International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 06 | June - 2022 Impact Factor: 7.185 ISSN: 2582-3930

SECURE DATA SHARING IN CLOUD

Shekhar Chouhan, final year student MIT WPU, Payal Shelke, Final year student MIT WPU,
Sanket Mahajan, Final year student MIT WPU, and Prof Vinayak Musale, MIT WPU

Abstract—now a days the use of Cloud computing is increasing due to its numerous features such as providing storage ,sharing video,audio content cloud computing can be defined as diiferent service which is uses the internet ,services like storage over a cloud

cloud computing provide different features but now a days security is everyone concern but the majority of cloud platforms fail to provide the solution for this as there primary concern is storage so here we have discuused about the methodolgy about securing data over a cloud

Index Terms—cloud computing, data, security, encryption, decryption, algorithm, sha 5, aes, des, rsa, Cp-Abe

I. Introduction

Cloud computing is the use of computing resources both hardware or software use that are used as a service over a internet The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. These services typically provide access to advanced software applications and high-end networks of server computers.

How does cloud computing work

The goal of cloud computing is to apply traditional super-computing, or high-performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios, to deliver personal-ized information, to provide data storage or to power large, immersive computer games.

The cloud computing uses networks of large groups of servers typically running low-cost consumer PC technology with specialized connections to spread data-processing chores across them. This shared IT infrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing

Characteristics and Services Models:

Self-help where needed: Customer can provide computing power over another, such as server time and network storage, as needed automatically without the need for personal inter-action with each service provider.

Extensive network access: Skills are available through the network and are accessed in standard ways that promote the use of small or thin client platforms (e.g., mobile phones, laptops, and PDAs).

Integration of resources: Computer service providers are integrated to serve multiple consumers using a multi-employer model, with a variety of visual and visual resources that are powerfully allocated and redistributed according to customer needs. Examples of applications include storage, processing, memory, network bandwidth, and virtual machines.

Quick Stretch: Skills can be provided quickly and easily, in some cases automatically, to get out quickly and be released quickly for quick access. For the consumer, the available energy supply usually seems unlimited and can be purchased at any price. at any time.

Limited service: Cloud systems automatically control and improve the use of the app by using the rating capabilities to a certain level appropriate to the type of service (e.g., storage, transparency to both the provider and the consumer of the service used

Benefits

1) Achieve moderate economy - increase volume or pro-ductivity by fewer people. Your costs per unit, project or product are reduced.
2) Reduce spending on technology infrastructure. Maintain easy access to your information using a small advance pay- ment. Pay as you go (weekly, quarterly or annu-ally), as needed.
3) Focus your employees on cheap. People all over the world can access the cloud, as long as they have an internet connection.
4) Adjust processes. work is more with reduced people
5) Monitor projects successfully. Stay within budget and before the time of the completion cycle.
6) Minor staff training is required. It takes a few people to do more work in the cloud, with a little learning curve in hardware and software issues.
7) Limit licensing for new software. Extend and grow without the need to purchase expensive software licenses or programs.

II. Literature survey

By going through various number of reserach paper already published based on cloud computing , encryption decryption algorithms and cryptogrpahic approaches .by going through different research papers we have identified various gaps and try to find there solutions

By reading a lot papers We have made this paper whihc will fullfill the research gap , the drawbacks and the disadvantages of the exisiting system

III. Goal

The aim or the motivation behind the secure data sharing in cloud is the secuirty concern we can easily solve the security concern from this technique as security is one of the weak strength of cloud computing services

we aim to solve this problem by using the approach of cryptography by using different encryption and decryption technique.There are number of encryption decryption tec-niques but we had worked on CP-ABE which is cipher text policy attribute based encryption.

The CP-ABE mainly contains five parts The Certificate Authority

The Attribute Authority The data owners

The Data Consumers The cloud

This algorithm Consist of various steps too starting with public key and master key ,then using client attribute list for details and in the end encryption and decryption.

IV. Proposed system

The cloud computing is mainly used for storing a huge amount of data on its cloud also we can share and download contents from there ,but while downloading the content from cloud there might be a chance to get hacked by hackers and then they can easily use all the data present on the cloud

So we can solve this problem by providing cloud with cryptographic approach ,when ever or whose ever wants to download or access the cloud can use the public or private keys for accessing

In this approach the users can use the cloud for the data download from other cloud user by using there private keys first the data user send a request to data provider that he wants to download that content from the cloud then the data provider will validate the user whether its an authorized or unauthorized user using the private key of the user ,after validation the data provider will give the access to the user ,then the user will see the content on cloud but will not able to download or view ,For that thing the user had to send a request todata provider using his(user) private key then the data provider will encrypt the file and send the decrypt key to the user if the decrypt keys will match to the user private key ,then the user will able to download the content in the encrypted form and then using his private key user can view that content in normal view .This same procedure can be used for uploading the contents also.

V. Implementation

If we talk about the implementation it consist of various parts like user login, authrorisation faculity , data provider, cloud platform, third party server if needed , different crypto-graphic algorithms like cp abe , aes , des and sha algorithm.

MODEL DESCRIPTION

This model contains different parts as stated above

1.User

2.Provider

3.Server

4.Authority

in this propsed system as mentioned above there are 4 different parts which plays import role in implementation

it includes that the user allocates or provide the data to the suer after checking the authentication of the user who want to access data .after validation the user can see the data but in the in crytpic form stored on the cloud server where the cyrptographic algorithms are used in backend so that the algorithm can work properly

In details we can say that in this secure data sharing in cloud the data can be shared in cloud with more security by using the approach of encrytpion and decryption algortihms

.The algorthims can be any type of encyrption decryption algorithm we have workd with CP-ABE and AES algorithm

.Where anyone can use the cloud have access the data if he/she is valid user ,can download the data in encrypted form and can decrypt it using its private key.

The use of cloud computing has been increasing day by day individual in the world now a requirecloud for different func-tion depending on requirements some uses for storage some uses for sharingno doubt The future scope of cloud computing will be very tremendous big IT giants like amazonhad there AWS platformand its demand is increasing similar have there azure and demand of this also . it will keep increasing as the vast features provided by the cloud computing. if its some loopholes or weakness can be corrected or find a for them that will be very beneficial for the cloud computing and its users. one of the weakness of cloud is the securityas discussed above and it can be solved using the approach.

There are vast number of encryption techniques which can be used to provide security to the cloud like there are DES SHA algorithm,MD5 algorithm which can be used

have used the CP ABE algorithm with AES algorithm after comparingusing all the algorithmand in the end these two algorithm provide best result

In the above diagram its the simple implementation of the secure data sharing in cloud using encryption decryption where in diagram

DP is provider which provides the data

CS is the cryptographic server

DU is the data user

AA is the Authority

the sequence will be starting with the 1 then 2 then 3 and finally on 4 according to the diagram the provider which provides the data to other user which are valid uses the cloud server where in back end a specific algorithm which is cp-abe algorithm is present for the encryption and decryption. After that Data user will get the encrypted data and will verify through the authority having the public or private key according to the need.

VI. Comparison

if we analyse the different algorithms in cryptographic approach we will get’

’

TABLE I
Compare

Algorithm	SIZE OF KEY	mainly used
DES	56	securing data
RSA	512-2048	securing large amount of data
CP-ABE	512-4096	securing man application

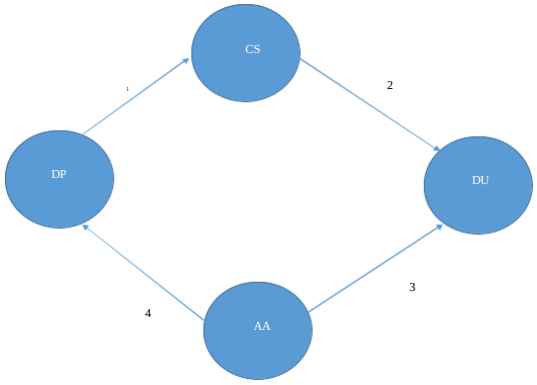

Fig. 1. Simple working of the propsed system

VII. Results

In the end we willl get a proposed sytem where a cloud will have a cryptographic approach which will have all the security concern which were lacking in somewhere in cloud environment and thus making cloud environment one of the best innovation technology existed til now

VIII. Conclusion

The cloud computing had a great features to its users due to its vast features its users getlot of feasibility and reliability. is one the best innovation in the technology field which ha solved many problems from storage to sharing has covered all the majority features due to this its uses had been increased rapidly from the past few years. if it more developed or advanced with time covering its weakness then it can have unstoppable growth. Thus combing it with the different approach can me it more developed specially in case of security., the cloud computing had solved a huge number of problems if it dint exist might be the problems never get solved

IX. Acknowledgement

In the end we will thankyou all the researchers reviewers teachers for there help

REFERENCES:

REFERENCES

[1]Elavarasan G 1 and Veni S2 " Data Sharing Attribute-Based Secure with Efficient Revocation in Cloud Computing 2020 International Conference on Computing and Information Technology, University of Tabuk, Kingdom o f Saudi Arabia. Volume: 01, Issue: ICCIT- 1441, Page No.: 382 - 387, 9th & 10th Sep. 2020."

[2]Dammannagari Nayani Reddy , Suharsha Vom-mina,"Secure Data Sharing in Multi-Clouds International Con- ference on Electrical, Electronics, and Optimization Tech- niques (ICEEOT) - 2016"

[3]Mazhar Ali, Student Member, IEEE, Revathi Dhamoth-aran, Eraj Khan, Samee U. Khan, Senior Member, IEEE, Athanasios V. Vasilakos, Senior Member, IEEE, Keqin Li, Fellow, IEEE, and Albert Y. Zomaya, Fellow, IEEE, "SeDaSC: Secure Data Sharing in Clouds"

[4]M. Nabeel, N. Shang and E. Bertino, "Privacy Preserv-ing Policy Based Content Sharing in Public Clouds," IEEE Transactions on Knowledge and Data Engineering, 2012.

[5]Hanshu Hong, ; Zhixin Sun, (2017). [IEEE 2017 IEEE 2nd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA) - Chengdu, China (2017.4.28-2017.4.30)] 2017 IEEE 2nd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA) - Towards secure data sharing in cloud computing using attribute based proxy re-encryption with keyword search.

[6]Dan Boneh, Ran Canetti, Shai Halevi, and Jonathan Katz. Chosen-ciphertext security from identity-based encryption. Siam Journal on Computing, 36:1301–1328, 2007.

[7]Shweta Agrawal Xavier Boyen Vinod Vaikuntanathan Panagiotis Voulgaris Hoeteck " Fuzzy Identity Based Encryp-tion from Lattices "

[8]LYES TOUATI,

Université de Technologie de Compiègne Compiègne, France " C-CP-ABE: Cooperative Ciphertext Policy Attribute-Based Encryption for the Internet of Things "

[9]Ranjith Balakrishnan Assistant Professor TIF AC-CORE in Pervasive Computing Technologies Velamrnal Engineering College, Surapet "SECURE MULTIOWNER DATA SHAR-ING IN THE CLOUD"

[10]Shani Raj, B. Arunkumar, "Enhanced encryption for light weight data in a multi-cloud system", Distributed and Parallel Databases, 2021

[11]Muthi Reddy P, Manjula S.H., Venugopal K.R."Secure Data Sharing in Cloud Computing : A Comprehensive Re-view," International Journal of Computer, vol.25, no.1,2017

[12]International Journal of Engineering Research in Com-puter Science and Engineering (IJERCSE) Vol 5, Issue 3, March 2018 564 A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing [1] R.Gokula Priya , [2] Unni-maya P Madhu, [3] M.Yuvashree, [4] M.Karthikeyan [1][2][3] Final Year Student, [4] Assistant Professor [1][2][3][4]Depart-ment of Cse, Sengunthar College of Engineering, Tiruchen-

gode