Providing Security in Multi-Cloud Environment with Secure Sharing Over Network

-1* **Anuradha Gaikwad, 2 Prof. Vijay Bagdi**
[1] Department of Wireless Communication and Computing, RTMNU University, AGPCET Nagpur, Maharashtra, India
[2] Assistant Professor Computer Science and Engineering, RTMNU University, AGPCET Nagpur, Maharashtra, India

Abstract:- With the web getting so well-known information sharing and security of individual information has increase a great deal more significance than some time recently. Cloud gives and effective approach to outsource the information either on the web or disconnected yet information security gets to be one of the real issues in untrustworthy cloud environment. The proposed framework addresses the security issues in cloud environment furthermore gives an approach to give better security in cloud environment. The proposed framework utilizes cryptographic symmetric calculation AES with key size of 256 for information encryption and Ultra Zip pressure which gives a pressure proportion up to half contingent upon the document sort. After encryption and pressure the information is splitted into various parts and every part is put away in isolated information server. The proposed work can be utilized as a part of various application like person to person communication destinations and document facilitating sites.

Keywords: *Cloud Computing, IaaS, Encryption, SaaS, PaaS, Distributed, Security, Privacy*

*****

I. INTRODUCTION

Distributed computing is design for giving registering administration through the web on request and pay per utilize access to a pool of shared assets to be specific systems, stockpiling, servers, administrations and applications, without physically getting them. So it spares overseeing expense and time for associations. Numerous enterprises, for example, managing an account, medicinal services and training are moving towards the cloud because of the effectiveness of administrations gave by the compensation per-utilize design in light of the assets, for example, preparing power utilized, exchanges completed, transmission capacity expended, information exchanged, or storage room possessed and so on. The principle issues that are distinguished out in cloud IaaS administrations are load adjusting in servers and information security gave to capacity frameworks.

1.1 CLOUD BASICS

Cloud computing, or "the cloud", concentrates on expanding the viability of the imparted assets. Cloud assets are typically imparted by numerous clients as well as progressively reallocated for every interest and pay for every utilization premise. This can work for dispensing assets to clients. For instance, a cloud machine that serves Indian clients amid Indian business hours with an application (e.g., email) may reallocate the same assets to serve China clients amid China's business hours with an alternate application (e.g., an application server). This methodology ought to build the utilization of processing power accordingly decreasing ecological harm which are needed for a mixed bag of capacities. With distributed computing, numerous clients can get to a solitary server to recover and access the information without purchasing licenses for diverse applications.

Distributed computing, or "the cloud", focuses on growing the suitability of the bestowed resources. Cloud resources are ordinarily granted by various customers and continuously reallocated for each intrigue and pay for each usage introduce. This can work for apportioning resources for customers. For example, a cloud machine that serves Indian customers in the midst of Indian business hours with an application (e.g., email) may reallocate similar resources for serve China customers in the midst of China's business hours with a substitute application (e.g., an application server). This approach should assemble the usage of preparing force in like manner diminishing environmental mischief which are required for a blended sack of limits. With circulated processing, various customers can get to a singular server to recoup and get to the data without obtaining licenses for differing applications.

1.2 CLOUD SERVICES

A. Software as a Service (SAAS)

Saas clients lease use of employments running inside the Clouds provider base, for example Salesforce. The applications are regularly offered to the clients through the Internet and are regulated absolutely by the Cloud provider. That suggests that the association of these organizations, for instance, redesigning and settling are in the provider’s commitment. The benefit of Saas is that all clients are running similar programming adjustment and new value can be easily organized by the provider and is thusly available to all clients.

B. Platform as a Service (PAAS)

PaaS Cloud suppliers offer an application stage as an administration, for instance Google App Engine. This empowers customers to send custom programming utilizing the devices and programming dialects offered by the supplier. Customers have control over the conveyed applications and environment-related settings. Similarly as with SaaS, the administration of the fundamental base exists in the obligation of the supplier.

C. Infrasturcture as a Service (IAAS)

Iaas passes on fittings resources, for instance, CPU, plate space or framework sections as an organization. These advantages are for the most part passed on as a virtualization organize by the Cloud provider and may be gotten to over the Internet by the client. The client has full control of the virtualized arrange and is not accountable for managing the fundamental base.

D. Storage as a Service

Limit as an organization (Staas) is an arrangement of activity in which a far reaching organization provider rents space in their stockpiling establishment on a participation commence. The economy of scale in the organization provider's structure licenses them to give stockpiling significantly more cost sufficiently than a great many people or associations can give their own specific stockpiling, when total cost of ownership is considered. Limit as a Service is often used to light up offsite support challenges. Faultfinders of limit as an organization indicate the unlimited measure of framework information transmission expected to coordinate their stockpiling utilizing an online organization.

II. BRIEF LITERATURE SURVEY:

There are numerous issues with current cloud and their models. Some of them are clients are frequently tied with one cloud supplier, figuring parts are firmly coupled, absence of SLA backings, absence of Multi-tenure backings, Lack of Flexibility for User Interface. [4]

A standout amongst the most imperative issues identified with cloud security dangers is information trustworthiness. The information put away in the cloud may experience the ill effects of harm amid move operations from or to the distributed storage supplier. Cachinet al. give cases of the danger of assaults from both inside and outside the cloud supplier, for example, the as of late assaulted Red Hat Linux's dispersion servers. Another case of ruptured information happened in 2009 in Google Docs, which set off the Electronic Privacy Information Center for the Federal Trade Commission to open an examination concerning Google's Cloud Computing Services. Another case of a hazard to information respectability as of late happened in Amazon S3 where clients experienced information debasement.

One of the outcomes that they propose is to use a Byzantine imperfection tolerant replication tradition inside the cloud. Hendricks et al. express that this outcome can sidestep data debasement made by a couple parts in the cloud. Of course, Cachinet al. attest that using the Byzantine blemish tolerant replication tradition inside the cloud is unacceptable as a result of the way that the servers having a place with cloud providers use similar system foundations and are physically put in similar spot [1]. According to Garfinkel, an other security danger that may happen with a cloud provider, for instance, the Amazon cloud organization, is a hacked mystery key or data intrusion. If someone accesses an Amazon account mystery key, they will have the ability to get to most of the record's events and resources [1].

Notwithstanding the way that cloud providers are aware of the malignant insider danger, they expect that they have fundamental responses for mollify the issue [1]. Rocha and Correia [1] center possible aggressors for Iaas cloud providers. For delineation, Grosse et al. [1] propose one result is to keep any physical access to the servers. Regardless, Rocha and Correia [1] battle that the aggressors outlined in their work have remote get to and needn't trouble with any physical access to the servers. Grosse et al. [1] propose a substitute result is to screen good to get access to the servers in a cloud where the customer's data is secured. In any case, Rocha and Correia [1] affirm that this part is profitable for watching specialist's direct similarly as whether they are after the security plan of the association or not, nonetheless it is not effective in light of the way that it recognizes the issue after it has happened.

A substitute philosophy to secure circulated figuring is for the data holder to store mixed data in the cloud, and issue unraveling keys to affirmed customers. By then, when a customer is denied, the data administrator will issue re-encryption requests to the cloud to re-scramble the data, to keep the repudiated customer from interpreting the data, and to create new unscrambling keys to generous customers, so they can continue getting to the data. On the other hand, since a dispersed registering environment is included various cloud servers, such summons may not be gotten and executed by most of the cloud servers on account of tricky framework correspondences [3].

A substitute way to deal with secure the data using differing crushing and encryption counts and to disguise its region from the customers that stores and recoups it. The fundamental complexity is that the system presented by Olfa Nasraoui [2] is an application based structure like which will keep running on the clients claim system. This application will allow customers to exchange record of assorted associations with security quirks including Encryption and Compression. The exchanged records may be gotten to from wherever using the application which is given.

The security of the Olfa Nasraoui [2] display has been examination on the commence of their encryption figuring and the key organization. It has been watched that the encryption estimation have their own specific traits; one computation gives security to the detriment of fittings, other is strong however uses more number of keys, one takes furthermore taking care of time. This range exhibits the diverse parameters which accept a central part while selecting the cryptographic estimation. The Algorithm found most ensuring is AES Algorithm with 256 piece key size (256k) [2].

A standard trick of cloud is data advertising. Cheng-Kang Chu, Sherman S. M. Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H. Deng [5] exhibit to securely, viably, and adaptably bestow data to others in circulated stockpiling. We depict new open key cryptosystems which convey relentless size figure messages with the end goal that capable task of unscrambling rights for any arrangement of figure works are possible. The interest is that one can add up to any arrangement of secret keys and make them as minimized as a single key, yet wrapping the compel of each and every one of keys being amassed. Toward the day's end, the puzzle key holder can release a predictable size aggregate key for versatile choices of figure substance set in dispersed stockpiling, however the other encoded reports outside the set remain mystery [5].

There are diverse examination challenges moreover there for grasping dispersed processing, for instance, for the most part directed organization level attestation (SLA), security, interoperability and steadfastness. This examination paper outlines what disseminated processing is, the distinctive cloud models and the rule security risks and issues that are at present inside the dispersed registering industry. This investigation paper moreover explores the key research and troubles that shows in conveyed processing and offers best practices to organization providers furthermore attempts wanting to power cloud organization to upgrade their final product in this genuine budgetary environment [7].

PROPOSED SYSTEM

The proposed work is planned to be carried out in the following manner.

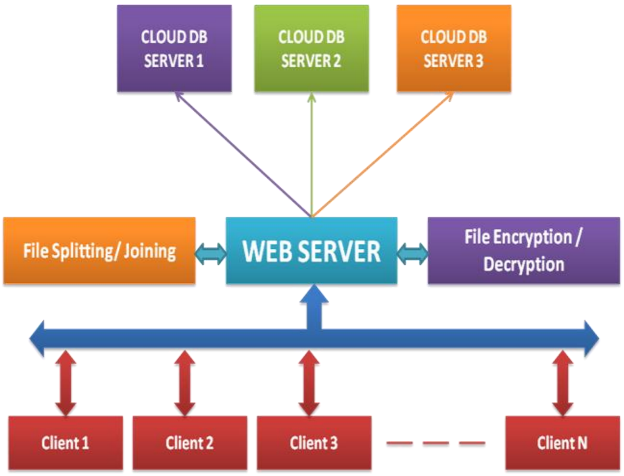
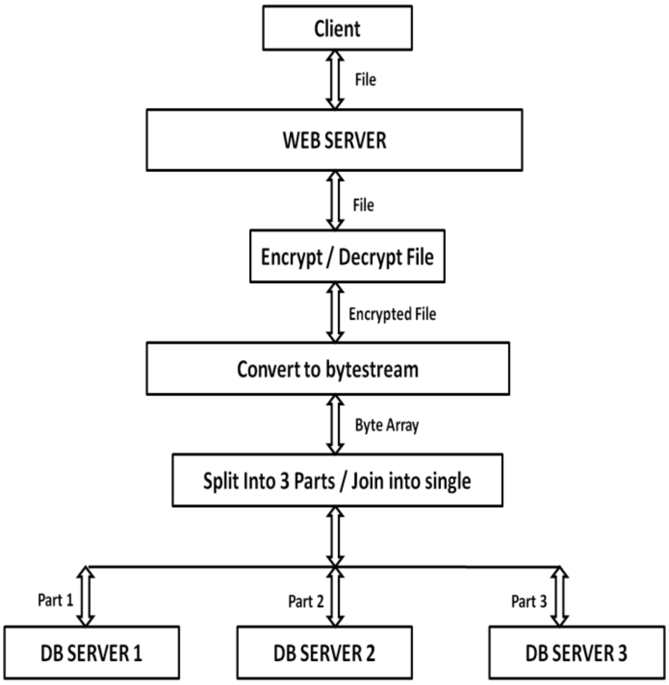


Fig: Basic Proposed System Architecture

The system will provide load balancing in terms of database as the file to be uploaded will be splitted into n parts and each part will be stored in a different cloud server. Consider an example where a file is splitted into two part out of which one is stored in google IaaS and other in Yahoo IaaS.

Basic Flow Diagram



Above given is the essential stream outline of the venture. In above outline at whatever point a customer sends a document transfer ask for, the web server takes the record scrambles it utilizing AES calculation then ZIP it and afterward parts the document into three a balance of and loads in three distinctive database servers.

AES calculation

AES depends on an outline rule known as a Substitution change organize. It is quick in both programming and equipment. Not at all like its antecedent, DES, AES does not utilize a Feistel organize. AES has a settled piece size of 128 bits and a key size of 128, 192, or 256 bits, while Rijndael can be indicated with square and key sizes in any various of 32 bits, with at least 128 bits.

The square size has a greatest of 256 bits, yet the key size has no hypothetical maximum.AES works on a 4×4 segment significant request grid of bytes, named the state (forms of Rijndael with a bigger piece estimate have extra segments in the state). Most AES counts are done in an exceptional limited field.

Working Of AES:

Propelled Encryption Standard or AES was imagined by Joan Daemen and Vincent Rijmen, and acknowledged by the US government in 2001 for top mystery affirmed encryption calculations. It is additionally alluded to as Rijndael, as it is based off the Rijndael calculation. Allegedly, this standard has never been broken.

AES has three endorsed key length: 128 bits, 192 bits, and 256 bits. To attempt to clarify the procedure in basic terms, a calculation begins with an arbitrary number, in which the key and information encoded with it are mixed however four rounds of numerical procedures. The key that is utilized to scramble the number should likewise be utilized to unscramble it.

The four rounds are called SubBytes, ShiftRows, MixColumns, and AddRoundKey. Amid SubBytes, a query table is utilized to figure out what every byte is supplanted with. The ShiftRows step has a specific number of columns where every line of the state is moved consistently by a specific counterbalance, while leaving the main line unaltered. Every byte of the second line is moved to one side, by a counterbalance of one, every byte in the third column by a balance of two, and the fourth line by a balance of three. This moving is connected to every one of the three key lengths, however there is a difference for the 256-piece square where the primary line is unaltered, the second line balance by one, the third by three, and the fourth by four. The MixColumns step is a blending operation utilizing an invertible direct change as a part of request to join the four bytes in every section. The four bytes are taken as information and created as yield.

In the fourth round, the AddRoundKey gets round keys from Rijndael's key timetable, and adds the round key to every byte of the state. Each round key gets included by joining every byte of the state with the relating byte from the round key. In conclusion, these means are rehashed for a fifth round, however do exclude the MixColumns step.

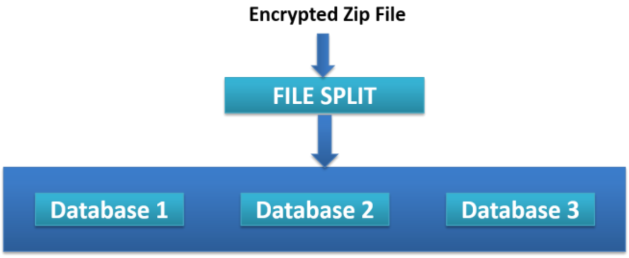
These calculations basically take fundamental information and change it into a code known as figure content. The bigger the key, the more prominent number of potential examples that can be made. This makes it greatly hard to descramble the substance, which is the reason AES has been Teflon-covered.

User Authentication

Basically whenever a user wants to use the system he/she is required to register onto the system if not registered. After registration the email is verified by sending the temporary password on mail itself. Ones the user has id and password he can login into the system and use system services.

File Merge/Split

Whenever a file is uploaded to server the web server it first encrypts the file the compress it and at last the file gets splitted into 3 equal parts and is stored in three different databases and revert is done while downloading



Modules of Project

User Authentication

As a mandatory service we have provided an authentication module that checks the username and password before logging into the cloud. We have also provided service for forget /password and email notifications.

Data Security Using AES 256

In our proposed system the data security is provided using AES symmetric algorithm with a key size of 256. Again we have worked on reducing the size of encrypted message using ultra zipping which can compress data up to 50% depending on file type.

Data Balancing in Database Servers

In proposed system the data gets splitted in three equal parts and each part is saved in different database schema. This feature helps in maintaining the data balancing in database servers.

III. CONCLUSION

IaaS is the establishment layer of the Cloud Computing conveyance demonstrate that comprises of numerous segments and innovations. Every segment in Cloud framework has its helplessness which may affect the entire Cloud's Computing security. Cloud computing business develops quickly notwithstanding security concerns, so coordinated efforts between Cloud gatherings would aid in overcoming security difficulties and push secure Cloud Computing administrations. In this project we have implemented a system that will provide better security in cloud environment. We have implemented a security architecture which provides strong security using AES algorithm.

IV. REFERENCES

[1] Cloud Computing Security: From Single To Multi-Clouds Mohammed A. Alzain , Eric Pardede , Ben Soh , James A. Thom 2012 45th Hawaii International Conference On System Sciences.

[2] Ensuring Data Integrity And Security In Cloud Storage Olfa Nasraoui, Member, IEEE, Maha Soliman, Member, IEEE, Esin Saka, Member, IEEE, Antonio Badia, Member, IEEE, And Richard Germain IEEE TRANSACTIONS ON CLOUD AND DATA ENGINEERING, VOL. 20, No. 2, February 2013.

[3] Reliable Re-Encryption In Unreliable Clouds Qin Liu ,Chiu C.Tan ,Jiewu, And Guojun Wang IEEE Communications Society Subject Matter Experts For Publication In The IEEE Globecom 2011 Proceedings.

[4] Service-Oriented Cloud Computing Architecture Wei-Tek Tsai, Xin Sun, Janaka Balasooriya 2010 Seventh International Conference On Information Technology

[5] Key-Aggregate Cryptosystem For Scalable Data Sharing In Cloud Storage Cheng-Kang Chu, Sherman S. M. Chow, Wen-Guey Tzeng, Jianying Zhou, And Robert H. Deng, Senior Member, IEEE, IEEE Transactions On Parallel And Distributed Systems. Volume: 25, Issue: 2. Year: 2014

[6] Mell-Peter, Grance-Timothy. September 2011. The NIST Definition Of Cloud Computing.

[7] C. Cachin, I. Keidar And A. Shraer, "Trusting The Cloud", ACM SIGACT News, 40, 2009, Pp. 81-86. Clavister, "Security in The Cloud", Clavister White Paper, 2008.

[8] H.Mei, J. Dawei, L. Guoliang And Z. Yuan, "Supporting Database Applications As A Service", ICDE'09:Proc. 25thintl.Conf. On Data Engineering, 2009, Pp. 832-843.

[9] C. Wang, Q. Wang, K. Ren and W. Lou, "Ensuring Data Storage Security In Cloud Computing", ARTCOM'10: Proc. Intl. Conf. On Advances In Recent Technologies In Communication And Computing, 2010, Pp. 1-9.

[10] Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina And Eduardo B Fernandez An Analysis Of Security Issues For Cloud Computing Hashizume Et Al. Journal Of Internet Services And Applications 2013.

[11] Gehana Booth, Andrew Soknacki, and Anil Somayaji Cloud Security: Attacks and Current Defenses 8th ANNUAL SYMPOSIUM ON INFORMATION ASSURANCE (ASIA'13), JUNE 4-5, 2013, ALBANY, NY.

[12] Brent Lagesse Challenges In Securing The Interface Between The Cloud And Pervasive Systems IEEE Pervasive Computing, Vol. 8, Pp. 14–23, October 2009. [Online].

[13] Wayne A. Jansen Cloud Hooks: Security And Privacy Issues In Cloud Computing Proceedings Of The 44th Hawaii International Conference On System Sciences – 2011.

[14] Mukesh Singhal And Santosh Chandrasekhar Collaboration In Multicloud Computing Environments: Framework And Security Issues Published By The IEEE Computer Society 0018-9162/13/$31.00 © 2013 IEEE

[15] Sushmita Ruj, Milos Stojmenovic, Amiya Nayak Decentralized Access Control With Anonymous Authentication Of Data Stored In Clouds IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS VOL:25 NO:2 YEAR 2014.

[16] Lukas Malina and Jan Hajny Efficient Security Solution for Privacy-Preserving Cloud Services 6TH INTERNATIONAL CONFERENCE ON TELECOMMUNICATIONS SIGNAL PROCESSING YEAR 2013

[17] Morgan, Lorraine Conboy, Kieran FACTORS AFFECTING THE ADOPTION OF CLOUD COMPUTING: AN EXPLORATORY STUDY Proceedings of the 21st European Conference on Information Systems 2012

[18] Sarita Motghare, P.S.Mohod International Journal of Advanced Research In Computer Science Volume 4, No. 4, March-April 2013

[19] Bryan Ford Icebergs in the Clouds: The Other Risks Of Cloud Computing SIGCOMM, August 2010

[20] Cheng-Kang Chu, Sherman S. M. Chow, Wen-Guey Tzeng, Jianying Zhou, And Robert H. Deng Key-Aggregate Cryptosystem For Scalable Data Sharing In Cloud Storage IEEE Transactions On Parallel And Distributed Systems. Volume: 25, Issue: 2. Year: 2014.

[21] Abhinandan P Shirahatti, P S Khanagoudar Preserving Integrity of Data and Public Auditing For Data Storage Security In Cloud Computing IMACST: VOLUME 3 NUMBER 3 JUNE 2012

[22] Allan A. Friedman and Darrell M. West Privacy and Security in Cloud Computing Number 3 October 2010

[23] Mohamed Nabeel, Elisa Bertino Privacy Preserving Delegated Access Control in Public Clouds PUBLISHING YEAR 2012

[24] Myrto Arapinis, Sergiu Bursuc, and Mark Ryan Privacy Supporting Cloud Computing: Confichair, A Case Study University Of Birmingham Nov. 2012

[25] Darko Andročec Research Challenges For Cloud Computing Economics Nov. 2011

[26] Abhinay B.Angadi, Akshata B.Angadi, Karuna C.Gull Security Issues with Possible Solutions In Cloud Computing-A Survey International Journal Of Advanced Research In Computer Engineering & Technology (IJARCET) Volume 2, Issue 2, February 2013