IJCTA, 9(26) 2016, pp. 47-56

Cryptographic Approach by Outsourcing Mobile data to Cloud

S. Velmurugan[1] and R. Thamarai Selvi[2]

ABSTRACT

In this paper describe the some important information about the cloud storage process and its working technique with proper identity checking. In this study work for the remote data integrity verification process during the data shearing in between the cloud. This task can make the cloud registered user verification during the data downloading process, because of we know that the cloud environment not only have the single cloud for providing the good service cloud have the multiple cloud storage for providing the good facilities for the registered user, so in this paper introduce the multiple cloud storage latest technique Identity Based Distributed Provable Data approach of registered client verification or its identity verification when the client use the cloud facilities from the multiple cloud at time.

Keywords: Mobile Data security, Cloud computing, Provable data possession, Identity-Based Distributed Provable

I. INTRODUCTION

Mobile Cloud Computing is an emerging knowledge and its popularity is increasing drastically day-by-day. Already a huge total of population has accepted it for their various personal and commercial uses and the counting is still incrementing. Although the advantages are understandable taking up users 'physical control' of their outsourced information, which unavoidably creates new security threats towards the accuracy of the information in cloud. To start working on data access control, initially a study is necessary to find out effectiveness of cryptographic algorithms so that data operations on mobile could be fast and consistent. User mobility, that means "anytime, anywhere" is turning in to an actuality. Making use of mobile tools, computing ability from cloud computing technology and Internet convenience jointly is making a new surge, which is mobile cloud computing for organization.

Cloud computing is a model for enabling ubiquitous, convenient, on-demand structure access to a common pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be speedily provisioned and unconfined with minimal management effort or service provider interaction.

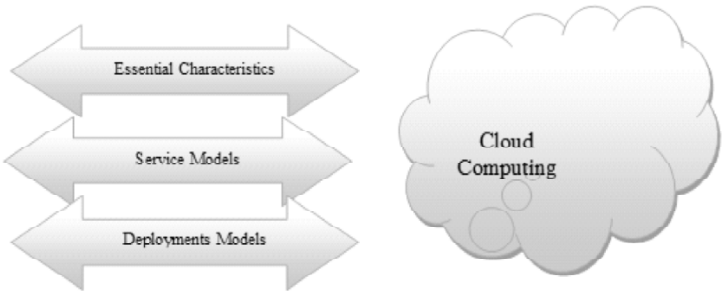

Figure: Cloud Computing

[1] Research Scholar, Computer Science, Bishop Heber College, Tiruchirapalli, Tamil Nadu, India

[2] Head & Assistant Professor, Department of Computer Applications, Bishop Heber College, Tiruchirapalli, Tamil Nadu, India

Key supervision is another vast area of research and still studies are going on to make key management more secured and resourceful. Let us in brief have a discussion regarding the security problems that take place with key management on mobile devices with outsourcing information on cloud server. Common security problems in key management are

- ✓ Effectiveness in mobile operations
- ✓ Strong protection of cryptographic algorithms
- ✓ Keys being fetch
- ✓ Keys being susceptible to hack or cooperation
- ✓ Supervision of all keys
- ✓ Requires to calculate linearly to manage many keys
- ✓ Permitting approved members access to their information

2. LITERATURE SURVEY

In [1] authors introduced a model for AES that allows a client that has outsourced data at an untrusted cloud to verify that the server possesses the unique data without downloading it. This model gener-ates a probabilistic proof of possession through example random set of blocks from the server, which significantly reduces cost. The data owner maintain a constant amount of data to verify the proof. The request/response protocol transmits a little, constant amount of data, which reduces network statement. Thus, the AES model for remote data integrity checking supports the large data sets in widely-distributed storage scheme. The key component of this scheme is the homomorphism verifiable tags.

In [2] authors introduce the proficient and secured outsourced information is addressed either by public key cryptography or requiring the member to outsource its data in encrypted form called EPDP (Efficient-PDP). This technique is based completely on symmetric key cryptography and not require any bulk encryption. It allows dynamic data that efficiently support operation, such as block updation, deletion . Two different approaches PDP and POR have been pro-posed. The POR is a public key based method allowing any verifier to query the server and obtain an interactive proof of data possession.

In [3] authors projected the POR scheme permits back-up service to produces a concise proof that a client can retrieve a file F, that is, that the ar-chive retain and dependably transmits file data sufficient for the user to recover F in its whole. A POR is a kind of cryp-tographic evidence of knowledge (POK), but one specially designed to handle a big file F. To discover POR proto-cols, in which the message expenses, memory ac-cesses for the proven, and storage necessities of the member are small parameters fundamentally independent of the length of F. The goal of a POR is to achieve these checks without client having to regain the files themselves. A POR can also provide service with quality assurances.

In [4] authors introduce the problem of ensure the integ-rity of data storage. In particular, to consider the job of allowing a third party auditor, on behalf of the user, to verify the integ-rity of the dynamic data stored in the cloud server. The introduction of third party auditor reduces the participation of the client through the auditing of whether their data in the cloud is certainly intact, which can be essential in achieving finan-cial system of scale for Cloud Computing.

In [5] authors careful the cloud data storage space protection, which has always been an important aspect of ensures the accuracy of member data in the cloud, it is denote inef-fective and flexible distributed verification scheme with two features. By utilize the homomorphism token with flexible distributed verification achieves the storage space correctness and data error localization. Unlike the most prior works, this system further supports secured and efficient dynamic operation son data block, including: data insert, update, delete and append.

3. PROPOSED WORK

In authentication-based public key cryptography, this study focus on remote data possession in multi-cloud storage. The protocol can be made resourceful by eliminate the certificate management. The propose the new remote data integrity checking model: identity based distributed. The system model and security model are formally proposed. Then, based on the bilinear pairings, the concrete identity based protocol can be designed. This protocol is provably secure. On the other hand, our protocol is more flexible besides the high effectiveness. Based on the client authorization, the proposed RDP protocol can realize private proof, delegated verification and public verification.

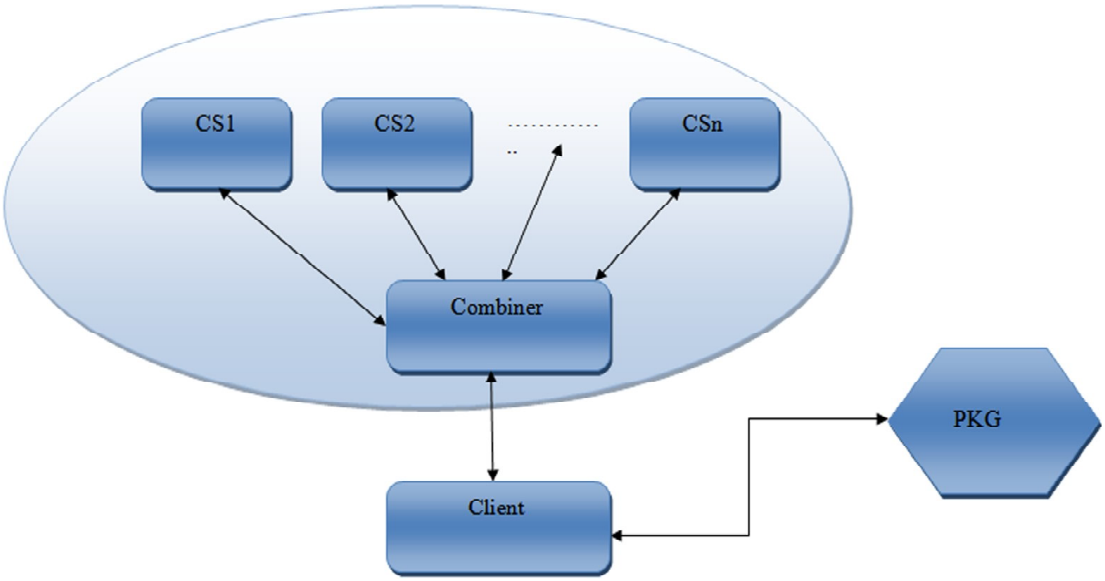

Figure: Multi Cloud Architecture

3.1. Algorithms

An efficient protocol is ID-DPDP protocol. It is built from bilinear pairings which will be briefly reviewed below.

Let G_1 and G_2 be two cyclic multiplicative groups with the same prime order q. Let e: G1 × G1 '! G2 be a bilinear map which satisfies the subsequent property:

1) Bilinearity: ∀g1, g2, g3 ∈ G1 and a, b ∈ Zq

   e(g1, g2g3) = e(g2g3, g1) = e(g2, g1)e(g3, g1)

   $e(g1^a, g2^b) = e(g1, g2)^{ab}$

2) Non-degeneracy: $\exists_{g4, g5} \in$ G1 such that e(g4, g5) 6=1G2 .

STRUCTURE MODEL AND SECURITY MODEL OF ID-DPDP

The ID-DPDP system model and security definition can be presented.

1) **Client:** Member data to be store on the multi-cloud for maintenance and computation can be either individual consumer or corporation.

2) **Cloud Server:** An entity, which is managed by cloud service provider, has significant storage space and calculation reserve to maintain the client data.

3) **Combiner:** An entity, which receives the storage request and distributes the block-tag pair to the equivalent cloud servers. When receiving the challenge, it splits the confront and distribute them to the special cloud servers. When receiving the response from the cloud servers, it combine them and send the mutual reply to the verifier.

4) **PKG (Private Key Generator):** An entity, while receiving the individuality, it output the corresponding private key

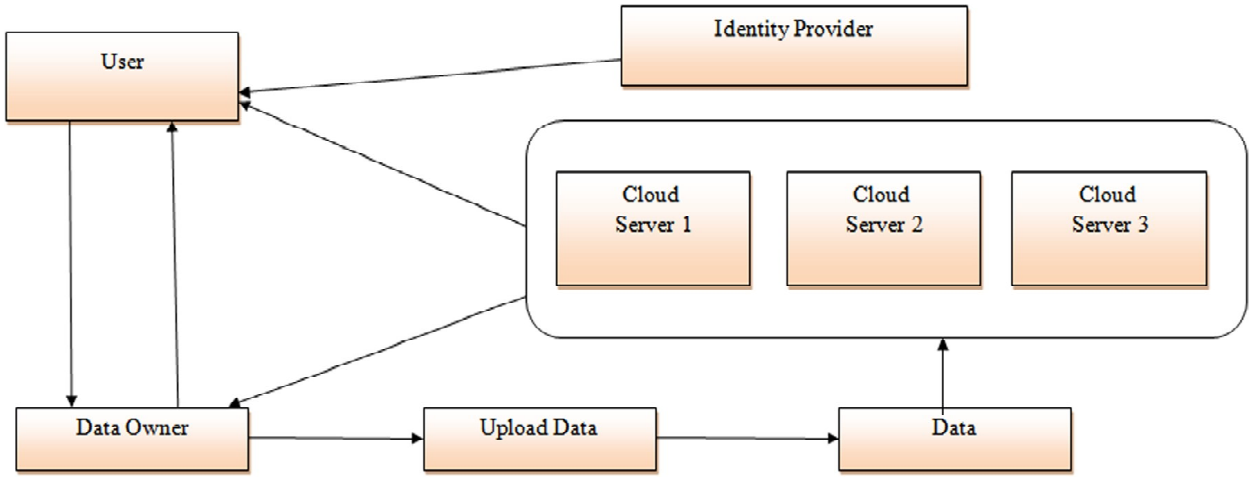

Figure: Process flow Diagram

In this proposed the Identity Based Distributed Provable Data approach in Cloud Storage for Identity verification of Data Distributed that include the solution for the limitation mention in the problem definition section in this paper. A Identity-based public key cryptography system that focuses on distributed provable data possession in multi-cloud storage as well in the single cloud environment this new approach is also able to reduce the conventional strategies of certificate management system this approach is also support the remote data integrity checking. The main advantage of this novel approach is more safety is present; this new protocol is more flexible, very fruitful for the client verification in the single cloud and multiple clouds.

Implementation

Registration

This module is designed for new users who visit this project. The new user has to register with the proper details. This system requires a proper user authentication for accessing the features behind in this system. For getting the rights to accessing the features user have to register their identity to this system. Once registered the system will provides the accessibility rights to the user to work in this system.

File Upload

Not all files are straight stored in multiple clouds, but only the files that are verified by the trusted TPA are uploaded. If any corrupted file is loaded, then that file cannot be saved instead they may be deleted by the TPA. The File may be encrypted using the cryptographic key in which is at random generated.

File Division

The Cloud User who has a huge amount of data to be stored in several clouds and has the permissions to access and manipulate stored data. The member Data is transformed into data block of different sizes for improving the efficiency of storage and as well as to improve the security of file.

File verification

Using the cryptographic key the file is encrypted and by using this key the file data may be decrypted by the third party auditor for the verification process

File download

Only the verified Files can be downloaded by the File member. If the user wants to download their documents, the data stored in multi-cloud is integrated and downloaded.

View All Files

All the Files in the web including verified data and not-verified are viewed by the Administrator.

View File Owners

Registered File Owners are viewed by the Administrator. Admin can have the facility to contact the file owners and can monitor the storage space used by the file owners.

File Deletion

The Uploaded file can be deleted by the File Owner. The protection can be increased if can be making a key certification along with the deletion process. One problem can arise is in the case of key remembrance.

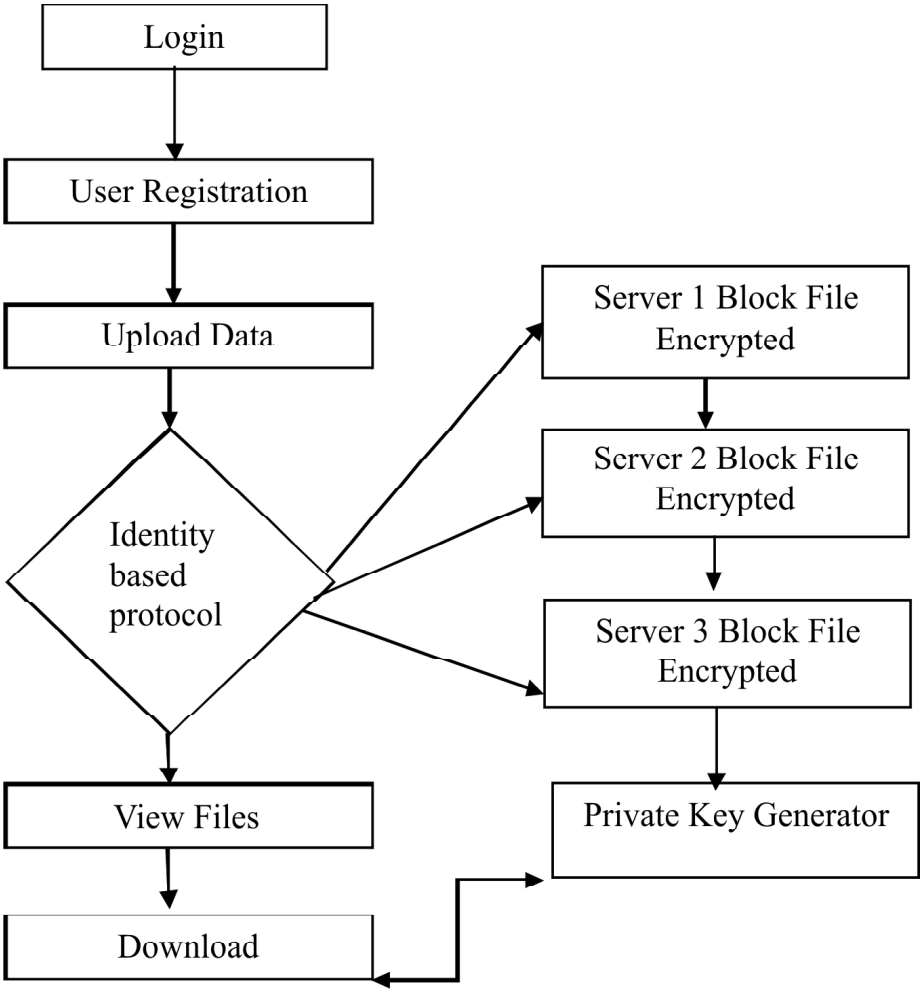

Figure : Cloud User Overall Process

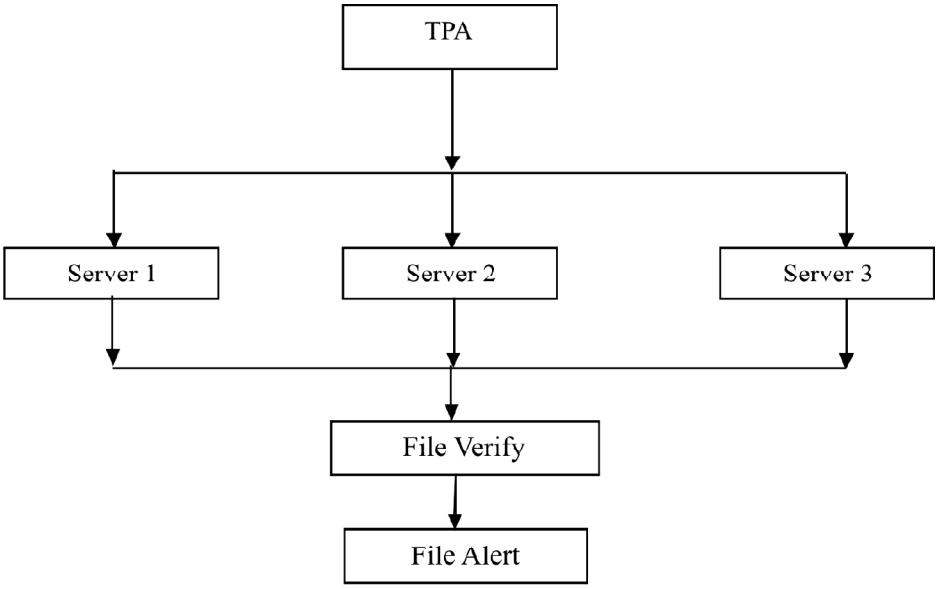

Figure: Cloud Server Overall Process

4. COMPARATIVE ANALYSIS

Table 1
Time Required for File Upload and Download in Milli Seconds

S.No	File Name	File Type	File Size	Time (ms) Encryption	Encryption	Decryption
1	server	txt	30KB	0	20	10
2	connect111	txt	338KB	16	20	40
3	machine	txt	1.34MB	40	70	60
4	client	txt	14.7MB	360	480	850
5	document	doc	22KB	10	10	20
6	Implementation	doc	165KB	10	10	25
7	v1	doc	1.16MB	70	10	70
8	Varsha REPORT	doc	9.25MB	190	10	530
9	VisaCard Platinum	xls	18KB	10	20	10
10	2013-14 TT	xls	165KB	10	10	10
11	Tg data comp	xls	523KB	30	20	30
12	FACULTY TT	xls	1MB	30	20	20
13	christmas fair	pdf	11KB	0	10	10
14	iiiij	pdf	158KB	10	15	30
15	Identity	pdf	1.07MB	20	30	60

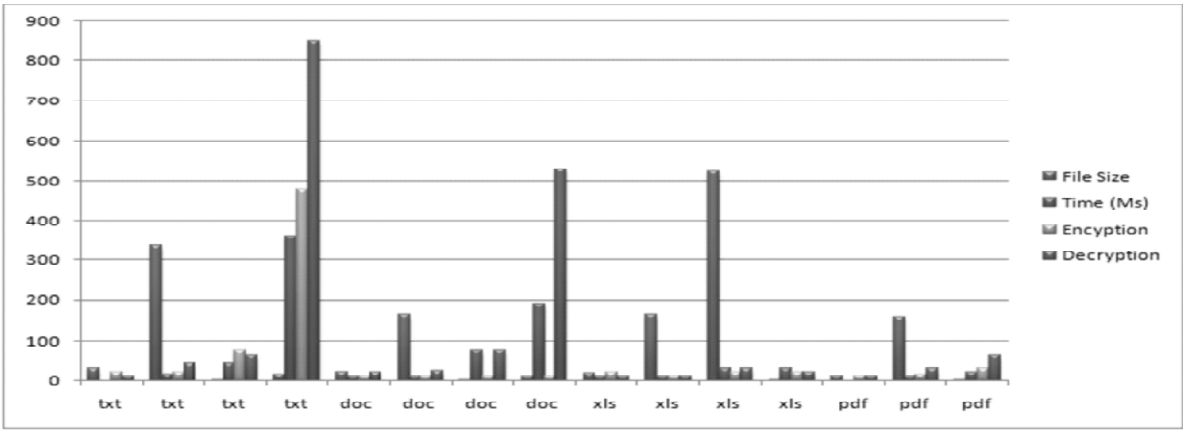

Figure: Graph of System results

5. EXPERIMENT RESULTS

The proposed method has been implemented using .NET Technology. Extensive experiment was conducted to check good organization of symmetric algorithms on mobile background for encryption and decryption of data before outsourcing data to cloud servers. Implementation reveals the performance of algorithms Identity based distributed for diverse number of operations separately. Below are the output of algorithm performance which was found in study.

Encryption memory

The amount of main memory required to execute the encryption algorithm, where the input amount of data depends on the user input is known as the encryption memory. The encryption memory is also termed as the time complexity of algorithm. The Chart 1 and the table 1 show the encryption memory.

Table 1
Memory Consumption

File Size (KB)	*Existing Technique*	*Proposed Technique*
10	**32681**	30992
50	33039	30638
100	31028	31028
500	31394	31394
1000	31884	31884
2000	32194	32197

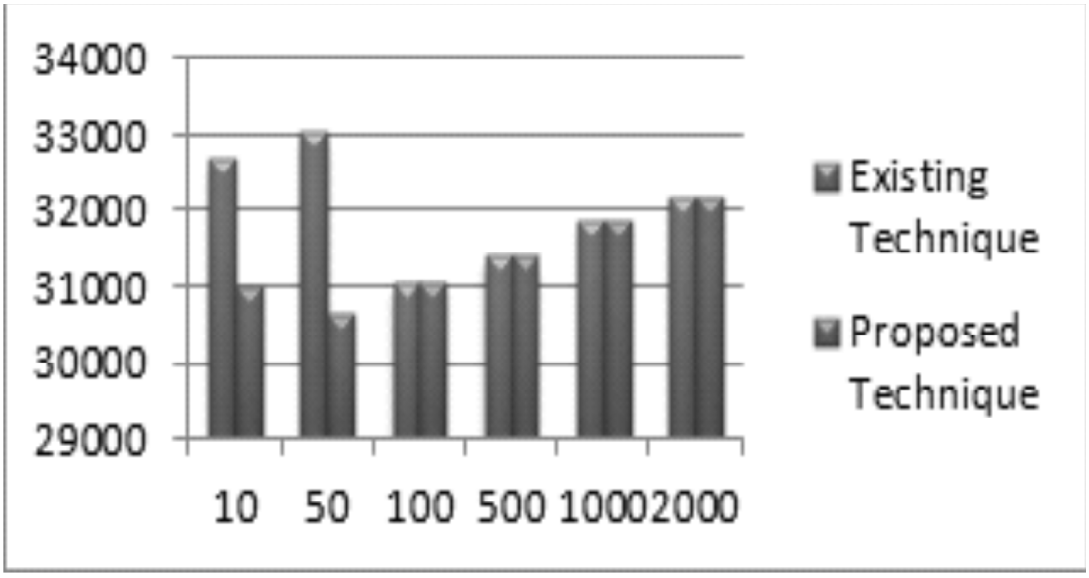

Chart 1: Mean Memory Consumption

Decryption memory

For a cryptographic algorithm the amount of main memory required, to recover the original text from cipher is explain as decryption memory. That can also be termed as space complexity of decryption. The Chart 2 and table 2 shows amount of memory consumed during data recovery. In the diagram X axis show the different file size used for experimentation and Y axis reports amount of main memory consumed.

Table 2
Decryption Memory Used

File Size (KB)	*Existing Technique*	*Proposed Technique*
10	29847	29019
50	30924	29383
100	31947	29981
500	32844	30284
1000	36649	35472
2000	37845	37918

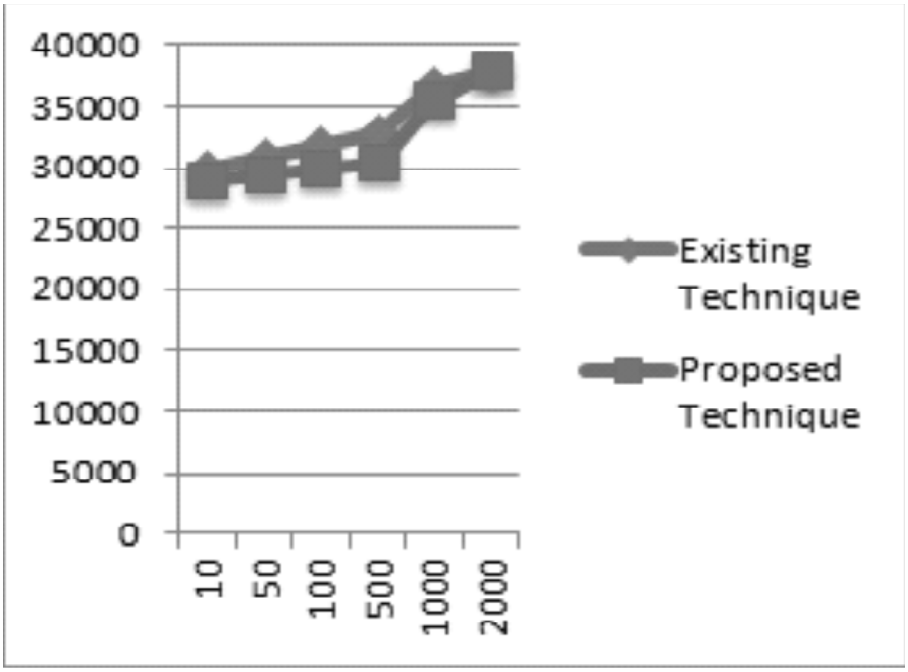

Chart 2: Mean Performance

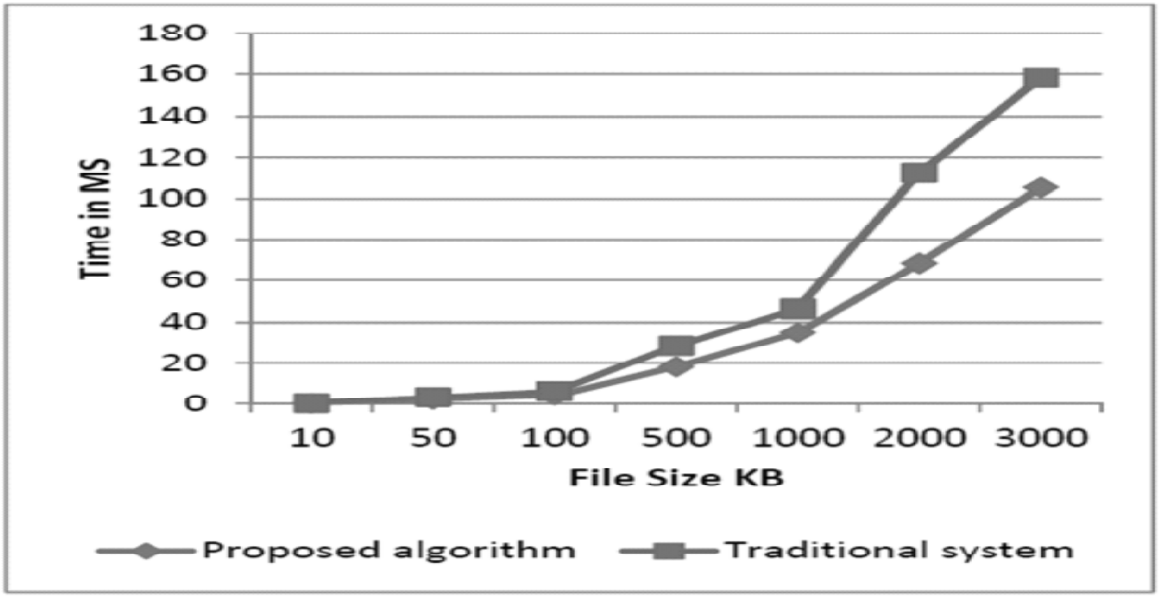

Chart 3: Decryption Time

Table 3
Decryption Time

Mobile Cloud Server Execution time		
File Size (KB)	*Existing Technique*	*Proposed Technique*
10	0.54	0.33
50	3.38	2.04
100	6.21	4.12
500	28.42	18.14
1000	46.52	34.93
2000	112.53	68.25
3000	158.45	105.39

6. CONCLUSION

In multi-cloud storage, this study formalize the identity based distributed system model and security form. Similar time, this procedure which is provably secure under the assumption that the CDH problem is hard. Besides of the removal of certificate organization, our protocol has also flexibility and high efficiency. At the same time, the proposed algorithm can realize private verification, delegated verification and public verification based on the member authorization. It is simple and require no complex computations, and yet yields accurate estimation.The distributed cloud storage is indispensable.

REFERENCES

[1] Kumar. K. Lu. Y.-H.Yung-Hsiang Lu., "Cloud Computing for Mobile Users: Can Offloading Computation Save Energy?", *Computer* **43(4)**, 51– 56, 2010.

[2] Simons P. De Truck F. Dhoedt. Demeester P., "Remote Display Solutions for Mobile Cloud Computing", *Computer* **44(8**), 46–53, 2011.

[3] Ayesha Malik. Muhammad Mohsin Nazir., "Security Framework for Cloud Computing Environment: A Review", *Journal of Emerging Trends in Computing and Information Sciences,* 2012.

[4] Shashi Mehrotra Seth. Rajan Mishra., "Comparative Analysis Of Encryption Algorithms For Data Communication", *IJCST* **2(2)**, 2011.

[5] Shahryar Shafique Qureshil. Toufeeq Ahmad1. Khalid Rafique2. Shuja-ul-islam3., "Mobile cloud computing as future for mobile applications – implementation methods and challenging issues", 2011.

[6] Mell P. Grance T., "The NIST definition of Cloud Computing Special Publication", 800–145, 2011.

[7] Zhang Q. Cheng L. Boutaba R., "Cloud Computing: state-of-the-art and research challenges", *Journal of Internet Services Applications* **1(1)**, 7–18, 2010.

[8] Pearson S. Y. Shen. M. Mowbray., "A Privacy Manager for Cloud Computing", *In Proceedings of the 1st International Conference on Cloud Computing*, 90-106, 2009.

[9] Wang Q. et al., "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing", In *Computer Security – ESORICS,* 2009.

[10] Hoang T. Dinh. Chonho Lee. Dusit Niyato. Ping Wang., "A Survey of Mobile Cloud Computing: Architecture Applications and Approaches In Wireless Communications and Mobile Computing", 2011.

[11] Wei Ren. Linchen Yu. Ren Gao. Feng Xiong., "Lightweight and Compromise Resilient Storage Outsourcing with Distributed Secure Accessibility in Mobile Cloud Computing", *Tsinghua Science And Technology* **16(5)** , 520-528, 2011.

[12] Liu Q. Wang G. Wu J., "Efficient sharing of secure cloud storage services", *IEEE 10th International Conference on Computer and Information Technology (CIT10),* 922-929, 2010.

[13] Jim Luo. Myong Kang. Aman Sagar. Sanjeev Kumar., "Application Lockbox for mobile device security Palladium in Cryptography", *HCTL Open International Journal of Technology Innovations and Research* **7(1)**, 2014.

[14] P. Syam Kumar. R. Subramanian. D. Thamizh Selvam., "Ensuring Data Storage Security in Cloud Computing using Sobol Sequence", *IEEE Journal*, 2010.

[15] Rahul Bhatnagar. Suyash Raizada. Pramod Saxena.,"Security In Cloud Computing", *International Journal For Technological Research In Engineering*, 2013.

[16] Venkata Sravan Kumar. Maddineni Shivashanker Ragi., "Security Techniques for Protecting Data in Cloud Computing", *Master SE*, 371-379, 2011.

[17] E. Lagerspetz. S. Tarkoma., "Mobile Search and the Cloud: The Benefits of Offloading", *IEEE International Conference on Workshops (PERCOM Workshops)*, 117–122, 2011.

[18] X. Zhang. J. Schiffman. S. Gibbs. A. Kunjithapatham. S. Jeong., "Securing Elastic Applications on Mobile Devices for Cloud Computing", *Proc*, 2012.