Designing Security Model for Un-Reliable Cloud IAAS Storage

Samta Ukey, Prof. Jayant Adhikari, Prof. Rajesh Babu
Department of Computer Science and Engineering
TGPCET Nagpur

***Abstract*:** With the internet getting so popular data sharing and security of personal data has gain much more importance than before. Cloud provides and efficient way to outsource the data either online or offline but data security becomes one of the major issues in unreliable cloud environment. The proposed system addresses the security issues in cloud environment and also provides a way to provide better security and load balancing in cloud environment. The proposed system uses cryptographic symmetric algorithm AES with key size of 256 for data encryption and Ultra Zip compression which provides a compression ratio up to 50% depending on the file type. After encryption and compression the data is splitted into multiple parts and each part is stored in separate data server. The proposed work can be used in many different application like social networking sites and file hosting websites.

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

*****

INTRODUCTION

Engineering development and its selection are two discriminating effective variables for any business/association. Cloud computing is a late innovation ideal model that empowers associations or people to impart different administrations in a consistent and practical way. Cloud computing exhibits an opportunity for pervasive frameworks to power computational and stockpiling assets to achieve assignments that would not typically be conceivable on such asset obliged gadgets. Distributed computing can empower programming and base planners to construct lighter frameworks that last more and are more convenient and versatile. Regardless of the favorable circumstances distributed computing offers to the originators of pervasive frameworks, there are a few impediments and constraints of distributed computing that must be tended to.

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.

1.2 CLOUD SERVICES

A. Software as a Service (SAAS)

Saas customers rent utilization of uses running inside the Clouds supplier base, for instance Salesforce. The applications are normally offered to the customers through the Internet and are overseen totally by the Cloud supplier. That implies that the organization of these administrations, for example, upgrading and fixing are in the suppliers obligation. The profit of Saas is that all customers are running the same programming adaptation and new usefulness can be effortlessly coordinated by the supplier and is in this way accessible to all customers.

B. Platform as a Service (PAAS)

PaaS Cloud providers offer an application platform as a service, for example Google App Engine. This enables clients to deploy custom software using the tools and programming languages offered by the provider. Clients have control over the deployed applications and environment-related settings. As with SaaS, the management of the underlying infrastructure lies within the responsibility of the provider.

C. Infrastructure as a Service (IAAS)

Iaas conveys fittings assets, for example, CPU, plate space or system segments as an administration. These assets are generally conveyed as a virtualization stage by the Cloud supplier and might be gotten to over the Internet by the customer. The customer has full control of the virtualized stage and is not in charge of dealing with the underlying base.

D. Storage as a Service

Capacity as an administration (Staas) is a plan of action in which an expansive administration supplier rents space in their stockpiling foundation on a membership premise. The economy of scale in the administration supplier's framework permits them to give stockpiling a great deal more cost adequately than most people or organizations can give their own particular stockpiling, when aggregate expense of possession is considered. Capacity as a Service is frequently used to illuminate offsite reinforcement challenges. Faultfinders of capacity as an administration point to the vast measure of system data transmission needed to direct their stockpiling using a web based administration.

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 [1]. 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 [1].

Despite the fact that cloud suppliers are mindful of the malevolent insider threat, they expect that they have basic answers for assuage the issue [1]. Rocha and Correia [1] focus conceivable assailants for Iaas cloud suppliers. For illustration, Grosse et al. [1] propose one result is to keep any physical access to the servers. Notwithstanding, Rocha and Correia [1] contend that the aggressors delineated in their work have remote get to and needn't bother with any physical access to the servers. Grosse et al. [1] propose an alternate result is to screen all right to gain entrance to the servers in a cloud where the client's information is put away. Be that as it may, Rocha and Correia [1] assert that this component is gainful for observing worker's conduct as far as whether they are after the protection arrangement of the organization or not, however it is not successful in light of the fact that it identifies the issue after it has happened.

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 [3].

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 [2] 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 [2] 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 256 bit key size (256k) [2].

A principle gimmick of cloud is information offering. Cheng-Kang Chu, Sherman S. M. Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H. Deng [5] 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 [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 [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. The paper handles key questions of the User 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].

Cloud computing is an adaptable, financially savvy, and demonstrated conveyance stage for giving business or shopper IT benefits over the Internet. Then again, distributed computing shows an included level of danger on the grounds that key administrations are frequently outsourced to an outsider, which makes it harder to keep up information security and protection, help information and administration accessibility, and show agreeability. Distributed computing powers numerous advances (SOA, virtualization, Web 2.0); it additionally inherits their security issues, which we talk about here, recognizing the fundamental vulnerabilities in this sort of frameworks and the most paramount dangers found in the writing identified with Cloud Computing and its surroundings and also to distinguish and relate vulnerabilities and dangers with conceivable arrangements[10].

Proposed System

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

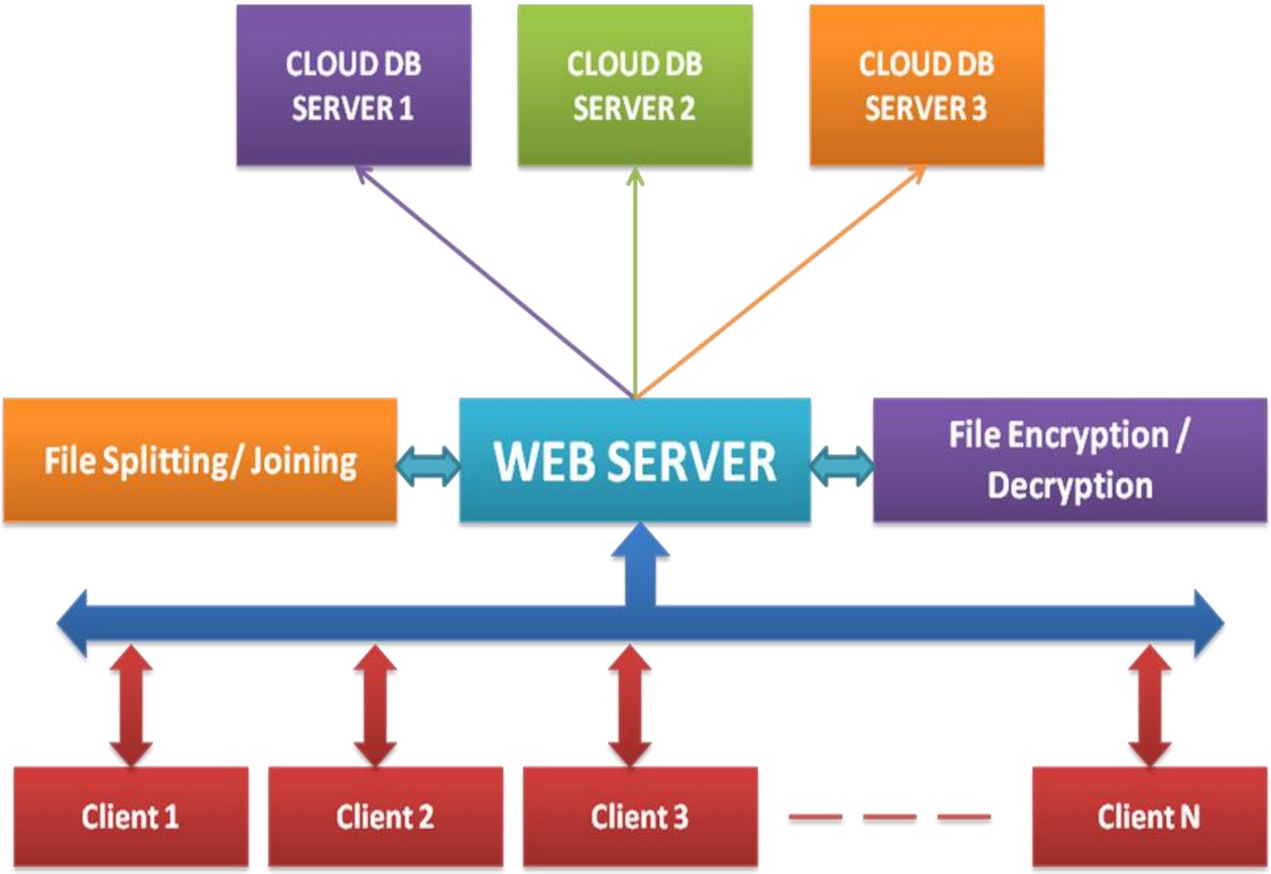
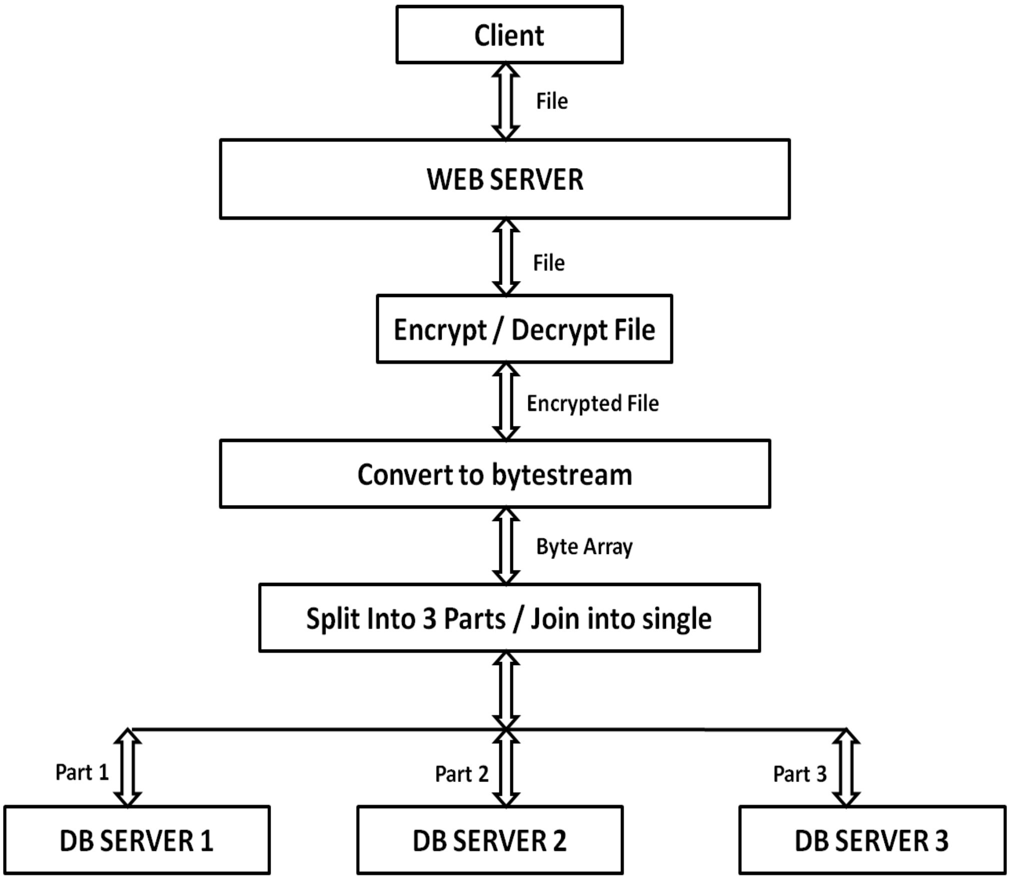


Fig: Basic Proposed System Architecture

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 basic flow diagram of the project. In above diagram whenever a client sends a file upload request, the web server takes the file encrypts it using AES algorithm then ZIP it and then splits the file into three equal parts and loads in three different database servers.

AES algorithm

AES is based on a design principle known as a Substitution permutation network. It is fast in both software and hardware. Unlike its predecessor, DES, AES does not use a Feistel network. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits, whereas Rijndael can be specified with block and key sizes in any multiple of 32 bits, with a minimum of 128 bits.

The block size has a maximum of 256 bits, but the key size has no theoretical maximum.AES operates on a 4×4 column-major order matrix of bytes, termed the state (versions of Rijndael with a larger block size have additional columns in the state). Most AES calculations are done in a special finite field.

Working Of AES:

Advanced Encryption Standard or AES was invented by Joan Daemen and Vincent Rijmen, and accepted by the US federal government in 2001 for top secret approved encryption algorithms. It is also referred to as Rijndael, as it is based off the Rijndael algorithm. Reportedly, this standard has never been cracked.

AES has three approved key length: 128 bits, 192 bits, and 256 bits. To try to explain the process in simple terms, an algorithm starts with a random number, in which the key and data encrypted with it are scrambled though four rounds of mathematical processes. The key that is used to encrypt the number must also be used to decrypt it.

The four rounds are called SubBytes, ShiftRows, MixColumns, and AddRoundKey. During SubBytes, a lookup table is used to determine what each byte is replaced with. The ShiftRows step has a certain number of rows where each row of the state is shifted cyclically by a particular offset, while leaving the first row unchanged. Each byte of the second row is shifted to the left, by an offset of one, each byte in the third row by an offset of two, and the fourth row by an offset of three. This shifting is applied to all three key lengths, though there is a variance for the 256-bit block where the first row is unchanged, the second row offset by one, the third by three, and the fourth by four. The MixColumns step is a mixing operation using an invertible linear transformation in order to combine the four bytes in each column. The four bytes are taken as input and generated as output.

In the fourth round, the AddRoundKey derives round keys from Rijndael's key schedule, and adds the round key to each byte of the state. Each round key gets added by combining each byte of the state with the corresponding byte from the round key. Lastly, these steps are repeated again for a fifth round, but do not include the MixColumns step.

These algorithms essentially take basic data and change it into a code known as cipher text. The larger the key, the greater number of potential patterns that can be created. This makes it extremely difficult to descramble the contents, which is why AES has been Teflon-coated.

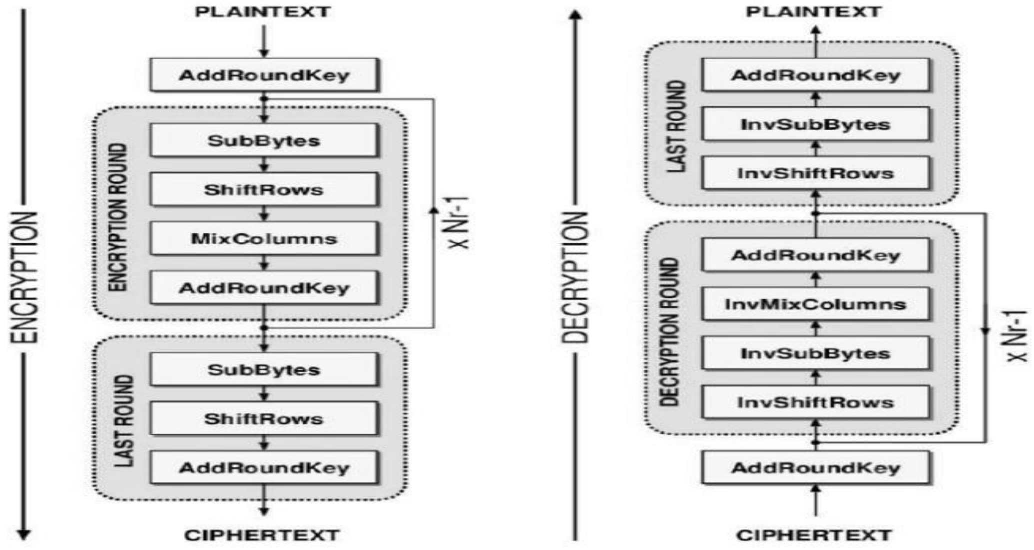


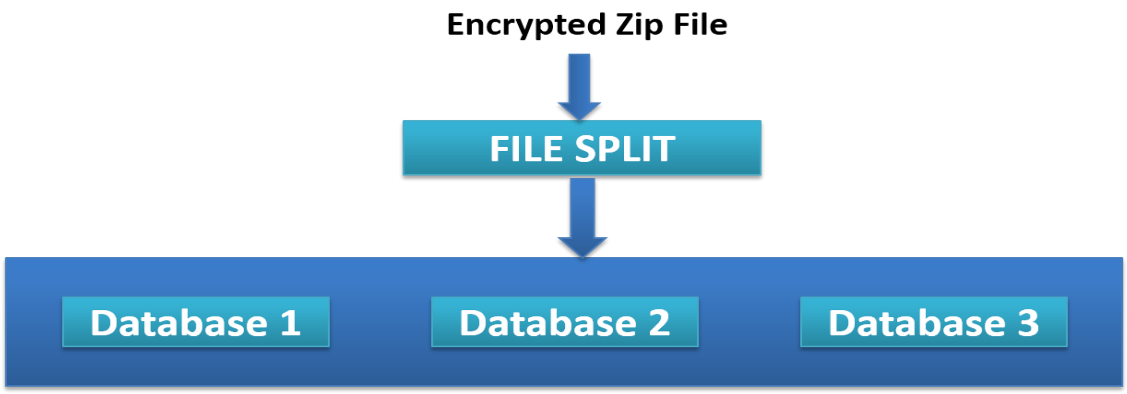
Fig: Working of AES algorithm

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 downloadin



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 said a percentage of the security worries about cloud computing furthermore proposed a framework that can help enhance the security of cloud IaaS administrations. Our methodology is intended to be executed in a multi nature.

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

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

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

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

[13] 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

[14] 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.

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

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

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

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

[19] 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.

[20] 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

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

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

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

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

[25] 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