IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-4, April 2019 E-ISSN: 2347-2693

Identity-Based Proxy-Oriented Data Uploading and Remote Data Integrity Checking in Public Cloud

A. Ashik hussain[1]*, R.C. Subashini[2]

C.S.E, *Oxford Engineering College Pirattiyur, Tiruchirappalli, Tamil Nadu*

*Corresponding Author: *hussainashik4@gmail.com*

DOI: https://doi.org/10.26438/ijcse/v7i4.400405 | Available online at: www.ijcseonline.org

Accepted: 14/Apr/2019, Published: 30/Apr/2019

***Abstract*—** Computing capacity and storage space need of these devices are ever-increasing tremendously, it demands the secure way of storing the data in cost efficient model. There are vast numbers of users who use cloud services through mobile devices such as mobiles, PDA, tablets, laptops outstanding to its portability feature. Cloud Computing has many advantages inherent in it, but yet there are several risks and constraint exists, for e.g. protection, data access control, efficiency, bandwidth, etc a novel remote data integrity checking model: IDP (identity-based proxy) in multi-cloud storage. The formal system model and security model are given. Based on the bilinear pairings, a concrete IDP protocol is designed.To analyze the efficiency of various well known cryptographic algorithms such as Identity-based cryptography,Proxy public key cryptography, these symmetric algorithms were implemented on cloud background and through the results derived from real time implementation of these algorithms on various handheld procedure, it is shown that which cryptographic technique can provide efficient and reliable security mechanism for information access control and security of user's outsourced information in cloud computing.

***Keywords*—** Data security, Cryptographic techniques; Identity-based cryptography, Proxy public key cryptography

I. INTRODUCTION

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. Normally Cloud storage services users to distantly outsource their data and have the benefit of on-demand high quality cloud application with no trouble of having local hardware and software tools. Although the advantages are understandable, such a overhaul is also 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 could be fast and consistent. User mobility, that means "anytime, anywhere" is turning in to an actuality. Making use of tools, computing ability from cloud computing technology and Internet convenience jointly is making a new surge, which is cloud computing for organizations.

Cloud computing comes with many advantages such as, due to high resource availability on cloud servers, member need not worry to have very high arrangement devices with them for efficiency and power performance also CSPs provide possessions in rental basis and are much more economical than buying expensive hardware. As user need to pay as per procedure and range of hardware chosen so it is scalable and user can limit their resources to make it under their budget. The most excellent part here is its global availability due to data storage on server side and accessibility over internet.

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 devices with outsourcing information on cloud server. Common security problems in key management are

- ✓ Effectiveness in 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

II. RELATED WORK

There exist many different security problems in the cloud computing. This paper is based on the research results of proxy cryptography, identity-based public key cryptography

and remote data integrity checking in public cloud. In some cases, the cryptographic operation will be delegated to the third party, for example proxy. Thus, we have to use the proxy cryptography. Proxy cryptography is a very important cryptography primitive. In 1996, Mambo *et al.* proposed the notion of the proxy cryptosystem.When the bilinear pairings are brought into the identity-based cryptography, identity based cryptography becomes efficient and practical. Since identity-based cryptography becomes more efficient because it avoids of the certificate management.

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 generates 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 proposed. 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 archive retain and dependably transmits file data sufficient for the user to recover F in its whole. A POR is a kind of cryptographic evidence of knowledge (POK), but one specially designed to handle a big file F. To discover POR protocols, in which the message expenses, memory accesses 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 integrity 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 financial system of scale for Cloud Computing.

In [6] 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 ineffective 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 blocks, including: data insert, update, delete and append

III. METHODOLOGY

3.1 Cryptographic Approach

The encryption algorithm is most frequently used technique to protect data within cloud environment. The data related to a customer can be categorized as public data and private data. The public data is sharable among trusted clients that provide an open environment for cooperation. Private data is client's confidential data that must be transferred in encrypted form for security and privacy. In this paper propose a suitable method that cryptographic algorithms with different key length are used in various environment. The number of devices such as smart phones and smart pads grows rapidly recently. These two keys are the same or easy to deduce each other. The representatives of symmetric cryptosystem are Identity-**based cryptography, Proxy public key cryptography** . For an asymmetric cryptosystem, the receiver possesses private key. and public key .The public key can be published but the private key should be kept secret. The legislature of asymmetric cryptosystem are RSA (Rivest Shamir Adleman) and ECC (Elliptic Curve Cryptosystem).

3.2 System Model and Security Model of ID-PUIC

The system model and security model of IDP protocol. An IDP protocol consists of four different entities which are described below:

1) Original Client: an entity, which has massive data to be uploaded to PCS by the delegated proxy, can perform the remote data integrity checking.

2) PCS (Public Cloud Server): an entity, which is managed by cloud service provider, has significant storage space and computation resource to maintain the clients' data.

3) Proxy: an entity, which is authorized to process the Original Client's data and upload them, is selected and authorized by Original Client. When Proxy satisfies the warrant m! Which is signed and issued by Original- Client, it

can process and upload the original client's data; otherwise, it can not perform the procedure.

4) *KGC* (Key Generation Center): an entity, when receiving an identity, it generates the private key which corresponds to the received identity.

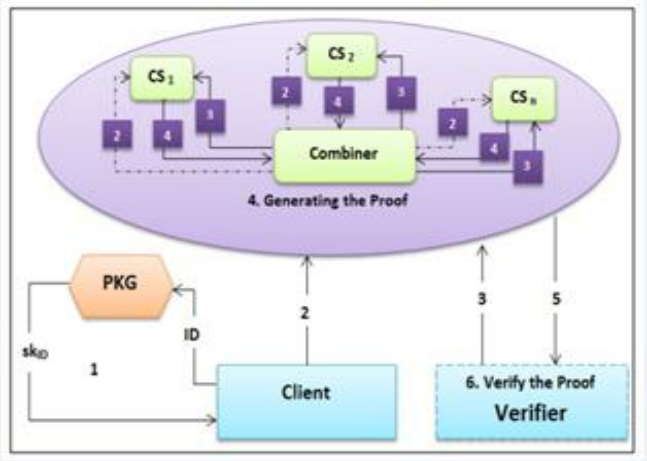

Fig .1 Architecture

3.3 System Model and Security Model of Proxy Public Key Cryptography

The proxy public key cryptography system model and security definition are presented in this section. An proxy public key cryptography protocol comprises four different entities which are illustrated in Figure 1. We describe them below:

1) *Client*: an entity, which has massive data to be stored on the multi-cloud for maintenance and computation, can be either individual consumer or corporation.

2) *CS* (Cloud Server): an entity, which is managed by cloud service provider, has significant storage space and computation resource to maintain the clients' data.

3) *Combiner*: an entity, which receives the storage request and distributes the block-tag pairs to the corresponding cloud servers. When receiving the challenge, it splits the challenge and distributes them to the different cloud servers. When receiving the responses from the cloud servers, it combines them and sends the combined response to the verifier.

4) *PKG* (Private Key Generator): an entity, when receiving the identity, it outputs the corresponding private key.

IV. RESULTS AND DISCUSSION

The proposed method has been implemented using .NET Technology. Extensive experiment were conducted to check good organization of symmetric algorithms on mobile background for encryption and decryption of data before outsourcing data to cloud servers. Implemented revealed performance of algorithms i.e. when executed for diverse no. of operations separately. Below are the output of algorithm performance which were found in study:

Structure Model and Security Model Of IDP

4.1 Cloud server

It is a CSP in cloud computing. Server uses glassfish server and web services to communicate with mobile applications. Here SOAP is used for connection between client and server. Two types of servers are used

a) Storage server:

Here outsourced information is stored in the form of encrypted files. It is used for storage purpose only no computation is done.

b) Trusted hashing server:

This is THS server used for store log of hash of files for backup. Its computing display place performs both computations as well as storage of hash.

Database:

SQLSERVER is used as a database. Here encrypted user files
are stored.

4.2 User 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 users have to register their identity to this system. Once registered the system will provides the accessibility rights to the users 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's Data is transformed into data blocks 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 datas 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 we are making key certification along with the deletion process. One problem can arise is in the case of key remembrance.

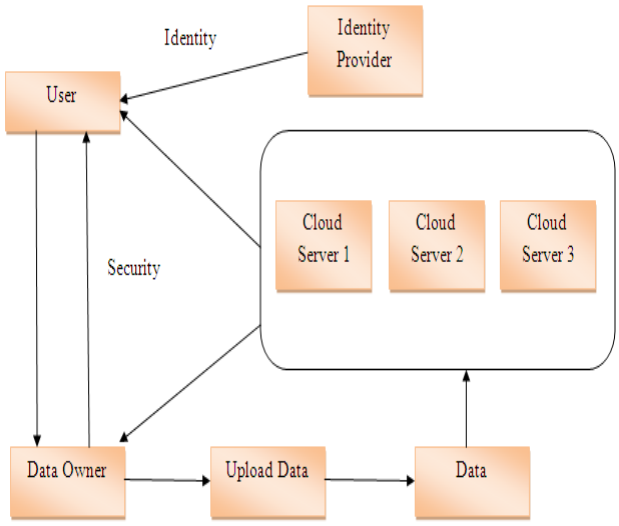

Fig: 2 Process flow Diagram

4.3 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)	Proposed technique	Traditional technique
10	30992	32681
50	30638	33039
100	31028	33924
500	31394	34292
1000	31884	34881
2000	32194	35028
3000	33920	35719

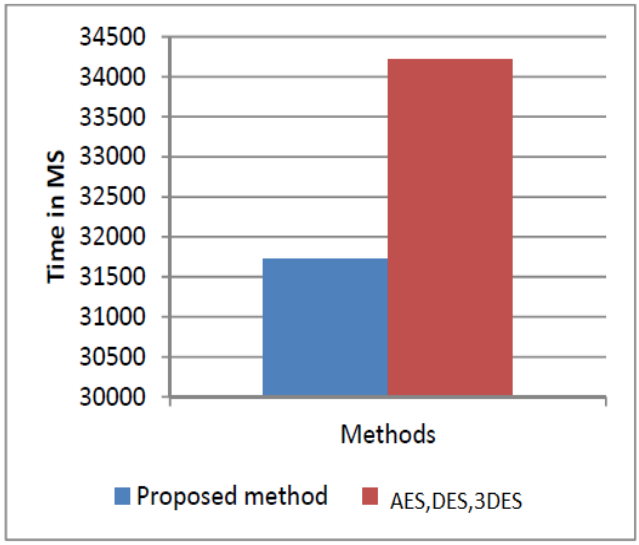

Chart1 mean memory consumption

4.5 Decryption memory
For a cryptographic algorithm the amount of main memory required, to recover the original text from cipher is defined 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 shows the different file size used for experimentation and Y axis reports amount of main memory consumed.

File size	Proposed technique	Traditional technique
10	29019	29847
50	29383	30924
100	29981	31947
500	30284	32844
1000	35472	36649
2000	37918	37845
3000	39519	40029

Table 2 decryption memory used

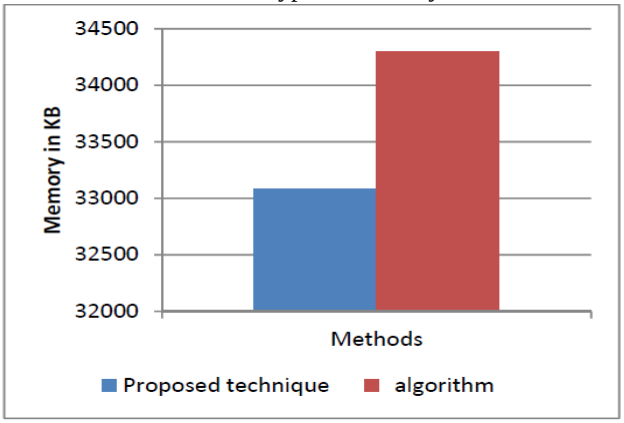

Chart 2 mean performance

Mobile Cloud Server Execution time

File size	Proposed algorithm	Traditional system
10	0.331	0.547
50	2.04	3.38
100	4.12	6.21
500	18.14	28.42
1000	34.93	46.52
2000	68.25	112.53
3000	105.39	158.45

Table 3 decryption time

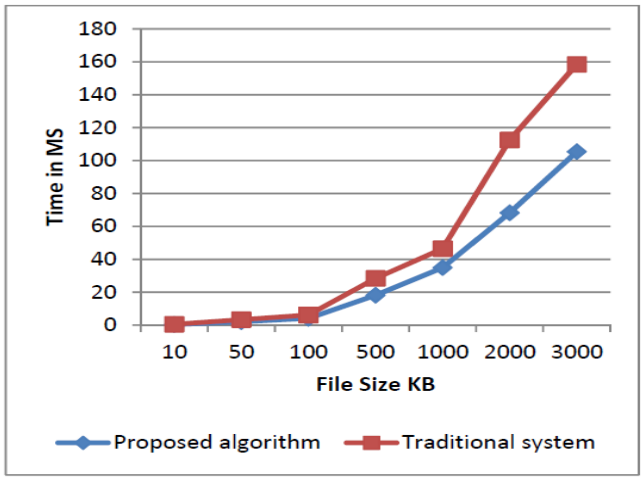

Chart 3 decryption time

V. CONCLUSION AND FUTURE SCOPE

In multi-cloud storage, this paper formalizes the IDP system model and security model. At the same time, we propose the first IDP protocol which is provably secure under the assumption that the CDH problem is hard. Besides of the elimination of certificate management, our IDP protocol has also flexibility and high efficiency. At the same time, the proposed IDP protocol can realize private verification, delegated verification and public verification based on the client's authorization.

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]. Simoens, P., De Turck, F., Dhoedt, B., 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 Vol. 2, Iss ue 2, June 20 I I .

[5]. Shahryar Shafique Qureshi1 , 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 (2011) The NIST definition of Cloud Computing. NIST, Special Publication 800–145, Gaithersburg, MD

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

[8]. Pearson, S., Y. Shen, and M. Mowbray, "A Privacy Manager for Cloud Computing", in Proceedings of the 1st International Conference on Cloud Computing. 2009, Springer-Verlag: Beijing, China. p. 90-106.

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

ESORICS 2009, M. Backes and P. Ning, Editors. 2009, Springer Berlin / Heidelberg. p. 355-370.

[10]. Hoang T. Dinh, Chonho Lee, Dusit Niyato, and 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,ISSNl1007-0214ll06/09llpp520 528.Volume 16, Number 5, October 2011.

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

[13]. Jim Luo And Myong Kang, 2011."Application Lockbox for mobile device security" Aman Sagar, Sanjeev Kumar, Palladium in Cryptography:HCTL Open International Journal of Technology Innovations and Research, Volume 7,January 2014, ISSN: 2321-1814, ISBN: 978-1-62951-250-1.

[14]. P. Syam Kumar, R. Subramanian and D. Thamizh Selvam, Ensuring Data Storage Security in Cloud Computing using Sobol Sequence, 978-1-4244- 7674-9/10., IEEE, 2010.

[15]. Rahul Bhatnagar, Suyash Raizada, Pramod Saxena, SECURITY IN CLOUD COMPUTING ,International Journal For Technological Research In Engineering, ISSN (Online) : 2347 4718, December - 2013.

[16]. Venkata Sravan Kumar, Maddineni Shivashanker Ragi, Security Techniques for Protecting Data in Cloud Computing, Master SE – 371 79 Karlskrona Sweden, November 2011.

[17]. K. Kumar and Y. H. Lu, "Cloud Computing For Mobile Users: Can Offloading Computation Save Energy?," IEEE Journal Computer, vol.43, pp. 51-56, April 2010.

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

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

[20]. W. Ren, L. Yu, R. Gao, and F. Xiong, "Lightweight and Compromise Resilient Storage Outsourcing with Distributed Secure Accessibility in Mobile Cloud Computing," vol. 16, pp.520-528, October 2011.

