Volume 5, Issue 11, November 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Data Security in the Cloud

[1]Anshika Negi, [2]Swati Malik, [3]Dr. Mayank Singh
[1, 2] M.Tech. Student, [3]HOD
[1, 2, 3] Department of Computer Science, Krishna Engineering College, Ghaziabad, Uttar Pradesh, India

Abstract: ***Cloud computing has changed the way associations approach IT, empowering them to wind up more dexterous, present new plans of action, give more administrations, and lessen IT costs. Cloud figuring innovations can be executed in a wide assortment of architectures, under distinctive administration and organization models, and can exist together with different advancements and programming configuration approaches. The Cloud computing scene keeps on acknowledging dangerous development. Keeping up control over the information is fundamental to cloud achievement. 10 years prior, big business information commonly dwelled in the association's physical base, naturally servers in the endeavour's server farm, where one could isolate touchy information in individual physical servers. Today, with virtualization and the cloud, information may be under the association's legitimate control, however physically live in base possessed and oversaw by another substance. Cloud computing has been assumed as the cutting edge structural planning of IT Enterprise. In the cloud, the information is exchanged among the server and customer. Rapid is the imperative issue in systems administration. Cloud security is the present dialogue in the IT world. This exploration paper helps in securing the information without influencing the system layers and shielding the information from unapproved sections into the server, the information is secured in server in light of clients' decision of security technique so information is given high secure need. Cloud computing has been chosen as the cutting edge construction modelling of IT Enterprise. As opposed to conventional arrangements, where the IT administrations are under fitting physical, intelligent and staff controls, Cloud Computing moves the application programming and databases to the vast server farms, where the administration of the information and administrations may not be completely reliable.***

Keywords: Cloud Computing, split method, splitting algorithm, cloud, security in cloud server.

I. INTRODUCTION

Cloud computing is the developing field in the current time. Cloud computing is characterized as the arrangement of assets or administrations offered through the web to the clients on their interest by cloud suppliers. It passes on everything as an administration over the web in light of client interest, for occasion working framework, system equipment, stockpiling, assets, and programming. As every single association is moving its information to the cloud, implies it utilizes the capacity administration gave by the cloud supplier. So there is a need to ensure that information against unapproved access, alteration or disavowal of administrations and so on. To secure the Cloud means secure the medications (estimations) and capacity (databases facilitated by the Cloud supplier). Security objectives of information incorporate three focuses to be specific: Availability Confidentiality, and Integrity. Privacy of information in the cloud is proficient by cryptography. Cryptography, in current days is considered mix of three sorts of calculations. They are

(1) Symmetric-key algorithms
(2) Asymmetric-key algorithms and
(3) Hashing. Integrity of data is ensured by hashing algorithms.

Information cryptography essentially is the scrambling of the substance of the information, for example, content, picture, sound, features to make the information unintelligible, imperceptible or unimportant amid transmission or capacity is termed Encryption. The primary point of cryptography is to deal with information secure from intruders. The inverse procedure of getting back the first information from encoded information is Decryption, which restores the first information. To scramble information at Cloud storage both symmetric-key and Asymmetric key calculations can be utilized. Cloud storage contains a substantial arrangement of databases and for such a vast database uneven key calculation's execution is slower when contrasted with symmetric-key calculations.

II. RELATED W ORK

Jing-Jang Hwang et al. , has proposed a plan of action for Cloud computing for information security utilizing information encryption and decoding algorithms[3]. In this strategy cloud administration supplier has in charge of information stockpiling and data encryption/unscrambling errands, which takes more computational overhead for procedure of information in cloud server. The fundamental inconvenience of this system is, there is no control of information for information proprietor i. e, information proprietor has totally trusted with cloud administration supplier

© 2015, IJARCSSE All Rights Reserved

and he has more computational overhead. Junzuo et al., proposed an Attribute Based Encryption (ABE) and evident information decoding technique to give information security in cloud based framework. They have been composed the information decoding calculation taking into account the client asked for characteristics of the out sourced scrambled information.

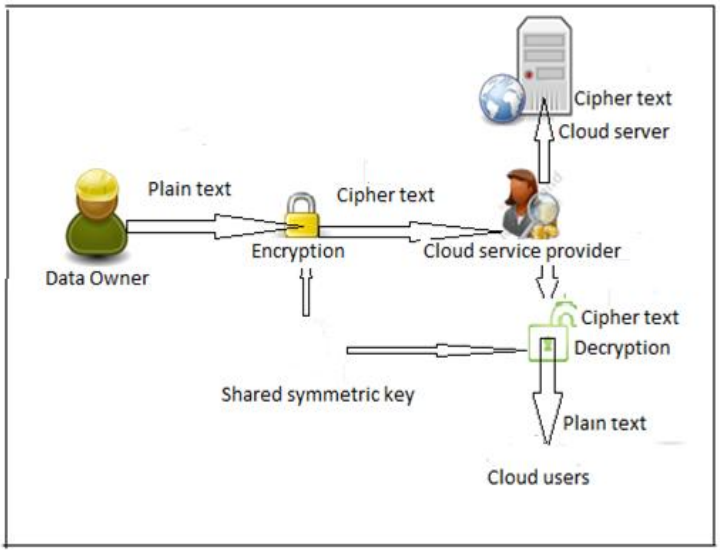


Fig: 1 Encryption –Decryption Process

One of the primary productivity downsides of this technique is, cloud administration supplier has more computational and stockpiling overhead for check of client properties with the outsourced scrambled information. While presenting outsider evaluator we can diminishes the capacity, calculation, and correspondence overheads of the cloud server, which enhances the effectiveness of the cloud information stockpiling. Fatemi Moghaddam et al. in, examined the execution of six distinctive symmetric key for information encryption calculations in Cloud computing environment. They have proposed two different cloud servers; one for information server and other for key cloud server and the information encryption and decoding procedure at the customer side. The principle downside of this technique is to keeping up two different servers for information security in cloud, which makes a more stockpiling and calculation overheads

III. SECURITY ISSUES TO THE CLOUD

The security necessities of a cloud and non-cloud server farm are genuinely similar. The Cloud Security Alliance's starting report contains an alternate kind of scientific classification in light of diverse security areas and procedures that should be followed by and large cloud arrangement. Some protection and security-related issues that are accepted to have long haul essentialness for Cloud computing are:

A. Governance

Administration suggests administration and oversight by the association over methodology, principles and approaches for application advancement and information innovation administration obtaining, likewise on the grounds that the style, usage, testing, utilize, and watching of sent or connected with administrations.

B. Compliance

Agreeability alludes to an affiliation's obligation to work in concurrence with built up laws, particulars and measures. One with the entire premier basic consistence issues confronting an organization is a data area implies capacity of information or data.

C. Malicious Insiders

This danger is surely understood to most associations. 'Vindictive insiders' effect on the association is significant. Malicious insiders are dangerous which has admittance to the information or data about the association being an individual from the association. As cloud shoppers application information is put away on Cloud storage gave by cloud supplier which additionally has the entrance to that information.

D. Account or service Hijacking

This risk happens because of phishing, misrepresentation and programming vulnerabilities. In this sort aggressor can become acquainted with basic regions onto the cloud from where he can take allow and steeling essential data prompting trade off of the accessibility, honesty, furthermore privacy to the administrations.

E. Hypervisor vulnerabilities

The Hypervisor is the principle programming part of Virtualization. There known security vulnerabilities for hypervisors and arrangements are still restricted and frequently exclusive.

© 2015, IJARCSSE All Rights Reserved

F. Insecure APIs

Unknown access, reusable tokens or password, clear-message confirmation or transmission of substance, resolute access controls or dishonourable approvals, constrained checking, and logging capacities and so forth security dangers may jump out at associations if the frail arrangement of interfaces and APIs are utilized.

IV. OBJECTIVE

The Main Objective are:

- To overcome Cloud Computing Security Challenges
- Techniques for Protecting Data in the Cloud
- Strategies for Secure Transition to the Cloud.

4.1 Cloud Computing Security Challenges

Data protection tops the list of cloud concerns today. "Cloud Computing" study, which measured cloud computing trends among technology decision makers.

When it comes to public, private, and hybrid cloud solutions, the possibility of compromised information creates tremendous angst. Organizations expect third-party providers to manage the cloud infrastructure, but are often uneasy about granting them visibility intosensitive data.

There are complex data security challenges in the cloud:

- ✓ The need to protect confidential business, government, or regulatory data
- ✓ Cloud service models with multiple tenants sharing the same infrastructure
- ✓ Data mobility and legal issues relative to such government rules as the EU Data Privacy Directive
- ✓ Lack of standards about how cloud service providers securely recycle disk space and erase existing data
- ✓ Auditing, reporting, and compliance concerns
- ✓ Loss of visibility to key security and operational intelligence that no longer is available to feed enterprise IT security intelligence and risk management
- ✓ A new type of insider who does not even work for your company, but may have control and visibility into your data

4.2 Techniques for Protecting Data in the Cloud

Traditional models of data protection have often focused on network-centric and perimeter security, frequently with devices such as firewalls and intrusion detection systems. But this approach does not provide sufficient protection against APTs, privileged users, or other insidious types of security attacks.

The encryption implementation must incorporate a robust key management solution to provide assurance that the keys are sufficiently protected. It's critical to audit the entire encryption and key management solution. Encryption works in concert with other core data security technologies, gleaning increased security intelligence, to provide a comprehensive multilayered approach to protecting sensitive data—and mitigate risk in or out of the cloud.

Therefore, any data-centric approach must incorporate encryption, key management, strong access controls, and security intelligence to protect data in the cloud and provide the requisite level of security. By implementing a layered approach that includes these critical elements, organizations can improve their security posture more effectively and efficiently than by focusing exclusively on traditional network-centric security methods.

"It is important to utilize security controls that protect sensitive data no matter where it lives, as point solutions by their very nature provide only limited visibility," says Tumulak. He emphasizes that an effective cloud security solution should incorporate three key capabilities:

- ✓ Data lockdown
- ✓ Access policies
- ✓ Security intelligence

4.3 Strategies for Secure Transition to the Cloud

The fundamental key to data security is to protect what matters. Solutions that enable companies to confidently transition to the cloud while still leveraging many of their traditional infrastructure and investments offer significant advantages.

Data Security solves the enterprise cloud security conundrum by protecting data inside of the operating environment while establishing security policies and maintaining control through a centralized management interface. One key differentiator is that works with cloud providers and enterprises to protect data regardless of whether it is located in physical, virtual, or cloud environments. This architecture enables enterprises to control access to the data itself, even as the virtual machine migrates to the virtual and cloud world. Organizations can establish access policies and achieve complete control of data in private, public, or hybrid cloud environments.

V. SPLIT ALGORITHM

File splitting and clubbing In Proposed system, we are splits the file in different portions then encode and store it on different cloud. Meta data necessary for decrypting and moving a file will be stored in metadata management server. File can club with another file.

Folder Lock in folder lock approach, while locking a folder we create xml file inside folder with a password. When user browse for a folder processing our program checks whether folder has xml file exist or not. if folder contain xml file then it popup for password insertion if not then it create xml file with password which user has inserted.

© 2015, IJARCSSE All Rights Reserved

The algorithm uses the password to encrypt the file with a unique number that creates the unique encrypted file. The same password is use to decrypt the file thus enabling maximum security of the file. Let us now see the algorithm in detail.

5.1. Algorithm

The encryption is done through the following steps
Step 1: Start.
Step 2: Accept file name and password.
Step 3: Generate unique random number from the password,which serves as the key.
Step 4: Split the file and the key into n splits.
Step 5: Encrypt the first split of the file with the firstsplit of the key, second split of file with second split of keyand so on.
Step 6: Combine the splits to get the file
Step 7: Stop

5.2 Encryption

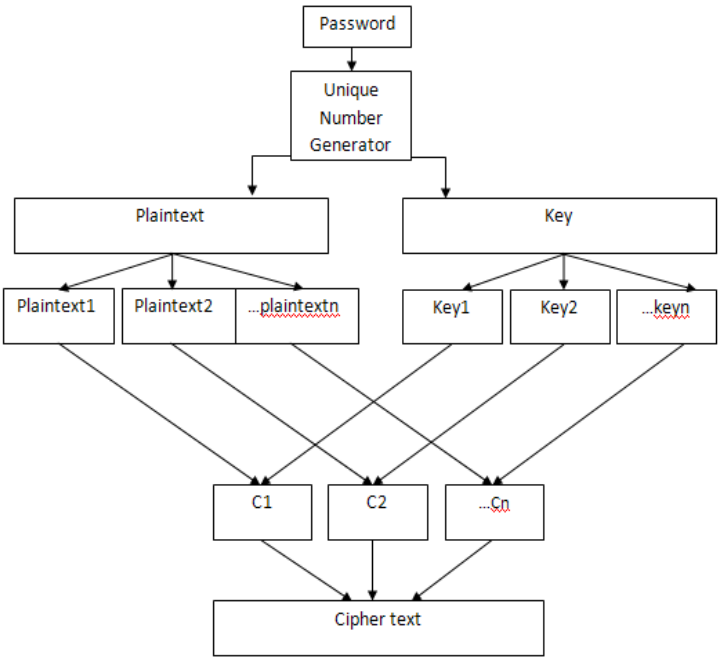


Figure 2: Encryption

5.3 Flowchart – decryption

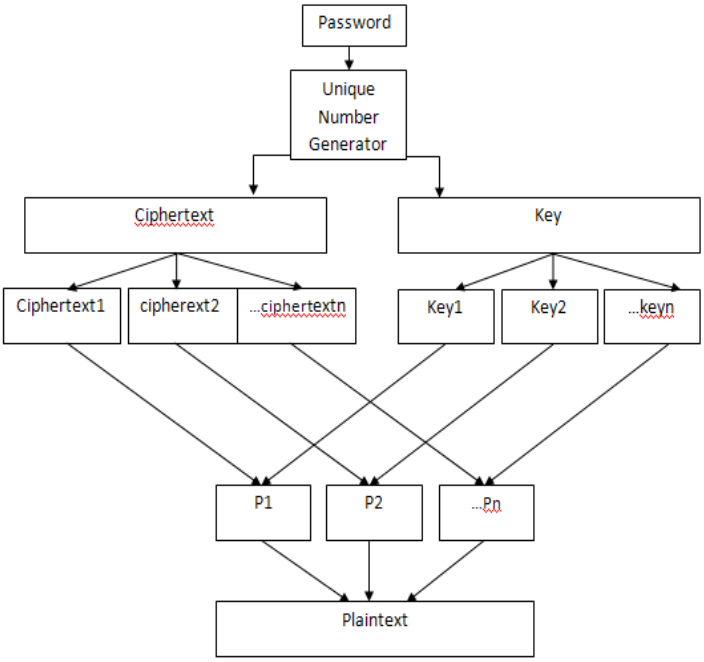


Figure 3: Split-file -key pair algorithm –Decryption

© 2015, IJARCSSE All Rights Reserved

VI. PROPOSED TECHNIQUE

The proposed algorithm is an attempt to present a new approach for complex encrypting and decrypting data based on parallel programming in such a way that the new approach can makeuse of multiple-core processor to achieve higher speed with higher level of security.

Encryption is the process of transforming information so it is unintelligible to anyone but the intended recipient. Decryption is the process of transforming encrypted information so that it is intelligible again. A cryptographic algorithm, also called a cipher, is a mathematical function used for encryption or decryption. In most cases, two related functions are employed, one for encryption and the other for decryption.

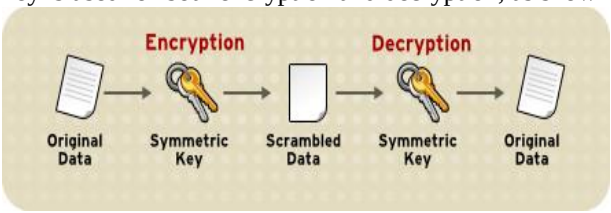
With most modern cryptography, the ability to keep encrypted information secret is based not on the cryptographic algorithm, which is widely known, but on a number called a key that must be used with the algorithm to produce an encrypted result or to decrypt previously encrypted information. Decryption with the correct key is simple. Decryption without the correct key is very difficult, and in some cases impossible for all practical purposes.

The sections that follow introduce the use of keys for encryption and decryption.

- Symmetric-Key Encryption
- Public-Key Encryption
- Key Length and Encryption Strength

Symmetric-Key Encryption

With symmetric-key encryption, the encryption key can be calculated from the decryption key and vice versa. With most symmetric algorithms, the same key is used for both encryption and decryption, as shown in Figure.



Implementations of symmetric-key encryption can be highly efficient, so that users do not experience any significant time delay as a result of the encryption and decryption. Symmetric-key encryption also provides a degree of authentication, since information encrypted with one symmetric key cannot be decrypted with any other symmetric key. Thus, as long as the symmetric key is kept secret by the two parties using it to encrypt communications, each party can be sure that it is communicating with the other as long as the decrypted messages continue to make sense.

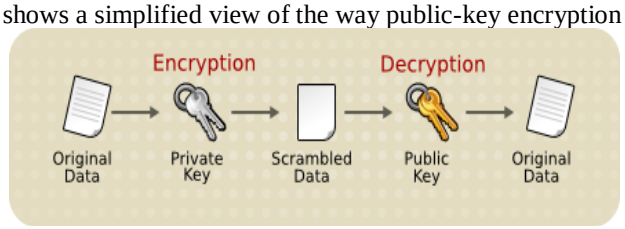
Symmetric-key encryption is effective only if the symmetric key is kept secret by the two parties involved. If anyone else discovers the key, it affects both confidentiality and authentication. A person with an unauthorized symmetric key not only can decrypt messages sent with that key, but can encrypt new messages and send them as if they came from one of the two parties who were originally using the key.

Symmetric-key encryption plays an important role in the SSL protocol, which is widely used for authentication, tamper detection, and encryption over TCP/IP networks. SSL also uses techniques of public-key encryption, which is described in the next section.

Public-Key Encryption

The most commonly used implementations of public-key encryption are based on algorithms patented by RSA Data Security. Therefore, this section describes the RSA approach to public-key encryption.

Public-key encryption (also called asymmetric encryption) involves a pair of keys-a public key and a private key-associated with an entity that needs to authenticate its identity electronically or to sign or encrypt data. Each public key is published, and the corresponding private key is kept secret. Data encrypted with your public key can be decrypted only with your private key. Figure 2 shows a simplified view of the way public-key encryption works.



The scheme shown in Figure lets you freely distribute a public key, and only you will be able to read data encrypted using this key. In general, to send encrypted data to someone, you encrypt the data with that person's public key, and the person receiving the encrypted data decrypts it with the corresponding private key.

Compared with symmetric-key encryption, public-key encryption requires more computation and is therefore not always appropriate for large amounts of data. However, it's possible to use public-key encryption to send a symmetric key, which can then be used to encrypt additional data. This is the approach used by the SSL protocol.

As it happens, the reverse of the scheme shown in Figure 2 also works: data encrypted with your private key can be decrypted only with your public key. This would not be a desirable way to encrypt sensitive data, however, because it

© 2015, IJARCSSE All Rights Reserved

means that anyone with your public key, which is by definition published, could decrypt the data. Nevertheless, private-key encryption is useful, because it means you can use your private key to sign data with your digital signature-an important requirement for electronic commerce and other commercial applications of cryptography. Client software such as Firefox can then use your public key to confirm that the message was signed with your private key and that it hasn't been tampered with since being signed. "Digital Signatures" describes how this confirmation process works.

Key Length and Encryption Strength

Breaking an encryption algorithm is basically finding the key to the access the encrypted data in plain text. For symmetric algorithms, breaking the algorithm usually means trying to determine the key used to encrypt the text. For a public key algorithm, breaking the algorithm usually means acquiring the shared secret information between two recipients.

One method of breaking a symmetric algorithm is to simply try every key within the full algorithm until the right key is found. For public key algorithms, since half of the key pair is publicly known, the other half (private key) can be derived using published, though complex, mathematical calculations. Manually finding the key to break an algorithm is called a brute force attack.

Breaking an algorithm introduces the risk of intercepting, or even impersonating and fraudulently verifying, private information. The key strength of an algorithm is determined by finding the fastest method to break the algorithm and comparing it to a brute force attack.

For symmetric keys, encryption strength is often described in terms of the size or length of the keys used to perform the encryption: in general, longer keys provide stronger encryption. Key length is measured in bits. For example, 128-bit keys for use with the RC4 symmetric-key cipher supported by SSL provide significantly better cryptographic protection than 40-bit keys for use with the same cipher. Roughly speaking, 128-bit RC4 encryption is 3×10^{26} times stronger than 40-bit RC4 encryption. (For more information about RC4 and other ciphers used with SSL, see "Introduction to SSL.") An encryption key is considered full strength if the best known attack to break the key is no faster than a brute force attempt to test every key possibility.

Different ciphers may require different key lengths to achieve the same level of encryption strength. The RSA cipher used for public-key encryption, for example, can use only a subset of all possible values for a key of a given length, due to the nature of the mathematical problem on which it is based. Other ciphers, such as those used for symmetric key encryption, can use all possible values for a key of a given length, rather than a subset of those values.

Because it is relatively trivial to break an RSA key, an RSA public-key encryption cipher must have a very long key, at least 1024 bits, to be considered cryptographically strong. On the other hand, symmetric-key ciphers can achieve approximately the same level of strength with an 80-bit key for most algorithms.

VII. CONCLUSION

Cloud computing is emerging as a new thing and many of the organizations are moving toward the cloud but lacking due to security reasons. So cloud security is must which will break the hindrance the acceptance of the cloud by the organizations. There are a lot of security algorithms which may be implemented to the cloud.

DES, Triple-DES, AES, and Blowfish etc are some symmetric algorithm. DES and AES are mostly used symmetric algorithms.DES is quite simple to implement then AES.

RSA and Diffie-Hellman Key Exchange is the asymmetric algorithms. In cloud computing both RSA and Diffie-Hellman Key Exchange is used to generate encryption keys for symmetric algorithms. But the security algorithms which allow operations (like searching) on decrypted data are required for cloud computing, which will maintain the confidentiality of the data. So we are going to implement Split algorithm so that we can split long file and then after we process the encryption and decryption technique.

Cloud computing is changing the way IT departments buy IT. Businesses have a range of paths to the cloud, includinginfrastructure, platforms and applications that are available from cloud providers as online services. Many people may beconfused by the range of offerings and the terminology used to describe them and will be unsure of the risk and benefits.Security is a major requirement in cloud computing while we talk about data storage. There are number of existingtechniques used to implement security in cloud. In this paper, we discussed number of symmetric and asymmetricalgorithms. Our future will be considering some problems related to existing security algorithms and implement a betterversion of Split algorithm.

VIII. FUTURE SCOPE

As discussed there are many security algorithms which are currently used in a cloud computing environment. Apart from this there are still there too many areas which require further enhancements like more efficient algorithms can be developed which can increase the security level in the environment. In future we will implement the advanced split algorithm in a cloud environment.

ACKNOWLEGMENT

I would like to thank to Prof. Mayank Singh, Head of Dept. Computer Science, Krishna Engineering College, Ghaziabad for their assistance in preparing and distributing the our review paper. I would also like to thank the practitioners who have kindly responded to our survey questionnaires. I thank also our college for motivating and encouraging doing my Research work in a Successful.

© 2015, IJARCSSE All Rights Reserved

REFERENCES

[1] AL.Jeeva, Dr.V.Palanisamy And K.Kanagaram "Comparative Analysis Of Performance Efficiency And Security Measures Of Some Encryption Algorithms" International Journal Of Engineering Research And Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue 3, May-Jun 2012, Pp.3033-3037.

[2] Neha Jain and Gurpreet Kaur 'Implementing DES Algorithm in Cloud for Data Security" VSRD International Journal of CS & IT Vol. 2 Issue 4, 2012, pp. 316-321.

[3] Simarjeet Kaur "Cryptography and Encryption In Cloud Computing", VSRD International Journal of CS & IT Vol. 2 Issue 3, 2012, pp. 242-249.

[4] Nelson Gonzalez, Charles Miers, Fernando Redigolo, Marcos Simplicio, Tereza Carvalho, Mats Naslund and Makan Pourzandi "A quantitative analysis of current security concerns and solutions for cloud computing",Springer Journal of Cloud Computing: Advances, Systems and Applications 2012.

[5] Ronald L. Krutz and Russell Dean Vines, Cloud Security: A Comprehensive Guide to Secure Cloud Computing Wiley Publishing, Inc. Indianapolis, Indiana 2010.

[6] Behrouz A. Forouzan, Cryptography and Network Security, McGraw-Hill Companies, Inc., New York, Special Indian Edition 2007.

[7] Wayne Jansen and Timothy Grance "Guidelines on Security and Privacy in Public Cloud Computing", National Institute of Standards and Technology, Special Publication 800-144, December 2011, 80 pages

[8] Akhil Behl "Emerging Security Challenges in Cloud Computing ", IEEE World Congress on Information and Communication Technologies, 2011 pp.217-222.

[9] RuWei Huang, Si Yu, Wei Zhuang and XiaoLin Gui, "Design of Privacy-Preserving Cloud Storage Framework"2010 Ninth International Conference on Grid and Cloud Computing.

[10] Dr. Chander Kant and Yogesh Sharma, "Enhanced Security Architecture for Cloud Data Security" InternationalJournal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013, pp.571-575.

[11] Cong Wang, Qian Wang, KuiRen and Wenjing Lou, "Ensuring Data Storage Security in Cloud Computing", InQuality of Service, 2009. 17th International Workshop on, page 19, 2009.

[12] Cong Wang, Qian Wang, Kui Ren and Wenjing Lou "Ensuring Data Storage Security in Cloud Computing." IEEE2009.

[13] Balachandra Reddy Kandukuri, Rama Krishna Paturi and Dr. AtanuRakshit, "Cloud security issues" In ServicesComputing, 2009. IEEE International Conference on, page 517520, 2009.

[14] Kashish Goyal, Supriya Kinger" Modified Caesar Cipher for Better Security Enhancement" International Journal ofComputer Applications (0975 – 8887) Volume 73– No.3, July 2013.

[15] Yogesh Kumar, Rajiv Munjal and Harsh Sharma,"Comparison of Symmetric and Asymmetric Cryptography withExisting Vulnerabilities and Countermeasures" IJCSMS International Journal of Computer Science and ManagementStudies, Vol. 11, Issue 03, Oct 2011.

© 2015, IJARCSSE All Rights Reserved