International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 4, 2016. ISSN: 2348-6600
Reference ID: IJCS-132 PAGE NO: 778-782

A Review on Achieving Security by Fragmentation and Replication of Data in Large-Scale Distributed File Systems

Dr.V.Jayaraj[1], Assistant Professor,
School of CSE & Applications, Bharathidasan University ,Trichy

S.Shakila Banu[2]
Research Scholar , Bharathidasan University Trichy

***Abstract*—** Outsourcing data to a third-party administrative control, as is done in cloud computing, gives rise to security concerns. The data compromise may occur due to attacks by other users and nodes within the cloud. Therefore, high security measures are required to protect data within the cloud. However, the employed security strategy must also take into account the optimization of the data retrieval time. In this paper, we propose Division and Replication of Data in the Cloud for Optimal Performance and Security (DROPS) that collectively approaches the security and performance issues. In the DROPS methodology, we divide a file into fragments, and replicate the fragmented data over the cloud nodes. Each of the nodes stores only a single fragment of a particular data file that ensures that even in case of a successful attack, no meaningful information is revealed to the attacker. Moreover, the nodes storing the fragments, are separated with certain distance by means of graph T-coloring to prohibit an attacker of guessing the locations of the fragments. Furthermore, the DROPS methodology does not rely on the traditional cryptographic techniques for the data security; thereby relieving the system of computationally expensive methodologies.

Keywords: Centrality, cloud security, fragmentation, replication, performance.

1 INTRODUCTION

Security is one of the most crucial aspects among those the wide-spread adoption of cloud computing [14, 19]. Cloud security issues sustained due to the core technology implementation as like virtual machine (VM) escape or session riding, etc. The service offerings by cloud as structured query language injection or weak authentication schemes and cloud characteristics like data recovery vulnerability and Internet protocol vulnerability, etc.) To secure cloud all of the participating entities must be secure. In a cloud the security of the assets does not solely depend on an individual's security measures because In any given system with multiple units, the highest level of the systems security is equal to the security level of the weakest entity [12] [5] and so the neighboring entities may provide an opportunity to an attacker .The off-site data storage cloud utility requires users to move data in cloud's virtualized and shared environment that may result in various security concerns. The Pooling and elasticity of a cloud allows the physical resources to be shared among many users [22]. Shared resources may be

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 4, 2016. ISSN: 2348-6600
Reference ID: IJCS-132 PAGE NO: 778-782

reassigned to other users at some instance of time that may result in data compromise through data recovery methodologies [2].The data [9]. Similarly, cross-tenant virtualized network access may also compromise data privacy and integrity. Improper media sanitization can also leak customer's private data [5]. The Unauthorized data access by users and processes must be prevented [4]. An any weak entity can put the whole cloud at risk. In such a scenario, the security mechanism must substantially increase an attacker's effort to retrieve a reasonable amount of data even after a successful intrusion in the cloud. The probable amount of loss (as a result of data leakage) present Division and Replication of Data in the Cloud for Optimal Performance and Security (DROPS) that judicially fragments user files into pieces and replicates them at strategic locations within the cloud.

2.RELATED WORK

The employed security strategy must also take into account the optimization of the data retrieval time. Division and Replication of Data in the Cloud for Optimal Performance and Security (DROPS) that collectively approaches the security and performance issues. The DROPS methodology divides a file into fragments, and replicate the fragmented data over the cloud nodes. Each of the nodes stores only a single fragment of a particular data file that ensures that even in case of a successful attack, no meaningful information is revealed to the attacker. Moreover, the nodes storing the fragments are separated with certain distance by means of graph T-colouring to prohibit an attacker of guessing the locations of the fragments.

1. A Hybrid Cloud Approach for Secure Authorized Replication[1] From This Paper we Referred-

In the proposed system we are achieving the data replication by providing the proof of data by the data owner. This proof is used at the time of uploading of the file. Each file uploaded to the cloud is also bounded by a set of privileges to specify which kind of users is allowed to perform the duplicate check and access the files. New replication constructions supporting authorized duplicate check in hybrid cloud architecture in which the duplicate check tokens of files are generated by the private cloud server with private keys. Proposed system includes proof of
data owner so it will help to implement better security issues in cloud computing.

2. Secured Authorized De duplication Based Hybrid Cloud Approach [2] From This Paper we Referred-

Convergent encryption provides data confidentiality in de-duplication. A user derives a convergent key from each original data copy and encrypts the data copy with the convergent key. In addition, the user also derives a tag for the data copy, such that the tag will be used to detect duplicates. To detect duplicates, the user first sends the tag to the server side to check if the identical copy has been already stored. Both the convergent key and the tag are independently derived, and the tag cannot be used to deduce the convergent key and compromise data confidentiality. Authorized data replication was proposed to protect the data security by including differential privileges of users in the duplicate check several new de-duplication constructions that support in authorized duplicate check in hybrid cloud architecture.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 4, 2016. ISSN: 2348-6600
Reference ID: IJCS-132 PAGE NO: 778-782

3. Implementation Replication System wi th Authorized Users [3] From This Paper we Referred-

This paper represents that, many techniques are using for the elimination of duplicate copies of repeating data, from those techniques, one of the important data compression technique is data duplication. Many advantages with this data duplication, mainly it will reduce the amount of storage space and save the bandwidth when using in cloud storage. To protect confidentiality of the sensitive data while supporting replication data is encrypted by the proposed convergent encryption technique before out sourcing. Problems authorized data duplication formally. Addressed by the first attempt of this paper for better protection of data security. This is different from the traditional Duplication systems. The differential privileges of users are further considered in duplicate check besides the data itself. In hybrid cloud architecture authorized duplicate check supported by several new duplication constructions. Based on the definitions specified in the proposed security model, our scheme is secure. Proof of the concept implemented in this paper by conducting test -bed experiments. A Client program is used to model the data users to carry out the file upload process. A Private Server program is used to model the private cloud which manages the private key and handles the file token computation. A Storage Server program issued to store and de -duplicates files.

The Client provides the function calls to support token generation and replication along the file upload process. We observed that the in format ion to Check replication and upload the files, Fetching the Signs using Hashing Algorithm, Checking for Duplication, file uploading, file downloading and attacker trying to attack(block) the cloud.

4. Location-aware type ahead search on spatial databases: emetics and efficiency [4] From This Paper we Referred-

Users often search spatial databases like yellow page data using keywords to and businesses near their current location. Such searches are increasingly being performed from mobile devices. Typing the entire query is cumbersome and prone to errors, especially from mobile phones. We address this problem by introducing type-ahead search functionality on spatial databases. Like keyword search on spatial data, type-ahead search needs to be location-aware, i.e., with every letter being typed, it needs to return spatial objects whose names (or descriptions) are valid completions of the query string typed so far, and which rank highest in terms of proximity to the user's location and other static scores. Existing solutions for type-ahead search cannot be used directly as they are not location-aware. We show that a straight-forward combination of existing techniques for performing type-ahead search with those for performing proximity search perform poorly. We propose a formal model for query processing cost and develop novel techniques that optimize that cost. Our empirical evaluations on real and synthetic datasets demonstrate the effectiveness of our techniques. To the best of our knowledge, this is the rest work on location-aware type-ahead search.

5. A Secured and Authorized Data Replication with Public Audi ting [5] From This Paper we Referred-

This paper studies private data replication technique for cloud storages. Intuitively, a private data replication protocol

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 4, 2016. ISSN: 2348-6600
Reference ID: IJCS-132 PAGE NO: 778-782

allows a client who holds a private data proves to a server who holds a summary string of the data that he/she is the owner of that data without revealing further information to the server. The proposed private data replication protocol is provably secure in the simulation based framework ass uming that the underlying hash function is collision resilient ,the discrete logarithm is hard and the erasure coding algorithm E can erasure up to fraction of the bits in the presence of malicious adversaries.

Drops Overview:

The DROPS methodology proposes not to store the entire file at a single node. The DROPS methodology fragments the file and makes use of the cloud for replication. The fragments are distributed such that no node in a cloud holds more than a single fragment, so that even in a successful attack on the node leaks no significant information. The DROPS methodology uses controlled replication. Each of the fragments is replicated only once in the cloud to improve the security. Although, the controlled replication does not improve the retrieval time to the level of full-scale replication, it significantly improves the security. In the DROPS methodology, user sends the data file to cloud. Upon receiving the file the cloud manager (a user facing server in the cloud that entertains user's requests) performs: (1) Fragmentation, (2) Nodes selection and stores one fragment over each of the selected node, and (c) Nodes selection for fragments replication. The cloud manager keeps record of the fragment placement and is assumed to be a secure entity

GOALS AND OBJECTIVE

Goals:

The division of a file into fragments is performed based on a given user criteria such that the individual fragments do not contain any meaningful information. Each of the cloud nodes ; we use the term node to represent computing, storage, physical, and virtual machines; contains a distinct fragment to increase the data security. A successful attack on a single node must not reveal the locations of other fragments within the cloud. To keep an attacker uncertain about the locations of the file fragments and to further improve the security, we select the nodes in a manner that they are not adjacent and are at certain distance from each other. The node separation is ensured by the means of the T-coloring.

Scope: The data owners lose the control over their sensit ive data once the latter is outsourced to a remote CSP which may not be trustworthy. This lack of control raises new formidable and challenging tasks related to data confidentiality and in- tegrity protection in cloud computing. Customers require that their data remain secure over the CSP. Also, they need to have a strong evidence that the cloud servers still 2 possess the data and it is not being tampered with orpartially deleted over time, especially because the internal operation details of the CSP may not be known to cloud customers. Encrypting sensitive data before outsourcing to remote servers can handle. The employed security strategy must also take into account the optimization of the data retrieval time. Division and Replication of Data in the Cloud for Optimal Performance and Security (DROPS) that collectively approaches the security and performance issues. The DROPS methodology divide a file into fragments, and replicate the fragmented data over the cloud nodes. Each of the nodes stores only a single fragment of a particular data file that ensures that even in case of a successful attack, no meaningful informat ion is revealed to the attacker. Moreover, the nodes

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 4, 2016. ISSN: 2348-6600
Reference ID: IJCS-132 PAGE NO: 778-782

storing the fragments are separated with certain distance by means of graph T-colouring to prohibit an attacker of guessing the locations of the fragments.

Conclusion:

In the proposed methodology, a cloud hosting and storage security scheme that collectively deals with the security and performance in terms of retrieval time. The data file was fragmented and the fragments are dispersed over multiple nodes. The nodes were separated by means of T-coloring. 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.

References

1. Jin Li, Yan Kit Li, Xiaofeng Chen, P atrick P . C. Lee, Wenjing Lou " A HybridCloud Approach for Secure Authorized De -duplicat ion" IEEE Transact ions on Paralleland Dist ribut ed Syst ems:PP Year 2014

2. MrVinod B JadhavProf Vinod SWadne Secured Authorized De-duplicat ionBased Hybrid Cloud Approach Int ernat ional Journal of Advanced Research in Comput erScience and Soft ware Engineering

.3. A.Abdul Samadhu, J.Rambabu, R.Pradeep Kumar, R.Santhya Det ailedInvest igat ion on a Hybrid Cloud Approach for Secure Aut horized Deduplication Internat ionalJournal for Research in Applied Science and Engineering Technology(IJRASET)

4. S. B. Roy and K. Chakrabart i, " Locat ion-aware type ahead search on spat ial databases: Emant ics and efficiency," in Proc.ACM SIGMOD Int . Conf. Manage. Dat a, 2011, pp. 361–37..

5. JadapalliNandini, RamireddyNavat eja Reddy Implement at ion De-duplicat ion Syst em wit h Aut horized Users Int ernat ional Research Journal of Engineering and Technology (IRJET).

6. Mazhar Ali, St udent Member, IEEE, Kashif Bilal, " Division and Replicat ion of Data in Cloud for Optimal Performance and Security" IEEE Transact ions on Cloud Comput ing

AUTHORS PROFILE

Authors Profile with photo's …

Author 1

Dr.V.Jayaraj[1], Assistant Professor,
School of CSE & Applications,
Bharathidasan University ,Trichy.

Authors Profile with photo's …

Author 2

S.Shakila Banu[2]
Research Scholar , Bharathidasan University Trichy.