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. 3, Issue 12, December 2015

A Survey on Secure and Optimal Performance Approach for Data Manipulation in Cloud

SachinNirne, Prof. D.H. Kulkarni

M.E.Student, Dept. of Computer Science &Engineering, Smt.Kashibai Navale College of Engineering , Pune, India

Professor, Dept. of Computer Science &Engineering, Smt.Kashibai Navale College of Engineering, Pune, India

ABSTRACT: Cloud storage empowers users to store their data remotely and enjoy the on-demand high quality cloud applications without the burden on local hardware and software management. The data compromise can occur because attack by nodes in the cloud and other users. Therefore, high security area required protecting data in the cloud; we introduce secure and optimal performance approach for data manipulation in cloud. In this methodology, when data owner wants to send file on cloud server first file is dividing into fragments and it then encrypted. These encrypted fragments data over the cloud nodes. Each node stores only one fragment of a particular data file to make ensure even in case that successful attack, no meaningful information is catching to the attacker. We use T-coloring concept for storing the fragments in nodes and separated with certain distance to prevent an attacker is predicting the fragments locations. To maintain integrity we are using the Third Party Auditor (TPA) which makes the audit report stored file on cloud and sent it to the data owner by mail. If attacker modified the file then TPA sends audit report as changed file to data owner and Proxy Agent. Finally proxy Agent which replace the modified code with original contents.

KEYWORDS: cloud security, Cloud Storage, fragmentation, Third Party Auditor (TPA), Performance.

I. INTRODUCTION

Cloud computing is enabling a model for ubiquitous, convenient, on demand network access to configurable computing a shared pool resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with nominal management effort or service provider interaction.

Public cloud - An open cloud is contained outside an association. An illustration of this sort of administration is Amazon Web Services Elastic Cloud Computing offering, which creates an "occurrence" of a system, server or application interconnected by general society Internet.

Private cloud - A private cloud is contained inside an association. A case of this kind of administration is an Enterprise Virtualization of PCs utilizing slim customer innovation where the cases of the PC are conveyed to the client's desktop from a brought together server plant.

Community cloud: Infrastructure shared by a few associations for a mutual cause and may be overseen by them or an outsider administration supplier.

Hybrid cloud: It is combination of both private and public cloud. Indeed, even the most secured private cloud likely has departure point(s) into the general population Internet, if for no other explanation than to get to worldwide framework administrations, for example, Domain Name System (DNS) resources [2].

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. 3, Issue 12, December 2015

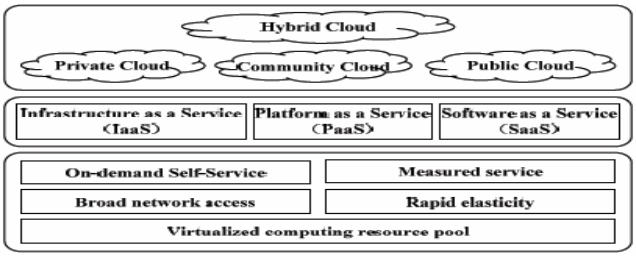

Fig.1. The NIST's definition model of cloud computing [8]

The Cloud computing has three administration models: Infrastructure as an administration (IAAS), Platform as an administration (PAAS) and Software as administration (SAAS).

Infrastructure as a Service (IaaS) this is base layer in cloud administration model . It can be utilized to convey the PC equipment as an administration. It empowers the supplier to offer boundless virtual server to client and make savvy utilization of facilitating equipment. Eg. Amazon, Rackspace and so forth.
Platform as a Service (PaaS) this is center layer in cloud administration model. It gives an authoritative domain to programming advancement for designers over the web. Engineers compose the code and the PaaS supplier gives an approach to transfer the code into the web. Eg. Google App Engine.
Software as a Service (SaaS) this is higher layer in the cloud stack. It is intended to just lease the product to the client. Eg. Facebook, SalesForce and so on. [3].

The cloud computing paradigm has reformed the usage and the information technology infrastructure management. Cloud computing essential characteristics are on-demand self-services, Broad network accesses, resource pooling, elasticity, and measured services. Security is difficult aspects among those prohibiting the wide-spread adoption [1]. Resources in virtualization like network, memory, processors, and storage ensures scalability and high availability of computing capabilities. Cloud can actively provision these virtual resources to hosted applications or to clients that use them to develop their own applications or to store data [4].

The cloud storage services have rapidly become increasingly popular. Users may store their data on the cloud and access their data any place at any moment. Considering user confidentiality, the data which stored on the cloud is protected and encrypted from access by other users [5]. Cloud storage data as it may be attractive particularly for users with unreliable storage demands, requiring an cheap storage tier or a low-cost, long-term archive [6]. The cloud service providers can do maliciously, attempting to hide data loss or corruption and claiming that the files are still storing correctly in the cloud for reputation or monetary reasons. Thus, because of above problem, users to implement an efficient protocol to perform outsourced data periodical verifications to ensure that the cloud indeed maintains their data correctly [7].

II. LITERATURE REVIEW

In [2] authors Mazhar Al, Kashif Bilal, Samee U. Khan, Bharadwaj Veeravalli, Keqin Li, Albert Y. Zomaya [1] The public cloud outsourced data need to be secured. Unauthorized data access by other users and Processes (whether unintentionally or intentionally) must be prevented. A cloud must ensure throughput, reliability, and security. A key factor determining a cloud throughput that stores data is the data retrieval time. In large-scale systems, the data reliability problems, data availability, and response time are handling with data replication strategies. However, replicas data over a number of nodes increases the intrusion surface for that appropriate data. For occurrences, storing a file with m replica in a cloud rather than one replica increases a node probability holding file to be chosen as attack victim, from 1/n to m/n , where n is the total number of nodes. So we can deduce that both security and performance for the next generation large-scale systems becomes critical, such as clouds. Therefore, it proposes, we collectively approach the issue of security and performance as a data secure problem. We started Division and Replication of Data in the Cloud for Optimal Performance and Security (DROPS) that legislatively fragments user files into pieces and replicates them at strategic locations within the cloud. The file division into fragments is performed based on a given user criteria such that the individual fragments does not consist any meaningful information. Every cloud node contains a distinct fragment to increase the security for data. A successful attack on a single node must not reveal the other fragments

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. 3, Issue 12, December 2015

locations within the cloud. To improve data retrieval time, the nodes have selected based on the centrality measures that ensure an improved access time. In addition to improve the retrieval time, we legislatively replicate fragments generate the highest read/write requests over these nodes. The nodes selection is performing in two phases. In the first phase, the nodes are selecting based on the fragments initial placement on the centrality measures. In the second phase, the nodes are selecting for replication.

Alessandro Mei, Luigi V. Mancini, and Sushil Jajodia,[9] It aims at designing a solution based on a large number of servers correlative to the decentralized algorithms in order that guarantee the availability and the system's functionalities scalability. The file system services does not contain centralized server, only a set of cooperating nodes to provide data storage, universal access, and restore to remote users in a scalable and dynamically reconfigurable way. Only clients have trusted while all servers are un-trusted; this change strongly affect to the security and availability models. In a fragmentation scheme, a file f is division into n fragments, all fragments have signed and distributed to n remote servers, one fragment per server. The user can reconstruct file f by accessing fragments arbitrarily chosen. The algorithm works in the read-m-write-all context. In general, m fragments read are performed from the closest servers among those that store the n file fragments. A write is performed to all the n servers. When m = 1, a fragmentation scheme coincides with an scheme for n replication, where n copies (replicas) of file f are stored to n different remote servers. A large-scale distributed file system normally bases file availability, confidentiality, and integrity on a combination of file fragmentation, file replication, and file encryption techniques. This paper proposes a model to assess file assurance stored in such a system, where the file assurance is the probability for file has not been compromised under the assumption that the system is the target attack successful.

Boyang Wang, Baochun Li, Hui Li[10] The data stored in an un-trusted cloud may lost easily or corrupted, because of hardware failures and human errors . To protect the cloud data integrity, it is best to perform public introducing so as to auditing a third party auditor (TPA), who offers its auditing service with more powerful computation and communication abilities than regular users. We propose Oruta, a new privacy preserving public auditing mechanism for shared data in an un-trusted cloud. In Oruta, we utilize ring signatures to construct homomorphic authenticators so that the third party auditor can verify the shared data integrity for a users group without retrieving the entire data , while on each block in shared data the signer identity kept private from the TPA. In addition, we further extend our mechanism to providing batch auditing, which may audit multiple data shared simultaneously in a single auditing task. Meanwhile, Oruta extend to use random masking to support data privacy during public auditing, and leverage index hash tables to support fully effective operations on shared data. An effective operation indicates an insert, delete or update operation on a single block in shared data.

Kui Ren ,Cong Wang, Qian, , Ning Cao, Wenjing Lou, [11] propose an active and soft distributed storage authentication scheme with certain dynamic data support to ensure the correctness and users' data availability in the cloud. We depend on era assure improving code in the file distribution measures to provide redundancies and guarantee the data perseverance against Byzantine servers [26], where a storage server may break down in random ways. This construction drastically lowers the communication and storage overhead as compared to the conventional replication-based file distribution approach. By applying the homomorphic token with authenticated erasure-coded data have distributed, our scheme achieves the storage correctness guarantee as well as data error localization. At any time data corruption has disclosed during the storage correctness authentication, our scheme can almost guarantee the data errors simultaneous localization, i.e., the misbehaving server(s) identification. In order to strike a good balance between error flexibility and data dynamics, we further analyze our token computation the algebraic property and erasure-coded data, and determine how to conventionally support dynamic operation on data blocks, while maintaining the storage correctness assurance at the same level. In order to save the time, computation resources, and even the related users online burden, we also provide the proposed the extension main scheme is used to support third-party auditing, where users can carefully delegate the integrity analyzing tasks to third-party auditors (TPA) and be care-free to use the cloud storage services.

. Lan Zhou,Vijay Varadharajan,and Michael Hitchens [12] To protect the data stored privacy in cloud is using access controls. In this context, role-based access control (RBAC) is a well-known access control model which can simplify security management specifically in large-scale systems. In RBAC, roles are used to associate users with

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. 3, Issue 12, December 2015

permissions on resources. In a cloud data storage system, the data owners would wish to specify the policies as to who can access their data and the cloud providers have required to correctly enforce the policies which specifies data owners. In order to enforce the fulfilled access control policies before putting the data onto the cloud, the data owners can encrypt the data in the way that only users that the owners wished to allow as specified in the access control policies can decrypt and access the data. It is specifically addresses the security issue of RBAC in cloud systems and proposes a modern scheme called Role-based Encryption (RBE). It is benefit noting that the RBAC system security using one of these schemes for supporting the assumption that the authorized users and roles behave in a trusted manner so they do not crack the RBAC policies. However, in a cloud storage system that uses RBAC to control the access to the data, an authorized user of the system may leak the data in the cloud to unauthorized users; or an authorized user may be prevented from accessing the role permissions that have been assigning legitimately to the user by the system malicious administrator. Such issues rely on trust aspects in these systems. These are mainly focus on trust models for using cryptographic RBAC schemes so as to secure data storage in cloud storage systems.

Jun Feng, Yu Chen, Wei-Shinn Ku, Zhou SuD- [13] propose a DOG (Data Division and Out-of-order keystream Generation), a large performance hardware implementation oriented stream cipher for distributed storage network. The D-DOG creates cipher blocks by splitting the plaintext data into multiple blocks and encrypting them, where the key-stream is generated by abstracting bits from the data blocks in a pseudo random out of- order manner. The D-DOG avoids one of the weaknesses actual in modern stream ciphers appear from the fixed length initialization vector (IV). Treating the data block as a binary stream, D-DOG generates the key-stream by extracting n bits from the plaintext in a pseudorandom manner. The key-stream length n is flexible and perhaps set according to different specific security requirements. The variable length key-stream makes brute force attacks much more difficult. And the pseudo random bit abstracting makes decrypted data stream still unrecognizable unless the key-stream bits are inserted back to the original position.

III. PROPOSED METHODOLOGY AND DISCUSSION

When data owner wants to send file on cloud server, first file is dividing into fragments and then fragments are encrypted. These encrypted fragments are then sending to cloud server. These fragments are then allocated using T-coloring concept of graph on cloud server. To maintain integrity we are using the Third Party Auditor (TPA) which makes the stored file audit report on cloud and sent audit report to the data owner by mail. If the file have modified by attacker then TPA sends audit report as modified file to data owner and Proxy Agent which replace the modified code with original contents. The proposed system based on the following model:

1. Splitting and Merging Module,
2. Encryption with block generation,
3. Decryption,
4. Fragment Allocation,
5. Third Party Auditor and
6. Proxy Agent.

IV. CONCLUSION

We propose a methodology which deals with cloud storage security and optimal performance in terms of retrieval time. Before uploading file we are fragmenting that file into multiple fragments and allocate that fragments using T-coloring technique in cloud. This provides security at client level as well as in network level. The fragmentation and dispersal ensured that no significant information was obtainable by an adversary in case of a successful attack. No node in the cloud, stored more than a single fragment of the same file. To protect the original data privacy against the TPA, we randomize the coefficients in the beginning rather than applying the blind technique during the auditing process. Considering that the data owner cannot always stay online in practice, in order to keep the

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. 3, Issue 12, December 2015

storage available and verifiable after a malicious corruption, we introduce a semi-trusted proxy into the system model and provide a privilege for the proxy to handle the reparation of the coded blocks and authenticators.

REFERENCES

1. Mazhar Al, Kashif Bilal, Samee U. Khan, BharadwajVeeravalli, Keqin Li, Albert Y. Zomaya "DROPS: Division and Replication of Data inCloud for Optimal Performance and Security" DOI 10.1109/TCC.2015.2400460, IEEE Transactions on Cloud Computing
2. Frederick R. Carlson Saint Petersburg College Saint Petersburg, Florida 352-586-2621 "Security Analysis of Cloud Computing "fcarlson@ieee.org
3. K.L.NEELA et al. "A Survey on Security Issues and Vulnerabilities on Cloud Computing"International Journal of Computer Science & Engineering Technology (IJCSET)
4. MukeshSinghal and Santosh Chandrasekhar, Tingjian Ge, Ravi Sandhu and Ram Krishnan, Gail-JoonAhn, Elisa Bertino," Collaboration in Multicloud Computing Environments: Framework and Security Issues IEEE Transactions on Cloud Computing VOL:46 NO:2 YEAR 2013
5. Po-Wen Chi and Chin-Laung Lei," Audit-Free Cloud Storage via Deniable Attribute-based Encryption" DOI 10.1109/TCC.2015.2424882, IEEE Transactions on Cloud Computing
6. Harpreet Singh, Er. Gagandeep Singh, ErMandeep Singh, "Securing Data Storage on Public Cloud by Encryption Based 2-Way Authentication" Volume 4, Issue 5, May 2014 ISSN: 2277 128X -International Journal of Advanced Research in Computer Science and Software Engineering
7. Jian Liu, Kun Huang, Hong Rong, Huimei Wang, and Ming Xian "Privacy-Preserving Public Auditing for Regenerating-Code-Based Cloud Storage" , IEEE Transactions on Information Forensics and Security, VOL. 10, NO. 7, JULY 2015
8. Vaibhav Jain Mr. Varun Sharma "Surveying and Analyzing Security challenges and Privacy in Cloud Computing" IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555 Vol. 3, No.5, October 2013.
9. Alessandro Mei, Luigi V. Mancini, and SushilJajodia "Secure Dynamic Fragment and Replica Allocation in Large-Scale Distributed File Systems" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 14, NO. 9, SEPTEMBER 2003
10. Boyang Wang, Baochun Li and Hui Li "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud" IEEE 5TH INTERNATIONAL CONFERENCE ON CLOUD COMPUTING YEAR 2014
11. Cong Wang, Student Member, IEEE, Qian Wang, Student Member, IEEE, Kui Ren, Senior Member, IEEE, Ning Cao, and Wenjing Lou, Senior Member, IEEE, "Toward Secure and Dependable Storage Services in Cloud Computing" IEEE TRANSACTIONS ON SERVICES COMPUTING, VOL. 5, NO. 2, APRIL-JUNE 2012.
12. LanZhou,VijayVaradharajan,and Michael Hitchens "Trust Enhanced Cryptographic Role-based Access Control for Secure Cloud Data Storage" DOI 10.1109/TIFS.2015.2455952, IEEE Transactions on Information Forensics and Security.
13. Jun Feng, Yu Chen, Wei-Shinn Ku, Zhou Su "D-DOG: Securing Sensitive Data in Distributed Storage Space by Data Division and Out-of-order keystream Generation" IEEE Communications Society subject matter experts for publication in the IEEE ICC 2010 proceedings.