INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

A Review of Security of Data Using Cryptographic Algorithms in Cloud Computing

Gurpreet Kaur [1], Manish Mahajan[2]

[1]M.Tech, Chandigarh Engineering Collage
gurpreetkpuar@gmail.com

[2]Chandigarh Engineering Collage
cec.manish@gmail.com

Abstract: *Cloud computing is the dramatic advancement of the computer technology. During the last many decades, the network and the computer technology changes, due to which it allows the humans to share the large amount of information. Cloud computing is necessary for all that information. Cloud computing is necessary for easily and virtualized resources. These resources include hardware, development platforms and the services. To meet these demands the system designers are constantly looking for new system architectures and algorithms. These are helpful to process larger collections of data more quickly than is feasible with today's systems. Now days computers become smaller and less expensive due to which it is very helpful to assemble the large and powerful system. The main problem in cloud computing is security and the data privacy. In this paper proposed the new level of data security solution with enhance the security of data using cryptographic algorithms.*

Index Terms: Cloud computing, Data security, algorithms, cryptography

1. INTRODUCTION:

Cloud computing is the emerging technology. It grows day by day. It is the broad solution that uses the information technology as its service. It supports the data and the applications by the use of internet and remote servers. It helps the users to transfer their personal data to another computer and used that data, with the help of internet. The person can access their data with no installation at all. Before cloud computing, websites and server based applications were executed on a specific system [1]. The cloud computing flexibility is a function of the allocation of resources on authority request and the cloud computing provides the act of uniting. Cloud computing is used to provides various computing and storage services over the Internet [2].

Cloud computing incorporates the incorporate the infrastructure, platform, and software as services. These services are provides by the service providers. The service provider rent data center hardware and software to deliver storage and computing services through the Internet. Internet users can receive services from a cloud as if they were employing a super computer which be using cloud computing. To storing data in the cloud instead of on their own devices and it helps to make the data access easy and possible for the users. They can run their applications on much more powerful cloud computing platforms with software deployed in the cloud which mitigating the users burden of full software installation and continual upgrade on their local devices.

Features of cloud computing

- **Scalable**

Cloud computing is scalable. Whenever user needs more resources, it can add it to the cloud anytime. The cloud computing is known as the infinite pool of resources.

- **Environment friendly**

Cloud computing makes efficient use of hardware which helps to reduce energy cost.

- **Cost efficient**

The cloud computing is cost efficient. For the cloud computing, we have to pay the amount, which we used just like electricity bill.

- **Up to date**

We need not to worry about the updates to the software's and hardware's that we are using in the cloud. The provider is responsible for the overall update process of all the components [3].

- **Improved performance**

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

Whenever we need some high configuration resources it will be available to the user on its demand [3].

Cloud Computing Architecture

Cloud computing system is divides into two sections: the front end and the back end. They connect to each other through a network, usually the internet. The front end is the side the computer user. The back end is the cloud section of the system. The front end includes the client's computer and the application. It requires accessing the cloud computing system. On the back end of the system are the various computers, servers and data storage systems that create the cloud of computing services.[4] A cloud computing system could include any computer program from data processing to video games.

Usually, each application will have its own dedicated server. A central server administers the system, monitoring traffic and client demands to ensure everything runs smoothly. It follows a set of rules called protocols and uses a special kind of software called middleware**.** Middleware allows networked computers to communicate with each other. Most of the time servers don't run at full capacity. Hence it is possible to fool a physical server. The physical server may think that there are multiple servers and each running with its own independent operating system. The technique is called server virtualization. By maximizing the output of individual servers, server virtualization reduces the need for more physical machines.

Cloud computing systems need at least twice the number of storage devices it requires to keep all its clients information stored. A cloud computing system must make a copy of all its clients information and store it on other devices.[4] The copies enable the central server to access backup machines to retrieve data that otherwise would be unreachable. Making copies of data as a backup is called redundancy.

Cloud Computing Applications

The applications of cloud computing are practically limitless. With the right middleware, a cloud computing system could execute all the programs a normal computer could run. Potentially, everything from generic word processing software to customized computer programs designed for a specific company could work on a cloud computing system. There are some basic applications of cloud computing:

- Clients would be able to access their applications and data from anywhere at any time. They could access the cloud computing system using any computer linked to the internet.
- Cloud computing systems would reduce the need for advanced hardware on the client side. You wouldn't need to buy the fastest computer with the most memory [5] because the cloud system would take care of those needs for you.
- Corporations that rely on computers have to make sure they have the right software in place to achieve goals. Cloud computing systems give these organizations company wide access to computer applications. The companies don't have to buy a set of software or software licenses for every employee.
- Servers and digital storage devices take up space. Some companies rent physical space to store servers and databases because they don't have it available on site. Cloud computing gives these companies the option of storing data on someone else's hardware, removing the need for physical space on the front end.

2. LITERATURE SURVEY:

Dr. A. Padmapriya et.al describes that the cloud computing is a broad solution that delivers IT as a service. Cloud is an internet based technology uses the internet & central remote servers to support data and applications.[6] It permits consumers and businesses putting to use without installation and approach their personal files at any computer with internet access. Before cloud computing, websites and server based applications were executed on a specific system. There are various security challenges present in the cloud computing, such as loss of data or data theft. The five types of issues are presented in the cloud computing: Data Issues, Privacy issues, infected application, Security issues, Trust Issues. There are various techniques are used to solve these problems. The encryption is a well known technology for protecting sensitive data.

Parsi Kalpana, Sudha Singaraju have proposed a method by implementing RSA algorithm to ensure the security of data in cloud computing. RSA algorithm used to encrypt the data to provide security so that only the concerned user can access it.[7] The purpose of securing data, unauthorized access does not allow. RSA consists of Public-Key and Private-Key. In the proposed Cloud environment, Pubic-Key

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS…..

is known to all, whereas Private-Key is known only to the user who originally owns the data. Thus, encryption is done by the Cloud service provider and decryption is done by the Cloud user or consumer. Once the data is encrypted with the Public-Key, it can be decrypted with the corresponding Private-Key only.

Sonal Guleria, Dr. Sonia Vatta describes that the Cloud computing is emerging field because of its performance, high availability, least cost and many others. In cloud computing, the data will be stored in storage provided by service providers**.** Cloud computing provides a computer user access to Information Technology (IT) services which contains applications, servers, data storage, without requiring an understanding of the technology. An analogy to an electricity computing grid is to be useful for cloud computing. To enabling convenient and on-demand network access to a shared pool of configurable computing resources are used for as a model of cloud computing.[8] Cloud computing can be expressed as a combination of Software-as-a-Service which refers to a service delivery model to enabling used for business services of software interface and can be combined creating new business services delivered via flexible networks and Platform as a Service in which Cloud systems offering an additional abstraction level which supplying a virtualized infrastructure that can provide the software platform where systems should be run on and Infrastructure as a Service which Providers manage a large set of computing resources which is used for storing and processing capacity. But still many business companies are not willing to adopt cloud computing technology due to lack of proper security control policy and weakness in safeguard which lead to many vulnerability in cloud computing. This paper has been written to focus on the problem of data security. To ensure the security of users' data in the cloud, we propose an effective and flexible scheme with two different algorithms .A user can access cloud services as a utility service and begin to use them almost instantly. These features that make cloud computing so flexible with the fact that services are accessible anywhere any time lead to several potential risks. The key intent of this research work is to investigate the existing security schemes and to ensure data confidentiality, integrity and authentication.

Pradeep Bhosale et.al discuss that today's world relies on cloud computing to store their public as well as some personal information which is needed by the user itself or some other persons. Cloud service is any service offered to its users by cloud. As cloud computing comes in service there are some drawbacks such as privacy of user's data, security of user data is very important aspects. In this paper author discuss about the enhancement of data security. Not only this makes researchers to make some modifications in the existing cloud structure, invent new model cloud computing and much more but also there are some extensible features of cloud computing that make him a super power.[9] To enhance the data security in cloud computing used the 3 dimensional framework and digital signature with RSA Encryption algorithm. In 3 Dimensional frameworks, at client side user select the parameters reactively between CIA (Confidentiality, Integrity & Availability) and before actual storing the data in cloud a digital signature is created using MD 5 Algorithm and then RSA Encryption algorithm is applied then it stored on cloud.

3. PURPOSED WORK

Now days, Information security is a critical issue in cloud computing environments. Clouds have no borders and the data can be physically located anywhere in any data centre across the network geographically distributed.[10] So the nature of cloud computing raises serious issues regarding user authentication, information integrity and confidentiality. With the cloud model, you lose control over physical security. In a public cloud, you are sharing computing resources with other companies. In a shared pool outside the enterprise, you do not have any knowledge or control of where the resources run. Simply because you share the environment in the cloud, may put your data at risk of seizure. Storage services provided by one cloud vendor may be incompatible with other vendor's services. Data integrity is assurance that the data is consistent and correct. Ensuring the integrity of the data really means that it changes only in response to authorized transactions [11]. The cloud service provider for cloud makes sure that the customer does not face any problem such as loss of data or data theft. There is also a possibility where a malicious user [12] can penetrate the cloud by impersonating a legitimate user, there by infecting the entire cloud.
They used the various algorithms to solve the problem like:

RSA Algorithm: RSA algorithm was introduced by Rivest, Shamir & Adleman of MIT; RSA is an

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

extensively used public key crypto mechanism it is based on exponentiation in a finite field over integers modulo a prime numbers. To encrypt a message M the sender has to obtain public key of recipient PU={e,n} to compute the cipher: C = Me mod n, where 0≤M<n and similarly for decryption the recipient uses their private key PR={d,n} and computes: M = Cd mod n it is
important that the message M must be smaller than the modulus n (block if needed).How it works , RSA uses Euler's Theorem: aø(n)mod n = 1 where gcd(a,n)=1 in RSA we have to initially calculate n=p.q such that ø(n)=(p-1)(q-1) one has to carefully chose e & d to be inverses mod ø(n) .

- **Key Generation**-RSA must determine two primes at random - p, q next is to select either e or d and compute the other primes p,q must not be easily derived from modulus n=p.q means must be sufficiently large and use probabilistic test exponents e, d are inverses, so use Inverse algorithm to compute at the other end.

AES Algorithm:

a) Key Expansion - round keys are derived from the cipher key using Rijndael's key schedule

b) Initial Round

AddRoundKey - each byte of the state is combined with the round key using bitwise xor

c) Rounds

1. Sub Bytes - a non-linear substitution step where each byte is replaced with another according to a lookup table.
2. Shift Rows - a transposition step where each row of the state is shifted cyclically a certain number of steps.
3. Mix Columns - a mixing operation which operates on the columns of the state, combining the four bytes in each column.
4. AddRoundKey

d) Final Round (no Mix Columns)

1. Sub Bytes
2. Shift Rows
3. AddRoundKey

e) Key generation

This module handles key generation by the server side. The server generates unique keys for users once they authenticate themselves with the server. The key is generated using instances of AES key generator class. This key is then transferred to the cloud client via the LAN Wi-Fi connection which receives and stores a copy for it for decrypting purpose. The key is a 16 byte or a 128 bit key. An Example of a key generated is: 8xRER4LyFiU3Hs9a40xExQ== After the key generation and encryption, the cipher text is sent to the client, the client uses the reverse process of the AES encryption. Decryption to obtain the original plaintext that was transferred by the server. Hence the client receives the intended file in a secure manner over the LAN.

5.3 SHA Algorithm

Secure Hash Algorithm converts an arbitrary size message to fixed size message digest or a hash code by processing message in blocks through some compression function either custom or block cipher based mode. Hash function can be applied to any sized message M and it produces fixed-length output h .therefore it is easy to compute**.** In our model for enhanced authentication the hash value of the message i.e. a message digest is generated using secure hash algorithm which is of constant size for any arbitrary length of data is concatenated with the digital
signature and the encrypted actual data as a string and the entire concatenated string is encrypted using the public key of the receiver and sent to that intended requesting recipient in the cloud therefore the deciphered message later used to generate the message digest (hash value) in turn by the secure hash algorithm for data integrity verification and digital finger print validated using RSA algorithm as conformance for the sender's authentication.

h= H (M) for any message M.

4. CONCLUSION AND FUTURE WORK

To solve these problems in clouds there are several techniques used. It has been described in about the overview of privacy issues within cloud computing and a detailed analysis on privacy threat based on different type of cloud scenario was explained, the level of threat seem to vary according to the application area. Their work has stated the basic guidelines for software engineers when designing cloud services in particular to ensure that privacy are not mitigated. The major focus of their schemes rests on the privacy risks, analysis on privacy threats, privacy design patterns and accountability with in cloud computing scenario. In [13] it clearly stated about the issues associated in choosing a security

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

mechanisms or security frameworks in the Cloud computing context and given a brief outline on flooding attacks. Also they have given an idea about, the threats, their potential impact and relevance to real-world cloud environment. It is well understood from their investigation, a significant pace for improving data security in cloud is to initial intensification of the security competence of both web applications and frameworks.

REFERENCES

[1] Cloud computing principles, systems and applications NICK Antonopoulos http://mgitech.wordpress.com.

[2] Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. (2009, Feb. 10). Above the clouds: A Berkeley view of cloud computing. EECS Dept., Univ. California, Berkeley, No. UCB/EECS-2009-28.

[3] http://en.wikipedia.org/wiki/Cloud_computing

[4] http://www.howstuffworks.com/cloud-computing/cloud-computing1.htm

[5] http://www.howstuffworks.com/cloud-computing/cloud-computing2.htm

[6] Cloud computing methodology, systems and applications lizhe wang, rajiv Ranjan.http://www.unitiv.com.

[7] Parsi Kalpana, Sudha Singaraju,"Data Security in Cloud Computing using RSA

[8] Sonal Guleria1, Dr. Sonia Vatta2,TO ENHANCE MULTIMEDIA SECURITY IN CLOUD COMPUTING ENVIRONMENT USING CROSS BREED ALGORITHM, Web Site: www.ijaiem.orgEmail:editor@ijaiem.org, editorijaiem@gmail.com, Volume 2, Issue 6, June 2013

[9] Pradeep Bhosale Priyanka Deshmukh Girish Dimbar Ashwini Deshpande , Enhancing Data Security in Cloud Computing Using 3D Framework & Digital Signature with Encryption, International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 8, October – 2012

[10] Siani Pearson"Taking account of Privacy when Designing Cloud computing Services CLOUD'09, May 23, 2009, Vancouver, Canada ,2009 IEEE

[11] Rohit Bhadauria, Rituparna Chaki, Sugata Sanyal, "A Survey on Security Issues in Cloud Computing", 2011

[12] John Harauz , Lori M.Kaufman ,Bruce potter,"Data security in world of cloud computing" by IEEE computer and reliability societies,jul/Aug 2009 pp 61-64

[13] Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacono, "On technical security issues in cloud computing" 2009, IEEE Computer Society