International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 5 Issue: 4 194 – 200

Security in Cloud Computing using AES & DES

Shabnam Kumari
A.P., Department of CSE, Sat Kabir Institute of Technology & Management, Bahadurgarh, Haryana, India
Shabnam022e@email.com

Reema
A.P., Department of CSE, Sat Kabir Institute of Technology & Management, Bahadurgarh, Haryana, India
arorareema@live.com

Princy
M.Techscholar.,Deptt of CSE, Sat Kabir Institute of Technology & Management, Bahadurgarh, Haryana, India
October.princy21@gmail.com

Sunita Kumari
A.P., Department of CSE, G.B Pant Engineering College, Okhla.
Sunita2009@gmail.com

Abstract- Cloud Computing has been visualized as the heirframework of IT consortium. Cloud Computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. This in turnimposes many new security challenges which are not clear yet. This paper gives a brief introduction of cloud computing its types and security issue and approachesto secure the data in the cloud environment. Cloud computing security is the set of control-based technologies and policies designed to adhere to regulatory compliance rules and protect information, data applications and **infrastructure** associated with cloud computing use.

Keywords: *Cloud Computing, security algorithm, AES, DES, RSA security issues*

*****

I. INTRODUCTION

Cloud Computing provides us a means by which we can access the applications as utilities,over the Internet. It allows us to create, configure, and customize applications online.

1.1 Cloud

The term **Cloud** refers to a **Network** or **Internet**. In other words, we can say that Cloud is something, which is present at remote location. Cloud can provide services over network, i.e., on public networks or on private networks, i.e., WAN, LAN or VPN. Applications such as **e-mail, web conferencing, customer relationship management (CRM),**all run in cloud.

1.2 Cloud Computing

Cloud Computing refers to **manipulating, configuring,** and **accessing** the applications online. It offers online data storage, infrastructure and application. We need not to install a piece of software on our local PC and this is how the cloud computing overcomes **platform dependency issues**. Hence, the Cloud Computing is making our business application **mobile** and **collaborative**.

Several trends are opening up the era of Cloud Computing, which is an Internet-based development and use of computer technology. The ever cheaper and more powerful processors, together with the software as a service (SaaS) computing architecture, are transforming data centers into pools of computing service on a huge scale. The increasing network bandwidth and reliable yet flexible network connections make it even possible that users can now subscribe high quality services from data and software that reside solely on remote data centers.

Moving data into the cloud offers great convenience to users since they don't have to care about the complexities of direct hardware management. The pioneer of Cloud Computing vendors, Amazon Simple Storage Service (S3) and Amazon Elastic Compute Cloud (EC2) [1] are both well known examples. While these internet-based online services do provide huge amounts of storage space and customizable computing resources, this computing platform shift, however, is eliminating the responsibility of local machines for data maintenance at the same time. As a result, users are at the mercy of their cloud service providers for the availability and integrity of their data. Recent downtime of Amazon's S3 is such an example.

From the perspective of data security, which has always been an important aspect of quality of service, Cloud Computing inevitably poses new challenging security threats for number of reasons. Firstly, traditional cryptographic primitives for the purpose of data security protection can not be directly adopted due to the users' loss control of data under Cloud Computing. Therefore, verification of correct data storage in the cloud must be conducted without explicit knowledge of the whole

data. Considering various kinds of data for each user stored in the cloud and the demand of long term continuous assurance of their data safety, the problem of verifying correctness of data storage in the cloud becomes even more challenging. Secondly, Cloud Computing is not just a third party data warehouse. The data stored in the cloud may be frequently updated by the users, including insertion, deletion, modification, appending, reordering, etc. To ensure storage correctness under dynamic data update is hence of paramount importance. However, this dynamic feature also makes traditional integrity insurance techniques futile and entails new solutions. Last but not the least, the deployment of Cloud Computing is powered by data centers running in a simultaneous, cooperated and distributed manner. Individual user's data is redundantly stored in multiple physical locations to further reduce the data integrity threats. Therefore, distributed protocols for storage correctness assurance will be of most importance in achieving a robust and secure cloud data storage system in the real world. However, such important area remains to be fully explored in the literature.

Recently, the importance of ensuring the remote data integrity has been highlighted by the following research works [3]–[7]. These techniques, while can be useful to ensure the storage correctness without having users possessing data, can not address all the security threats in cloud data storage, since they are all focusing on single server scenario and most of them do not consider dynamic data operations. As an complementary approach, researchers have also proposed distributed protocols [8]–[10] for ensuring storage correctness across multiple servers or peers. Again, none of these distributed schemes is aware of dynamic data operations. As a result, their applicability in cloud data storage can be drastically limited.

1.3 Basic Concepts

There are certain services and models working behind the scene making the cloud computing feasible and accessible to end users. Following are the working models for cloud computing:

1.3.1 DEPLOYMENT MODELS

Deployment models define the type of access to the cloud, i.e., how the cloud is located? Cloud can have any of the four types of access: Public, Private, Hybrid and Community.

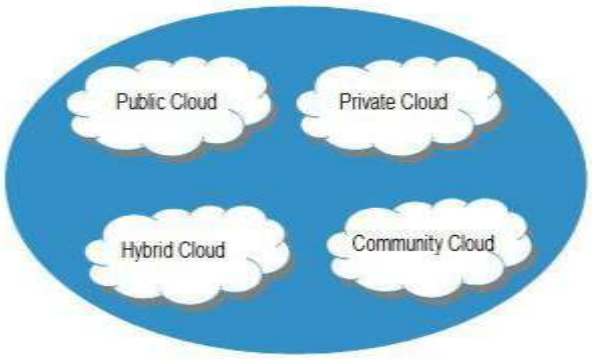

Fig.1:-Deployment models

PUBLIC CLOUD

The **Public Cloud** allows systems and services to be easily accessible to the general public. Public cloud may be less secure because of its openness, e.g., e-mail. The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

PRIVATE CLOUD

The **Private Cloud** allows systems and services to be accessible within an organization. It offers increased security because of its private nature. The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.

COMMUNITY CLOUD

The **Community Cloud** allows systems and services to be accessible by group of organizations. The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.

HYBRID CLOUD

The **Hybrid Cloud** is mixture of public and private cloud. However, the critical activities are performed using private cloud while the non-critical activities are performed using public cloud. The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability.

1.3.2 SERVICE MODELS

Service Models are the reference models on which the Cloud Computing is based. These can be categorized into three basic service models as listed below:

Cloud Software as a Service (SaaS). SaaS allows the user to access applications or software installed on the cloud infrastructure ie: the firm would access software online. By way of example, the iCloud service, soon to be provided by

Apple, is a SaaS service by which users access what is effectively a data backup and distribution service.

Cloud Platform as a Service (PaaS). PaaS allows the firm to install or deploy software on infrastructure operated by the CSP ie: a firm can upload its own software applications (or acquired applications) onto a server provided by the CSP.

Cloud Infrastructure as a Service (IaaS). IaaS allows a firm to access infrastructure operated by the CSP. The firm would not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components. By way of example a firm would rent a remote server (or cluster of remote servers) on which the firms data is stored.

Each of the service models make use of the underlying service model, i.e., each inherits the security and management mechanism from the underlying model, as shown in the following diagram

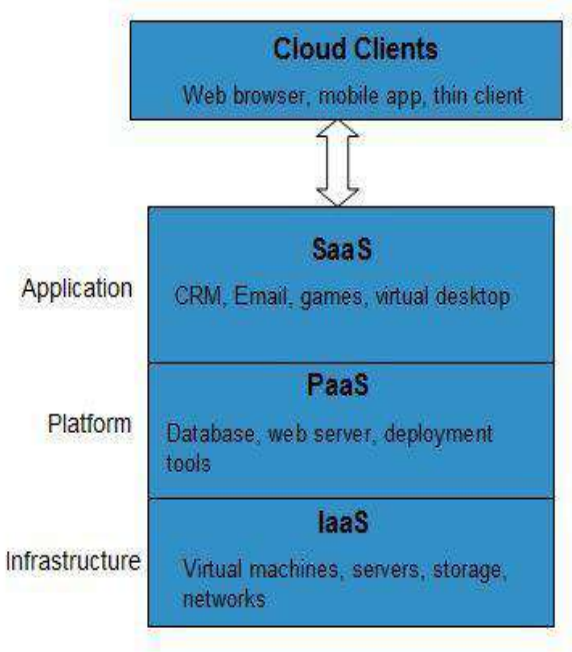

Fig. 2:- Service models

II. LITERATURE REVIEW

Cloud computing is useful to think of a cloud as a collection of hardware and software that runs in a data centre and enables the cloud computing model and data security. These can be analyzed by reviewing some existing researchs. Juhichoudhary and Anuragmishra clear that cloud services and applications requires all standard security through several cryptographic methods such as proxy re-encryption(PRE) scheme, Type based PRE, Key-private PRE, Identity based PRE, Attribute based PRE and Threshold PRE . This paper surveys different proxy re-encryption schemes used in cloud storage system. The advantages and disadvantages of the algorithms have been studied. The future work will be concerned with the development of better PRE schemes which works in distributed environment[12].K.Pranathi and M.Sai Sri Lakshmi Yellari perform detailed study about the types of algorithms in the research paper. The type of encryptions, decryptions they followed and the extent to which they can provide security for the data resisting against the maximum number of attacks occur on them. As DES algorithm has prone to numerous attacks being the popular algorithm for encryption is ruled out besides having AES algorithm which has been the most efficient algorithm although with more number of rounds it has to undergo, also Diffie-Hellman and ElGamal algorithms for their weak keys have been ruled out.Opting RSA algorithm for providing Data Security on Cloud for better user access and the Confidentiality, Integrity and Authentication it provides, made it a better option so far for its implementation on Cloud for Data Security[13].According to CompTIA 4th Annual Conference Full Report (2013), it states that as cloud components are becoming more prevalent in IT architectures, more companies are relying on cloud computing for business processes such as storage (59%), business continuity/disaster recovery (48%), and security (44%). This strong usage and strong market indicators show that cloud computing is becoming a default part of the IT landscape. Although adoption rates are high and market numbers are positive, there is still confusion related to cloud computing. This confusion will hinder end users and channel firms from fully transforming their IT practices and offerings. Only 46% of channel firms with cloud offerings described their cloud business as completely mature—an established, strategic part of business plans. In the past few years there have been tremendous increases in use of cloud computing in both business, government and even educational sector, this increase was due to worldwide availability of internet and high competition in the cloud market that brought about utilising computing resources at minimum cost (Rahimli, 2013).According to Rajani Sharma, Rajender Kumar Trivedisurveyed basic of cloud computing and security issues in the cloud computing. Some security issues are the key concern in the cloud computing. Especially privacy and integrity of data are the key concern security issues. when users store their data in the provided cloud they don't have the information where the data is stored. Therefore cloud service provider must provide audit tools to the users to examine regulate how there is stored, protected, used and verify policy implementation. But Scrutinizing of illegal activities is a difficult task because data for multiple users may be collocated. To solve this problems audit tools must be contractually committed with proof. In the cloud as data is stored publically and they really don't know where the data is being stored, they don't know the exactlocation of the data, due to this data stored in the cloud has a higher risk of being accessed by un-authorized person during storage as well as transmission[14].According to SeongHan Shin and KazukuniKobara ,they fully utilize the

leakage-resilient authentication and data management system which is constructed by tightly coupling the LR-AKE(Leakage-Resilient Authenticated Key Exchange) protocols with data (key) management. This system not only guarantees a high level of security against active attacks as well as leakage of stored secrets (i.e., credentials and keys) but also makes a user possible to securely store/retrieve data keys in a distributed manner.They show how the leakage-resilient authentication and data management system works for secure cloud storage. Also, we introduce the LR-AKE client interface (called, LR-Passwords). What a cloud user have to do with LR-Passwords is just to input his/her personalpassword. That's all! If the password is correct, the recovered data keys are automatically cached into the memory duringthe determined time period. All these concerns are based on "Data Security Issues in Cloud".

Data Confidentiality: The cloud seeker should be assured that data hosted on the cloud will be confidential [5].

Data Integrity:The cloud provider should make the client aware of what particular data is hosted on the cloud, theorigin and the integrity mechanisms put in place.

Data Availability: when accidents such as hard disk damage, IDC fire, and network failures occur, the extent thatuser's data can be used or recovered and how the users verify their data by techniques rather than depending on thecredit guarantee by the cloud service provider alone.

Data Location: Cloud Computing offers a high degree of data mobility. This, then, requires a contractual agreement,between the Cloud provider and the consumer that data should stay in a particular location or reside on a givenknown server. Also, cloud providers should take responsibility to ensure the security of systems (including data) andprovide robust authentication to safeguard customers' information [1].

Data Relocation*:* Data is initially stored at an appropriate location decide by the Cloud provider. However, it isoften moved from one place to another. Cloud providers have contracts with each other and they use each others'resources.

Data Privacy: Privacy is the ability of an individual or group to seclude them or information about themselves andthereby reveal them selectively.

III. CHALLENGES:-

Cloud Computing research addresses the challenges of meeting the requirements of next generation private, public and hybrid cloud computing architectures, also the challenges of allowing applications and development platforms to take advantage of the benefits of cloud computing. The research on cloud computing is still at an early stage. Many existing issues have not been fully addressed, while new challenges keep emerging from industry applications. Some of the challenging research issues in cloud computing are given below are:-

3.1 Service Level Agreements (SLA's): Cloud is administrated by service level agreements that allow several instances of one application to be replicated on multiple servers if need arises; dependent on a priority scheme, the cloud may minimize or shut down a lower level application. A big challenge for the Cloud customers is to evaluate SLAs of Cloud vendors. Most vendors create SLAs to make a defensive shield against legal action, while offering minimal assurances to customers. So, there are some important issues, e.g., data protection, outages, and price structures, that need to be taken into account by the customers before signing a contract with a provider [32].

3.2 Cloud Data Management: Cloud data Can be very large (e.g. text-based or scientific applications), unstructured or semistructured, and typically append-only with rare updates Cloud data management an important research topic in cloud computing. Since service providers typically do not have access to the physical security system of data centers, they must rely on the infrastructure provider to achieve full data security. Even for a virtual private cloud, the service provider can only specify the security setting remotely, without knowing whether it is fully implemented.

3.3 Data Encryption: Encryption is a key technology for data security. Understand data in motion and data at rest encryption. Remember, security can range from simple (easy to manage, low cost and quite frankly, not very secure) all the way to highly secure (very complex, expensive to manage, and quite limiting in terms of access).

3.4 Interoperability: This is the ability of two or more systems work together in order to exchange information and use that exchanged information. Many public cloud networks are configured as closed systems and are not designed to interact with each other. The lack of integration between these networks makes it difficult for organizations to combine their IT systems in the cloud and realize productivity gains and cost savings.

3.5 Access Controls: Authentication and identity management is more important than ever. And, it is not really all that different. What level of enforcement of password strength and change frequency does the service provider invoke? What is the recovery methodology for password and account name? How are passwords delivered to users upon a change? What about logs and the ability to audit access? This is not all that different from how you secure your internal systems and data, and it works the same way, if you use strong passwords, changed frequently, with typical IT security processes, you will protect that element of access.

3.6 Reliability & Availability of Service: The challenge of reliability comes into the picture when a cloud provider delivers on-demand software as a service. The software needs to have a reliability quality factor so that users can access it under any network conditions (such as during slow network connections). There are a few cases identified due to the unreliability of on demand software. One of the examples is Apple's MobileMe cloud service, which stores and synchronizes data across multiple devices. It began with an embarrassing start when many users were not able to access mail and synchronize data correctly

3.7 Common Cloud Standards: Security based accreditation for Cloud Computing would cover three main areas which are technology, personnel and operations. Technical standards are likely to be driven by organizations, such as, Jericho Forum1 before being ratified by established bodies, e.g., ISO2 (International Standard Organization). Currently, one of the main problems is that there are many fragmented activities going in the direction of Cloud accreditation, but a common body for the coordination of those activities is missing. The creation of a unified accreditation body to certify the Cloud services would also be a big challenge [23].

3.8 Platform Management: Challenges in delivering middleware capabilities for building, deploying, integrating and managing applications in a multi-tenant, elastic and scalable environments. One of the most important parts of cloud platforms provide various kind of platform for developers to write applications that run in the cloud, or use services provided from the cloud, or both An operating system provides basic support for executing the application, interacting with storage, and more, while other computers in the environment offer services such as remote storage.

IV. SECURITY ALGORITHM

4.1 DES ALGORITHM The Data Encryption Standard (DES) is a block cipher. It encrypts data in blocks of size 64 bits each. That is 64 bits of plain text goes as input to DES, which produces 64 bits of cipher text. The same algorithm and key are used for encryption and decryption, with minor differences. The key length of this algorithm is 56 bits; however a 64 bits key is actually input. DES is therefore a symmetric key algorithm. The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST).

DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only). General Structure of DES is depicted in the following illustration –

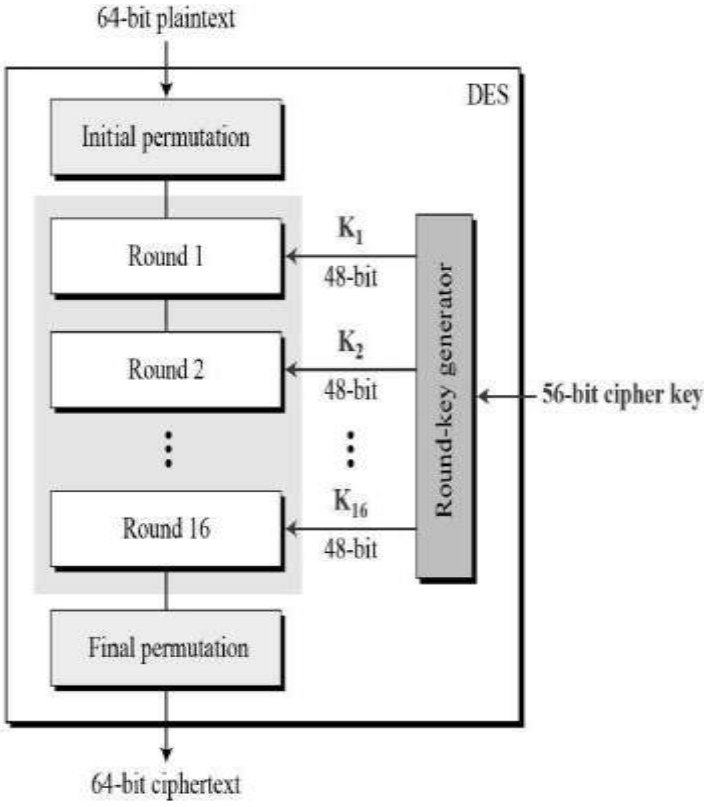

Fig 3:-Data Encryption Algorithm

Data Encryption Standard is one of the most widely accepted, publicly available cryptographic systems. It was developed by IBM in the 1970s but was later adopted by the National Institute of Standards and Technology (NIST), as Federal Information Processing Standard 46 (FIPS PUB 46).

Advantages: The Avalanche Effect is the major advantage which states that "A slight in a char or bit change in the plaintext will drastically change the cipher text" [3].

Disadvantages: Memory Requirement and Simulation Time is more in case of DES.

4.2 AES ALGORITHM Advanced Encryption Standard (AES), also known as Rijindael is used for securing information. AES is a symmetric block cipher that has been analyzed extensively and is used widely now-a-days. How AES works in cloud environment? AES, symmetric key encryption algorithm is used with key length of 128-bits for this purpose. As AES is used widely now-a-days for security of cloud. Implementation proposal states that First, User decides to use cloud services and will migrate his data on cloud. Then User submits his services requirements with Cloud Service Provider (CSP) and chooses best specified services offered by provider. When migration of data to the chosen CSP happens and in future whenever an application

 ISSN: 2321-8169
194 – 200

uploads any data on cloud, the data will first encrypted using AES algorithm and then sent to provider. Once encrypted, data is uploaded on the cloud, any request to read the data will occur after it is decrypted on the users end and then plain text data can be read by user. The plain text data is never written anywhere on cloud. This includes all types of data. This encryption solution is transparent to the application and can be integrated quickly and easily without any changes to application. The key is never stored next to the encrypted data, since it may compromise the key also. To store the keys, a physical key management server can be installed in the user's premises. This encryption protects data and keys and guarantees that they remain under user's control and will never be exposed in storage or in transit. AES has replaced the DES as approved standard for wide range of applications**.**

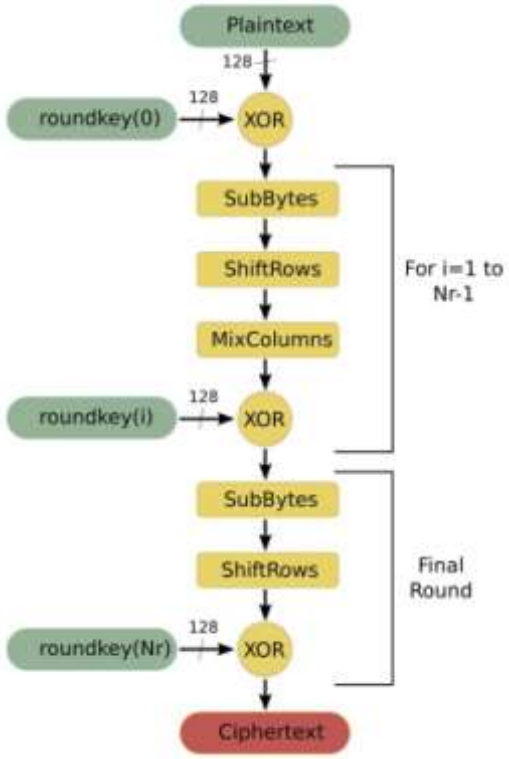

Fig 4:-Advanced Encryption Standard

Advanced Encryption Standard, is the new encryption standard recommended by NIST to replace DES in 2001. AES is one the most efficient symmetric algorithm.

Advantages:

- It provides strong security from the attackers.
- But as the years passed by it was prone to a few attacks which were lesser when compared to DES, till datethe only attack on it was Brute Force attack.

Disadvantages:

- The major drawback is that it could not withstand with the attacks like Brute Force, Linear crypt Analysis,because during its design this attack wasn't invented.

V. IMPLEMENTATION AND RESULTS

VI. CONCLUSION

The strength of cloud computing is the ability to manage risks in particular to security issues. Security algorithms mentioned or encryption and decryption can be implementing in future to enhance security over the network. In this,

we will extend our research by providing algorithm implementations and producing results to justify our concepts of security for cloud computing. Cloud computing is defined as the set of resources or services offered through the internet to the users on their demand by cloud providers. As each and every organization is moving its data to the cloud, means it uses the storage service provided by the cloud provider. So there is a need to protect that data against unauthorized access, modification or denial of services etc.

REFERENCES

[1] LeenaKhanna, AnantJaiswal, "Cloud Computing: Security Issues and Description of Encryption Based Algorithms to Overcome Them", IJARCSSE 2013.

[2] G Devi, Pramod Kumar "Cloud Computing: A CRM Service Based on a Separate Encryption and Decryption using Blowfish algorithm" IJCTT 2012 .

[3] Burton, H. (2014). 'Cloud computing - Separating fact from fiction'. The Guardian, 2014.Retrieved 10th January, 2015 from http://www.theguardian.com/medianetwork/partner-zone-microsoft/cloud-computingseparating-fact.

[4] Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J. and Brandic, I. (2009). "Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility," Future Generation Computer Systems (25)6.

[5] Cisco (2013). The Cloud in Africa: Reality Check. Retrieved December 15th, 2014 from http://www.cisco.com/web/ZA/press/2013/112813.html.Com pTIA (August, 2013). Trends in Cloud Computing: Full Report, August 2013. Retrieved 17th March, 2015 from www.comptia.org

[6] Heiser, J. and Nicolett, M. (2008). Assessing the Security Risks of Cloud Computing. Gartner.Hinchcliffe, D. (5th June, 2009). Eight ways that Cloud Computing will Change Businesses,Retrieved March 13th, 2015 from http://www.zdnet.com/blog/hinchcliffe/eight-waysthat-Cloud-computing-will-changebusiness/488

[7] International Data Corporation (IDC) (2012). White Paper: Cloud Computing's Role in JobCreation, 2012. Retrieved 9th February, 2015 from http://people.uwec.edu/HiltonTS/ITConf2012/NetApp2012Paper.pdf

[8] Jinzy, Z. (2010). Cloud Computing Technologies and Applications, Handbook of Cloud Computing, 2010, retrieved 6th March, 2015 from http://www.springer.com/978-1-4419-6523-3

[9] Kim, W. (2009). Cloud Computing: Today and Tomorrow.Journal of Object Technology. 8(1):p. 65-72.

[10] J. Baek, R. Safavi-Naini, and W. Susilo. Public key encryption with keyword search revisited. In International conference on Computational Science and Its Applications, pages 1249-1259. Springer-Verlag, 2008.

[11] Q.Wang, C.Wang, J. Li, K. Ren, and W. Lou. Enabling public verifiability and data dynamics for storage security in cloud computing. In European Symposium on Research in Computer Security (ESORICS '09), volume 5789 of Lecture Notes in Computer Science, pages 355{370.Springer, 2009.

[12] MIT International Journal of Computer Science and Information Technology, *Vol. 6, No. 1, January 2016, pp. 1-6* 6 ISSN 2230-7621©MIT Publications .

[13] International Journal of Latest Trends in Engineering and Technology (IJLTET) ISSN: 2278-621X.

[14] International Journal of Engineering Research ISSN:2319-6890)(online),2347-5013(print) Volume No.3, Issue No.4, pp : 221-225 01 April 2014.

ACKNOWLEDGEMENT

I would like to thank my guide Ms. ShabnamKumari for her indispensible ideas and continuous support, encouragement, advice and understanding me through my difficult times and keeping up my enthusiasm, encouraging me andfor showing great interest in my dissertation work, this work could not finished without her valuable comments and inspiring guidance.