International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 23 Issue 8 –NOVEMBER 2016.

User Revocation with Public Auditing for Shared Data in cloud

P.DIVYA VANI[#1],P.LAKSHMAN RAO[*2] and SAYEED YASIN[*3]

[#] *Student, M.Tech (C.S.E), Nimra College of Engineering & Technology, A.P., India.*

[*2] *Assistant professor , Dept. of Computer Science & Engineering, Nimra College of Engineering & Technology, A.P., India.*

[*3] *Associate professor & Head, Dept. of Computer Science & Engineering, Nimra College of Engineering & Technology, A.P., India.*

***Abstract*— Cloud computing is Internet-based computing, whereby shared resources, software, and information are provided to computers and other devices on demand. shared data modification in the cloud, signature is being provided to each individual who access the data in cloud. Once the data is modified by the user on a block, the user must ensure that the signature is provided on that specific block. When a user gets revoked from the group, the blocks which were previously signed by this revoked user must be re-signed by an existing user. This straightforward method allows an existing user to download the entire data and re-sign it. But during user revocation, it is inefficient due to the large size of shared data in the cloud. In this paper, we propose to failures of human or hardware and even Software errors cloud data is associated with data integrity. Several mechanisms have been proposed in order to allow both the data owners as well as the public auditors to audit cloud data integrity efficiently without retrieving the entire data from the cloud servers. A Third Party Auditor (TPA) will perform integrity checking and the identity of the signer on each block in shared data is kept private from them. In this paper, we only survey for auditing the integrity of shared data in the cloud with efficient user revocation while still conserving identity privacy.**

***Index Terms*— Cloud computing, Public auditing, privacy-conserving, shared data, user revocation.**

I. INTRODUCTION

Most of the previous works concentrate on auditing the integrity of personal information. Different from these works, some of recent works concentrate on how to preserve identity privacy from public verifiers when auditing the integrity of shared information. Unfortunately, none of the above methods considers the efficiency of user revocation when auditing the correctness of shared information in the cloud. With shared information, when a user did some changes in a block, she also needs to calculate a new signature for the changed block. Due to the modifications from different users, different blocks are signed by different users. The cloud computing field is growing day by day with an increasing number of businesses and government establishments going for cloud computing based services. [1] The cloud computing incorporate combination of:- 1. IaaS (Infrastructure as a Service) 2. PaaS (Platform as a Service) 3. SaaS (Software as a Service) These are collectively called as *aaS (Everything as a Service) which means a service oriented architecture. Cloud computing is mainly used for resource sharing and with very low-maintenance. The cloud service providers (CSPs), such as Amazon, are able to provide a various services to cloud users with the help of powerful various datacenters. Cloud Providers provides a fundamental service is data storage (Storage as-a service). An organisation allows its group members in the same group or department to store and share files in the cloud. By utilizing the cloud, the group members can be completely released from its local data storage and maintenance. A significant risk arises in confidentiality of those stored files. So, the users are not fully trusted the cloud servers operated by cloud provider while sensitive data stored in the cloud.

A. Cloud Computing :

Cloud computing is nothing but internet based computing which made revolution in today's world. It is the biggest innovation which uses advanced computational power and improves data sharing and data storing capabilities. Cloud is a large group of interconnected computers, which is a major change in how we store information and run application. Cloud computing is a shared pool of configurable computing resources, ondemand network access and provisioned by the service provider [1].The advantage of cloud is cost savings. The prime disadvantage is security. The cloud computing security contains to a set of policies, technology & controls deployed to protect data, application & the associated infrastructure of cloud computing. Some security and privacy issues that need to be considered. The only thing was the cloud computing lacks regarding the issues of data integrity, data privacy, and data accessed by unauthorised members.

B. Data integrity:

Integrity is nothing but consistency. It is a major factor that affects on the performance of the cloud. Data integrity contains protocols for writing of the data in a reliable manner to the persistent data storages which can be retrieved in the same format without any changes later. Maintaining integrity of shared data is quite difficult task. Numbers of mechanisms

have been proposed [2]-[15] to protect integrity of data. Concept of attaching Signature to each block of data is used in these mechanisms. Data Integrity is most important of all the security issues in cloud data storages as it ensures completeness of data as well as that the data is correct, accessible, consistent and of high quality. Data model consist of three types of integrity constraints: Entity integrity, Referential integrity, Domain integrity

C. *Public Data Auditing in Cloud:*

On cloud we can able to store data as a group and share it or modify it within a group. In cloud data storage contains two entities as cloud user (group members) and cloud service provider/ cloud server. Cloud user is a person who stores large amount of data on cloud server which is managed by the cloud service provider. User can upload their data on cloud and share it within a group. A cloud service provider will provide services to cloud user. The major issue in cloud data storage is to obtain correctness and integrity of data stored on the cloud. Cloud Service Provider (CSP) has to provide some form of mechanism through which user will get the confirmation that cloud data is secure or is stored as it is. No data loss or modification is done by unauthenticated member. To achieve security data auditing concept is come into picture. This can be achieved in 2 ways as without trusted third party. With trusted third party based on who does the verification. In cloud computing architecture data is stored centrally and managing this centralised data and providing security to it is very difficult task. TPA is used in this situation. The reliability is increased as data is handled by TPA but data integrity is not achieved. TPA uses encryption to encrypt the contents of the file. It checks data integrity but there is threat of TPA itself leaks user's data.

II. PROPOSED SYSTEM:

In this paper, we propose Panda, a novel public auditing mechanism for the integrity of shared data with efficient user revocation in the cloud. In our mechanism, by utilizing the idea of proxy re-signatures, once a user in the group is revoked, the cloud is able to resign the blocks, which were signed by the revoked user, with a re-signing key. As a result, the efficiency of user revocation can be significantly improved, and computation and communication resources of existing users can be easily saved. Meanwhile, the cloud, which is not in the same trusted domain with each user, is only able to convert a signature of the revoked user into a signature of an existing user on the same block, but it cannot sign arbitrary blocks on behalf of either the revoked user or an existing user. By designing a new proxy re-signature scheme with nice properties, which traditional proxy resignatures do not have, our mechanism is always able to check the integrity of shared data without retrieving the entire data from the cloud. Moreover, our proposed mechanism is scalable, which indicates it is not only able to efficiently support a large number of users to share data and but also able to handle multiple auditing tasks simultaneously with batch auditing. In addition, by taking advantages of Shamir Secret Sharing, we can also extend our mechanism into the multi-proxy model to minimize the chance of the misuse on re-signing keys in the cloud and improve the reliability of the entire mechanism.

III. LITERATURE SURVEY

A. *Public Auditing for Shared Data with Efficient User Revoation in the Cloud*

AUTHORS: B. Wang, B. Li, and H. Li

With data storage and sharing services in the cloud, users can easily modify and share data as a group. To ensure shared data integrity can be verified publicly, users in the group need to compute signatures on all the blocks in shared data. Different blocks in shared data are generally signed by different users due to data modifications performed by different users. For security reasons, once a user is revoked from the group, the blocks which were previously signed by this revoked user must be re-signed by an existing user. The straightforward method, which allows an existing user to download the corresponding part of shared data and re-sign it during user revocation, is inefficient due to the large size of shared data in the cloud. In this paper, we propose a novel public auditing mechanism for the integrity of shared data with efficient user revocation in mind. By utilizing the idea of proxy re-signatures, we allow the cloud to re-sign blocks on behalf of existing users during user revocation, so that existing users do not need to download and re-sign blocks by themselves. In addition, a public verifier is always able to audit the integrity of shared data without retrieving the entire data from the cloud, even if some part of shared data has been re-signed by the cloud. Moreover, our mechanism is able to support batch auditing by verifying multiple auditing tasks simultaneously. Experimental results show that our mechanism can significantly improve the efficiency of user revocation.

B. *Provable Data Possession at Untrusted Stores*

AUTHORS: G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song

We introduce a model for provable data possession (PDP) that allows a client that has stored data at an untrusted server to verify that the server possesses the original data without retrieving it. The model generates probabilistic proofs of possession by sampling random sets of blocks from the server, which drastically reduces I/O costs. The 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. Thus, the PDP model for remote data checking supports large data sets in widely-distributed storage system.

We present two provably-secure PDP schemes that are more efficient than previous solutions, even when compared with schemes that achieve weaker guarantees. In particular, the overhead at the server is low (or even constant), as opposed to linear in the size of the data. Experiments using our implementation verify the practicality of PDP and reveal that the performance of PDP is bounded by disk I/O and not

by cryptographic computation.

C. Ensuring Data Storage Security in Cloud Computing

AUTHORS: C. Wang, Q. Wang, K. Ren, and W. Lou

Cloud computing has been envisioned as the next-generation architecture of IT enterprise. In contrast to traditional solutions, where the IT services are under proper physical, logical and personnel controls, cloud computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. This unique attribute, however, poses many new security challenges which have not been well understood. In this article, we focus on cloud data storage security, which has always been an important aspect of quality of service. To ensure the correctness of users' data in the cloud, we propose an effective and flexible distributed scheme with two salient features, opposing to its predecessors. By utilizing the homomorphic token with distributed verification of erasure-coded data, our scheme achieves the integration of storage correctness insurance and data error localization, i.e., the identification of misbehaving server (s). Unlike most prior works, the new scheme further supports secure and efficient dynamic operations on data blocks, including: data update, delete and append. Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks.

D. Enabling Public Verifiability and Data Dynamic for Storage Security in Cloud Computing

AUTHORS: Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou

Cloud Computing has been envisioned as the next-generation architecture of IT Enterprise. It moves the application software and databases to the centralized large data centers, where the management of the data and services may not be fully trustworthy. This unique paradigm brings about many new security challenges, which have not been well understood. This work studies the problem of ensuring the integrity of data storage in Cloud Computing. In particular, we consider the task of allowing a third party auditor (TPA), on behalf of the cloud client, to verify the integrity of the dynamic data stored in the cloud. The introduction of TPA eliminates the involvement of the client through the auditing of whether his data stored in the cloud are indeed intact, which can be important in achieving economies of scale for Cloud Computing. The support for data dynamics via the most general forms of data operation, such as block modification, insertion, and deletion, is also a significant step toward practicality, since services in Cloud Computing are not limited to archive or backup data only. While prior works on ensuring remote data integrity often lacks the support of either public auditability or dynamic data operations, this paper achieves both. We first identify the difficulties and potential security problems of direct extensions with fully dynamic data updates from prior works and then show how to construct an elegant verification scheme for the seamless integration of these two salient features in our protocol design. In particular, to achieve efficient data dynamics, we improve the existing proof of storage models by manipulating the classic Merkle Hash Tree construction for block tag authentication. To support efficient handling of multiple auditing tasks, we further explore the technique of bilinear aggregate signature to extend our main result into a multiuser setting, where TPA can perform multiple auditing tasks simultaneously. Extensive security and performance analysis show that the proposed schemes are highly efficient and provably secure.

E. Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing.

AUTHORS: C. Wang, Q. Wang, K. Ren, and W. Lou,

Cloud computing is the long dreamed vision of computing as a utility, where users can remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources. By data outsourcing, users can be relieved from the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the possibly large size of outsourced data makes the data integrity protection in Cloud Computing a very challenging and potentially formidable task, especially for users with constrained computing resources and capabilities. Thus, enabling public auditability for cloud data storage security is of critical importance so that users can resort to an external audit party to check the integrity of outsourced data when needed. To securely introduce an effective third party auditor (TPA), the following two fundamental requirements have to be met: 1) TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user; 2) The third party auditing process should bring in no new vulnerabilities towards user data privacy. In this paper, we utilize and uniquely combine the public key based homomorphic authenticator with random masking to achieve the privacy-preserving public cloud data auditing system, which meets all above requirements. To support efficient handling of multiple auditing tasks, we further explore the technique of bilinear aggregate signature to extend our main result into a multi-user setting, where TPA can perform multiple auditing tasks simultaneously. Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient.

IV. RELATED WORK

A. Panda: Public auditing for Shared Data with Efficient User Revocation in the Cloud [1]. In this paper with data storage and sharing services in the cloud, users can easily modify and share data as a group. To ensure shared data integrity can be verified publicly, users in the group need to compute signatures on all the blocks in shared data. Different blocks in shared data are generally signed by different users due to data modifications performed by different users. For security reasons, once a user is revoked from the group, the

blocks which were previously signed by this revoked user must be re-signed by an existing user.

B. A View of Cloud Computing [2]. Cloud computing, the long-held dream of computing as a utility, has the potential to transform a large part of the IT industry, making software even more attractive as a service and shaping the way IT hardware is designed and purchased. Developers with innovative ideas for new Internet services no longer require the large capital outlays in hardware to deploy their service or the human expense to operate it. They need not be concerned about over provisioning for a service whose popularity does not meet their predictions, thus wasting costly resources, or under provisioning for one that becomes wildly popular, thus missing potential customers and revenue.

C. Provable Data Possession at Untrusted Store [3]. In this paper author introduce a model for provable data possession (PDP) that allows a client that has stored data at an untrusted server to verify that the server possesses the original data without retrieving it.The model generates probabilistic proofs of possession by sampling random sets of blocks from the server, which drastically reduces I/O costs. The 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.

D. Compact Proofs of Retrievability [4]. In this paper, first scheme was built from BLS signatures and secure in the random oracle model, features a proof-of-retrievability protocol in which the client's query and server's response are both extremely short. This scheme allows public verifiability: anyone can act as a verifier, not just the file owner.Second scheme, which builds on pseudorandom functions and is secure in the standard model, allows only private verification. It features a proof-of-retrievability protocol with an even shorter server's response than our first scheme, but the client's query is long.

E. Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing [5]. This work studies the problem of ensuring the integrity of data storage in Cloud Computing. In particular, the task of allowing a third party auditor (TPA), on behalf of the cloud client, to verify the integrity of the dynamic data stored in the cloud. The introduction of TPA eliminates the involvement of client through the auditing of whether his data stored in the cloud is indeed intact, which can be important in achieving economies of scale for Cloud Computing. In particular, to achieve efficient data dynamics, we improve the Proof of Retrievability model by manipulating the classic Merkle Hash Tree (MHT) construction for block tag authentication. Extensive security and performance analysis show that the proposed scheme is highly efficient and provably secure.

F. Ensuring Data Storage Security in Cloud Computing [6]. In this Paper, author focus on cloud data storage security, which has always been an important aspect of quality of service. To ensure the correctness of users' data in the cloud, we propose an effective and flexible distributed scheme with two salient features, opposing to its predecessors. By utilizing the homomorphic token with distributed verification of erasure-coded data, our scheme achieves the integration of storage correctness insurance and data error localization, i.e., the identification of misbehaving server (s). Unlike most prior works, the new scheme further supports secure and efficient dynamic operations on data blocks, including: data update, delete and append. Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks.

Here we try to introduce a Trusted Third Party like a ticket granting server (Resource Broker). If a user wants to access the data stored in a cloud server the user must get authentication key from the TTP then, the authentication key will be verified then only the user will be allowed to access the data which is stored in the cloud server. The user must get the authentication key for each and every time. By this we can avoid the misbehaved nodes. If a user wants to join into the cloud, first step the user have to prove their identity. In this system the user first communicates with the TTP and reveals their identity. Then the TTP check with the identity provided by the user and verify for the trust worthy of the user. If found trustworthy then it will give a secure key Then the user has to enter into the cloud with the secret key which was given by the TTP. If the key match with the key given by TTP, then the user will be allowed to access the Data. The one TTP is used to do generate initial keys, generate revocation list and maintain user detail. The other TTP does check integrity of the data in the cloud and does the key regeneration during revocation process.

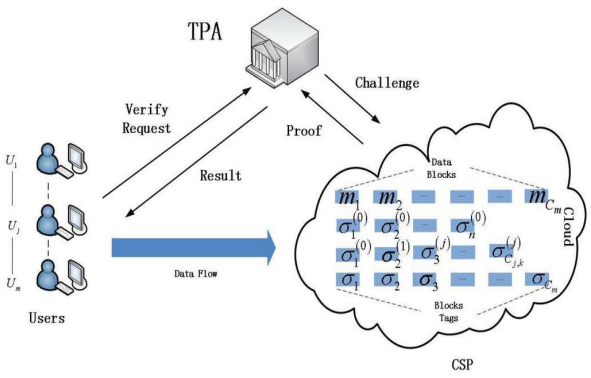

Figure: System Architecture

V. CONCLUSION AND FUTURE WORK

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 semi-trusted cloud to re-sign blocks that were signed by the revoked user with proxy re-signatures. Experimental results show that 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," in the Proceedings of IEEE INFOCOM 2013, 2013, pp. 2904–2912.
[2] 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.
[3] 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, 2007, pp. 598–610.
[4] H. Shacham and B. Waters, "Compact Proofs of Retrievability," in the Proceedings of ASIACRYPT 2008. Springer-Verlag,2008,pp. 90–107.
[5] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," in the Proceedings of ACM/IEEE IWQoS 2009, 2009, pp. 1–9.
[6] 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 2009. Springer-Verlag, 2009, pp. 355–370.
[7] 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, 2010, pp. 525–533.
[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 the Proceedings of ACM SAC 2011, 2011, pp. 1550–1557.
[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. 220–232, 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] N. Cao, S. Yu, Z. Yang, W. Lou, and Y. T. Hou, "LT Codes-based Secure and Reliable Cloud Storage Service," in the Proceedings of IEEE INFOCOM 2012, 2012, pp. 693–701.
[12] J. Yuan and S. Yu, "Proofs of Retrievability with Public Verifiability and Constant Communication Cost in Cloud," in Proceedings of ACM ASIACCS-SCC'13, 2013.
[13] H. Wang, "Proxy Provable Data Possession in Public Clouds," IEEE Transactions on Services Computing, accepted.
[14] 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, 2012, pp. 295–302.

Ms P.DIVYAVANI is a student of NIMRA College of Engineering and Technology, IBRAHIMPATNAM, VIJAYAWADA. She is presently pursuing her M.Tech degree from JNTU, Kakinada.

Mr. P.LAKSHMANA RAO is presently working as Assistant professor in CSE department. Nimra college of engineering and Technology, Jupudi, Nimra Nagar,VIJAYAWADA. He has obtained B.Tech degree from ,A.N.U GUNTUR and M.Tech, degree from JNTU, Kakinada. He has published several research papers in various national and international Journals.

SAYEED YASIN received his MTECH in Computer Science & Engg from JNTU Hyderabad. He is pursuing Ph.D., in Rayalaseema University, Kurnool. He is currently working as an Associate Professor & Head in Nimra College of Science & Technology the Department of Computers Science and Engineering & Technology, Jupudi, Ibrahimpatnam,Vijayawada-521456. He has more than Eight years of experience in teaching field. His area of interests are wireless networks & programming, & Mobile Computing.