# Cryptographic Data Security over Cloud

**Er. Lalit Gehlod**
Asst.Professor, Dept.Of Computer Engineering,
Institute Of Engineering & Technology,
Devi Ahilya University, Indore, India.

**Govind Patidar**
Dept. Of Information Technology,
Institute Of Engineering & Technology,
Devi Ahilya University, Indore, India.

**Abstract— During the file access and storage the files are travelling through the secured network to the host, thus the security in the files are required to incorporate with the files. For securing the files in the cloud various cryptographic approaches are used but most of them increase the computational cost of file storage. Thus a new technique is required to develop which efficiently used for data storage and data access.**
**Therefore the presented work is intended to find an approach by which the security in file hosting and management can play an important role. Therefore the given technique incorporates the SHA and AES encryption algorithms to secure the files in the server and for increasing the transfer rate of the data the file is used. The implementation of the proposed secure technique is performed using the JAVA technology and their performance in terms of time complexity and storage overhead computed.**
**The results claim the efficient methodology of file hosting and distribution in the cloud storage additionally that is efficient during the fast upload and downloads. Thus the proposed technique is adoptable and secure for secure storage services.**

**Keywords—cloud computing, SHA (Secure Hash Algorithm), AES (Advanced Encryption Standard) algorithm, sharable resources, cryptographic approach, computational cost, and Transfer rate.**

## 1. INTRODUCTION

Cloud computing is an efficient weapon for new generation technology. Using cooperative and huge infrastructure this environment provides essential and efficient computing resources. In this environment, resources are shared among all of the servers, users and individual clients. These sharable resources are any kind of data files or any computational resource like memory or other. Due to storage and sharable characteristics the cloud becomes open for all. Therefore, data or files of an individual can be available for all other users of the cloud. Thus the data or files become more vulnerable to attack or untrusted data access. Hence, it is very easy for an intruder to access, misuse and destroy the original form of data. An intruder can also interrupt the communication. Hence, it is extremely essential for the cloud to be secure. On the other hand, it is also necessary to protect the data or files in the midst of unsecured processing and during file transfer. In order to solve these issues new security architecture for cloud computing platform is proposed in this study. Cloud computing is defined as a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications [1].

The basic concept of the proposed security model is to provide access control and privacy using the cryptographic process of data manipulation. In addition of that for secure access design an authentication system by which the original client data and the data owner can be distinguishable during file access and data management. Therefore, the security system is lead to provide authentication and security. This technique helps to reduce the computational complexity of the previously available data model and enhancing the request and response time for the security system.

Cloud computing is a general term for anything that involves delivering hosted services over the Internet. These services are broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS).
IAAS is “Infrastructure as a Service”. Here you are provided the physical infrastructure (server, storage, network, etc.) by a vendor which you can access over internet and use to install your software, build or deploy your applications. Infrastructure as a service (IaaS) is a standardized, highly automated offering, where compute resources, complemented by storage and networking capabilities are owned and hosted by a service provider and offered to customer’s on-demand. Customers are able to self-provision this infrastructure, using a Web-based graphical user

interface that serves as an IT operations management console for the overall environment [2]. IaaS is defined as computer infrastructure, such as virtualization, being delivered as a service [3].

PaaS is "Platform as a Service". Here a server along with a software environment (database web server etc.) is provided. You can use the environment to build your applications and deploy it for use by your organization. Cloud platform services, or Platform as a Service (PaaS), are used for applications, and other development, while providing cloud components to software. PaaS makes the development, testing, and deployment of applications quick, simple, and cost-effective. With this technology, enterprise operations, or a third-party provider, can manage OSes, virtualization, servers, storage, networking, and the PaaS software itself [4].
SaaS is "Software as a Services". In this you have the complete application for a given purpose which you use with or without customization Software as a Service (SaaS) is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet [5][6]. It is sometimes referred to as "on-demand software.

## 2. BACKGROUND

This section reports the different techniques and research articles that support the privacy preserving and data owner management.

Cloud Computing is the long dreamed vision of computing as a utility, where users can remotely store their data into the cloud. By data outsourcing, users can be relieved from the burden of local data storage and maintenance. In order to enabling public audit ability for cloud data storage security is of critical importance. To securely introduce an effective third party auditor (TPA), the following two fundamental requirements: 1) TPA should be able to efficiently audit data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user; 2) The third party auditing process should bring in no new vulnerabilities towards user data privacy. In this paper, ***Cong Wang et al [7]*** utilize and uniquely combine the public key based homomorphic authenticator with random masking to achieve the privacy-preserving public cloud data auditing system, which meets all requirements. To support efficient handling, author further explore the technique of bilinear aggregate signature to extend the main result into a multi-user setting, where TPA can perform multiple auditing tasks. Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient.

For protecting data privacy, sensitive data have to be encrypted before outsourcing, which obsoletes traditional data utilization based on plaintext keyword search. Thus, enabling an encrypted cloud data search service is important. In this paper, ***Ning Cao et al [8]*** define and solve the challenging problem of privacy-preserving multi-keyword ranked search. Author establishes a set of strict privacy requirements for a secure cloud data system. Among various multi-keyword semantics, they choose the efficient similarity measure of "coordinate matching," In further "inner product similarity" to quantitatively evaluate similarity measure. First a basic idea for the MRSE based on secure inner product computation, and then give two significantly improved MRSE schemes to achieve various privacy requirements. To improve search experience, further extend these schemes to support more search semantics. Thorough analysis investigating privacy and efficiency guarantees of proposed schemes is given. Experiments on the real-world data set further show proposed schemes indeed introduce low overhead on computation and communication.

In this paper ***C. Selvakumar et al [9]*** introducing a partitioning method for data storage which avoids the local copy at the user side by using partitioning method. This method ensures high cloud storage integrity, enhanced error localization and easy identification of misbehaving server. To achieve this, remote data integrity checking concept is used. This work aims to store data in reduced space with less time and computational cost.

Storing data in a third party's cloud system causes serious concern over data confidentiality. General encryption schemes protect data confidentiality, but also limit the functionality of the storage system. W. ***Sharon Inbarani et al [10]*** propose a threshold proxy re-encryption scheme and integrate it with decentralized erasure code such that a secure distributed storage system is formulated. The distributed storage system not only supports secure and robust data storage and retrieval, but also lets a user forward his data in the storage servers to another user without retrieving the data back.

According to ***EmilianoMiluzzo et al [11]*** Cloud service providers invest significant effort into designing, building, and empowering cloud infrastructures. At the same time, technological advances are commoditizing small devices with powerful compute, storage, and communication capabilities at unprecedented scale.

***KalyaniBangale et al [12]*** present a method to secure data collection server by protecting and developing backups for Health Care Cloud. The Objective of SRHDCS is to provide Auto Response Server, Better Solutions for Data Backup and Restore using Cloud, Availability of data remotely using safer protected data transmission and Confidentiality of data remain intake. The SRHDCS can collect data and send to a centralized repository in a platform independent format without network consideration. The purpose of SRHDCS is to help users (basically admin) to collect information from any remote location even if network connectivity is not available at that point of time.

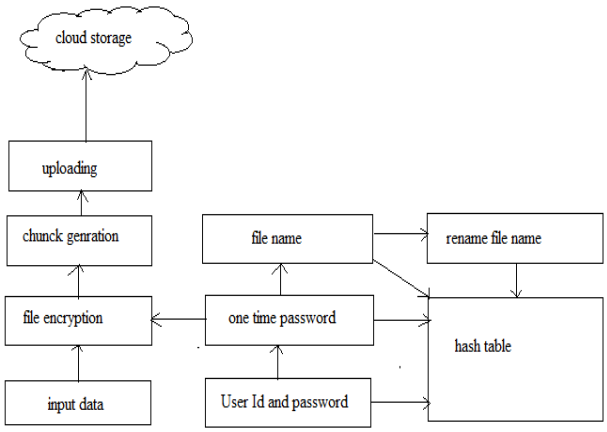
***V. Malligai et al [13]*** studied about cloud and says Mobile device such as smart phones has increasingly become powerful. Smart phones are not only with voice oriented device but also equipped with wide capabilities with internet access. As mobile devices become more like PC's, it tends to carry and store all kinds of data, in cloud that can be accomplished for Google Android phones. The primary objective of "cloud based mobile data storage system" is to create a full-fledged Android app where we can store all kind of data in cloud and access. The user can retrieve all data in mobile itself and can also access this data through web. Thus it reduces the overhead of using only mobile to get back the data which serves the purpose of making our data secure and flexible to be available anywhere.

We can store and retrieve the data as we like using cloud computing. To maintain the data security in distributed environment ***P.Srinivas et al [14]*** propose an effective and flexible distributed scheme with Token Generation algorithm for data files checking as a secure and dependable cloud storage service. A new scheme was introduced to encrypt with the user specified key parameters to make the resource more robust. The encrypted blocks into cloud and perform token checking on this encrypted blocks which gives more security to data. Author verifies the data effectively in case of any block modifications of files before storing to Clouds by token acknowledgment. The proposed scheme is highly efficient and resilient against attacks like Byzantine server failures, malicious data modification attack. Two way verification of file blocks which results more robust and ensure that data will not be modified before reaching to clouds.

Encryption helps protecting user data confidentiality, it leaves the well-functioning yet practically-efficient secure search functions over encrypted data a challenging problem. In this paper, ***Wenhai Sun et al [15]*** present a privacy-preserving multi-keyword text search (MTS) scheme with similarity-based ranking to address this problem. To support multi-keyword search and search result ranking, they propose to build the search index based on term frequency and the vector space model with cosine similarity measure to achieve higher search result accuracy. They also propose a tree-based index structure and various adaption methods for multi-dimensional (MD) algorithm so that the practical search efficiency is much better than that of linear search. To further enhance the search privacy, author propose two secure index schemes to meet the stringent privacy requirements under strong threat models. Finally, they demonstrate electiveness and efficiency of proposed schemes through experimental evaluation.

## 3. METHODOLOGY

The overview of the proposed systems components and their subcomponents are discussed in this section. Below figure shows the basic system design and their process involved in the presented system architecture.




**Input data:** the input data is the files and data which is required to store in the cloud storage thus the files are processed first before storing in the cloud storage.

**File encryption:** in this phase the input file is encrypted using a hybrid AES and SHA base encryption technique. In order to encrypt the data the input file is processed using the SHA hash algorithm that generates the key. This key and the file input data is used with the AES algorithm for encrypting the files.

**Uploading:** After encryption has performed successfully on data or file, encrypted file is uploading on the cloud storage

**Cloud storage:** that is a cloud based storage server which provides the hosting space. Successfully uploaded data are stored in cloud storage. And at the

fetching time data will be fetching on the cloud stored.

**User Id and password:** for uploading the file the basic authentication is required which accepts userid and password.

**One time password:** after authentication using id and password system generate a one-time key for accessing the user account. This key is always new for same user; the key generation is a random method by which a six character value is generated. This key is valid for single user session and entire operations.

**File name:** the file name is extracted to keep preserve during file search.

**Rename file:** two different file contents may have the same file name for uniqueness the file is renamed.

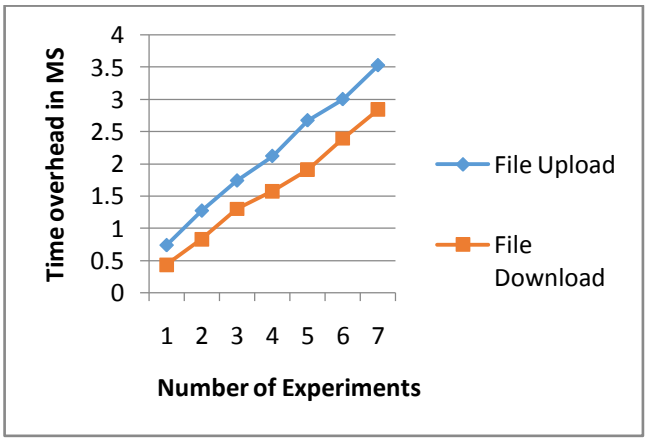
**Hash table:** the hash table includes the file name, new file name, one time password, and user id for performing search and handling file owner.

## 4. RESULT AND ANALYSIS

The proposed work is to provide the secure mechanism for file upload and hosting services thus the additional resource consumption and the requirements are evaluated in these sections. The evaluated performance parameters are reported as:

### 4.1 Time Overhead

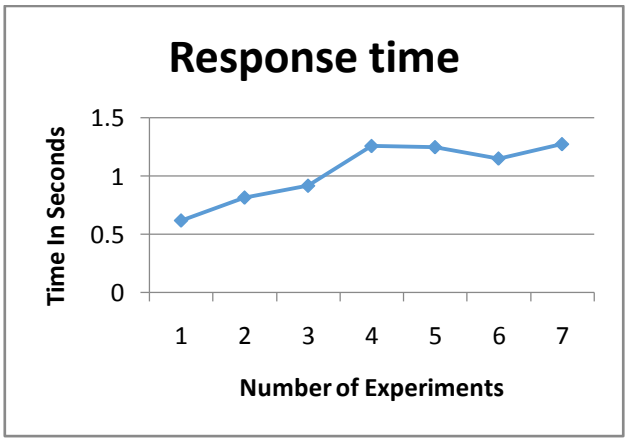
The additional time consumed during the secure file hosting and download is known as the time overhead of the system. Below figure shows the time overhead of the system during file upload and download.




The time overhead of the proposed system in terms of upload time and download time is measured and reported using above given figure. In this diagram the red line shows the time overhead during the file download and the blue line shows the time overhead during the download. In this diagram the X axis shows the different experiment performed with the different file size and the Y axis shows the amount of time additionally consumed during file upload and download. According to the evaluated results the obtained time overhead for security point of view is adoptable as compared to normal file hosting.

### 4.2 Response Time

The amount of time required to accept the user request and get respond by the server is given as the response time of the system.

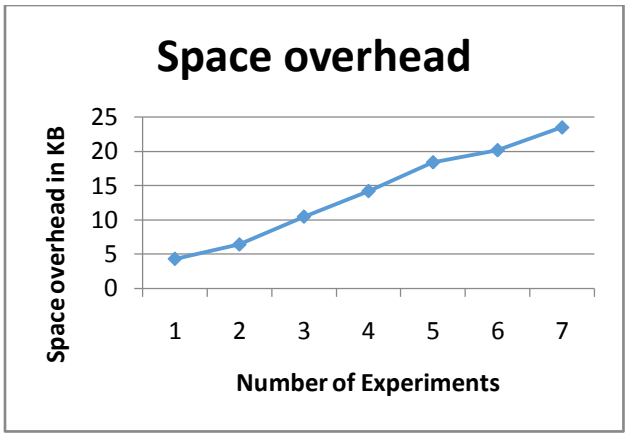



The evaluated average response time of the server is reported in the above given diagram, in this diagram the X axis contains the number of experiments performed and the Y axis contains the time requirement for getting the response from the server. According to the obtained results the response time of the server is much similar to the normal file servers thus the proposed system is efficient as the normal file servers.

### 4.3 Space Overhead

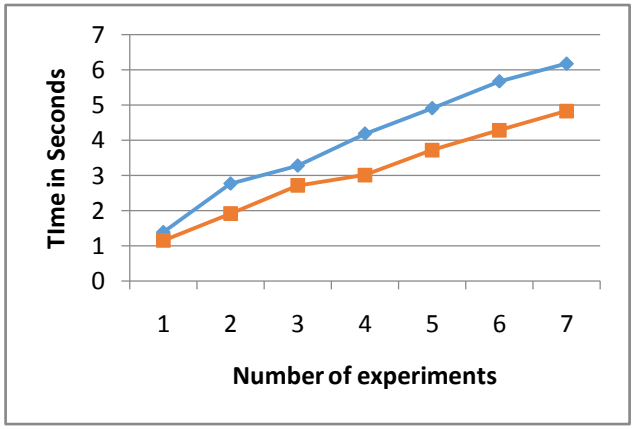
The amount of data increases during the file encryption and the data transmission is given as the space overhead. That is evaluated in terms of KB (kilobytes) and reported using the below figure. In this diagram the Y axis contains the space overhead of the system in terms of KB and the X axis contains the different experiments performed. The obtained results shows that the proposed system having the less space overhead as the traditional encryption algorithms generates.




### 4.4 Encryption Time

The amount of time required to encrypt or decrypt an input file is known as the encryption time of the system. The encryption time of the system is measured in terms of seconds and reported in the below figure. In this diagram the red line shows the time consumption of the system during the decryption time and the blue line shows the amount of time consumed during the encryption. In order to represents the results the X axis shows the number of experiments performed with the system and the Y axis shows the amount of time consumed in terms of seconds. According to the obtained results the performance of the proposed system provides the optimum encryption and decryption time for large files also. Additionally the encryption time is always higher than the decryption time.




## 5. CONCLUSION AND FUTURE WORK

Cloud computing is new generation computing technology, which provides a number of grate and manageable resources and the computational power for remote users also. The computational cloud is also usages for the storage and file hosting but this aspect of the cloud is less secure and not much reliable thus in this presented work the cloud computing is investigated for improving the security and their hosting services.

The key issues are arises when the user consumes the facility of the public internet access in this situations the network is not much secure for transmission of secure and private data. Thus not only the security in host is required that is also required to transmit the files in secure manner. Thus a new model for enhancing the current security needs is proposed that utilizes the cryptographic manner for file hosting and distribution. Additionally the cryptographic overhead is compensated using the fragmentation of large files. This feature increases the security as well as the speed of data transmission from remote host to another host.

The implementation of the proposed secure and enhanced technique is given using JAVA technology and their performance in terms of time consumption and other parameters are evaluated. The obtained performance is summarized using the given table.

The performance of the proposed file sharing and secure hosting technique is implemented successfully additionally that provides the security in less time and resource consumption

The proposed work is implemented successfully and also evaluated using different performance parameters. The implemented model is found optimum and efficient but in near future that is required to enhance the system for searching the data using the cryptographic approach.

## 6. ACKNOWLEDGEMENT

We thank immensely our management for extending their support in providing us infrastructure and allowing us to utilize them in the successful implementation of our project.

## 7. REFERENCES

[1].http://www.webopedia.com/TERM/C/cloud_computing.html
[2].http://www.gartner.com/it-glossary/infrastructure-as-a-service-iaas/
[3]. http://www.webopedia.com/TERM/I/IaaS.html
[4].http://apprenda.com/library/paas/iaas-paas-saas-explained-compared/
[5].http://www.slideshare.net/cloudreview_in/cloud-computing-overview-benefits.
[6].http://searchcloudcomputing.techtarget.com/definition/Software-as-a-Service
[7] Cong Wang, Qian Wang, and KuiRen, Wenjing Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing", 978-1-4244-5837-0/10/$26.00 ©2010 IEEE

[8] Ning Cao, Cong Wang, Ming Li, KuiRen, and Wenjing Lou, "Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 1, JANUARY 2014

[9] C. Selvakumar, G. JeevaRathanam, M. R. Sumalatha, "PDDS - Improving Cloud Data Storage Security Using Data Partitioning Technique", 978-1-4673-4529-3/12/$31.00 c 2012 IEEE

[10] W. Sharon Inbarani, G. ShenbagaMoorthy, C. Kumar Charlie Paul, "An Approach for Storage Security in Cloud Computing- A Survey", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 2, Issue 1, January 2013

[11] EmilianoMiluzzo, "I'm Cloud 2.0, and I'm Not Just a Data Center", 1089-7801/14/$31.00 © 2014 IEEE Published by the IEEE Computer Society

[12] KalyaniBangale, KarishmaNadhe, Nivedita Gupta, Swati Singh Parihar, GunjanMankar, "Smart Remote Health Care Data Collection Server", International Journal of Computer Science and Mobile Computing, Vol. 3, Issue. 2, February 2014, pg.415 – 422

[13] V. Malligai, V. Venkatesa Kumar, "Cloud Based Mobile Data Storage Application System", International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014) © 2014, IJARCST All Rights Reserved 126 Vol. 2 Issue Special 1 Jan-March 2014

[14] P. Srinivas, K. Rajesh Kumar, "Secure Data transfer in Cloud Storage Systems using Dynamic Tokens", International Journal of Research in Computer and Communication technology, IJRCT, ISN 278-5841, Vol 2, Isue 1, January ,2013.

[15] Wenhai Sun, Bing Wang, Ning Cao, Ming Li, Wenjing Lou, Y. Thomas Hou, Hui Li, "Privacy-preserving Multi-keyword Text Search in the Cloud Supporting Similarity-based Ranking", ASIA CCS'13, May 8–10, 2013, Hangzhou, China. Copyright 2013 ACM 978-1-4503-1767-2/13/05