act as the proxy and convert signatures for users.

Real Time Example:

In a Group record sharing environment if a client wishes to revocate from a gathering then the many-sided quality added to the documents shared by that client where another person in the gathering need to take power over their documents by downloading and reassigning key to that record. Keeping in mind the end goal to conquer that we select a third individual where his work is to screen the records of the revocated client and reassign it to another person in the gathering taking into account proprietors need with no overhead of download. Here we create private and open key taking into account the prime no. The fundamental point of this paper is to hunt down private and open records. If there should be an occurrence of open records clients can alter their documents and redesign to it.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

IV. ARCHITECTURE DIAGRAM

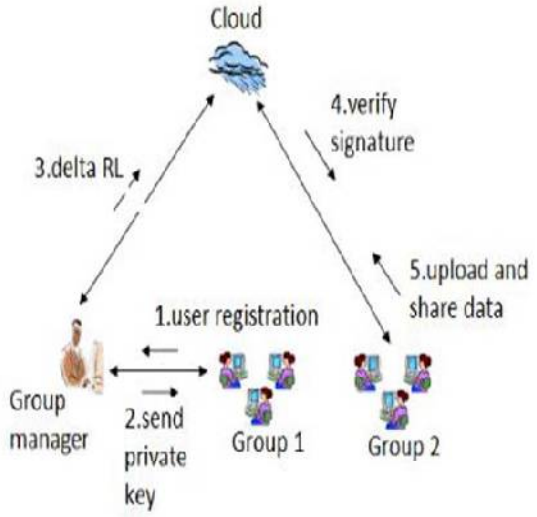

Fig.3 Architecture Diagram

File Upload

Record proprietor permitted to transfer information on the cloud either for their private or open use. They go about as a Group Manager for the document they transfer in cloud. Both the first client and gathering clients can get to, download and change shared information. Shared information is isolated into various squares. A client in the gathering can adjust a square in shared information by performing a supplement, erase or upgrade operation on the piece.

File Auditing

In the event that a client altered information then the examiner will screen the client and report to the proprietor about the altered information. The gathering administrator will screen the adjustments in the document and in the event that he establishes any error reviewer has full rights to revocate from his specific gathering. The general population verifier can review the uprightness of shared information without recovering the whole information from the cloud, regardless of the fact that a few pieces in shared information have been re-marked by the cloud.

Re-assigning

On one hand, once a client is repudiated from the gathering, the squares marked by the denied client can be proficiently surrendered. All the more particularly, the intermediary can change over a mark of Alice into a mark of Bob on the same square. In the interim, the intermediary is not ready to realize any private keys of the two clients, which implies it can't sign any piece for the benefit of either Alice or Bob.

Group Sharing

Information proprietor will store their information in the cloud and share the information among the gathering individuals. Who transfer the information have rights to alter and download their information in the cloud. He can likewise set rights to different clients in his gathering to alter or download information**.**

Access control

Cloud Server permits just the approved gathering part to store their information in the cloud offered by cloud administration suppliers as Sass and it won't permit unapproved bunch part to store their information in the cloud.

User Revocation

In the event that a client wishes to renounce from a gathering their solicitation with respect to disavowal will be sent to the inspector where reviewer will check to it and repudiate the client from gathering. The client repudiation is secure in light of the fact that just existing clients can sign the squares in shared information. indeed, even with a re-marking key, the cloud can't create a substantial mark for a subjective square for the benefit of a current client. What's more, in the wake of being denied from the gathering, a renounced client is no more in the client list, and can no more create legitimate marks on shared information.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

SYSTEM MODEL:

A framework model for the distributed storage structural engineering, which incorporates three principle system substances: clients , a cloud server , and a trusted outsider. • User: an individual or gathering substance, which possesses its information put away in the cloud for online information stockpiling and figuring. Distinctive clients might be subsidiary with a typical rganization, and are allocated with autonomous powers on certain information field.

• **Cloud server:**

A substance, which is overseen by a specific cloud administration supplier or cloud application administrator to give information stockpiling and registering administrations. The cloud server is viewed as a substance with unlimited stockpiling and computational assets**.**

• **Trusted third party**:

A discretionary and unbiased element, which has propelled abilities for the benefit of the clients, to perform information open reviewing and question intervention. In the distributed storage, a client remotely stores its information through online frameworks, stages, or programming for cloud administrations, which are worked in the circulated, parallel, and agreeable modes. Amid cloud information getting to, the client self-rulingly interfaces with the cloud server without outer obstructions, and is appointed with the full and free power all alone information fields. It is important to ensure that the clients' outsourced information can't be unapproved gotten to by different clients.

Design Goals:

To effectively confirm the respectability of imparted information to proficient client renouncement, our open inspecting component ought to accomplish the accompanying properties: (1) Correctness: The TPA can accurately check the honesty of shared information. (2) Efficient and Secure User Revocation: On one hand, once a client is denied from the gathering, the squares marked by the repudiated client can be effectively re-marked. Then again, just existing clients in the gathering can create substantial marks on shared information, and the denied client can no more figure legitimate marks on shared information. (3) Public Auditing: The TPA can review the respectability of shared information without recovering the whole information from the cloud, regardless of the fact that a few squares in shared information have been re-marked by the cloud. (4)Access control: Cloud Server permits just the approved gathering part to store their private information in the cloud offered by cloud administration suppliers as SaaS and it won't permit unapproved bunch part to store their information in the cloud. (5)Data secrecy: Data proprietor will store their information in the cloud and share the information among the gathering individuals. Who transfer the information have rights to adjust and erase their information in the cloud. (6)Traceability: if there should arise an occurrence of any question happens it can without much of a stretch traceable. In the event that other gathering part erase the other gathering individuals' information can be effectively perceptible.

V. CONCLUSIONS

In this paper, we proposed a new public auditing mechanism for shared data with efficient user revocation in the cloud. When a user in the group is revoked, we allow the cloud to re-sign blocks that were signed by the revoked user with proxy re-signatures. The cloud can improve the efficiency of user revocation, and existing users in the group can save a significant amount of computation and communication resources during user revocation.

REFERENCES

[1] B. Wang, B. Li, and H. Li, ―Public Auditing for Shared Data with Efficient User Revoation in the Cloud,‖ IEEE Transaction on service computing 2014.

[2] B. Wang, B. Li, and H. Li, ―Public Auditing for Shared Data with Efficient User Revoation in the Cloud,‖ in the Proceedings of IEEE INFOCOM 2013, 2013, pp. 2904–2912

[3] 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,‖ Communications of the ACM, vol. 53, no. 4, pp. 50–58, Apirl 2010.

[4] B. Wang, S. S. Chow, M. Li, and H. Li, ―Storing Shared Data on the Cloud via Security-Mediator,‖ in Proceedings of IEEE ICDCS 2013, 2013.

[5] B. Wang, H. Li, and M. Li, ―Privacy-Preserving Public Auditing for Shared Cloud Data Supporting Group Dynamics,‖ in the Proceedings of IEEE ICC 2013, 2013.

[6] 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," Communications of the ACM, vol. 53, no. 4, Apirl 2010, pp. 50–58.

[7] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," in the Proceedings of ACM CCS 2007, pp. 598–610.

[8]S. R. Tate, R. Vishwanathan, and L. Everhart, "Multi-user Dynamic Proofs of Data Possession Using Trusted Hardware,"

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

[9] B.Wang, B. Li, and H. Li, "Certificateless Public Auditing for Data Integrity in the Cloud," in Proceedings of IEEE CNS 2013, pp. 276–284.
[10] B. Chen, R. Curtmola, G. Ateniese, and R. Burns, "Remote Data Checking for Network Coding-based Distributed Stroage Systems," in the Proceedings of ACM CCSW 2010, pp. 31–42.
[11]H. Shacham and B. Waters, "Compact Proofs of Retrievability," in the Proceedings of ASIACRYPT. Springer-Verlag, 2008, pp.90–107.
[12]H. Wang, "Proxy Provable Data Possession in Public Clouds," IEEE Transactions on Services Computing, accepted.
[13] B. Wang, B. Li, and H. Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud," in the Proceedings of IEEE Cloud 2012, pp. 295–302.
[14] B. Wang, B. Li, and H. Li, "Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud," in the Proceedings of ACNS, June 2012, pp. 507–525.
[15]M. Blaze, G. Bleumer, and M. Strauss, "Divertible Protocols and Atomic Proxy Cryptography," in the Proceedings of EUROCRYPT 98. Springer-Verlag, 1998, pp.127–144.
[16] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," in the Proceedings of ACM/IEEE IWQoS, 2009, pp. 1–9.
[17]Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamic for Storage Security in Cloud Computing," in the Proceedings of ESORICS. Springer-Verlag, 2009, pp. 355–370.
[18]C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," in the Proceedings of IEEE INFOCOM, 2010, pp. 525–533.
[19]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.
[20] 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 the Proceedings of ACM SAC, 2011, pp. 1550–1557.
[21] C. Wang, Q. Wang, K. Ren, and W. Lou, "Towards Secure and Dependable Storage Services in Cloud Computing," IEEE Trans-actions on Services Computing, vol. 5, no. 2, pp. 220–232, 2011.
[22]A. Shamir, "How to share a secret," in Communication of ACM, vol. 22, no. 11, 1979, pp. 612–613.
[23] B. Wang, H. Li, and M. Li, "Privacy-Preserving Public Auditing for Shared Cloud Data Supporting Group Dynamics," in the Proceedings of IEEE ICC 2013.
[24]B. Wang, S. S. Chow, M. Li, and H. Li, "Storing Shared Data on the Cloud via Security-Mediator," in Proceedings of IEEE ICDCS, 2013.
[25]Greenberg A, Jain N et al (2009) VL2: a scalable and flexible data center network. In: Proc SIGCOMM
[26]Guo C et al (2008) DCell: a scalable and fault-tolerant network structure for data centers. In: Proc SIGCOMM
[27]Guo C, Lu G, Li D et al (2009) BCube: a high performance, server-centric network architecture for modular data centers. In: Proc SIGCOMM
[28] Hadoop Distributed File System, hadoop.apache.org/hdfs
[29] Hadoop MapReduce, hadoop.apache.org/mapreduce
[30] Hamilton J (2009) Cooperative expendable micro-slice servers (CEMS): low cost, low power servers for Internet-scale services In: Proc of CIDR
[31] IEEE P802.3az Energy Efficient Ethernet Task Force, www.ieee802.org/3/az
[32]Kalyvianaki E et al (2009) Self-adaptive and self-configured CPU resource provisioning for virtualized servers using Kalman filters. In: Proc of international conference on autonomic computing
[33] Kambatla K et al (2009) Towards optimizing Hadoop provisioning in the cloud. In: Proc of HotCloud
[34]Kernal Based Virtual Machine, www.linux-kvm.org/page/ MainPage
[35] Krautheim FJ (2009) Private virtual infrastructure for cloud computing. In: Proc of HotCloud
[36] Kumar S et al (2009) vManage: loosely coupled platform and virtualization management in data centers. In: Proc of international conference on cloud computing
[37] Li B et al (2009) EnaCloud: an energy-saving application live placement approach for cloud computing environments. In: Proc of international conf on cloud computing
[38] Meng X et al (2010) Improving the scalability of data center networks with traffic-aware virtual machine placement. In: Proc INFOCOM

BIOGRAPHY

Prof. Autade P.P. is a Assistant Professor in the Electronics & Telecommunication Engineering Department, SVIT College of Engineering, Nashik, Savitribai Phule Uop University. She received Master in Engineering (ME) degree in 2014 from Savitribai Phule UoP, MS, and India. Her research interests are Computer Networks.