# *Achieving Cloud Security using Third Party Auditor, MD5 and Identity-Based Encryption*

Bhale Pradeepkumar Gajendra∗, Vinay Kumar Singh†, More Sujeet †,
∗Department of Computer Science and Engineering
National Institute of Technology Jalandhar,
Jalandhar, Punjab 144011, India
Email: bhalepradeepkumar.iiit@gmail.com
†Indian Institute of Technology Delhi,India
Email: vinaykumar.iitd@gmail.com
†Jawaharlal Nehru Engineering College, Aurangabad, Maharashtra, India
Email:sujeet.more@gmail.com

***Abstract*—In recent years, Cloud computing has enjoyed a tremendous rise in popularity. It provides facilities for users to use cloud applications or platform without the need of any software installation and access the data or application from anywhere, with the help of internet. The cloud computing is divided into three fragments: Application, Service and Platform. Each of fragment provides different cloud services for business and individuals. Many organizations use this cloud service without any software, they run all their applications on the cloud and use on demand services. In Cloud, consumers, store their personal files or data on cloud server and consumers use that data or files whenever needed. Many consumers store or place their personal data on the cloud, so security and privacy are very important issue in cloud. These two issues can lead to a number of security concerns related to data transmission, integrity control, access control, identity management, logging and auditing, etc. Yet, research in the area of cloud computing receiving great attention from industry, academia and government. Since these domains have numerous complex issues, there are multiple open problems for research and opportunities for making noteworthy contributions, one of these issues is the data transmission in cloud computing. This proposal is concerned to overcome the security trade-off and improve the performance of data transmission and increase the security through Third Party Auditor and Identity Based Encryption.**

***Keywords—Cloud computing, Third Party Auditor, Identity Based Encryption, RSA, MD5.***

## I. INTRODUCTION

Cloud computing is a new technology for compute dataand applications on server. It use higher computational power and provide higher scalability and storage capacity. It allows users to use applications without install of any software from anywhere via internet. The security is important for all cloud users.so for improving security of data transmission, this dissertation use hybrid algorithm (RSA and MD5). And provide security of users uploaded files by Third Party Auditor. Cloud computing is a technology that provide many kind of services over the internet.it provide web based on demand services like online business applications, mails, online file storage, social networking sites etc.

In cloud computing an individual or business organizationutilizes hardware, storage space and software program ofcloud. Cloud computing provide infinite computing resourcesfor cloud users, they can use any of the resources or allthe resources without know how exactly these resources areoffered and maintained. Cloud computing use internet andcentral remote server to maintain data and applications. Userdata stored at remote location and access through internet.Cloud computing has two models:

- Deployment model
- Service model

The deployment model managed the entire cloud infrastructure. It has following type of clouds:

- Public Cloud
- Private Cloud
- Hybrid Cloud
- Community Cloud

The service model offers three types of services which areused by cloud consumers.

- Software Service
- Platform Service
- Infrastructure Service

The below figure shows that the cloud is an internet. In thismany users system are connected to cloud for using manyapplications and services provided by cloud server. Manycompanies like Google, Yahoo, Amazon, and Microsoft workon cloud and share their resources among different cloud users.Cloud consumers use verity of services virtually provided bycloud servers. For example the Yahoo offers mailing service,in this user can access mail service form anywhere with thehelp of internet.Cloud calculating

encompasses many services, which varyusing the degree of abstraction of underlying computer hardware and software program from customers. At the lowestlevel of abstraction, also known as infrastructure being a service, in this company only virtualizes hardware in addition tostorage. This companies include Amazon EC2 [1] in additionto competing offerings from IBM [2].At the opposite end on the spectrum, called software being a service, the company offers different applications like word finalizing, email inaddition to manages each of the necessary computer hardware
and software program.

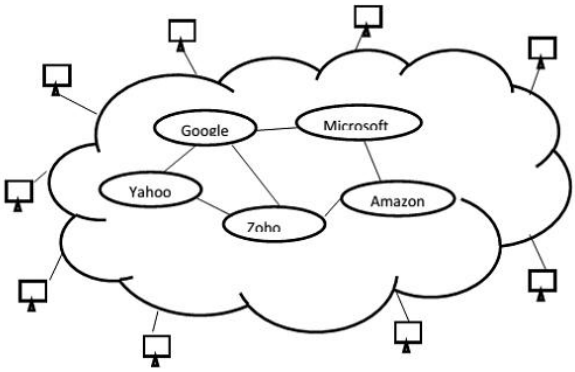


Fig. 1. Cloud Computing Environment.

*A. Cloud Computing Front end / Back end Architecture:*

We divide the cloud model into two parts (front end and back end) each of the ends is connected through a network, usually via Internet:

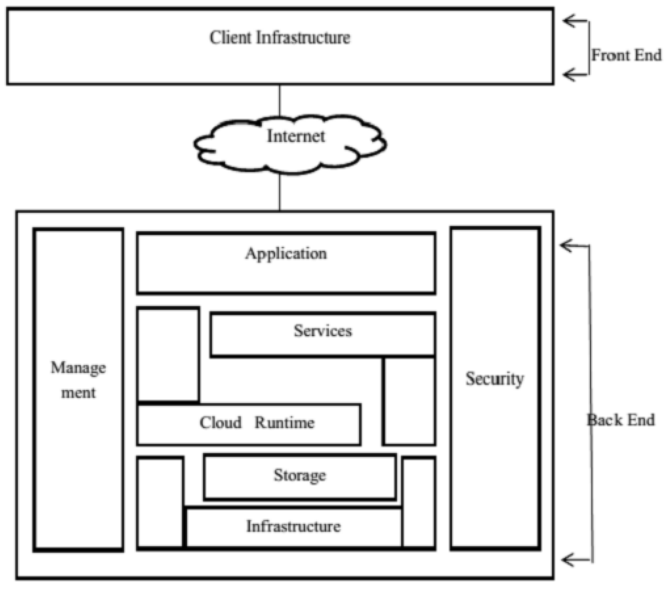


Fig. 2. Cloud Computing Architecture:.

- **Front End:** Refers to the client part of cloud computing system. It consists of interfaces and applications that are required to access the cloud computing platforms, e.g., Web Browser.
- **Back End:** It is a cloud itself. It consists of all resources that are required to provide cloud computing services. It comprises of huge data storage, virtual machines, securitymechanism, services, deployment models, servers, etc. This paper is focused on cloud computing security and privacy issues. Therefore the research seeks to answer the following questions:
    1. Is connection between the Cloud Computing provider and customer is always adequately protected?
    2. Is there a transparency for customers on how, when, why and where their data is processed?
    3. How to achieve integrity and confidentiality of data in cloud computing environment?

And because the above questions We are investigating the complex cloud computing security issues and our aim is to present an answer to overcome the security trade-off and improve the performance of data transmission and increase the security through Third Party Auditor and Identity-Based Encryption.

## II. LITERATURE REVIEW

In the paper [3], authors proposed a new model used for the integrity check on the cloud computing environment and they use TPA and digital signature technique for achieving the integrity over cloud computing. This concept helps user to verify the data from unauthorized access that extract from the data. In this paper authors use windows azure platform for evaluating their work with digital signature

In result, they observe their model is worked well. The main objective of their work was to study the ability to verification of users data with the absent of the editing and the deleting. The approach used for the encryption in the verification process was the digital signature.

In the paper [4], authors describe the Cloud computing technology has number of issues i.e. privacy issue, security issue, telecommunications capacity, anonymity, government surveillance, reliability among others. The most important issue is security and how cloud provider assures the security of data. Generally, Cloud computing has number of customers such as ordinary users, organizations and enterprises group. All customers of cloud have different motivation of work. The most important problem is security for all customers. For the perspective of different users the security point of view is different.

This paper analyses the importance of security to cloud. The authors compared three algorithms namely Data Encryption Standard (DES), RSA, Homomorphic encryption for data security in cloud. They are compared based on four characters;

key used, scalability, security applied to and authentication type.

In the paper [5], authors provide security using the key management and encryption technology. Encryption basically is the method to turn information into unintelligible format using different algorithm, in cloud computing it is used for security purpose as it changes the data stored on cloud into an unintelligible form .the key management is a method with which use special encrypted keys to access all the data. This paper show how data is encrypted and keys are generated for application security on cloud through two methods. First through porticors ovf template using VMare EXSI server and VSphere client and secondly, using AWS account directly. Data encryption is critical in protecting the security of data at rest in the cloud. But when it comes to the cloud, managing and protecting the encryption keys effectively is as important as Encryptingthe data.

In the paper [9], authors Presents hybrid asymmetric-key encryption algorithm has been suggested based on RSA Small-e and Efficient RSA according to the security issues in cloud computing environments. In the proposed algorithm, the number of exponents has been increased to three and a dual encryption process has been applied to raise the security level of the algorithm in comparison of original RSA. According the simulation results, the total execution time in HE-RSA was increased up to approximately 50 percent less than the original RSA and this increase may be reasonable and acceptable according to the security level and the efficiency of HE-RSA.

The proposed algorithm were suggested for using in cloud computing environments and increasing the reliability of this new technology, but the most challenging issue in using HERSA encryption algorithm in cloud servers is time and memory limitations during the encryption and decryption process in servers according to the sharing performances. It is suggested to encrypt the stored data with a symmetric-key algorithm such as AES in cloud servers and after that encrypt the secret key with HE-RSA for sharing actions. This means, only the secret key would be encrypted with this algorithm and the encryption and decryption process will be more efficient and needless to say it would be less time consuming and memory deficient.

In the paper [10,8], authors proposed RSA algorithm for security of data in cloud. RSA is public key algorithm, it use both public and private key. In their proposed work, they used RSA algorithm for encryption purpose. Firstly, the user data are encrypted through RSA then it is stored in the cloud storage, when user wants to access their data they send request to cloud provider for data. The provider applies verification and authentication on the user, if user is authenticating then the cloud service provider deliver the data to cloud users. No unauthorized user access the data on cloud.

RSA is public-private key algorithm. The public key known to all, but private key known only the owner of data. Encryption is done by cloud provider using public key and the decryption process is done by cloud user using private key. In the paper [11], the authors provide multicast key management technique for security of data on cloud. The number of users use cloud computing technology and store their data on cloud. It use internet and remote server to maintain user data and applications. So, security is important issue in cloud there are many security problems arises one of them is data transaction between cloud server and cloud consumer. For the security authors introduce a new method for securing the data on cloud by multicast key management. For this they grouped all cloud consumers according to their need of data then they provide a new key for each user. Multicast key is dynamic session key which will be vary at the specific time period, whenever new user enter on the cloud , new key will generate for user after specific time period user should renew key for other usages of cloud. At the result authors observed, the multicast key management technology provide better security through keying and rekeying process for the secure data transactions.

## III. PROPOSED WORK AND IMPLEMENTATION

### *A. Description:*

Cloud computing offers many cloud services for individual users and many small and large companies. Users use cloud services in manyforms such as form of software, platform and form of infrastructure. The important issue of cloud computing is security of data in cloud storage. For securing the data in cloud, we use Identity-Based encryption algorithm and MD5 authentication algorithm.

Identity-based encryption algorithms consist of 3 phases:

- Key Generation (Ex)
- Encryption (E)
- Decryption (D)

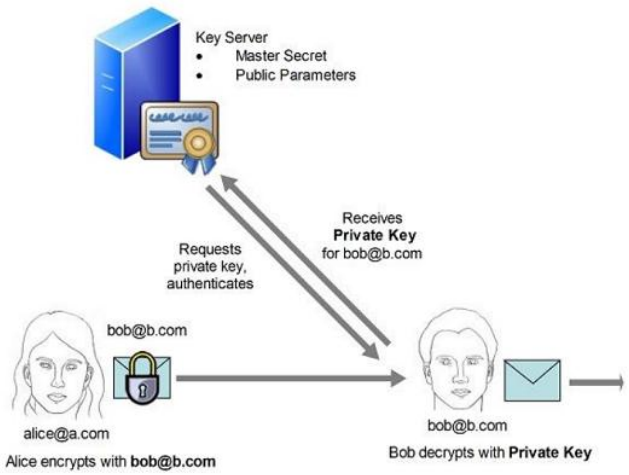


Fig. 3. Identity-Based Encryption (IBE) [7].

**Key Generation:** This is a first phase of IBE algorithm. It is done between the cloud service provider and the cloud consumer. A master key (Km) and public unique identity UID {0, 1}* and Ex (Km, UID) compute the equivalent private key (Ks)

**Encryption:** The encryption is process of converting the plaintext data into a cipher text data. Let us MSG is plaintext data and C is cipher text data. In Encryption algorithm public unique identity UID and a message MSG, E (UID, MSG) computes a cipher text C.

**Decryption:** The decryption is process of converting the cipher text data into its original plaintext data. In Decryption algorithm private key Ks and cipher text C, D (Ks, C) returns the plaintext.

For authenticate purpose, we use MD5 algorithm. MD5 refers to message digest algorithm. It is a one way hash function or a cryptographic function. MD5 take an arbitrary length input and produce a 32 bit message digest. In our proposed work, the server generates the hash value of each user uploaded data by using MD5 algorithm. Firstly, data are encrypted by IBE then the hash value of users data generated by MD5 algorithm. We focus on user-facing software as a service applications such word processing, email, social networking and security application. We provide a hybrid algorithm (IBE and MD5) for securing stored data. The security analysis of original RSA and Hybrid Algorithm has been investigated according to three attack approaches: the Brute Force, Mathematical Attacks, and Timing attacks.

*B. System Architecture:*

In our system we created three entities.

- Cloud Consumer or Cloud User
- Cloud Server or Cloud Admin
- Cloud Auditor or TPA

All the functionality of these entities is different. Cloud Consumer or user is used services, provided by cloud service provider. Cloud users upload the data or files on server. And also view their uploaded files, upload time, download time and hash value of files. The cloud admin or server generate hash values of user's uploaded files and keep users files in secure manner. Hash values are unique for each file. And admin also view users file status like file name, file Id ,file size, file type, uploaded date and time ,no. of downloads of file, IP address of users system, which is used to upload the files, view upload and download time of files. And the cloud auditor is a Third Party Auditor, who audits the user's uploaded files under the server permission.

**Description of system architecture:** There are 3 entities:

Cloud admin, client admin, TPA admin. The client admin upload data or files on the server, data are encrypted and decrypted using Identity-Based encryption algorithm. The cloud admin store encrypted files on the server and generate a hash value of client files using MD5 algorithm. When the client admin sends request to TPA admin for audit their files, then cloud admin send file Id and hash value of files that want user audit. TPA admin verifies users file and examine them under server permission.

**Uploading Steps:-**

1) Each user logs on to the workstation using an own ID and Password.

2) No of user connected to a storage array via network.

3) The client computer sends a request to the storage array for storing a file.

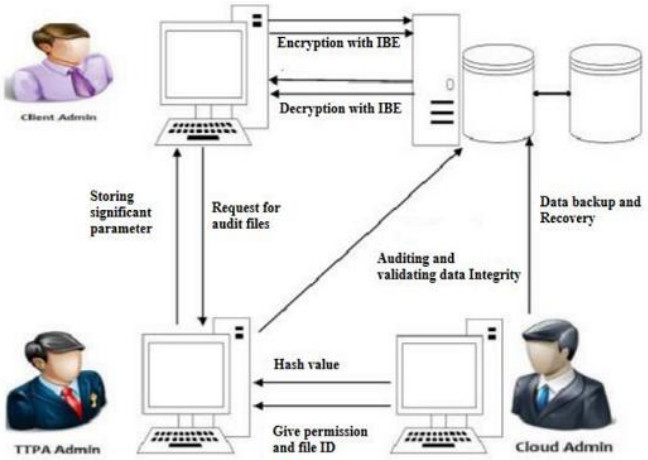


Fig. 4. System Architecture.

4) The file is uploaded to server and encrypted with the help of IBE. The file is encrypted at the time of transferring RSA works which will be encrypting data.

5) The MD5 will be working in a data storage array for generating hash value.

**Downloading Steps:-**

1) When the client sends a request to a server for download file, it sends a request, consist of valid ID and Password.

2) The storage array checks the permission and ensures that the user is authorized to use that service.

3) If the user is authorized then reply the client machine and give respond as a file.

4) The client computer sends the desired file name and file Id that want to access.

5) The storage array decrypts the file and the server automatically allows the client to access the appropriate resources.

*C. System Flow Chart:*

The cloud server requires the file and the public key for encryption process as represented in system workflow. The Figure shows that first of all user start the process with the help of the login ID and Password after that it will be verified by the server. Then the user uploads the file which is encrypted
with the help of the IBE. The server generates hash values of user uploaded files. Then users send requests to the TPA for audit their file. The user request consists of request ID and

request Status. After that, the server sends the hash value and ID of that file which user wants to audit. Then, TPA verifies user requests by hash value send by the server, then audit the user files.

When users want to download file the decryption process is started. At the time of the decryption process IBE algorithm is used for decrypt user files. After verification of users file by TPA, all process done in the system then it will be confirmed that user upload the true file and download it. Mainly cloud storage work on the security principles, but in this research proposal given concept helps faster uploading and downloading process.

In this system we use an IBE algorithm to encrypt and decrypt the user uploaded files. IBE is working on the server side. The MD5 is used to generate the hash value of user uploaded files at server side. TPA audit all files of user after verification is complete, then user decrypt file and successful download their files.

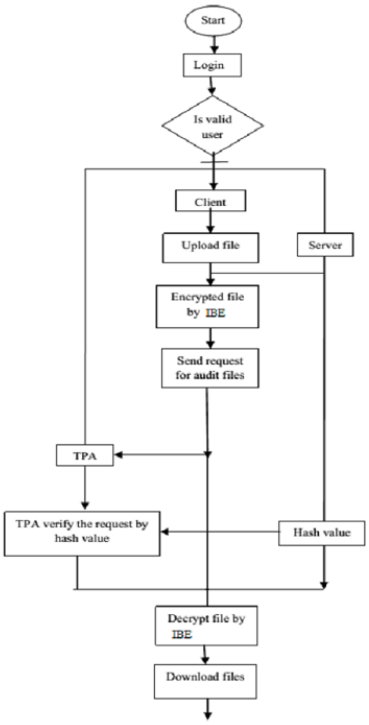


Fig. 5. Cloud Computing Architecture:

*D. Step wise Execution:*

The suggested system is developed as a web based solution in real cloud (Red hat Open Shift-PaaS) for performing the security goals. The system is having two execution ends, one is client end for service request and usages and the second is auditor ends, which monitors the services and user behaviors.

The following steps are needed to follow for verifying theapplicability of user and purpose of the operation.

**Step 1:** Firstly, user register on system by filling details like name, user Id, Password, contact no. in registration form.

**Step 2:** Login to the system by some defined user id and password; it could be recreated by using Sign up function.

**Step 3:** User can upload the file and server apply RSA for encryption of file or data. In the Encryption process original user data converted into non readable code.

**Step 4:** During this encryption some other factors related to the effectiveness of the approach are shown for comparison purpose, such as Throughput, Encryption Time, and Decryption Time.

**Step 5:** User can also view the previously uploaded and encrypted files, also they can download it. And user alsoview the status of all their files, hash value of files, upload time, download time of files , uploading date and time and encryption and decryption time of files.

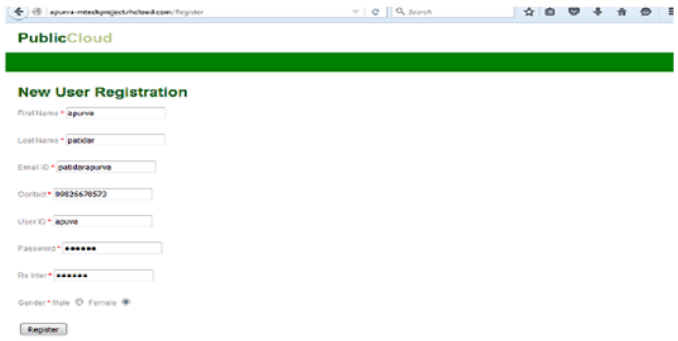


Fig. 6. Registration Page.

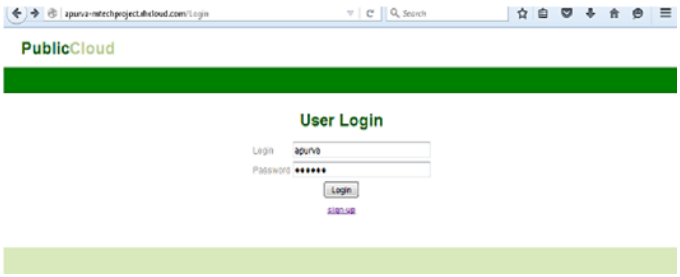


Fig. 7. Login Page.

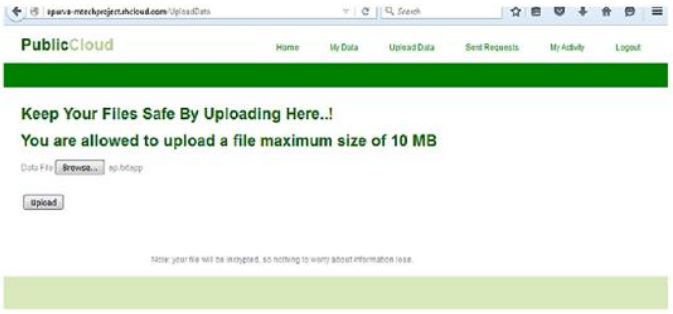


Fig. 8. Upload file.

**Step 6:** After the user upload file, the Server generate hash value of user files. Just click on Generate button in hash value column and server also view users file status.

**Step 7:** Server also view users file details like file ID, hash value, upload time, download time, encryption time, decryption time etc.

**Step 8:** User sends request to cloud auditor for audit their files. Request consist of request Id, request date, etc.

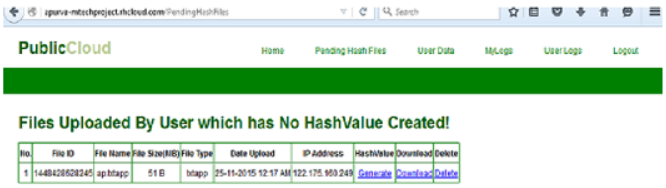


Fig. 9. Server Generate hash value.

**Step 9:** TPA audits the user files as per user request. TPA audit files under the server permission,server give permission in the form of the hash value. The request is consist of request ID, date and IP address of the system which are used to send a request.

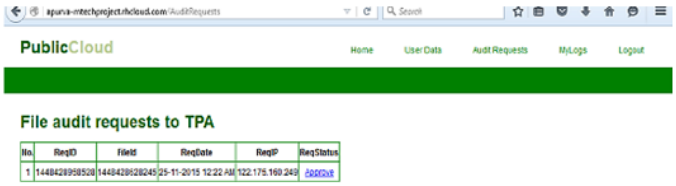


Fig. 10. TPA audit file.

**Step 10:** User can make changes in files means delete the file and again an upload number of files.User can download files .The files are decrypted by IBE.

## IV. RESULT ANALYSIS

In this paper we use many different parameters like size, speed, key, security, encryption time and the decryption time of files. And evaluate all this parameter on the basis of different approaches, i.e. RSA, MD5 and IBE approach.

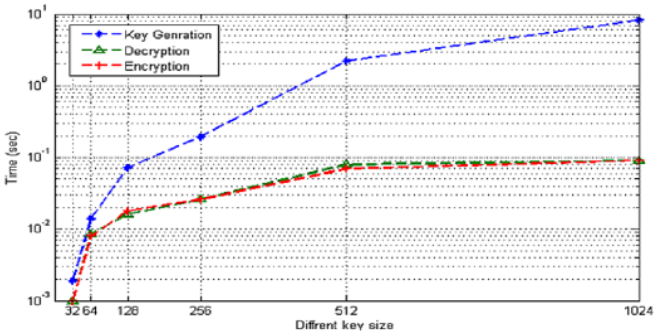


Fig. 11. RSA computing complexity on the basis of different key size

The Fig. 11 describes the RSA approach on the basis of Key Generation, Decryption and Encryption time of files. The blue line shows the key Generation, Green line show Decryption time new and the red line show Encryption time. Time measured in second.

The Fig. 12 describes the IBE approach on the basis of Key Generation, Decryption and Encryption time of files. The blue line shows the key Generation, Green line show Decryption time new and the red line show Encryption time. Time measured in second.

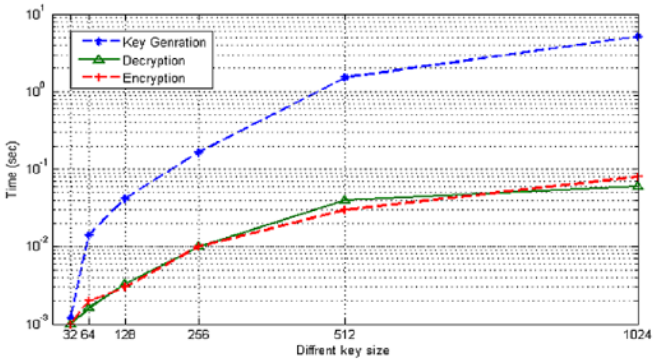


Fig. 12. IBE Encryption time complexity on the basis of different key size

## V. CONCLUSION

In this research paper we provide security in the cloud with the help of the Third Party Auditor. This is done to enhance the hardness in security by the IBE encryption algorithms by adding some more security codes. Encryption is the vital part of information sharing so we will put our efforts into an encryption area for IBE algorithm with digital abstract algorithm MD5 so that we can make security harder by giving a hybrid algorithm. The Third Party Auditor can be used to ensure the security and integrity of data. Third party auditor can be a trusted third party to give confidence to the cloud user and cloud service provider that their data is safe.

## REFERENCES

[1] Chin-Ming Hsu, A group digital signature technique for authentication in Proceedings. IEEE 37th Annual 2003 International Conference.
[2] Chandran S. and Angepat M., Cloud Computing: Analyzing the risks involved in cloud computing environments in Proceedings of Natural Sciences and Engineering, Sweden, pp. 2- 4,2010
[3] V.Masthanamma, G.Lakshmi Preya, An Efficient Data Security in Cloud Computing Using the RSA Encryption Process Algorithm International Journal of Innovative Research in Science, Engineering and Technology.
[4] Praveen Kumar Donta, Performance Analysis of Security Protocols University of North Florida
[5] Buyya, Venugo, Cloud Computing and emerging IT platforms: Vision, hype, and reality for delivering Computing as the 5th Utility, [2008].
[6] Metri P. and Sarote G.,Privacy Issues and Challenges in Cloud Computing
International Journal of Advanced Engineering Sciences and Technologies, vol.5, no. 1, pp.5-6,2011.
[7] Bhale Pradeepkumar.G, T.S. Ravi Chandra, Kolla Raja Sekhar,Detecting Rogue Bridge Access Point Using Threshold Cryptography International Journal of Advances in Engineering and Technology, Vol. 7, Issue 4, pp. 1347-1358,2014.
[8] A. Shamir, How to share a secret, vol. 22. ACM, 1979, pp. 612613.
[9] Faraz Fatemi Moghaddam, Maen T. Alrashdan, and Omidreza Karimi ”A Hybrid Encryption Algorithm Based on RSA Small-e and Efficient-RSA for Cloud Computing Environments” Journal of Advances in Computer Network, Vol. 1, No. 3, September 2013.
[10] N.Padmaja, Priyanka Koduru ”Providing Data Security in Cloud Computing using public key cryptography” International Journal of Engineering Sciences Research,Vol 04, Special Issue 01, 2013
[11] Dawoud, W.; Takouna, I.; Meinel, C., ”Infrastructure as a service security: Challenges and solutions,” in Informatics and Systems (INFOS),
2010 The 7th International Conference on , vol., no., pp.1-8, 28-30 March