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

A High Security Authentication System for Hybrid Cloud storage with Deduplication Approach

Muhanad Jabar Yaser
**Department of Computer Science,
Shatrah Technical Institute, South Technical University, Iraq.**

Jamal Mhawesh Challab
**Department of Computer Science,
Directorate General of Education Thi-Qar, Iraq.**

Abstract:

Data deduplication is widely used in cloud computing to eliminate the redundant data storage with intelligent compression process. Hybrid cloud is composed with the private cloud and public cloud utilization. The latest trends of cloud storage are enriched with the end-to-end encryption mechanism. Combining deduplication process with end-to-end encryption mechanism are costly. Providing semantic security with cost effectiveness is the high task for the research scholars. In this paper a high security authentication mechanism is introduced in association with the deduplication process in Hybrid Cloud Storage. In this paper we proposed a prototype model to show the intelligent compression with high security authentication system for performing any storage operations. The experimental results have replicated the concept of providing security and duplicate check scheme while storing in the Hybrid Cloud.

Key words:

Security Authentication, Hybrid Cloud, deduplication process, confidentiality.

Introduction:

Cloud computing storage has encountered many problems and attacks from the cyber criminals. Deduplication is one of the modest methods suggested for storage of cloud computing. Deduplication is a process to identify the duplicate records to be stored in the cloud computing. Hybrid cloud computing is configured with the multi-user storage systems to support increasing demand from the cloud consumers [1].

The remote storage mechanism should be configured with the security mechanism to prevent the attacks and eavesdropping. By its virtue Cloud computing is enriched with the virtualization mechanism. It is enriched with the security storage with user authentication. When the storage is enriched with increased data storage from different users with high volume of data, the stored data has to be shared by multi-users with possible security authentication mechanism. The stored data should be embedded with access rights mechanism with specific privileges. Granting the privileges is not a problem but the data growth incessantly in the cloud computing is a challenging issue to provide the privileges to the new data time to time deposited into the cloud storage centers.

Intelligent Compression process gives much benefits for storage mechanism with automatic encryption and storage process. The essential process should be configured with digital encryption process, deduplication and user authentication with specific privileges would be a costly process [2]. The proposed proof of concept is need to be configured with an architecture to facilitate the increased security, user authentication mechanism and deduplication process for digitally encrypted documents for cloud storage. The proposed architecture should support all types of privileges to the user on the stored data.

Cite this article as: Muhanad Jabar Yaser & Jamal Mhawesh Challab, "A High Security Authentication System for Hybrid Cloud storage with Deduplication Approach", International Journal & Magazine of Engineering, Technology, Management and Research, Volume 5, Issue 3, 2018, Page 93-98.

Related work:

Cloud computing is providing predominantly the security and privileges with the deduplication process with the help of virtualization process. The previous research works have suggested deduplication process for the cloud storage. The deduplication process suggested in the previous papers have suggested the convergent encryption to provide the confidentiality by generating a convergent key. The previous research papers have emphasized the need of deduplication process to ensure the storage saving without duplication and redundancy in cloud computing. [3]
Cloud computing has three entities. These are Cloud Service Providers (CSPs), Cloud Service Consumers (CSCs) and Cloud Users (CU). Cloud service providers facilitate the services in cloud computing. [4] The Cloud Service Consumers will utilize the services and own the data of their own. Cloud users are the customers or related to cloud service consumers. The cloud users will access the data and view the data. The cloud service consumers will be storing the sensitive data. The cloud service consumers will update the data and delete the data.

The data storage and manipulation rights will be reserved to only cloud consumers. The cloud users will access the data. They will not be probably authorised to do any manipulation in the data storage. The data access and modification privileges will be given to only cloud consumers according to their hierarchy. [5] Data accessing privileges will be granting to the cloud consumers. The data accessing privileges will be given by the administrator of the cloud service consumers. The cloud service providers will be facilitating different services to the cloud consumers. The services are namely Software as a service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). [6] To store the data in the cloud computing the data centers will be provided by the Cloud Service Providers. These data centers are located at unknown locations. This is the reason that the high level security is demanded in cloud computing.

The increased demand over cloud computing has created overwhelming popularity to use the services of cloud computing. The cloud servers could be used by the cloud service consumers at higher rate. Different users of the cloud service providers will be storing the data. The storage of data may have redundancy. The save the space of the cloud computing the redundant data has to be eliminated. The elimination of redundant data should be incorporated with the deduplication process.

Proposed work:

The proposed work is incorporating the redundant data in cloud storage. At the same time the user data access privileges should be well defined according to the necessity and priority. The data security should also predominant point to be considered in storing the data.
The proposed work should be developed with a security architecture to provide the deduplication process and user privileges granting mechanism in accordance with the user needs.

It is a cloud storage so that the data stored should be converted into encrypted format. The proposed cloud storage is designed for a Hybrid cloud computing environment. Hybrid cloud environment is rich with private cloud and public cloud. The data owner is considered as an Administrator. The other users of the cloud service consumer should be granted with permissions to store the data, modify the data with their operations. Granting and revoking of the permissions should be reserved for administrator. The users should request for permissions and the granting of the permissions may be given or not. The proposed work is a simulation work developed with the application development tool. The proposed prototype should demonstrate the data storage, data encryption mechanism, deduplication process and user privileges granting and revocation process. The proposed prototype should demonstrate the data storage in the hybrid cloud computing servers and demonstrate the user’s activities with the data storage and other operations.

The proposed work should demonstrate the private cloud storage and public cloud storage mechanism. The private cloud storage can provide the user privileges to store the data. The public cloud storage should be incorporated with the digital encryption standards. The private keys generations and granting of privileges by the administrator should be reserved for private cloud. The stored data in private cloud will be shared by the public cloud and time to time it will be retrieved and computed according to the requests of the users.

Basic Security with DES:

The data stored in the public cloud should be encrypted. The digital encryption standards applied to the data should meet the symmetric encryption standards. The symmetric encryption will generate a secret key. To encrypt the data key generation algorithms should be incorporated. The symmetric encryption algorithm will generate the secret key k it will bestored in the cypher text. When it is decrypted automatically the secrete key will be used by the encryption algorithms and convert the encrypted text into original format. In this process Convergent encryption is used to facilitate the data confidentiality in deduplication. Convergent encryption is a process associated with the deduplication as well as encryption mechanism. [7]

Methodology:

The private cloud and public cloud are two concepts involved in the methodology. The user will get the privileges to store the data into the private cloud. When the user is storing data it will be uploaded to the public cloud. The data uploaded into public cloud will be converted into encrypted format by the encrypted algorithms. While encrypting the data by encryption algorithms the secrete key will be generated. The generated secret key will be stored in the private cloud. The encryption algorithms are associated with the deduplication process. Deduplication process will check the redundancy of the uploaded document before it is encrypted. If the document is present in cloud computing data center, it will be rejected for upload. If the document is not present in the data center it will accept for store it in the data center of the public cloud. The proposed methodology will allow the administrator to grant the permissions to the users who are trying to upload the documents into the public cloud. Granting of the permissions and revoking the permissions will be reserved for the administrator. [8]

System Architecture:

The system architecture is enriched with the public cloud and private cloud architecture. The architecture is also enriched with security implementations and granting of permissions to the users. The hybrid cloud computing architecture is for Cloud Service Providers (CSP). The deduplication process should be incorporated to the system architecture. The system architecture should be enriched with the security implementations and user authentication permissions granting and revocation processes. The system architecture should have disaster recovery process and backup procedures. The storage space will be reduced with these backup and recovery process. The system architecture should be incorporated with the authorized duplicate check.

The system architecture should be incorporated with differential authorization mechanism to perform the duplicate check in the public cloud servers. [9] The system architecture should be embedded with unforgeability of file token and duplicate check token in the private cloud server. The system architecture should check the indistinguishability of file check and duplicate file check. Data confidentiality is predominantly configured in the proposed system architecture. The proposed system architecture should be a blend of deduplication process, user authentication mechanism and security incorporation. The proposed system architecture should be demonstrated in prototype application.[10]

Security incorporation:

The security implementation should cover the deduplication process and user authentication mechanism. The security check has to be done for duplicate check in the public cloud for the redundancy of the files. The duplicate check token has to be raised by the system if the duplicate file is found. Let's assume file 'p' is uploaded into public cloud server. The security check should be done for the files available in the public cloud for file 'p'. if the file 'p' is found in public cloud server the token should be raised and stored in the private cloud that the file is already exist.

The security check should be implemented for every file that are uploaded by the users to public cloud servers. The security mechanism should ensure the file doesn't have any adversaries. The security check should implemented not only for public cloud servers as well as for private cloud server for any adversaries. Every file uploaded by the users should be checked for virus traces and virus code proximity. If the file is traced with virus code then it should be stopped for uploading into the servers. It should be sent quarantined and the user access should be blocked. The time of upload and place from where it has been uploaded should be recorded for audit purposes.

Security implementation is essentially important to the Hybrid cloud operations while storing the file systems into the private cloud and public cloud. Private cloud storage is meant for storing the secrete keys and authentication and authorization information of the users. The public cloud is playing predominant role in storing the user documents in the data centers. The data should be throughrouly checked and then only it should be checked for deduplication process. [11]

Results:

The results have been obtained from different files upload into the public cloud servers. The uploaded file is converted into encrypted format and generated a security key.

The deduplication method is checked with the storage blocks of the public cloud server and the redundancy process is checked to avoid duplicate file storage into the public cloud server. We experimented the results of user authentication system. The user will have to have the permission to upload the file. If the option is not available the user has to send the request to the administrator to grant the permissions to upload the file. The administrator will grant the permissions to upload the files. Then the user will have to send the request to modify the file. The administrator will provide the grants to update the file. Then the system will allow the user to update the file by the user corrections and deletions of part of the file. The granting and revocation of access rights will be reserved to the administrator only.

The file is uploaded by the user into the data centers of the cloud computing. The uploaded file should be checked with the deduplication and then it will be converted into the encrypted format. The key should be stored in the private cloud storage folder. Once the deduplication process is completed the file system should store the data in the public cloud servers in encrypted format. Whenever the user wants to do some modifications the file should be decrypted by using the secret key accessed from the private cloud and decrypt the file format into normal and original format. The use should be facilitated to do the modifications in the file and upload the file into the server. The public server storage should always check the deduplication and convert the file into encrypted format and generate the public key and store the same in the private cloud.

Results evaluation:

The experimental results have demonstrated the process of the uploading and other user operations in the prototyping at the same time the user permissions have been granted by the administrator. The granting and revoking permissions have been demonstrated in the prototyping. The important functionalities like deduplications, digital encryption storage and user granting permissions and revocation of permissions have been demonstrated properly.

Conclusion:

The proposed a prototype model to show the intelligent compression with high security authentication system for performing any storage operations. The hybrid cloud computing operations have been implemented successfully with the private cloud and public cloud storage with user authentication, security implementations and deduplication check within the framework developed for this operations. The project is developed on the basis of deduplication method in association with the security implementation and user authentication methods of hybrid cloud operations by different users. The experimental results have replicated the concept of providing security and duplicate check scheme while storing in the Hybrid Cloud.

Future Enhancements:

The future enhancements of this project are need to be implemented in Azure cloud computing with possible security operations and deduplication process. Actually in Azure cloud computing the security operations are pre-defined and well tested to restrict the vulnerabilities. The future enhancement of this project should demonstrate the real private cloud operations and real public cloud operations in azure cloud computing space.

References:

[1] Jin Li, Yan Kit Li, Xiaofeng Chen, Patrick P. C. Lee, Wenjing Lou (2016) A Hybrid Cloud Approach for Secure Authorized Deduplication published in IEEE Transactions on Parallel and Distributed Systems.

[2] Golthi Tharunn, Gowtham Kommineni, Sarpella Sasank Varma, Akash Singh Verma (2015) Data Deduplication in Cloud Storage published in International Journal of Advanced Engineering and Global Technology I Vol-03, Issue-08, August 2015.

[3] Jan Stanek, Alessandro Sorniotti, Elli Androulaki, and Lukas Kencl() A Secure Data Deduplication Scheme for Cloud Storage work supported by Czech Technical University in Prague, grant No. SGS13/139/OHK3/2T/13.

[4] Jadapalli Nandini, Ramireddy Navateja Reddy (2015) Implementation Of Hybrid Cloud Approach For Secure Authorized Deduplication published in International Research Journal of Engineering and Technology (IRJET) Volume: 02 Issue: 03 | June-2015.

[5] G.Prashanthi, Z.Shobarani (2015) A Hybrid Cloud Approach for Secure Authorized Deduplication International Journal of Innovative Research in Computer and Communication Engineering An ISO 3297: 2007 Certified Organization Vol.3, Special Issue 4, April 2015.

[6] Jagadish , Dr.Suvarna Nandyal (2013) A Hybrid Cloud Approach for Secure Authorized Deduplication published in International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064.

[7] Celina George (2015) Efficient Secure Authorized Deduplication in Hybrid Cloud using OAuth published in International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 3, March 2015.

[8] M. Bellare, S. Keelveedhi, and T. Ristenpart (2013) Dupless:Server aided encryption for deduplicated storage.

[9] M. W. Storer, K. Greenan, D. D. E. Long, and E. L. (2008) Miller. Secure data deduplication. In Proc. of StorageSS published in IEEE 2008.

[10] K. Zhang, X. Zhou, Y. Chen, X.Wang, and Y. Ruan.(2011)Sedic: privacy aware data intensive computing on hybrid clouds. In Proceedings of the 18th ACM conference on Computer and

communications security,CCS'11, pages 515–526, New York, NY, USA, 2011. ACM.

[11] M. Bellare, S. Keelveedhi, and T. Ristenpart. Dupless: Serveraided encryption for deduplicated storage. In USENIX Security Symposium, 2013.