IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-5, Issue-8 E-ISSN: 2347-2693

Identity Based Distributed Provable Data Possession in Multi Cloud Storage

A. Abinaya[1*], K. Fathima Bibi[2],

[1*]Dept. of Computer Science Rajah Serfoji Govt. College(Autonomous), Thanjavur, India
[2]Dept. of Computer Science Rajah Serfoji Govt. College(Autonomous), Thanjavur, India

[*]*Corresponding Author: abinayaanbazhagan93@gmail.com, Tel.: +91-9943065890*

Available online at: www.ijcseonline.org

Received: 14/Jul/2017, Revised: 27/Jul/2017, Accepted: 19/Aug/2017, Published: 30/Aug/2017

***Abstract*—** Online data integrity checking is very main in cloud storage space. It can make the users verify whether their outsourced data is kept intact without downloading the whole data. In some application scenarios, the clients have to store their data on multi-cloud servers. At the same time, the integrity examination protocol must be efficient in order to save the verify cost. Thus a novel remote data integrity checking model: identity-based distributed provable data possession (ID-DPDP) is proposed for a multi-cloud storage. Based on the bilinear pairing, a concrete ID-DPDP protocol is design. The current paper proposed ID-DPDP protocol is provably protected under the hardness assumption of the standard computational diffie-hellman (CDH) problem. In addition to the structural to the advantages of elimination of certificate management, the ID-DPDP protocol is efficient and flexible. Based on the user authorization, the proposed ID-DPDP protocols perform private verification, delegated verification, and public verification.

***Keywords*—** *Cloud computing, Provable data possession, Identity-Based Distributed Provable*

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. 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 organizations.

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.

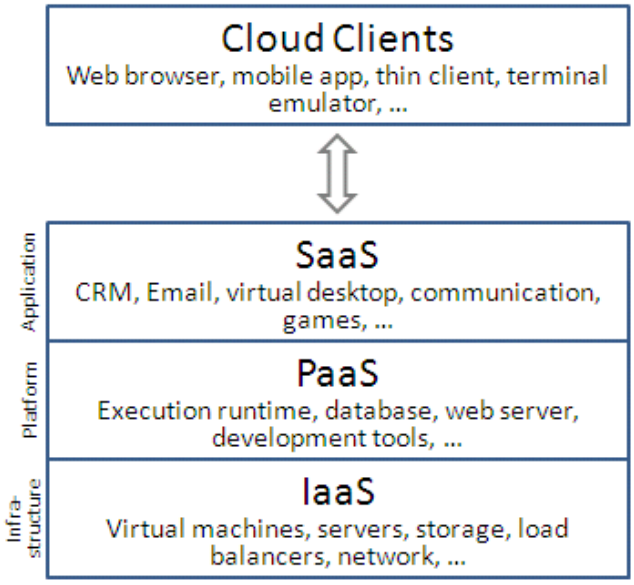

Figure 1: Cloud Computing [1-11]

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

II. RELATED WORK

In [1] the PDP model, the verifier can check remote data integrity with a high probability. Based on the RSA, they esigned two provably secure PDP schemes. After that, Ateniese *et al.* proposed dynamic PDP model and concrete scheme although it does not support insert operation. Author introduced the efficient and protected outsource data is addressed either by public key cryptography or requiring the member to outsource its data in encrypted form called PDP.

In [2] storage-outsource service and resource-sharing network have become popular; the problem of powerfully proving the integrity of data stored at untrusted servers has received increased attention. In the provable data possession (PDP) model, the member preprocesses the data and then send it to an untrusted server for storage space, while keeping a small amount of meta-data. The member later on ask the server to prove that the store information has not been tamper with or deleted without downloading the actual data. The original PDP scheme applies only to static (or append-only) files advantages high latency ,At the same time a cloud member are limited ,technique DPDP Scheme drawbacks Memory access are low and storage necessities is not enough.

In [3] cloud computing has been envisioned as the on-demand self-service, ubiquitous network access, location independent resource pooling, rapid resource elasticity, usage-based pricing and transference of risk. Today, technical research works focus on Remote data possession Checking protocols permit to check that a remote server can access an uncorrupted file with the help of third party verifiers. In this paper, Sebe et al.'s protocol is adapted to support efficient remote data possession checking in critical information infrastructure without the help of a third party auditor.

In [4] provable data possession (PDP) is a technique for ensuring the integrity of data in storage outsourcing. In the production of an EPDP scheme for distribute cloud storage to maintain the scalability of service and information migration, in which consider the existence of several cloud server to cooperatively store and maintain the user data.

In [5] authors proposed 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 retains and reliably transmits file data sufficient for the user to recover F in its whole. A POR is a kind of cryptographic proof of knowledge (POK), but one specially designed to handle a large file F. To explore POR protocols, in which the communication expenses, memory accesses for the proven, and storage necessities of the client are small parameters essentially independent of the length of F. The goal of a POR is to accomplish these checks without client having to retrieve the files themselves. A POR can also provide service with quality assurances.

In [6] authors introduced the problem of ensuring the integrity of data storage. In particular, to consider the task of allowing a third party auditor (TPA), on behalf of the user, to verify the integrity of the dynamic data stored in the cloud server. The TPA reduce the participation of the client through the auditing of whether their data in the cloud is indeed intact, which can be important in achieving financial system of scale for Cloud Computing.

III. METHODOLOGY

3.1 Exiting model

In cloud computing online data integrity checking is main security problem. The member massive data is outside his control. The malicious cloud server may corrupt the member's data in order to gain more benefits. The formal system model and security model are existing models. In the PDP model verify can confirm remote data integrity with a high possibility. Based on the RSA, they designed two provably secure PDP schemes. PDP allows a verifier to verify the remote data integrity without retrieving or downloading the whole data. The verifier only maintains small metadata to perform the integrity checking. PDP is an motivating online data integrity checking model. In this verify can check the remote data integrity and retrieve the remote data at any time. On some cases, the client may delegate the remote data integrity checking task to the third party. It results in the third party auditing in cloud computing.

3.1.1 DRAWBACKS OF THE PDP METHODOLOGY

- Does not provide effectiveness in online data integrity checking.
- More exclusive for cloud maintains process.
- The existing system provides less flexibility.
- Data losses accrue.

3.2 PROPOSED WORK

Online data integrity checking is of crucial import in cloud storage. In multi-cloud environment, distributed provable data possession is an important element to secure the remote data. This proposes a novel remote data integrity checking model: Identity-Based Distributed Provable Data Possession (ID-DPDP) in multi-cloud storage. The proposed ID-DPDP protocol is provably protected below the hardness hypothesis of the standard Computational Diffi Hellman (CDH) problem. The proposed ID-DPDP protocol can realize private verification, delegated verification and public verification.

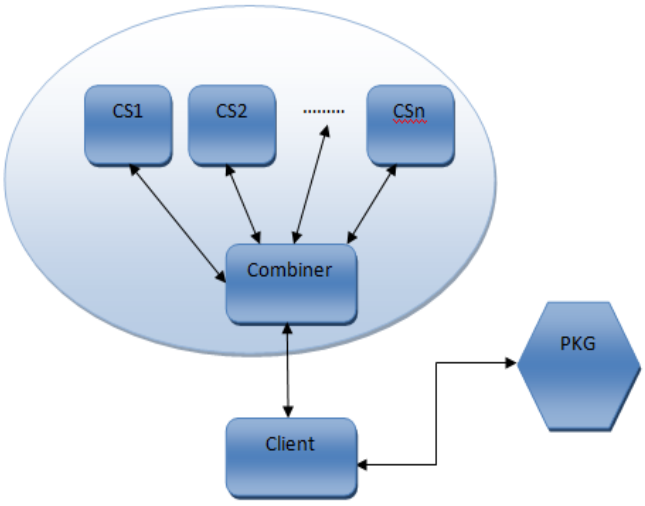

Figure 2: Multi Cloud Architecture

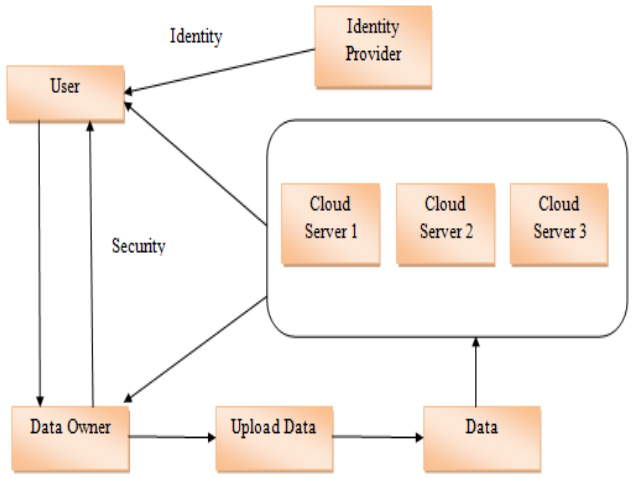

Figure 3: Process flow diagram

ALGORITHM OF ID-DPDP

It is a efficient ID-DPDP protocol. 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: $G1 \times G1 \rightarrow G2$ be a bilinear map which satisfies the subsequent property:

1) Bilinearity:

$\forall g1, g2, g3 \in G1$ and $a, b \in Zq$

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

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

2) Non-degeneracy

$\exists_{g4, g5} \in G1$ such that e (g4, g5) $g6 = 1G2$

3) Computability

∀g6, g7 ∈ G1, there is an efficient algorithm to calculate e (*g6*, *g7*)

The ID-DPDP scheme relies on the hardness of Computation Diffie-Hellman(CDH) problem and the easiness of Decisional Diffe-Hellman(DDH) problem.

Step: 1 (CDH Problem on G1): Let g be the generator of *G1*. Given g, *ga*, gb ∈ *G1*for randomly chosen a, b ∈ zq, calculate *gab* ∈ *G1*.

Step: 2 (DDH Problem on *G1*): Let g be the generator of *G1*. Given (*g*, *ga*, *gb*, ˆ*g*) ∈ *G4*1 for randomly chosen *a*, *b* ∈ Z* *q*, decide whether g^{ab} ?= ˆ*g*.

Performance Analysis

Table : 1 Time Required For File Upload And Download In Milli Seconds

File Name	File Type	File Size	Time (ms) Encryption	Encryption	Decryption
Server	txt	30KB	0	20	10
Connect111	txt	338KB	16	20	40
Machine	txt	1.34MB	40	70	60
Client	txt	14.7MB	360	480	850
Document	doc	22KB	10	10	20
Implementation	doc	165KB	10	10	25
v1	doc	1.16MB	70	10	70
Varsha REPORT	doc	9.25MB	190	10	530
VisaCard Platinum	xls	18KB	10	20	10
2013-14 TT	xls	165KB	10	10	10
Tg Data Comp	xls	523KB	30	20	30
Faculty Tt	xls	1MB	30	20	20
Christmas fair	pdf	11KB	0	10	10
iiiij	pdf	158KB	10	15	30
Identity	pdf	1.07MB	20	30	60

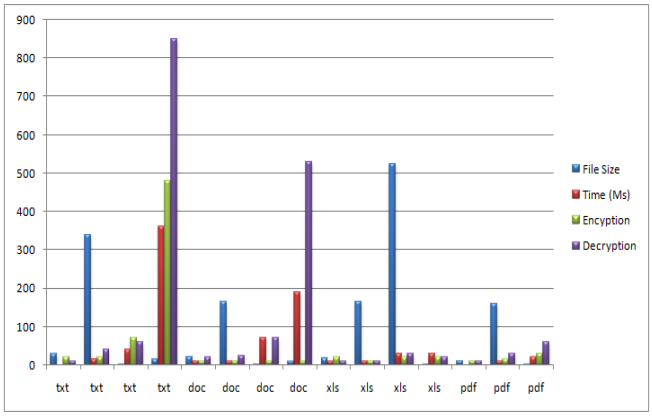

Figure 3: Process flow diagram

IV. RESULTS AND DISCUSSION

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 were 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 figure 5 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

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 figure 6 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.

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

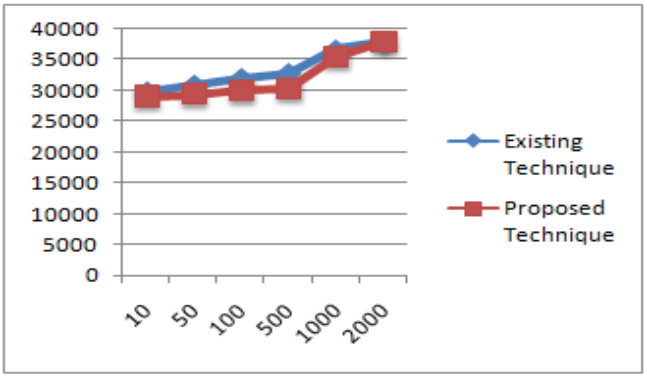

Figure 6: Decryption memory used

Cloud Server Execution time

Table 3 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

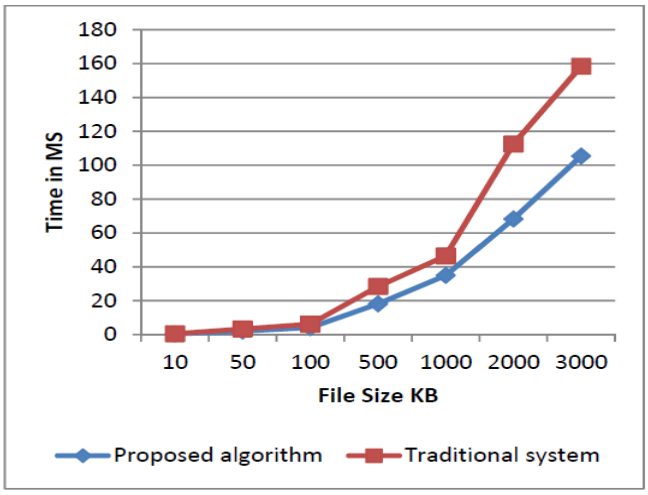

Figure 7. Execution time

V. CONCLUSION AND FUTURE SCOPE

In multi-cloud storage, this study formalizes the identity based distributed system model and security form. At the same time, this procedure is provably secure under the assumption that the CDH problem is hard. Besides the removal of certificate organization, the proposed protocol shows flexibility and high efficiency. At the same time, the proposed algorithm can realize private verification, delegated verification and public verification based on the member's authorization. When the proposed protocol is compared for efficiency in terms of time and memory, it proved to be advantages for small sized file as for as memory consumption is concerned. The proposed works faster. It is simple and requires no complex computations, and yet yields accurate estimation. The distributed cloud storage is indispensable. As part of future work would extend our work to explore more effective CPDP constructions. Finally, it is still a challenging problem for the generation of tags with the length irrelevant to the size of data blocks. An explore such a issue to provide the support of variable-length block verification

REFERENCES

[1]. P. Ranjima, Sumathi. D , M. Mathew, P. Sivaprakash, "*Secure Cloud Storage with Access Control: A Survey*", International Journal of Computer Sciences and Engineering, Vol.2, Issue.8, pp.124-126, 2014.

[2]. Erway C.C., Kupcu A., C. Papamanthou "*Dynamic Provable Data Possession in multicloud storage*", CCS'09, pp. 2136-233, 2014.

[3]. Seb´e F., Domingo-Ferrer J., Mart´ınez-Ballest´e A., DeswarteY., "*Remote Data Integrity checking in Critical Information Infrastructures*", IEEE Transactions on Knowledge and Data Engineering, 2015(8), pp.1-6, 2015.

[4]. Zhu Y., Hu H., Ahn G.J., Yu M., "*Cooperative Provable for Integrity Verification in Multi cloud Storage*", IEEE Transactions on Parallel and Distributed Systems, 23(12), pp. 2251-2234, 2015

[5]. Curtmola R., Khan O., Burns R., Ateniese G., "*MR-PDP: Multiple- Replica Provable Data Possession*", ICDCS'09, pp. 415-460, 2016.

[6]. Barsoum A. F., Hasan M. A., "*Replication of Data over Cloud Servers*", CACR, University of Waterloo, Report2010/32, 2016.

[7]. Shivlal Mewada, Umesh Kumar Singh and Pradeep Sharma, "*Security Enhancement in Cloud Computing (CC)*", International Journal of Scientific Research in Computer Science and Engineering, Vol.1, Issue.1, pp.31-37. 2013.

[8]. Bincy Paul and M. Azath, "*Survey on Preserving Data Privacy in Cloud*", International Journal of Computer Sciences and Engineering, Vol.2, Issue.12, pp.57-61, 2014.

[9]. Wang, Q., et al., "*Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing*", in Computer Security – ESORICS 2014, M. Backes and P. Ning, Editors. 2009, Springer Berlin/Heidelberg. p.355-370.

[10]. Mohd.A. Salam, A.C. Pandey, "*Mobile Cloud Computing: Taking Web-Based Mobile Applications to the Cloud*", International Journal of Computer Sciences and Engineering, Vol.2, Issue.1, pp.35-42, 2014.

[11]. S. Tamilarasan, P.K. Sharma, "*A Survey on Dynamic Resource Allocation in MIMO Heterogeneous Cognitive Radio Networks based on Priority Scheduling*", International Journal of Computer Sciences and Engineering, Vol.5, No.1, pp.53-59, 2017.

Authors Profile

A. Abinaya pursued Master of Science in Computer Science from Bharathidasan University in 2015. She is currently pusuing M.Phil in Computer Science from Rajah Serfoji Govt. College, Thanjavur affilliated to Bharathidasan University. Her main research work focusses on Cloud Computing.

Dr. K. Fathima Bibi is currently working as an assitant Professor at Rajah Serfoji Govt. College, Thanjavur in the department of Coputer Science. She has published 10 research papers in reputed international journals including Elesiver Scopes indexed and conferences including IEEE and its also available online. Her main research work focusses on Data Mining and Netwoek Security. She has 15 yrs of teaching experience and 10 yrs of Research Experience.

