International Journal of Future Generation Communication and Networking
Vol. 13, No. 3, (2020), pp. 1627–1636

In Session Load Balancing with data security in cloud Services

Mr. Shubham Turale, Prof. K.V.Warkar

Department of Computer Engineering B.D.C.E Wardha

Abstract

This paper methodology helps solves the security issues in cloud IaaS (i.e. Infrastructure as a Service) which mainly includes use of cloud request processors and database servers. This paper mainly includes securing the data by encrypting it using symmetric Encryption algorithm and splitting the data in multiple parts and stores it in different database servers. Also load balancing is used to avoid higher loads on individual servers using hybrid approach.

Keywords: Cloud, IaaS, Security, Load balancing

1 Introduction

Cloud computing is architecture for providing computing service via the internet on demand and pay per use access to a pool of shared resources namely networks, storage, servers, services and applications, without physically acquiring them. So it saves managing cost and time for organizations. Many industries, such as banking, healthcare and education are moving towards the cloud due to the efficiency of services provided by the pay-per-use pattern based on the resources such as processing power used, transactions carried out, bandwidth consumed, data transferred, or storage space occupied etc. The main issues that are identified out in cloud IaaS services are load balancing in servers and data security provided to storage systems. In this paper we propose a system which provides better security and load balancing in cloud IaaS service.

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.

ISSN: 2233-7857 IJFGCN

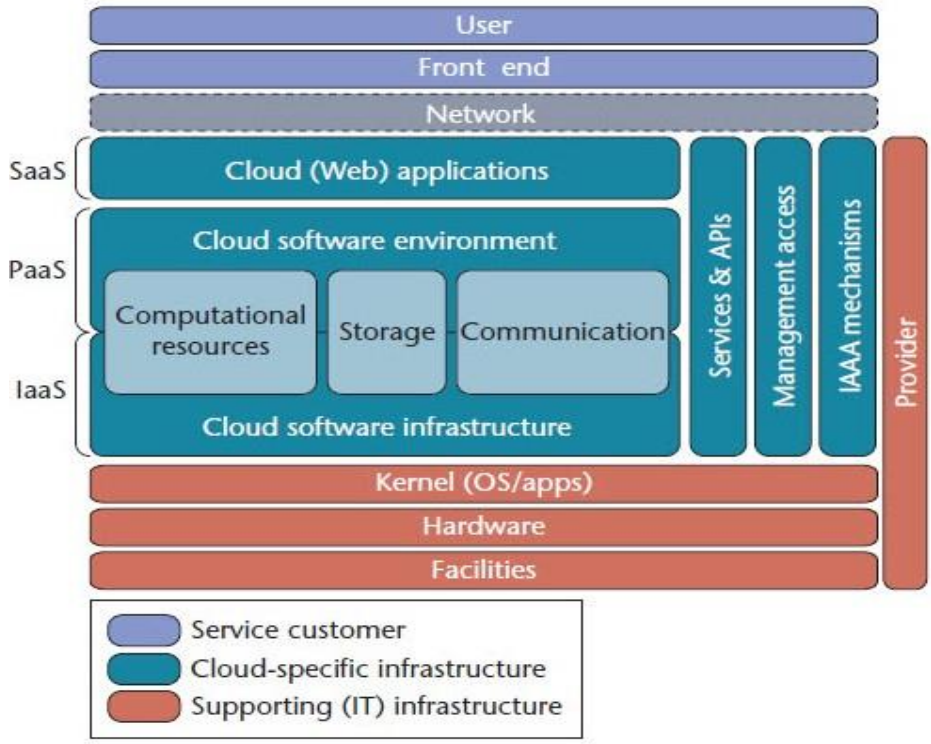

Fig 1.1: Basic Cloud Environment

RELATED WORK

There are many issues with current cloud and their architectures. Some of them are users are often tied with one cloud provider, computing components are tightly coupled, lack of SLA supports, lack of Multi-tenancy supports, Lack of Flexibility for User Interface. [4]

One of the most important issues related to cloud security risks is data integrity. The data stored in the cloud may suffer from damage during transition operations from or to the cloud storage provider. Cachinet al. give examples of the risk of attacks from both inside and outside the cloud provider, such as the recently attacked Red Hat Linux's distribution servers. Another example of breached data occurred in 2009 in Google Docs, which triggered the Electronic Privacy Information Centre for the Federal Trade Commission to open an investigation into Google's Cloud Computing Services. Another example of a risk to data integrity recently occurred in Amazon S3 where users suffered from data corruption.

One of the results that they propose is to utilize a Byzantine flaw tolerant replication convention inside the cloud. Hendricks et al. express that this result can evade information defilement created by a few parts in the cloud. Then again, Cachinet al. assert that utilizing the Byzantine flaw tolerant replication convention inside the cloud is unsatisfactory because of the way that the servers having a place with cloud suppliers utilize the same framework establishments and are physically placed in the same spot. As per Garfinkel, an alternate security hazard that may happen with a cloud supplier, for example, the Amazon cloud administration, is a hacked secret key or information interruption. In the event that somebody gets access to an Amazon account secret key, they will have the capacity to get to the majority of the account's occasions and assets. This paper presents Byzantine flaw tolerant system but it is still vulnerable to dictionary attacks[1].

ISSN: 2233-7857 IJFGCN

An alternate approach to secure the information utilizing diverse squeezing and encryption calculations and to conceal its area from the clients that stores and recovers it. The main contrast is that the framework introduced by Olfa Nasraoui is an application based framework like which will run on the customers own framework. This application will permit clients to transfer record of diverse organizations with security peculiarities including Encryption and Compression. The transferred records might be gotten to from anyplace utilizing the application which is given.

The security of the Olfa Nasraoui model has been investigation on the premise of their encryption calculation and the key administration. It has been watched that the encryption calculation have their own particular attributes; one calculation gives security at the expense of fittings, other is solid however utilizes more number of keys, one takes additionally handling time. This area demonstrates the different parameters which assumes a paramount part while selecting the cryptographic calculation. The Algorithm discovered most guaranteeing is AES Algorithm with 128 bit key size. The main disadvantage of this paper is the key size of AES which can be further extended to 256 bit [2].

An alternate methodology to secure distributed computing is for the information holder to store scrambled information in the cloud, and issue decoding keys to approved clients. At that point, when a client is renounced, the information manager will issue re-encryption orders to the cloud to re-scramble the information, to keep the disavowed client from decoding the information, and to produce new unscrambling keys to substantial clients, so they can keep on getting to the information. Then again, since a distributed computing environment is involved numerous cloud servers, such summons may not be gotten and executed by the majority of the cloud servers because of problematic system correspondences. This paper proposes a system which requires periodic key generation and re-encryption techniques which gives overhead of encrypting again and again therefore decreasing the throughput of the system [3].

A principle gimmick of cloud is information offering. Cheng-Kang Chu, Sherman S. M. Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H. Deng demonstrate to safely, effectively, and adaptably impart information to others in distributed storage. We portray new open key cryptosystems which deliver steady size figure messages such that proficient assignment of unscrambling rights for any set of figure writings are conceivable. The curiosity is that one can total any set of mystery keys and make them as minimized as a solitary key, yet enveloping the force of every last one of keys being accumulated. At the end of the day, the mystery key holder can discharge a consistent size total key for adaptable decisions of figure content set in distributed storage, however the other encoded documents outside the set stay secret. This paper doesn't provide any solution on how data will be stored in cloud. They just use visibility control to hide data from users [5].

There are different examination challenges likewise there for embracing distributed computing, for example, generally oversaw administration level assertion (SLA), security, interoperability and dependability. This examination paper diagrams what distributed computing is, the different cloud models and the principle security dangers and issues that are at present inside the distributed computing industry. This exploration paper additionally investigates the key research and difficulties that shows in distributed computing and offers best practices to administration suppliers and also endeavors planning to power cloud administration to enhance their end result in this serious financial atmosphere. This paper addresses many different issues in cloud computing related to administration services [7].

Cloud based data storage systems have many complexities regarding critical/confidential/sensitive data of client. The trust required on Cloud storage is so far had been limited by users. The role of the paper is to grow confidence in Users towards Cloud based data storage. This paper handles key questions of the User

ISSN: 2233-7857 IJFGCN

about how data is uploaded on Cloud, maintained on cloud so that there is no data loss; data is available to only authorized User(s) as per Client/User requirement and advanced concepts like data recovery on disaster is applied [8].

Gehana Booth, Andrew Soknacki, and Anil Somayaji introduced an abnormal state characterization of momentum research in distributed computing security. Dissimilar to past work, this characterization is composed around assault systems and relating resistances. Particularly, they plot a few risk models for distributed computing frameworks, talk about particular assault systems, and order proposed protections by how they address these models and counter these components. This examination highlights that, while there has been significant exploration to date, there are still real dangers to distributed computing frameworks, for example, potential base trade off, that need to be better addressed. This paper addresses potential dangers that may arise in distributed computing [11].

System Architecture

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

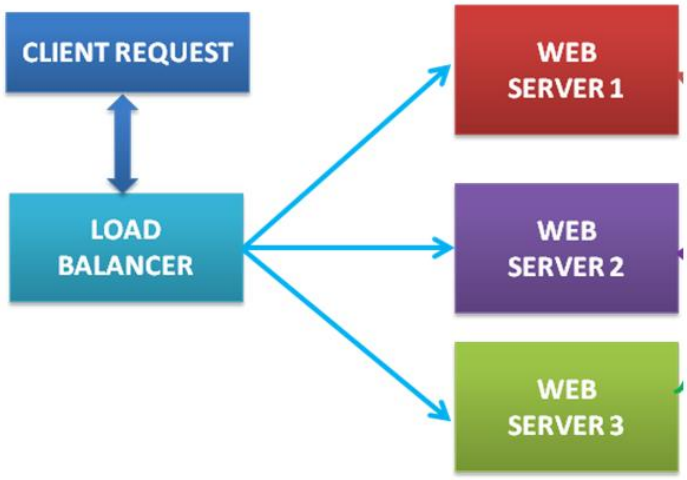

Fig 3.4: System Architecture

The system will provide load balancing both in terms of database as well as processing power and 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 Hotmail IaaS and other in Amazon IaaS.

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. Before login user needs to get himself registered in the system by placing a valid mail id password and other required details. Once user registers the password is mailed to that user which can be used for further login. At the first attempt the user is asked to update the password provided by the system.
The details of classes used for implementation is given belowUser Service :

ISSN: 2233-7857 IJFGCN

This class contains all the functions require for registration login and forgot password services. This class is connected to User class which connects to database for registration and valid verification.

Algorithm for User Authentication:

Algorithm Authenticate (String Username, String Password)
Step 1: Connect to MySql database using Connection Object.
Connection con = DriverManager.getConnection();
Step 2: Using Statement Object execute a query to check whether username or password are valid or not.
Statement stmt = conn.createstatement();
ResultSet rs = stmt.executeQuery();
Step 3: Check if rs equals NULL then return false
Else return true.
Step 4: Return.

Algorithm for User Authentication:

Algorithm Register ()
Step 1: Read all the values from the form into variables.
Step 2: If any value equals NULL then return.
Else
Goto Step 3
Step 3: Connect to MySql database using Connection Object.
Connection con = DriverManager.getConnection();
Step 4: Using Statement Object execute a query to insert values into database.
Statement stmt = conn.createstatement();
Int count = stmt.executeUpdate();
Step 3: Check if count equals zero then return false
Else return true.
Step 4: Return.

2. Load Balancing

In the proposed system a load balancing algorithm is given to balance the load in the web servers that handle request from different clients. In normal scenario a user is allocated to a server as soon as he visits the website or login from some machine and after that the request from that client is handled by that server itself. But in our system a user request is always map to a server if it is available at the time of request so even after logging into the system the user request can be mapped to another server if the allocated server get crashed.

Algorithm for Load Balancer:

Algorithm LoadBalancer (Request request)
Step 1: Accept the request into a given request object.
Step 2: Check the load in web servers according to threshold value (T).
Step 3: If no of jobs < T then goto step 4
Else
Send request to another server and goto step 4

ISSN: 2233-7857 IJFGCN

Step 3: Check whether the server is available or not. (Running or failed). If server is running allocate the job else try sending request to another server.
Step 4: Return.

RESULT ANALYSIS

1 Comparison between Symmetric Algorithms

Table 5.1 Comparison between Symmetric Algorithms

Input	ECC	ECC Cloud	DES	DES Cloud	BLOWFISH
10 Kb	11.5	1.5	7.5	2	4
13 Kb	14.7	2	10	2.5	4.7
39 Kb	21	3	31.5	6.5	8.25
56 Kb	24.5	3.75	50.25	9.25	15.7

Time given in milliseconds

2.Graph evaluation of Split Size

ISSN: 2233-7857 IJFGCN

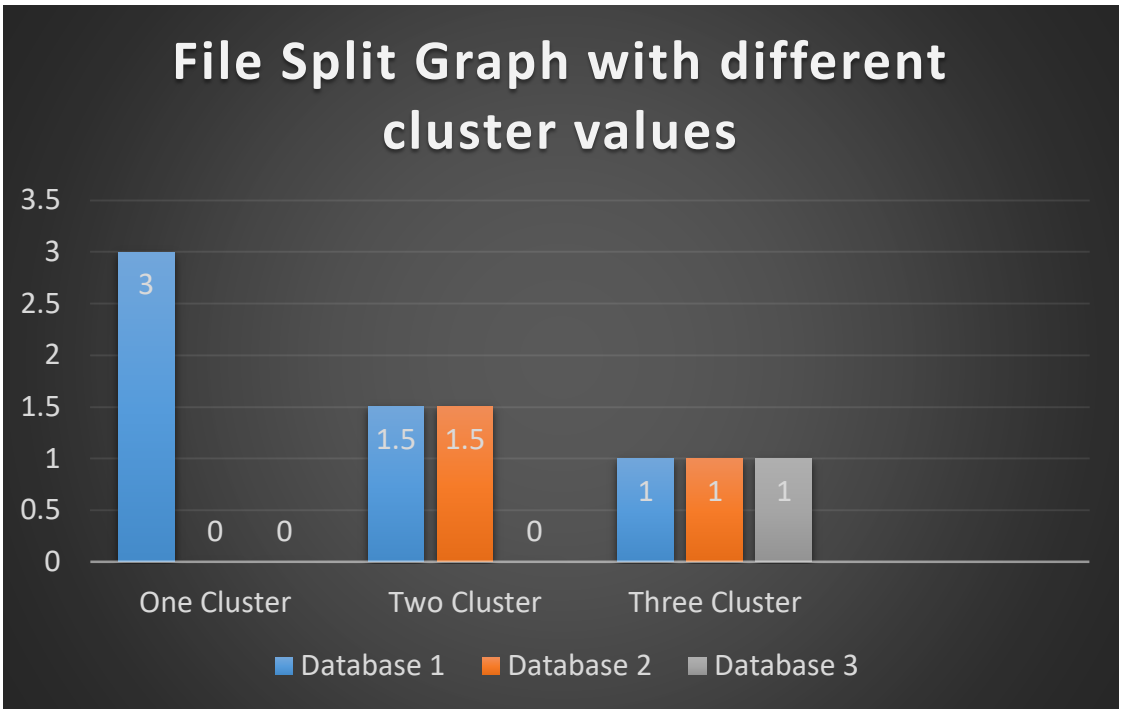

Figure 2 Graph evaluation of Split Size

3. Graph Evaluation of Encryption, Splitting and Uploading time

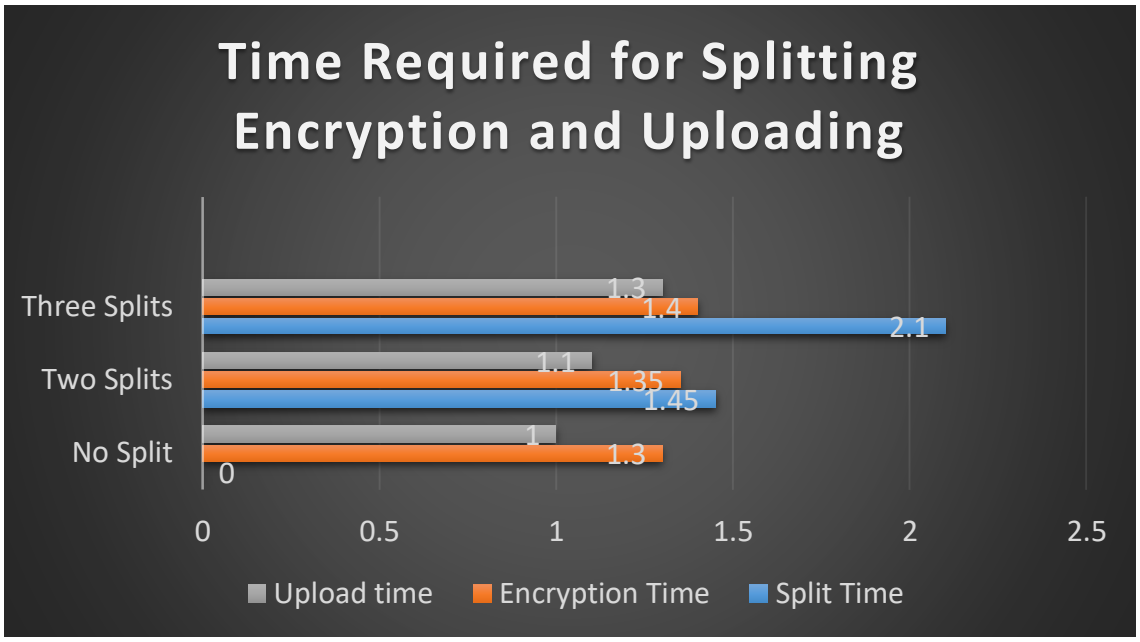

Figure3 : Graph Evaluation of Encryption, Splitting and Uploading time

ISSN: 2233-7857 IJFGCN

4. Graph Representation of Server Status

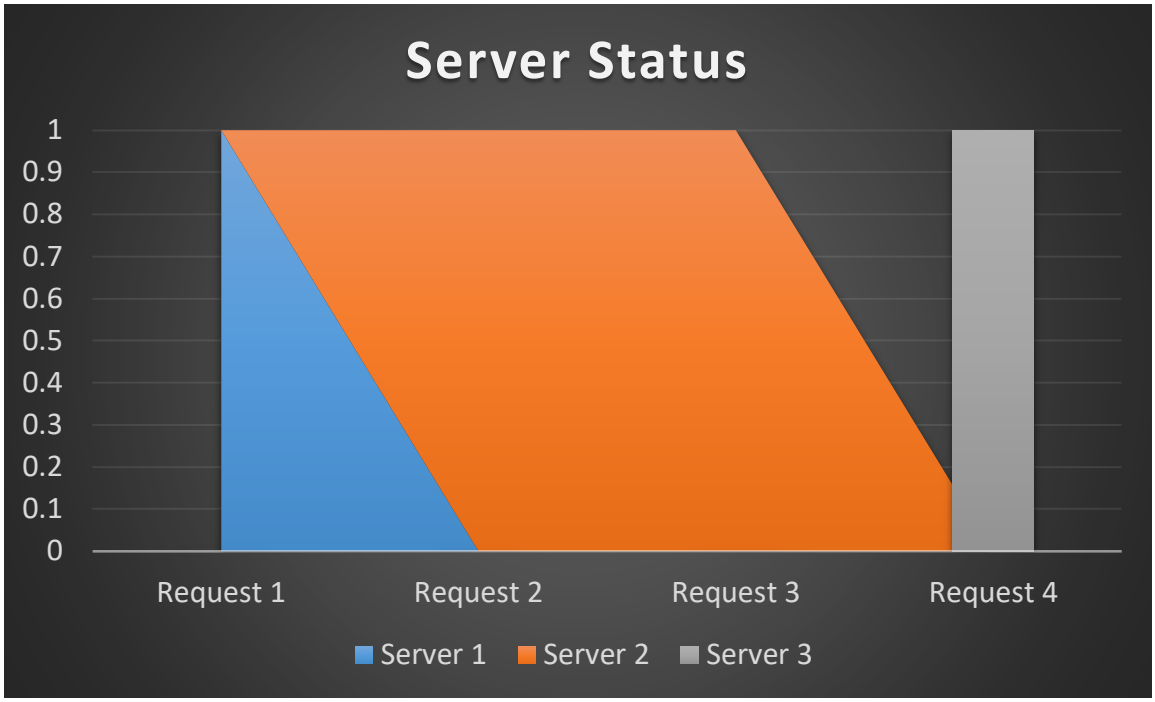

Figure 4 Graph Evaluation of Server Status

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 paper we have proposed a system that will provide better security and load balancing in cloud environment. We have proposed a security architecture which provides strong security using AES algorithm and load balancing using a modified round robin algorithm.

Future Scope

In future we plan to provide more security to system using multiple encryption algorithm at ones. We also plan to provide file sharing feature in the system so that user will be able to share their file. We will also like to provide an extra feature of data availability which will help increase reliability of system even if one of the server crashes.

REFERENCES

[1] Xiong Fu, Jain Li, Wenjie Liu, Song deng, Junchang Wang. Data Replica Placement policy based on load Balance in cloud storage syste. IEEE ITNEC 2019.

ISSN: 2233-7857 IJFGCN

[2] Olfa Nasraoui, Member, IEEE, Maha Soliman, Member, IEEE, Esin Saka, Member, IEEE, Antonio Badia, Member, IEEE, And Richard Germain "Ensuring Data Integrity And Security In Cloud Storage" IEEE TRANSACTIONS ON CLOUD AND DATA ENGINEERING, VOL. 20, No. 2, February 2013.
[3] Qin Liu ,Chiu C.Tan ,Jiewu, And Guojun Wang "Reliable Re-Encryption In Unreliable Clouds" IEEE Communications Society Subject Matter Experts For Publication In The IEEE Globecom 2011 Proceedings.
[4] Wei-Tek Tsai, Xin Sun, Janaka Balasooriya "Service-Oriented Cloud Computing Architecture" Seventh International Conference On Information Technology 2010.
[5] Cheng-Kang Chu, Sherman S. M. Chow, Wen-Guey Tzeng, Jianying Zhou, And Robert H. Deng, Senior Member, IEEE, "Key-Aggregate Cryptosystem For Scalable Data Sharing In Cloud Storage "IEEE Transactions On Parallel And Distributed Systems. Volume: 25, Issue: 2. Year: 2014.
[6] Mell-Peter, Grance-Timothy. "The NIST Definition Of Cloud Computing" September 2011.
[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.
[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.

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

ISSN: 2233-7857 IJFGCN

[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.

ISSN: 2233-7857 IJFGCN