Research Article Impact Factor: 0.621 ISSN: 2319-507X
Krunal Chandewar, IJPRET, 2014; Volume 2 (8): 457-464 IJPRET

INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

FRAMEWORK OF DATA INTEGRITY VERIFICATION FOR MULTI CLOUDS USING CPDP SCHEME

KRUNAL N. CHANDEWAR, SHAILESH T. KHANDARE

Master of Engg. in Computer Science & Engg., Sgbau Amravati University
BNCOE, Pusad, Yavatmal India.

Accepted Date: 15/02/2014 ; Published Date: 01/04/2014

Abstract: Cloud computing has become increasingly popular as it offers users the illusion of having unlimited computing resources. It also provides greater scalability, availability, and reliability than users could achieve with their own resources. So, Security in terms of integrity is most important aspects in cloud computing environment. In this paper, we address the construction of an efficient PDP scheme for distributed cloud storage to support the scalability of service and data migration, in which we consider the existence of multiple cloud service providers to cooperatively store and maintain the clients' data.

Keywords: Provable Data Possession, Interactive Protocol, Multiple Cloud, Cooperative, Storage Security, Provable Data Possession

PAPER-QR CODE

Corresponding Author: MR. KRUNAL N. CHANDEWAR

Access Online On:

www.ijpret.com

How to Cite This Article:

Krunal Chandewar, IJPRET, 2014; Volume 2 (8): 457-464

INTRODUCTION

Cloud Computing is the internet based storage for files and applications. It is faster profit growth by providing scalability, low cost, pay as much as used at anywhere and any place. Security & integrity of data is most important aspect during data storage in clouds [1].

Cloud computing refers to the delivery of computing resources over the Internet. Instead of keeping data on your own hard drive or updating applications for your needs, you use a service over the Internet, at another location, to store your information or use its applications Doing so may give rise to certain privacy implications. Cloud computing is the delivery of computing services over the Internet. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations [3].

Examples of cloud services include online file storage, social networking sites, webmail, and online business applications. The cloud computing model allows access to information and computer resources from anywhere that a network connection is available. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications [5].

MOTIVATION

The security of our data is most important aspect and to provide security firstly PDP scheme is proposed. Secondly SPDP scheme is proposed then DPDP scheme is proposed after then CPOR Scheme is proposed and the Limitation of this CPOR scheme is a Lack of some security issues for large files which are removed by our proposed CPDP scheme.

RELATED WORK

1) PROPOSED SYSTEM

In proposed system for integrity verification CPDP Scheme shall be used which will be used for verifying integrity of data in multi cloud using cryptosystem at TTP. For cloud formation, Windows Azure Services Platform Framework shall be used. With the help of Azure emulator, Multi cloud will be formed. Databases will be in MS-SQL.

The proposed work shall be categorised into four modules. The first module shall be cloud formation module where we shall be creating a cloud with the help of azure emulator. The second module shall be secure cloud to cloud interaction module for making trust between two clouds. The subsequent module shall be related with interaction between multiple clouds with integrity using trusted third party in this phase data will be accessed from multiple clouds with integrity and without communication and computation overhead. The final module shall be based on results to show experimental results where encrypted and decrypted data is shown.

2) SYSTEM ARCHITECTURE

In this architecture, a data storage service involves three different entities:

1. Clients who have a large amount of data to be stored in multiple clouds and have the permissions to access and manipulate stored data .

2. Cloud service providers who work together to provide data storage services and have enough storages.

3. Trusted Third Party who is trusted to store verification parameters.

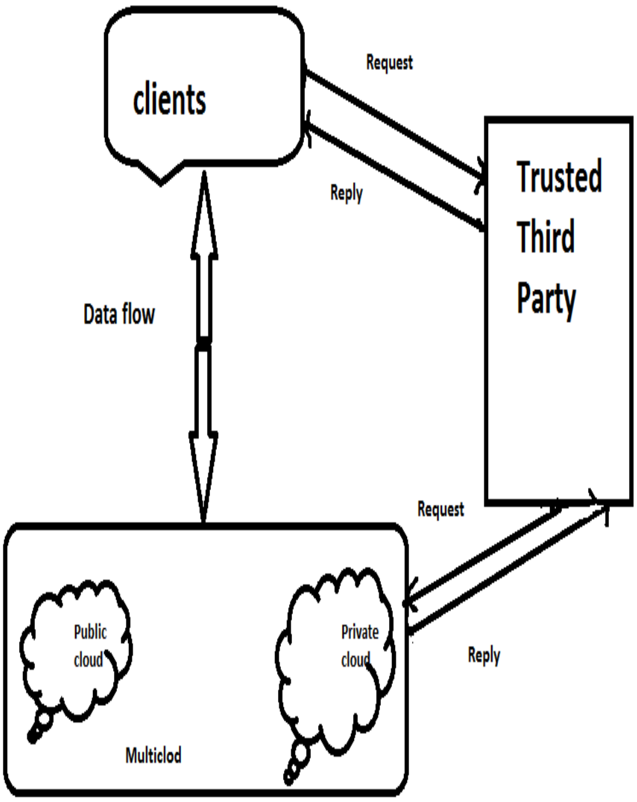


Fig. 1 Data integrity for cross cloud environment

3) FLOW CHART

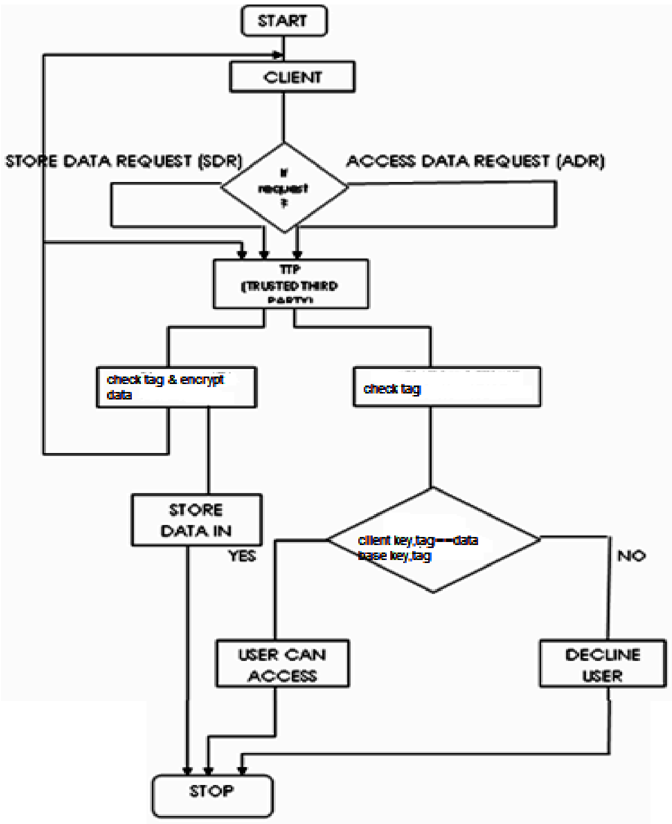


Fig. 2 Flow of working system

4) WORKING OF ALGORITHM AT TTP

CPDP in Cloud is S = (KeyGen, TagGen, Proof)

- KeyGen, (1κ): Takes a security parameter κ as input, and returns a secret key sk or a public-secret key pair (pk, sk).
- TagGen (sk, F,P): Takes inputs a secret key sk, a file F, and a set of cloud storage providers P = $\{Pk\}$, and returns the triples (st,vp,at).
- Proof (P, V): A protocol of proof of data possession between csps (P = $\{Pk\}$) and a verifier (V), that is $\langle \Sigma(F(k)$, at $(k)) \longleftrightarrow V\rangle$ $(pk$, vp) = { 1 $F = \{F(k)\}$ is intact $Pk \in$P { 0 $F = \{F(k)\}$ is changed V Returns a bit {0|1}

KeyGen(1^κ): Let $\mathbb{S} = (p, \mathbb{G}, \mathbb{G}_T, e)$ be a bilinear map group system with randomly selected generators $g, h \in \mathbb{G}$, where $\mathbb{G}, \mathbb{G}_T$ are two bilinear groups of a large prime order p, $|p| = O(\kappa)$. Makes a hash function $H_k(\cdot)$ public. For a CSP, chooses a random number $s \in_R \mathbb{Z}_p$ and computes $S = g^s \in \mathbb{G}$. Thus, $sk_p = s$ and $pk_p = (g, S)$. For a user, chooses two random numbers $\alpha, \beta \in_R \mathbb{Z}_p$ and sets $sk_u = (\alpha, \beta)$ and $pk_u = (g, h, H_1 = h^\alpha, H_2 = h^\beta)$.

TagGen$(sk, F, \mathcal{P})$: Splits F into $n \times s$ sectors $\{m_{i,j}\}_{i\in[1,n], j\in[1,s]} \in \mathbb{Z}_p^{n\times s}$. Chooses s random $\tau_1, \cdots, \tau_s \in \mathbb{Z}_p$ as the secret of this file and computes $u_i = g^{\tau_i} \in \mathbb{G}$ for $i \in [1, s]$. Constructs the index table $\chi = \{\chi_i\}_{i=1}^n$ and fills out the record χ_i [a] in χ for $i \in [1, n]$, then calculates the tag for each block m_i as

$$\begin{cases} \xi^{(1)} \leftarrow H_{\sum_{i=1}^s \tau_i}(F_n), & \xi_k^{(2)} \leftarrow H_{\xi^{(1)}}(C_k), \\ \xi_{i,k}^{(3)} \leftarrow H_{\xi_k^{(2)}}(\chi_i), & \sigma_{i,k} \leftarrow (\xi_{i,k}^{(3)})^\alpha \cdot (\prod_{j=1}^s u_j^{m_{i,j}})^\beta, \end{cases}$$

where F_n is the file name and C_k is the CSP name of $P_k \in \mathcal{P}$. And then stores $\psi = (u, \xi^{(1)}, \chi)$ into TTP, and $\sigma_k = \{\sigma_{i,j}\}_{\forall j = k}$ to $P_k \in \mathcal{P}$, where $u = (u_1, \cdots, u_s)$. Finally, the data owner saves the secret $\zeta = (\tau_1, \cdots, \tau_s)$.

Proof$(\mathcal{P}, V)$: This is a 5-move protocol among the Provers ($\mathcal{P} = \{P_i\}_{i\in[1,c]}$), an organizer ($O$), and a Verifier ($V$) with the common input (pk, ψ), which is stored in TTP, as follows:

1) **Commitment**$(O \to V)$: the organizer chooses a random $\gamma \in_R \mathbb{Z}_p$ and sends $H_1' = H_1^\gamma$ to the verifier;
2) **Challenge1**$(O \leftarrow V)$: the verifier chooses a set of challenge index-coefficient pairs $Q = \{(i, v_i)\}_{i\in I}$ and sends Q to the organizer, where I is a set of random indexes in $[1, n]$ and v_i is a random integer in $\mathbb{Z}_p^*$;
3) **Challenge2**$(\mathcal{P} \leftarrow O)$: the organizer forwards $Q_k = \{(i, v_i)\}_{m_i \in P_k} \subseteq Q$ to each P_k in $\mathcal{P}$;
4) **Response1**$(\mathcal{P} \to O)$: P_k chooses a random $r_k \in \mathbb{Z}_p$ and s random $\lambda_{j,k} \in \mathbb{Z}_p$ for $j \in [1, s]$, and calculates a response

$$\sigma_k' \leftarrow S^{r_k} \cdot \prod_{(i,v_i)\in Q_k} \sigma_i^{v_i}, \quad \mu_{j,k} \leftarrow \lambda_{j,k} + \sum_{(i,v_i)\in Q_k} v_i \cdot m_{i,j}, \quad \pi_{j,k} \leftarrow e(u_j^{\lambda_{j,k}}, H_2),$$

where $\mu_k = \{\mu_{j,k}\}_{j\in[1,s]}$ and $\pi_k = \prod_{j=1}^s \pi_{j,k}$. Let $\eta_k \leftarrow g^{r_k} \in \mathbb{G}$, each P_k sends $\theta_k = (\pi_k, \sigma_k', \mu_k, \eta_k)$ to the organizer;
5) **Response2**$(O \to V)$: After receiving all responses from $\{P_i\}_{i\in[1,c]}$, the organizer aggregates $\{\theta_k\}_{P_k\in\mathcal{P}}$ into a final response θ as

$$\sigma' \leftarrow \Big(\prod_{P_k\in\mathcal{P}} \sigma_k' \cdot \eta_k^{-s}\Big)^\gamma, \quad \mu_j' \leftarrow \sum_{P_k\in\mathcal{P}} \gamma \cdot \mu_{j,k}, \quad \pi' \leftarrow \Big(\prod_{P_k\in\mathcal{P}} \pi_k\Big)^\gamma. \tag{1}$$

Let $\mu' = \{\mu_j'\}_{j\in[1,s]}$. The organizer sends $\theta = (\pi', \sigma', \mu')$ to the verifier.

Verification: Now the verifier can check whether the response was correctly formed by checking that

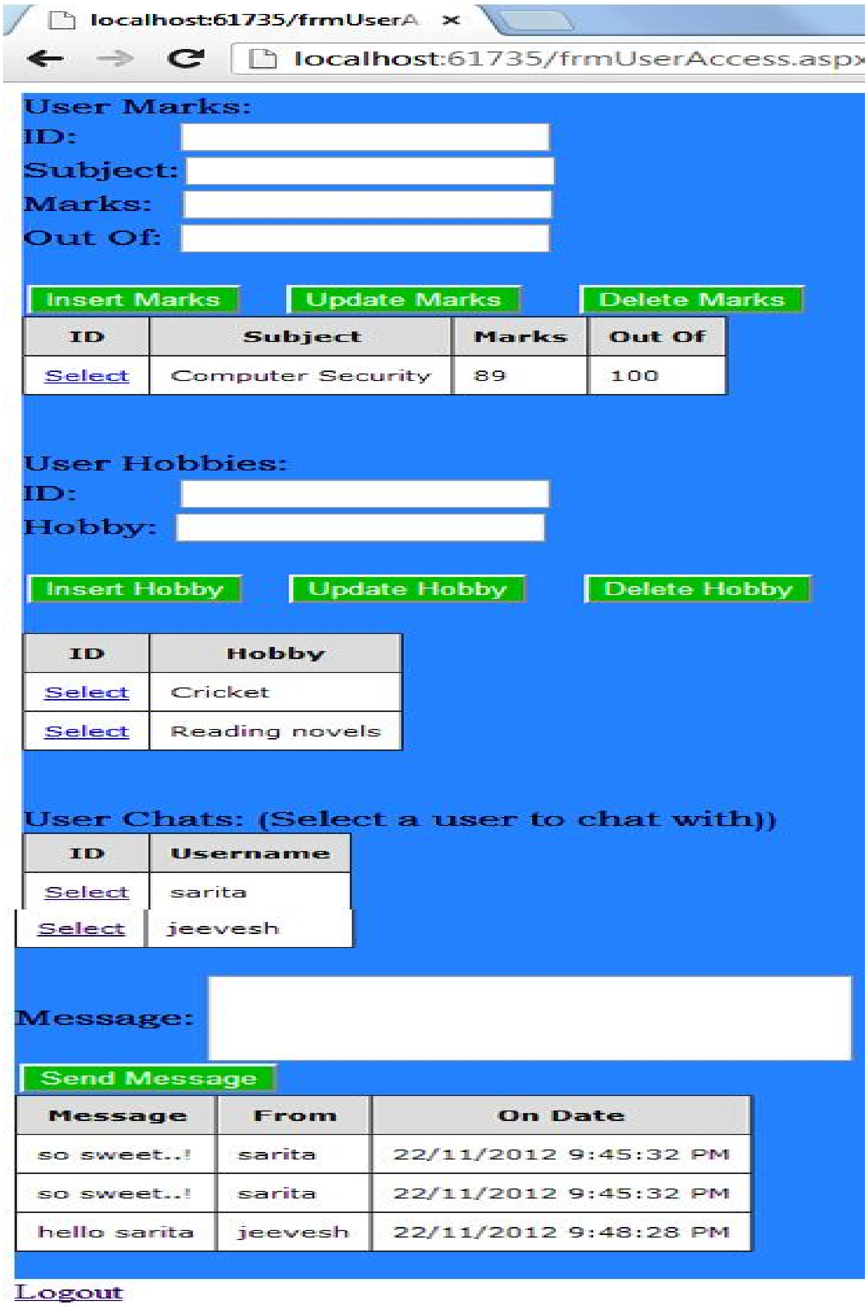
$$\pi' \cdot e(\sigma', h) \stackrel{?}{=} e\Big(\prod_{(i,v_i)\in Q} H_{\xi_k^{(2)}}(\chi_i)^{v_i}, H_1'\Big) \cdot e\Big(\prod_{j=1}^s u_j^{\mu_j'}, H_2\Big). \tag{2}$$

a. For χ_i = "B_i, V_i, R_i" in Section 2.3, we can set $\chi_i = (B_i = i, V_i = 1, R_i \in_R \{0,1\}^*)$ at initial stage of CPDP scheme.

Fig.3 Working of algorithm

5) *SNAP SHOT*

- Client data storage



- Public-key, Private-key, Encryption, Decryption, time span and data size

Publc Key:

ECK5B�H{��:��)��>�wʀkj�t��;�bk!U��M��

Private Key:

���Ţ�.�!J�UV<Q�b¸¸>���a3��

Encrypted Data:

æ�G&��c�!���b�9�K�F��H�K$��sR)���
��0V�Np"���&xxOÖK)t5z�c!�`�����1�|q��ug,
%�!iy<������~U��tf$l�Y�@,B�����`�Y��510
UEW�:*�□ₒ,□□□},w□v16"□j□~□□wB`□h̃□3□□□□ K□□G'
��鄆|Ybup2��o���S n*T�8J�(�壄�,G+�k9�{Ä□□L
□□□□□ᵞ□Qk□ħ□y□'□y

Decrypted Data:

[hobbies][hobby][id]3[/id][user_id]4[/user_id][hobby]Cricket[/hobby]
[subject]M3[/subject][marks]96[/marks][out_of]100[/out_of][/mark][
[id]1[/id][username]pankaj[/username][password]pankaj[/password][/
[password]aakash[/password][/user][user][id]4[/id][username]sarita[/

Data transfered securely. click here to go to Nagpur Cloud
Total Time required:533 ms
Total Data Size:718 bytes

Conclusions

In this paper we are creating cloud by using AZURE frame work then we stored data in cloud by using TTP cryptosystem for greater security hence we concluded. We also showed that our scheme provided all security properties required by zero knowledge interactive proof system, so that it can resist various attacks even if it is deployed as a public audit service in clouds by using this construction we are Deprecating all the limitation which is to be found in previously derived scheme.

REFERENCES

1. G. Ateniese et.al., “Provable Data Possession at Untrusted Stores”, 14th ACM Conference on Computer and Communications Security,2007

2. R.D. Pietro et.al.,", Scalable and Efficient Provable Data Possession”,2008

3. C.C. Erway et.al.," Dynamic Provable Data Possession", November 29, 2009

4. A. Juels et.al.,“ Pors: proofs of retrievability for large files”, ACM Conference on Computer and Communications Security, 2007, pp. 584–597.

5. Y. Zhu et.al.“Cooperative Provable Data Possession for Integrity Verification in Multi-Cloud Storage” ,IEEE Transactions On Parallel And Distributed Systems, Digital Object Indentifier 10.1109/TPDS 2012.66 April 2012.

6. Armbrust, et.al.,“Above the clouds: A berkeley view of cloud com-puting,” EECS Department, University of California, Berkeley, Tech. Rep., Feb 2009

7. Bialecki et. al., “Hadoop: A framework for running applications on large clusters built of commodity hardware,”2005

8. Borja et.al., “An Open Source Solution for Virtual Infrastructure Management in Private and Hybrid Clouds”,2009

9. Hu, et.al., “On a class of pseudorandom sequences from elliptic curves over finite fields,” IEEE Trans-actions on Information Theory, vol. 53, no.7,pp.2598–2605,2007.