Volume 1, Issue 1, April 2016 ISSN: 2456-0006
International Journal of Science Technology Management and Research
Available online at: www.ijstmr.com

An Efficient Algorithm for Securing Data in Cloud Computing

Bhushan Patil
Electronics & Telecommunication
R.C.Patel Institute of Technology
Shirpur, India
patilbhushan007@gmail.com

Punam Patil
Computer Engineering
R.C.Patel Institute of Technology
Shirpur, India
patilpunam25@gmail.com

Abstract: ***To share and provide according to demand an information, resources and number of software's is collectively called as cloud computing. To secure the huge amount of data is important part in networking. Therefore, Data security over cloud is main and an important issue. So different techniques are arises as the technology change. At various levels in a cloud, different techniques are used. So in this paper we gave overview on various technologies related to encryption, decryption techniques, to provide the security as numbers of users are connected continuously to network. We also presented how encryption based techniques used to store data over cloud.***

Keywords: ***Cloud Computing, Encryption, Data security, Decryption***

INTRODUCTION

With the emerging trends in technologies as advancement there is a huge amount of data is used and preferred by different number of user on a network at the same time, related to resources, software an also information exchange. So generally the term referred is a "Cloud Computing". In cloud computing for the number of services the user has to pay first for that facility and then to use that as pay-as-per-use facility. That means in cloud computing the tasks from individual system are moved across through cloud to number of/or multiple systems at a time.

As the advancement, it has used in small as well as large type of organization to used internet based services which reduces start up-cost, capital expenditure and access applications as per needed only. Cloud computing provides services related to IT like, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). There are various algorithms used for to secure data in cloud computing. There are four ways in which cloud services are deployed are Public cloud, Private cloud, Hybrid cloud and Managed cloud. To provide security in cloud it can be achieved by using cryptography technique, which is the science of overthrow information to ensure confidentiality, privacy, integrity, authentication, access control. The major functions of cryptography are encryption and decryption.

The basic structure of cloud computing is as shown in below figure 1 as,

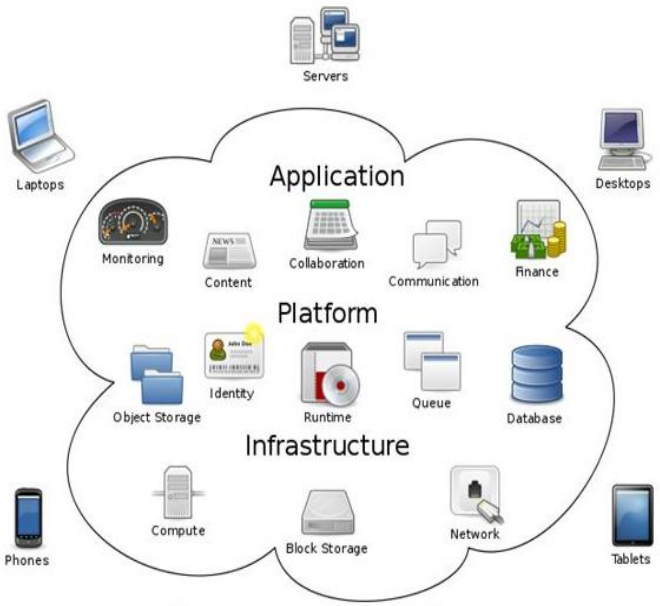


Fig.1 Basic Structure of cloud computing

There are number of characteristics of cloud computing like as service oriented, it has loose coupling, strong fault tolerant, it based on TCP/IP and also it provides high security. In cloud computing, this is made up with three different elements like Client, Data Center and Distributed servers. A client includes computers, laptops, tablet computers, mobile phones, or PDA. The Datacenter is the collection of servers where the application is house for which subscription is given by client. The below table 1 shows the various General Terms used in Cloud Computing.

Table I
General Terms in Cloud Computing

Sr. No.	General Term	Concept
1	**CDIBA** (Cloud Data Integrity Backup Agent)	It defines set of rules for backup data on cloud which is in "cloud zone".
2	**CS** (Cloud Servers)	Managed by the cloud service providers.
3	**CSPA** (Cloud Service Provider Agent)	It provides security service tasks according to Service Level Agreements.
4	**CSP** (Cloud Service Provider)	It expert in building and managing the distributed servers
5	**DSA** (Digital Signature Algorithm)	The authenticity of a digital message input and output
6	**MAS** (Multi Agent System)	Different number of agents communicate with each other
7	**POR** (Proof of Retrieve ability)	It detects data corruption & gives guarantee of file retrieve ability.
8	**QOS** (Quality of Service)	It is the activity which promotes customer satisfaction
9	**RSA** (Rivest, Shamir and Adleman)	It used for encryption and authentication
10	**TPA** (Third Party Auditor)	It verifies over that of cloud server

SERVICES IN CLOUD COMPUTING

Various types of services are offered by cloud computing like Utility Services, Managed services, Service Commerce, Web Based services etc. But mainly three types of services which are provided by cloud computing for IT are given as below. The below figure 2 shows the three types of services used.

i) Infrastructure as a Service
ii) Platform as a Service
iii) Software as a Service

Fig. 2 Services in cloud computing

The below table 2 depicts the three types of services with its basic idea, advantages and disadvantages as,

Table II
Services types in Cloud Computing

Types of Service	Description	Examples	Advantage	Disadvantage
Infrastructure as a Service **(IaaS)**	provides basic storage with computing capabilities	Amazon, Google, Microsoft, IBM	has control over operating systems, storage, deployed applications	customer does not manage or control the underlying cloud infrastructure
Software as a Service **(SaaS)**	service on demand, a complete application is offered to customer	Google, Salesforce, Microsoft, Zoho	only a single application needs to be hosted and maintained	limited user-specific application configuration settings
Platform as a Service **(PaaS)**	Customer has freedom to build its own applications	Linux, Apache, MySql and PHP platform, restricted J2EE, Ruby	customer does not manage or control the underlying cloud infrastructure, network, servers, operating systems, or storage	control over the deployed applications and possibly over the application hosting environment configurations

Therefore as per above table II we can overview about various services in cloud computing in different perspective give us, SaaS provides a high level of security and also a large amount of integrated features but PaaS offers less integrated features as it offers to developers for building of their own applications and in nature it is more extensible than SaaS. IaaS less security capabilities and functionalities as applications used, O.S (Operating System), contents are managed by customers itself.

PROPOSED WORK

All To provide the security, we proposed simple and effective method at storage level of cloud is encryption and decryption. As at storage level, data encryption provides integrity and also confidentiality. The below diagram shows simple schematic for encryption and decryption process.

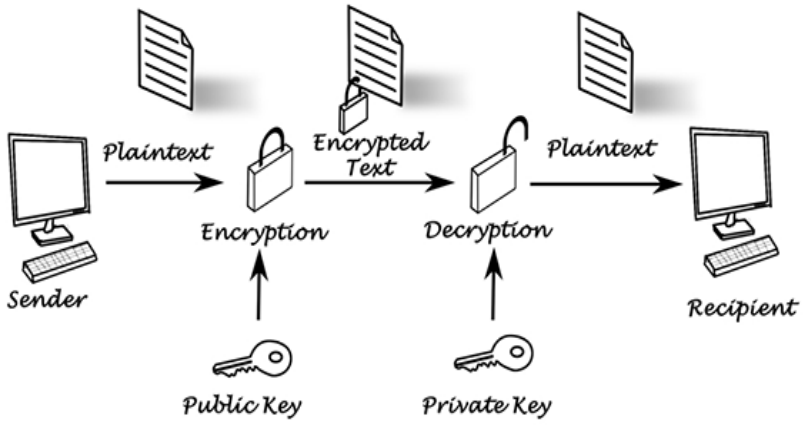


Fig.3 Encryption and Decryption

A. Encryption:

To provide security, a most effective and efficient approach is Encryption, which is used to encrypt the file. To read an encrypted file, there is a need of secret key. Encryption is a process of converting plain text into cipher text. After encryption the file will be in cipher form.

One of the common approaches used to encrypt with shared key algorithm and public key is randomly generated. For this purpose we create public and private RSA key for encrypting the files and then stored it in a cloud. The size of generated private key is 2048 bits. Generally, Secret key is related to symmetric encryption and public key is asymmetric encryption.

ALGORITHM OF ENCRYPTION:

1: Read data one character at a time i.e. character by character.
2: Assignment of 5-digit binary code to character & form table.
3: For same length, use encrypted block to convert into another block of character & then take column-wise value.
4: Result store characters block in encrypted format & continue this for all words.
5: Find length for each word and also total length of character.
6: Stop

B. Decryption:

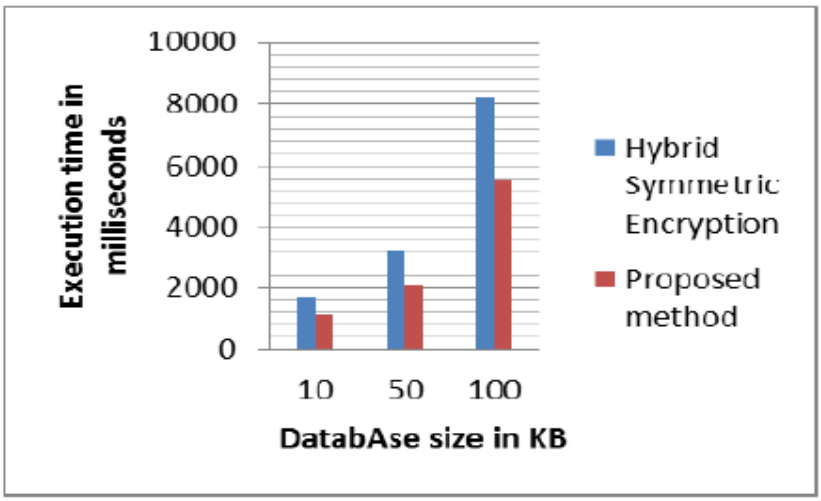
As opposed to encryption technique, Decryption technique is work. It is used to decrypt the files and also private key is generated to access the files from cloud. For each end user separate private key is generated to access data from any location by providing security. In this technique, Non-shared private key is used to decrypt files. The private key is an asymmetric technique. When decrypting files private key is generated for accessing to ensure file access control.

ALGORITHM OF DECRYPTION:

1: Decryption performed for a given key as per block size & take value row wise.
2: Then decrypt each character by block size and evaluate value row wise
3: Repeat same value for each word from encryption
4: With use of key value & block find word length from block

COMPARITIVE RESULTS & DISCUSSION

The proposed algorithm is compared with Hybrid encryption techniques on basis of efficiency. With this we used different database size and then calculate execution time required for that. From the below graph it is clear that proposed method take less time to encrypt the data.



CONCLUSION AND FUTURE WORK

The proposed approach with 5-bit code is extendable. As number of characters increases there is no requirement of extra bit code as other bit uses extra bit in code. Therefore that process is difficult one and also in lengthy form. Also proposed approach give best result as compared to Hybrid encryption techniques. In future we extend this approach to include special characters in encryption and decryption process.

REFERENCES

1. Prakash G L, Dr. Manish Prateek, and Dr. Inder Singh, "Data Security Algorithms for Cloud Storage System using Cryptographic Method", International Journal of Scientific & Engineering Research, ISSN 2229-5518, PP. 54-61, Volume 5, Issue 3, March -2014.
2. Swapnil V.Khedkar , A.D.Gawande, "Data Partitioning Technique to Improve Cloud Data Storage Security", Internation.al Journal of Computer Science and Information Technologies (IJCSIT), PP. 3347-3350, Vol. 5 (3), 2014.
3. Weichao Wang, Zhiwei Li, Rodney Owens, Bharat Bhargava, "Secure and Efcient Access to Outsourced Data", CCSW'09, Chicago, Illinois, USA, November 13, 2009.
4. Dr. L. Arockiam, S. Monikandan, "Data Security and Privacy in Cloud Storage using
5. Hybrid Symmetric Encryption Algorithm", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue 8, August 2013.
6. Poonam M. Pardeshi, Prof. Bharat Tidke, "Improving Data Integrity for Data Storage Security
7. in Cloud Computing", (IJCSIT) International Journal of Computer Science and Information Technologies, PP. 6680-6685, Vol. 5 (5), 2014.
8. Dr.M.Gobi, Karthik Sundararaj, "A Secured Cloud Security Using Elliptic Curve cryptography", Proceedings of the UGC Sponsored National Conference on Advanced Networking and Applications, 27th March 2015.