Accounting and Privacy Preserving of Data Owner in Cloud Storage

A. Mohan, P. Vamshikrishna

Abstract: ***People use the support of distributed computing however can't completely believe the cloud suppliers to have protection and confidential information. To guarantee secrecy, data owners relocate encoded information rather than plain texts. To divide the encoded documents with different clients, Ciphertext-Policy Attribute-based Encryption (CP-ABE) can be utilized. But this cannot become secure against some other assaults. Many other schemes did not gave guarantee that the cloud provider has the power to check whether a downloader can unscramble or not. Consequently, these files are accessible to everybody who is approachable to the cloud storage. An intentionally harmful assailant can download a great many records to start Economic Denial of Sustainability (EDoS) attacks, it will to a great extent expend the cloud asset. The owner will bear all the expenses for the cloud storage but the cloud provider doesn't provide the whole information about the access or usage. There is no transparency for the owner. We have to solve these concerns. In order to this we are going to propose a solution for securing the encrypted data from EDoS attacks and providing the owner whole usage information about the cloud storage. We are implementing by using the arbitrary access policy of CP-ABE.***

Keywords: ***Access control, cloud storage, privacy-preserving***

I. INTRODUCTION

Cloud computing allows us in such a way we can approach the applications in the internet. It permits us to make, arrange, and task the business applications in online. Cloud storage is a model in which data is kept on remote servers accessed from the internet. Cloud computing is the term for the since quite a while ago imagined vision of figuring as the state of being useful. By the increasing demand of the cloud based data services, data owners are influenced to store their huge amount of personal multimedia data files and tasks into remote cloud servers in a way they can protect their data.by using the plentiful capacity and calculation assets for cost minimization and adaptability, the redistributing of information stockpiling and calculation to the cloud raises security and protection problems. Cloud storage has benefits, such as available or operating at all times, a system in which you pay for as service before you use it and cheap. During these years, maximum amount of information are moved operations to public cloud for it's persistence counting private and professional files which brings a trust issue to data owners by which the public cloud isn't trusted, and the information ought not be spilled to the cloud supplier without acceptance from data owners. They largely trust the cloud supplier to shield their touchy information. The cloud suppliers and their Laboure's can peruse any archive despite of the prevailing circumstances of data owner's access policy. The cloud provider can make something larger than the actual resource usage of the document stockpiling and ask the payers more cash without giving exact records, since cloud do not have a framework for obvious count of the asset utilized. Data owners who keep files on cloud servers would like to maintain the access on their own hands and keep the information mystery against the cloud and harmful usage. Encryption is not only sufficient. For the confidentiality purpose information proprietors can scramble the records by which they can put an entrance strategy with the goal that lone approved clients can unscramble the report. Cloud services are usually supplied by some large enterprises like Google, Amazon, Microsoft. They have to maintain better reputation and trust from cloud storage services to their consumers. For organizing a fine-grained information proprietor side access control openly distributed mechanism storage, attribute–based encryption is used. From various ABE schemes CP-ABE is concerned in public cloud storage, in which cipher text is encrypted in an entrance strategy and just clients whose credits fulfill the entrance strategy can only have the permission to decrypt the cipher text. The cryptography method driven does not guarantee the cloud provider against several other attacks. So if the cloud supplier doesn't ensure the entrance control, it can't control the unapproved clients. One form of attack that is begun by this limitation is Distributed Denial of Services. Attribute based encryption is a cryptographic technique. In this technique different attributes are used for the encryption purposes. In CP-ABE scheme, the cipher text encrypts message with the help of access structure while an unscrambling key is related with a lot of traits. The decoding condition is rises to if and just if the characteristic set satisfies the recommended admittance structure [1].

Manuscript received on March 27, 2021.
Revised Manuscript received on April 05, 2021.
Manuscript published on April 30, 2021.
*****Correspondence Author

A.Mohan*, Asst. professor, Department Computer Science and Engineering, CBIT, Hyderabad, Telangana, India. amohan_cse@cbit.ac.in

P.vamshikrishna, PG student, Department Computer Science and Engineering, CBIT, Hyderabad, Telangana, India. perumandlavamshi15@gmail.com

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

II. LITERATURE SURVEY

Architecture and testing challenges in a cloud computing environment. A layered methodology is the fundamental base in the design of the architecture.[2] The basic layer of data center consists of the core cluster and access layers. Researches such as automated service provisioning which is the power of procuring and delivering assets sought after. Virtual machine relocation encourages us to adjust load over the server farm.[2] Server consolidation helps us to max the resource utilization by using less amount of energy usage in the cloud environment. Information Security is an unequivocal component that legitimizes security. Ventures are uncertain to purchase an affirmation of business information security from merchants. They dread of losing the information and the information secrecy of its buyers. In numerous models, the genuine stockpiling area is kept bargained, including onto the security uneasiness of the endeavors. In the present model firewalls present across the data centers are the one's protect the sensitive information. In the present scenario, cloud suppliers are answerable for keeping the information security and the undertakings would need to rely upon them. It is compulsory that both application and data systems expose those standard interfaces. Cloud providers need to able to exchange and make use of information standards so that organizations can combine any cloud providers capabilities into the solutions. Many critical security challenges in a cloud computing environment such as data service outsourcing security in which particular individual and enterprises produce data that must be kept aside and utilized and they are provided to redistribute their unpredictable information to the cloud inferable from its more noteworthy adaptability and cost productivity. In this information encryption is the best approach to secure information protection and battle spontaneous access in the cloud. Access control is another mechanism in which different users has pleasure distinctive access benefits concerning the data.[3] One methodology is to scramble the information in a separated way and reveal the comparing security keys to the main approvedclients.By outsourcing workloads to the cloud, users computational power is no longer limited by their devices. Instead, they can enjoy the clouds literally unlimited computing resources in a pay-per-use manner without committing any large capital better than locally. In a quality-based encryption framework ciphertexts are not really scrambled to one specific client. Rather both the client's private keys and ciphertexts will be related with a lot of qualities or a strategy over at ascribes. A client has the ability to unscramble a ciphertext if there is a correlation exists between his private key and the code text.[5] In this framework pre a limit framework where ciphertexts were doled out to a classification with a lot of properties and a client's private key is associated with an edge boundary k and set of traits.

III. PROPOSED METHODOLOGY

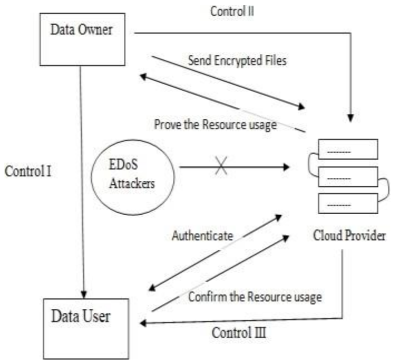

Fig:1 System model

Data owners:

Data owners are the proprietor and distributer of records and pay for the asset utilization on document dispersion. Information proprietors and information overseers ought to have a mutual perspective on the propriety of the different alleviation assaults. These thusly, ought to be examined with officials liable for security.

Data users:

Data users want to obtain some files from the cloud provider stored on the cloud storage. In this the data users that don't fulfill the entrance strategy can't download records. For a data user to download a file from data owner it should be approved by both the data owner and also by the provider.

Cloud provider:

Cloud provider holds the encoded capacity and is always online. It records the resource consumption and charges data owners based on the record. Cloud provider customers access cloud resources through internet and programmatic access and are only billed for resources and services used according to a subscribed payment method.In the below flowchart encryption algorithm is shown in this first we take plain data and we will give secret key. we have to convert that into bytes and after that we need to shift the rows. By the mix sections and include round key we are scrambling the information

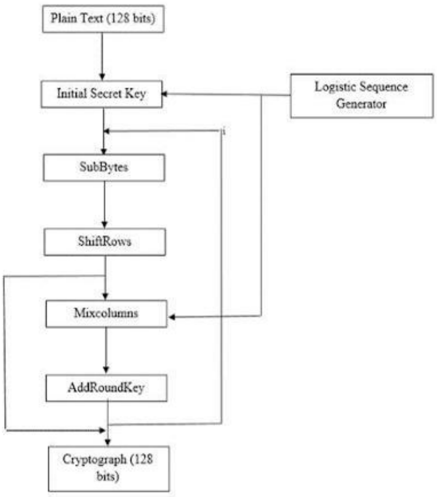

Fig: 2 Advanced encryption standard

IV. IMPLEMENTATION

In this data owner after registering, it needs cloud to accept that data owner. In the same way after registering the data user it also needs to be accepted or authorized by the cloud. Then the data owner has to be upload the text file. Then the data users has to request for the document which is transferred by the information proprietor for downloading. In this information proprietor sends the mystery key for the cloud to approve which file is to be downloaded by the data user. Then the user can download the file. The data owners should be a business person who understands the business impact of a security incident resulting in loss of availability, confidentiality or integrity.

This enables the data owner to make informed decisions on the actions to be taken to mitigate the impact of security occurrence.

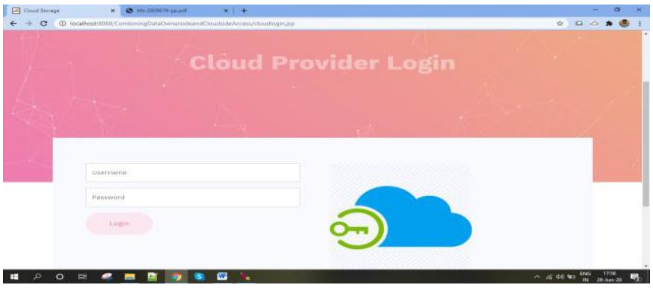
Cloud Storage
localhost:8080/CombiningDataOwnersideandCloudsideAccess/cloudlogin.jsp
Cloud Provider Login
Username
Password
Login

Fig 3. Cloud provider login page

In this cloud authorises and approves theregistering of the information proprietors and information clients so that solitary affirmed clients can login and view their files and for the data users for downloading. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources

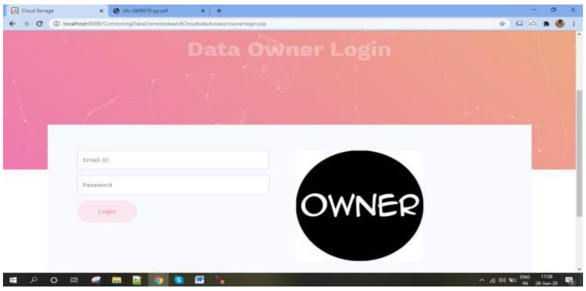

Fig 4. Data owner login page

In this data owner after registering it asks the cloud provider to authorize it so that data owner can upload the files. Data owner is accountable for providing data discarding because more the sensitive data, the more important this becomes

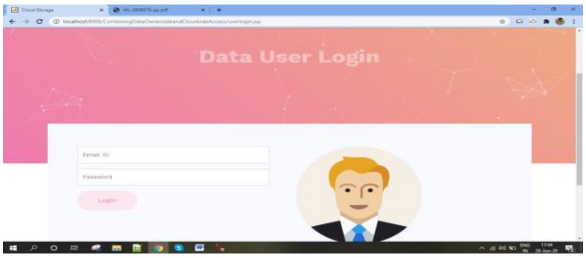

Fig 5. Data user login page

In this data owner after registering it asks the cloud provider to authorize it so that data owner can upload the files. Data owner is accountable for providing data discarding because more the sensitive data, the more important this becomes.

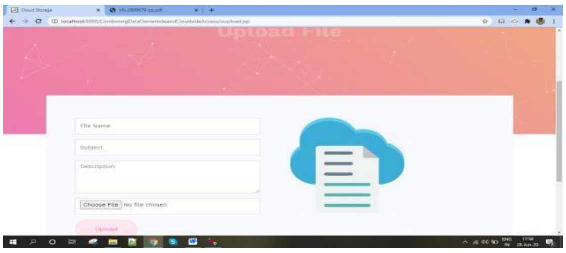

Fig 6. Uploading a file

In this data owner uploads the file which is to be downloaded by the data user after approved by both the cloud provider and data owner which is known as cloud combined access control.

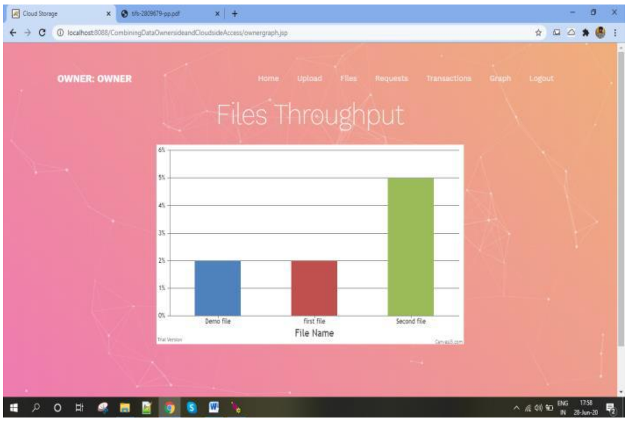

Fig 7. graph file throughput

Thee graph indicates after data owner upload the file which is accepted by the cloud is that how many times the file has been downloaded by the data user. In the above blue colour which indicates a particular use has downloaded demo file two times. In the graph x-axis indicates text file and y-axis number of times the file has been downloaded. The brown colour which indicates first file(name of the file) has been downloaded two times by the data user. The green colour which indicates sec file(name of the file) has been downloaded five times by the data user.

V. CONCLUSION

In this the owners has access control over the data he has uploaded to the cloud. As many cloud providers miss use the files which they have from the owners here without owner permission user cannot download the file.By this cloud combined and information proprietor side access control in encrypted cloud storage is resistant to attacks and provides resource consumption accounting

REFERENCES

1. KaipingXue ,Weikeng Chen, Wei Li, Jianan Hong, and Peilin Hong- "Combining Data Owner-Side and Cloud- Side Access Control for Encrypted Cloud Storage"- IEEE Trans. on Inf. Forensics and Security, vol.13, no. 8, August. 2018.

2. Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: State-of-theart and research challenges," J. internet Services Appl., vol. 1, no. 1, pp. 7–18, 2010.
3. K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," IEEE Internet Comput., vol. 16, no. 1, pp. 69–73, Jan./Feb. 2012.
4. M. H. Sqalli, F. Al-Haidari, and K. Salah, "EDoS-shield—A two-steps mitigation technique against EDoS attacks in cloud computing," in Proc. 4th IEEE Int. Conf. Utility Cloud Comput. (UCC), Dec. 2011, pp. 49–56.
5. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in Proc. IEEE Symp. Security Privacy (SP), May 2007, pp. 321–334.
6. Yang Zhao, Mao Ren,Songquaniang, GuobinZhu,HuXiong," An efficient and revocable storage CP-ABE scheme in the cloud computing." Computing Springer(2019)
7. YingjieXue ,Na Gai, David S.L.Wei, Peilin Hong." "An Attribute-Based Controlled Collaborative Access Control for Public Cloud Storage. IEEE Transactions on Information Forensics and Security,NOV 2019.

AUTHORS PROFILE

A. Mohan, working as a assistant professor ,Dept of CSE, Chaitanya Bharathi institute of technology, Hyderabad. He is pursuing ph.d in JNTUK ,He has done His Masters In Computer Science and Engineering In Chaitanya Bharathi Institute Of Technology,osmain university Hyderabad. He Is Having 9 Years Of Teaching Experience, Publishes various papers in International journal and conferences on Neural network, computer network and data mining. His area of interest cloud computing, Data Mining, Neural Network and Deep learning.

P.Vamshikrishna, Received his M.Tech Degree in computer Science and Engineering from Chaitanya Bharathi institute Of Technology,Osmania university Hyderabad, Telangana.His area of interest is cloud computing, DATA MINING, and Neuralnetwork.

© Copyright: All rights reserved.