Research Journal of Applied Sciences, Engineering and Technology 11(1): 70-78, 2015
DOI: 10.19026/rjaset.11.1677
ISSN: 2040-7459; e-ISSN: 2040-7467
© 2015 Maxwell Scientific Publication Corp.
Submitted: February 27, 2015 Accepted: March 20, 2015 Published: September 05, 2015

Research Article

DYBACON: An Auditor for Secure Kinetic Cloud Storage

G. Soniya Priyatharsini and P. Visu
Department of CSE, Vel Tech University, Avadi, Chennai-62, Tamil Nadu, India

Abstract: Cloud computing is a significant shift of computational paradigm where computing as a utility and storing data remotely have a great potential. Cloud server provides a low cost, flexible, location independent platform for storing client's data. It can provide user along with varieties of service, framework, applications and storage of a huge amount of data; it includes information which is important. Along with the capabilities of the cloud computing, its security is the biggest question mark. It needs associate an independent third party auditing service to see the data integrity within the cloud server. Already past integrity checking methods will solely serve for static archive data and so cannot be applied to the auditing service since the data within the cloud may be dynamically updated. To combine the security drawback, this study proposes a secured protocol. This study initially sketch a frame for an auditing protocol, then extend the protocol to support dynamic auditing and batch auditing for each multiple clouds and multiple owners. With the support of ILEDM, this study is tracking the recent upgrades of the data within the cloud. So the replay attack can be reduced. The analysis and simulation results show that this projected auditing protocols are secure and dynamic, significantly it reduce the value of the computation of the auditor.

Keywords: Cloud security, dynamic cloud data security, third party auditor

INTRODUCTION

Introduction to cloud: The computer world is that the only industry that is more fashion-driven than anything. Cloud computing gets its name as a symbol for the Internet. Commonly, the Internet is represented in network pictures as a cloud.

Cloud computing will mean various things to numerous kinds of folks and after all the protection privacy considerations can take issue between a client adopting a public cloud apps, a traditional sized enterprise employing a made to order group of business applications on a cloud platform. The shift of every class of user to cloud systems brings a dissimilar package of advantages and risks (Naseem and Sasankar, 2014).

Most of us are already familiar with cloud computing and have "data" in the cloud without noticing (Neelu and Laila, 2014). Our e-mail, social media network interactions (FB), online images (Flickr) and videos (YouTube) and even our work documents (GoogleDocs) are in the "cloud". Streaming music services (Pandora, Spotify, etc.) offer a never-ending jukebox where you can build a playlist based on an artist or genre.

The basic cloud architecture is explained Fig. 1. Most of us enjoy reading books via Kindle's cloud, use the iPhone application Siri (an intelligent personal assistant and knowledge navigator) and drive cars equipped with GPS Navigation systems. Online photo and video management (Flickr, Picasa, Snapfish, YouTube, Vimeo) help us manage our media that is scattered across various devices (digital cameras, media cards, flash drives, external drives, tablets and phones). This vast online storage for our stuff is referred to as the cloud. The term Cloud Computing simply means the use of computing resources (hardware, software and/or data in the cloud) delivered over a network. The resources may be owned, administered and operated by some other organization. We can access these resources from anywhere using computers (desktops, laptops), servers and mobile devices (smartphones, tablets and

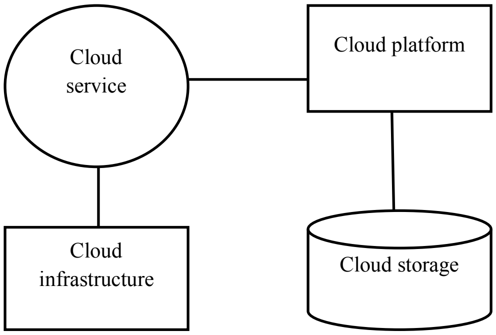

Fig. 1: Basic cloud architecture

Corresponding Author: G. Soniya Priyatharsini, Department of CSE, Vel Tech University, Avadi, Chennai-62, Tamil Nadu, India

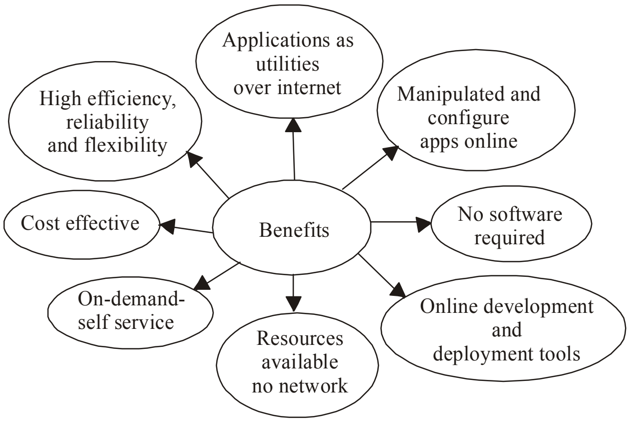
Applications as utilities over internet
High efficiency, reliability and flexibility
Manipulated and configure apps online
Cost effective
Benefits
No software required
On-demand-self service
Online development and deployment tools
Resources available no network

Fig. 2: Benefits of cloud

phablets). These on-line, social and increasingly mobile computing devices enable us to access our stuff in the cloud anywhere, anytime, any device and on anytime.

Benefits of the cloud computing: The benefits of the cloud computing encompass various sectors and following are some of the benefits from an educational perspective.

Backup: All cloud computing service providers offer automatic backup facilities and the user does not have to worry about losing any data stored in the cloud.

Accessibility: Any data stored in the cloud (lesson plans, lecture slides, assignments, laboratory and users manuals, grades, teachers notes, etc.) can easily be uploaded and accessed from any mobile device (smartphone, tablet and phablet).

Cost savings: Cloud computing allows users to store all kinds of data including documents, photos, eBooks, music, video, etc. and users do not need to invest in purchasing data storage devices (USB flash drives, thumb drives, portable external hard drives, or optical drives such as CDs and DVDs, etc.). Also, users do not need to spend money on expensive data backup solutions.

Collaboration: Cloud computing enables multiple users to work on the same data simultaneously making group projects viable and promotes division of responsibilities and sharing of ideas with others.

Reliability: Cloud computing providers are reliable companies with years of research and development such as Amazon, Google, Microsoft, etc.

Green computing: Digital storage in the cloud reduces printing and photocopying. This form of storage also diminishes the need for file cabinets and opens up more classroom and office space.

Scalability: Users does not have to spend in the architecture upfront and only need to pay for the resources they need and use.

Security: Accessing the cloud requires authentication (login id and password etc.) so your data is not accessible to unauthorized users.

Saves time and effort: Cloud computing reduces the amount of time and effort users spend searching for storage solutions and writing/reading data to/from external storage devices.

In short, the Fig. 2 shows the benefits of the cloud. Though outsourcing data to the cloud is economically tempting for long broad-range storage, it doesn't promptly provide any guarantee on data integrity and chance. This drawback, if not properly forward, might impede the success of cloud infrastructure. A third party auditor that has experience and capabilities will do an additional profitable work and satisfy each cloud service providers and owners.

Cloud environment: Sanjay *et al*. (2014) presented different design challenges categorized under security risks, Data risks, Performance risks and other Design risks. Figure 3 explains the cloud computing architectures, which contains the following.

The outstandingness of the place of cloud computing in future gathered networks was undoubted. Table 1 explains the different layers of cloud. That was because the apparent benefits of the cloud as a midway of storage with omnipresence of access platforms and lowest hardware necessity on the user side. Riskless transmission of data from both sides of the cloud is still a serious issue that wants to be considered.

The auditing protocol should have the following properties (Sanjay *et al*., 2014):

- **Confidentiality:** The reviewing protocol should keep owner's data confidential against the auditor.

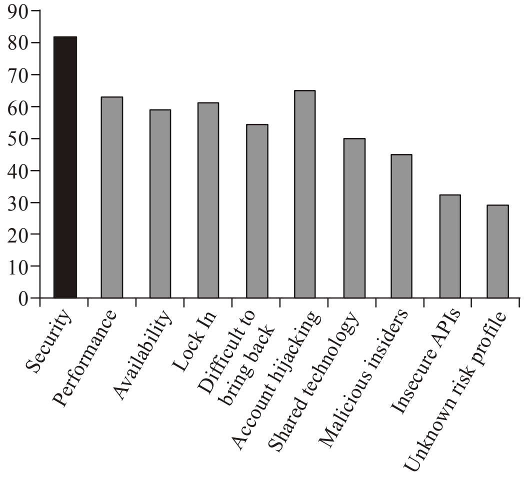

Fig. 3: Threats in cloud computing

Table 1: Components of cloud computing

Layer	Components of cloud computing
5 aspects	• On demand self service
	• Vast network access
	• Resource sharing
	• Brisk flexibility
	• Scope of service
3 commitment layouts	• SaaS
	• PaaS
	• IaaS
4 formation layouts	• Community
	• Hybrid
	• Private
	• Public

- **Dynamic auditing:** The reviewing protocol should support the dynamic updates of the data in the cloud.
- **Batch auditing:** The reviewing protocol should also be support the batch auditing for multiple owners and multiple clouds.

Challenges in shifting to the cloud: Even though there are much more benefits in the cloud some top organizations are still in confusion to shift their data to the cloud. It is because the serious issues met by the data owners previously. Figure 3 explains the threats in cloud computing. It highlights the high level threat in red color.

From the above chart it can be considered that the security is the main problem for the users to move to the cloud. Thus if we reduce the security challenges then many of the data owners can be shifted to cloud computing. We summarize the security issues in all the three service delivery models.

Security in the cloud: If we like to modify cloud-driven growth and innovation through security, we have a transparent framing on what is the meaning of security. Security has been particularly hard to define in the normal case. The recognized goals of information security are Privacy, Availability and Flexibility. Privacy refers to keeping the data personal. Availability means being able to use the system as expected. Integrity is a term determination that the data in the cloud is what is assumed to be there (Visu *et al*., 2012a).

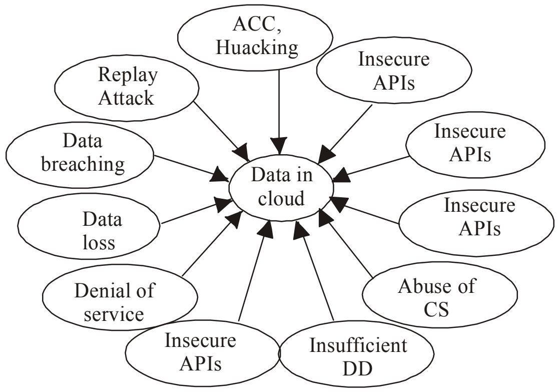

Fig. 4: Security threats in cloud

Previously, organizations would buy computer equipment. It may be hardware or software and manage it themselves. Nowadays huge number of organizations prefers to use cloud computing and expanded IT services. The work of associate degree of an organization's IT officer has modified as a consequence: Rather than fixing the hardware or installing software, IT persons currently got to tackle IT service contracts with dealers (Infrastructure, datacenter, cloud, etc.). The consumer ought to explain security necessities to the cloud supplier via parameters within the Service Level Agreement (SLA) which may be unceasingly monitored (the maximal time to patch e.g.,) and admit with the service provider to receive enough observing data such as results from vulnerability scans or incident reports once ineffective in patching. Without supplies and explanations about security framework and privacy surveying, it is hard for the customer to uphold security and to grasp if the service provider distribute correspondingly to the security necessities.

Providing security to the computer systems have not been a simple task. Cloud computing and cloud service suppliers ought to address variety of challenges that affects security within the cloud. They are Replay attack, Data Breaches, Data Loss, Account Hijacking, Insecure APIs.

Thus from the Fig. 4, it is explained in short about the security threats. From the above details it is stated that the main security problem in cloud computing is the replay attack. This leads to the lack of data updating in the server side. Thus by reducing the replay attack the owner's data can be secured efficiently.

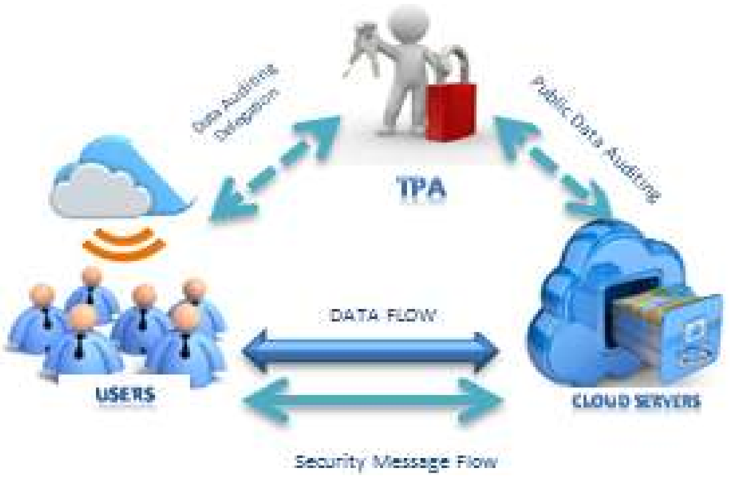

Fig. 5: Third party auditor

LITERATURE REVIEW

Auditing: The Service level agreement is not transparent to the users (ENISA, 2011). There comes the need to have auditing to check for SLA breach. There are two types of auditing rely upon which is being audited: External Audit and Internal Audit. Internal Audit audits the process that takes place in supplying the service. External Audit audits the QOS such as CPU availability, SLA parameters and performance. Audit can be both dynamic and static. In static auditing, auditing is done periodically to verify the integrity of data. Examples are taken from the data and it is verified for integrity of data. In dynamic auditing, auditing is done on dynamic data. The dynamic data operations are insertion, modification and deletion. Batch auditing is required when there are multiple cloud servers and multiple owners. The issues arise in which entity can carry out auditing. If auditing is done by Cloud providers they may hide their faults and disruptions. On the other hand if the user does the auditing, it adds the overhanging to them. The solution is to have a third party entity to do the auditing. The third party should be impartial to both the Cloud provider and Cloud User.

Third Party Auditor (TPA): The Cloud user transfers the data to Cloud server using the network. The client data may contains very sensitive data like Password, user personal information, Bank details, Business client details, important key Word, etc. Cloud service providers normally use Secure Socket Layer, Point to Point Tunneling protocol, VPN for secure transaction. This study explains the history that attackers and intruders have win over this type of security services. When sending the data between cloud service providers and the user. It is very tough to prevent malicious attack. But users need legally assurance about the security over their data. For this we need an authentication process which is based on the third party. Figure 5 shows the third party intrusion between the users and the cloud servers.

This third party should common for both the Cloud Providers and cloud user. The third party monitors the activities of user and the cloud provider. Normally client and service providers will have an agreement (Service level Agreement). This is an agreement which is legal between cloud provider and also the client. Both have to take place of the rules and regulations indicated in the SLA. This agreement includes the Cloud service provider's QOS, Standard of the service, service overseeing and controlling. The Cloud service may give lot of execution and service offers to the cloud user due to market contest. But any point of time he has to go through it. The cloud service providers for their own benefits they will hide the data errors from the cloud user. To prevent this problem and to control the security standard we need a (TPA) Third Party Auditor (Koteeswaran *et al*., 2012). The Auditor will monitor both the Service Provider and client side activities. TPA will follow the auditing rules and techniques, also they will have list of auditing plan of action. The TPA should know with the SLA between cloud user and cloud service provider. TPA will play trustable role between this two parties. TPA can have the ability to validate the completeness of the data which saved in the cloud. Auditing should not influence the privacy of the cloud users.

Here the cloud user mainly concern about their security of data. As the data is stored In order to check the data integrity at un-trusted servers becomes a big concern with cloud environment. Data Security comprises of Data Confidentiality, Data Availability and Data integrity.

The auditing process contains of three different types of phases such as planning, execution and reporting:

Table 2: Comparisons of remote integrity methods

Techniques used	Advantages	Restrictions
Provable data possession	PDP assures the cloud data integrity into the multi cloud. Beyond using PDP it can improve the scalability of service and data migration.	To achieve the support of dynamic data, the current proofread of PoR or PDP scheme is developed by fooling the basic Markle Hash Tree (MHT)
Cooperative provable data possession	(CPDP) proves the safety of the design is based on the zero knowledge prove system, zero-knowledge properties completeness and multi-prover.	It has a disputing problem for the formation of tags with the lengthiness irrelevant to the amount of data blocks
Dynamic provable data possession	Dynamic operations like insert, update, modify, delete are supported by the dynamic PDP.	The authenticated insert and deletes functions are permitted by the dynamic operations with rank based authenticated directories and also with a skip list. Though it is economical
Basic life support algorithm use for security	At the same time the auditor performs auditing jobs for different users.	Not able to hold up both the dynamic data correctness and also the public verification
Interactive provable data possession	These techniques apply the data portioning/ fragment techniques to additional split each data block into simpler subdivisions.	Communication costs are high compare to other techniques
Discretionary access control	Useful for small user populations where permissions are managed easily and also the user set remaining part comparatively stable.	Does not scale well, It is difficult to maintain
Role based access control	Very efficient to enforce access controls when the organization has set of roles for users based on required privileges to perform their function with the appropriate set of privileges. Roles can also be combined in a hierarchical scheme.	Can be combined with other schemes to manage pools of users in the same roles
Mandatory access control	Excellent to enforce access controls when the organization has an information along with process in place that vet users before granting clearances to individuals that are used to gain access to resources.	Measures to extremely large user populations

- Planning
- Execution
- Reporting

Currently, many remote verifying protocols were suggested to grant the auditor to verify the data completeness on the remote server (Al-Attab and Fadewar, 2014; Juels and Jr., 2007). Table 2 describes the comparisons among some already existing remote integrity checking.

In Shah *et al*. (2007), Yamamoto *et al*. (2007) and Sebe *et al*. (2008) proposed a dynamic auditing protocol, but this method may reveal the contents of the data towards the auditor due to it needs the server to transmit the linear combinations of data blocks to the auditor. The authors from the studies (Filho and Barreto, 2006; Rajathi and Saravanan, 2013) support the batch auditing for variety of owners. They enhanced their dynamic auditing design to be privacy-preserving. Moreover, due to the very huge number of the data tags, their checking protocols may obtain a heavy storage overhead on the server. A cooperative provable data possession scheme can support the batch auditing for multiple clouds (Schwarz and Miller, 2006; Wang *et al*., 2011). It also extends to support the dynamic auditing (Juels and Jr., 2007; Wang *et al*., 2010). Many of the authors used index scheme in dynamic auditing (Zhu *et al*., 2011a). But the error correction is not guaranteed to support dynamic data operations. Authenticating ranked search (Zhu *et al*., 2011b) is used in this study. But it is only used for the single keyword search and not for multi keyword search.

The authors used the search algorithm based on tree structure (Monalisa Devi and Sounder Rajan, 2014) to generate a fixed size tag by aggregating all of the tags to minimize the network computation cost and used the Reed Solomon code to recover the perverted blocks. The main drawback of this method is the responsiveness from the server side is slow due to the fastest query retrieval. Mehdi *et al*. (2014) marked that this issue and designed a first dynamic RDA scheme based on using the algebraic signature properties. Auditing protocol and monitoring tool to track link analysis algorithm in Ning (2012) and Visu *et al*. (2012b) mentioned by Kalaiarasi *et al*. (2014) has the problem with the performance. It will be slow. This is because due to many processes and many dbs.

The work by Ateniese *et al*. (2008) is marked that the dynamicity issue in the dynamic possession protocol schemes by combining the skip list, rank-based information and verification dictionary. This method limits the number of updates in server. Each node in this data structure wants to store the number of reachable nodes from this node as a rank. Even though the dynamic PDP method (Ning, 2012) assures the integrity of variety-sized data blocks, it is unable to check the integrity of individual block. Also it cost the heavy computation cost.

Wang *et al*. (2011) employed a combination of the Merkle hash tree (Erway *et al*., 2009) and bilinear aggregate signature (Sathyendrasingh and Niresh, 2012) to propose a dynamic remote data auditing in cloud computing. The main assignment of this method is in manipulating the classic MHT construction by sorting the leaf nodes from left to right in order to support dynamic update and conclude the insert, delete, or modify positions by go after this sequence and computing the root in MHT. Moreover, the method opens the cloud data to the third party auditor and cost heavy computation.

This study proposes a secure dynamic auditing and an efficient protocol. It can fulfill the below indexed basics.

The authentic augmentation can also be abstract as below:

- First of all, propose a privacy preserving and efficient storage auditing protocol. Then design an auditing framework for cloud storage systems for less communication cost between the auditor and the server.
- Next expand the auditing protocol to hold by the data dynamic operations, which is effectual secure. Here ILEDM is used to maintain the updated recent data of the owner's data. This cut down the replay attack from the server side.
- Finally the auditing protocol is extended to support batch auditing for not only various clouds but also various owners.

PROBLEM STATEMENT

In Cloud computing security, the notable security challenges are (Kan and Xiaohua, 2012; Cong *et al*., 2013; Harfoushi *et al*., 2014; Madhuri and Natikar, 2014; Hemalatha and Manickachezian, 2014) loss of control, lack of trust and multi tenancy. In particular, the main challenge due to lack of trust is the replay attack from server side. Replay attack is defined as the Server use previous data version to pass auditing. It may use update to data owner's current version. From the literature survey, the problem found is, Index table is used to reduce replay attack. It is used to record abstract information of data. But the problem here is the delay of data retrieval from the index table.

Privacy preserving protocol: Cloud outsource data storage service involves large amount of data and four entities Data Owner to be stored in the cloud. CSP provides enough storage space, computation resources and has enough data storage service. Third Party Auditor manage the outsourced data under the responsiveness of DO Authorized Applications right to access and manipulate the stored data. TPA is reliable and independent throughout the audit functions. TPA able to maintains, manages and organizes outsourced data support dynamic data operations for Authorized Applications. The commonly used techniques are Bilinearity property of the bilinear pairing and multi owners for multi clouds, indexing techniques for efficient dynamic auditing. Most of the papers used a frame work for the privacy preserving technique which is shown below.

The above architecture explains the details working technique.

Tranche 1: Owner initialization: The owner runs the key generation algorithm KeyGento generate the secret hash key, the public tag key. After forming the data tags, the owner sends each data component and its corresponding data tags to the server.

Tranche 2: Confirmation auditing: Here, the protocol only involves two-way communication: Proof and Challenge. Meanwhile the confirmation auditing phase, the owner needs the auditor to check whether the owner's data is correctly stored on the server.

The auditor then sends the auditing result to the owner. If the result is true, the owner is converted that its data is correctly stored on the server and it may choose to delete the local version of the data.

Tranche 3: Sampling auditing: The sampling auditing is carried out by the auditor periodically by a sample set of data blocks (Fig. 6).

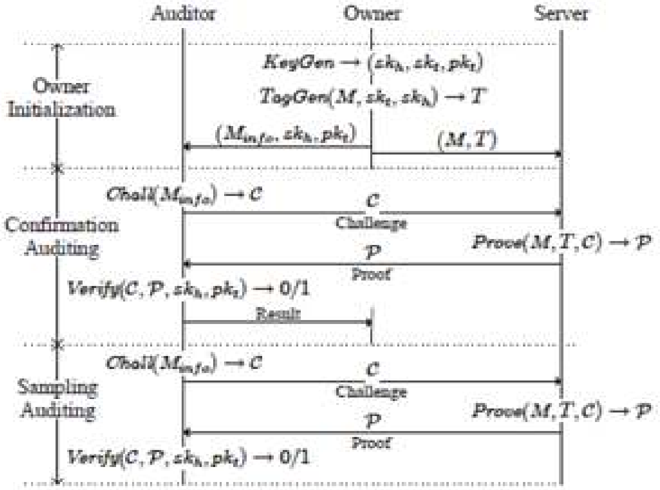
Auditor
Owner
Server
Owner Initialization
$KeyGen \rightarrow (sk_h, sk_t, pk_t)$
$TagGen(M, sk_t, sk_h) \rightarrow T$
(M_{info}, sk_h, pk_t)
(M, T)
Confirmation Auditing
$Chall(M_{info}) \rightarrow C$
C
Challenge
$Prove(M, T, C) \rightarrow \mathcal{P}$
$\mathcal{P}$
Proof
$Verify(C, \mathcal{P}, sk_h, pk_t) \rightarrow 0/1$
Result
Sampling Auditing
$Chall(M_{info}) \rightarrow C$
C
Challenge
$Prove(M, T, C) \rightarrow \mathcal{P}$
$\mathcal{P}$
Proof
$Verify(C, \mathcal{P}, sk_h, pk_t) \rightarrow 0/1$

Fig. 6: Architecture for privacy preserving protocol

Table 3: IHT with random values

No.	Bi	Vi	Ri		
0	0	0	0	←	Used to head
1	1	2	r1	←	Update
2	2	1	r2	←	
3	4	1	r3		Delete
4	5	1	r5	←	
5	5	2	r5		Insert
.	.	.			
.	.	.			
.	.	.			
n	n	1	r n	←	Append
n+1	n+1	1	r n+1		

Table 4: Indexing table

No.	Bi	Vi	Ri	
0	0	0	0	⇐ Used to head
1	1	2	r1	⇐ Update
2	2	1	r2	
3	4	1	r3	⇐ Delete
4	5	1	r5	
5	5	2	r5	⇐ Insert
	.	.	.	
	.	.	.	
	.	.	.	
n	n	1	r n	
n+1	n+1	1	r n+1	⇐ Append

Dynamic auditing protocol: Application users utilize various cloud application services via AAs (Preeti and Vineet, 2014). TPA able to manages, organizes and maintains outsourced data support dynamic data operations for AAs (Ugale Santosh, 2014; Ohmin *et al*., 2014; XiaoChun *et al*., 2014; Mehdi *et al*., 2014). The techniques used are (Table 3):

- Secure Tags and Fragment Structure
- Sampling Periodic Audit
- Index Hash Table

Secure tags and fragment structure: Files are combined with tags to improve the performance.

Sampling periodic audit: Checking of the data is done periodically. Periodic sampling greatly decreases the work of audit services.

Index hash table: File changes are recorded and generate hash value for each block. IHT contains of version number, serial number, random integer and block number. All the record in IHT differs from one another to prevent the forgery of data blocks and tags.

So a technique should be found to reduce the search time and reduce the time spend for the computation. That technique should also be easy to access any particular data. It has to full fill the 3 qualities of the perfect auditing such as Confidentiality, dynamic auditing and batch auditing. It should also keep track with the information of data transactions.

METHODOLOGY

This study proposed a highly secured privacy preserving protocol along with the dynamic auditing and batch auditing (Table 4).

In privacy preserving protocol, data privacy problem is the main challenge. The main reason behind this is explained here:

- Public data
- Secured data

In addition to this, Data fragment technique and Homomorphic tag verifiers are added to increase the

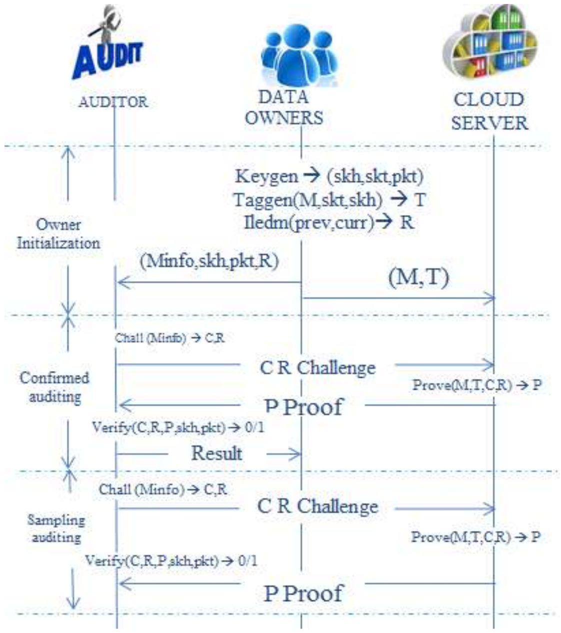

Fig. 7: Architecture for privacy preserving operations

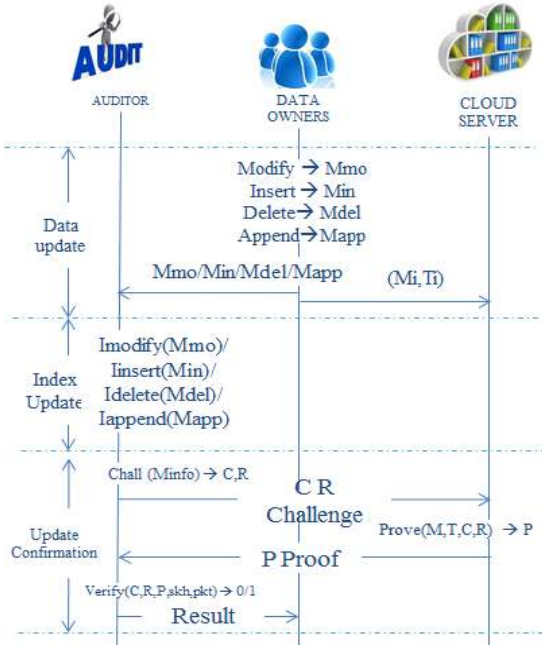

Fig. 8: Dynamic auditing framework

performance of our auditing system. They reduce the number of tags. It reduces the communication cost (Fig. 7).

Currently, Cloud servers in cloud computing audit the owner's data to check the integrity (Ramkumar and Ashwin, 2014).

In dynamic auditing (Fig. 8), to avoid the replay attack from the server side indexing techniques are used here. With the help of the I Table, the abstract information of the transaction of data has recorded. This will be created by the owner and maintained by the third party auditor. With addition to the indexing, one more separate Inclusion Logic of Eaves Dropping Mitigater (ILEDM) is added. This ILEDM keeps the recent update of the owner's data. Using this content of ILEDM an auditor can check whether the data from the server side is update or not. This will be very challengeable process to the auditor and have to spend a lot. So, it is needful to join and check all the data together (Vijay and Mohan Reddy, 2014; Khalil *et al*., 2014; Pasupathi and Ganesh Kumar, 2013; Shikha, 2014).

RESULTS

The study presents a construction of dynamic auditing services for outsourced and un-trusted storage. This also presents an efficient ILEDM method to minimize the computation costs. The experiments showed that the solution has a constant amount of small overhead. It also minimizes the communication costs.

CONCLUSION

This study presents an efficient remote data auditing technique to confirm the data security storage in cloud computing. For the purpose of achieving the above goal, bi-linearity pairing is used here. This study also design a new data structure, namely, indexing i.e., I Table with ILEDM technique, to support kinetic data update, which includes insert, delete, append and modify operations. This ILEDM technique allows us to keeps track on the recent update of the owner's data in the server with the help of the I Table. It also allows the checker to audit the large scale data and perform a large number of insert, update and delete operations with minimum computation overhead on the verifier and server. The security and achievement analysis shows the efficiency and provability of our scheme.

RECOMMENDATIONS

As a part of future work, this study can extend the scheme to perform faster with some new techniques. This study can also advance the new scheme to reduce the computation cost.

REFERENCES

Al-Attab, B.S. and H.S. Fadewar, 2014. Security issues and challenges in cloud computing. Int. J. Emerg. Sci. Eng., 2(7), ISSN: 2319-6378.

Ateniese, G., R.D. Pietro, L.V. Mancini and G. Tsudik, 2008. Scalable and efficient provable data possession. Cryptology ePrint Archive, Report 2008/114 (2008).

Cong, W., S.S.M. Chow, W. Qian, R. Kui and L. Wenjing, 2013. Privacy-preserving public auditing for secure cloud storage. IEEE T. Comput., 62(2).

ENISA, 2011. Survey and analysis of security parameters in cloud SLAs across the European public sector. Survey and analysis. SLAs Survey Report, European Network and Information Security Agency.

Erway, C.C., A. Ku pc¸u , C. Papamanthou and R. Tamassia, 2009. Dynamic provable data possession. Proceeding of the 16th ACM Conference on Computer and Communication Security, pp: 213-222.

Filho, D.L.G. and P.S.L.M. Barreto, 2006. Demonstrating data possession and uncheatable data transfer. IACR Cryptology ePrint Archive, Report2006/150, 2006, Retrieved from: http://eprint.iacr.org/.

Harfoushi, O., B. Alfawwaz, N.A. Ghatasheh, R. Obiedat, M. Mua'ad and H. Faris, 2014. Data security issues and challenges in cloud computing: A conceptual analysis and review. Commun. Network, 6: 15-21.

Hemalatha, S. and R. Manickachezian, 2014. Dynamic auditing protocol using improved RSA and CBDH for cloud data storage. Int. J. Adv. Res. Comput. Sci. Softw. Eng., 4(1).

Juels, A. and B.S.K. Jr., 2007. PORs: Proofs of retrievability for large files. In: Ning, P., S.D.C. di Vimercati and P.F. Syverson (Eds.), proceeding of the ACM Conference on Computer and Communications Security, ACM, pp: 584-597.

Kalaiarasi, V., R. Gugapriya, K. Nirmaladevi and Mr. P. Anandhajayam, 2014. Detecting and eliminating fraudulence using cloud storage. Proceeding of the International Conference on Engineering Technology and Science (ICETS'14).

Kan, Y. and J. Xiaohua, 2012. An efficient and secure dynamic auditing protocol for data storage in cloud computing. IEEE T. Parall. Distrib., 24(9): 1717-1726.

Khalil, I.M., A. Khreishah and M. Azeem, 2014. Cloud computing security: A survey. Computers, 3: 1-35.

Koteeswaran, S., J. Janet, E. Kannan and P. Visu, 2012. Terrorist intrusion monitoring system using outlier analysis based search knight algorithm. Eur. J. Sci. Res., 74(3): 440-449.

Madhuri, R.R. and S.B. Natikar, 2014. Providing data utility on cloud using slicing approach and dynamic auditing protocol using third party auditor to maintain integrity of data. Int. J. Comput. Sci. Inf. Technol., 5(1).

Mehdi, S., A. Adnan, G. Abdullah, K.K. Muhammad and B.A. Nor, 2014. Towards dynamic remote data auditing in computational clouds. Sci. World J., 2014: 12.

Monalisa Devi, N.S. and T. Sounder Rajan, 2014. Secure Auditing for outsourced data in cloud using homomorphic token and erasure code. Int. J. Innov. Res. Comput. Commun. Eng., 2(1): 2086-2091.

Naseem, S. and A.B. Sasankar, 2014. Cloud computing challenges and related security issues. Proceeding of the International Conference on Advances in Engineering and Technology (ICAET-2014), pp: 19-23.

Ning, C., 2012. Secure and reliable data outsourcing in cloud computing. Ph.D. Thesis, Faculty of the Worcester Polytechnic Institute.

Ohmin, K., K. Dongyoung, S. Yongjoo and Y. Hyunsoo, 2014. A secure and efficient audit mechanism for dynamic shared data in cloud storage. Sci. World J., 2014: 10.

Pasupathi, K. and D. Ganesh Kumar, 2013. Security in cloud for multi-owner using anonymous ID. Int. J. Emerg. Technol. Res., 1(1).

Preeti, G. and S. Vineet, 2014. An efficient and secure data storage in mobile cloud computing through RSA and hash function. Proceeding of the International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT). Ghaziabad, pp: 334-339.

Rajathi, A. and N. Saravanan, 2013. A survey on secure storage in cloud computing. Indian J. Sci. Technol., 6(4): 4396-4401.

Ramkumar, A. and R. Ashwin, 2014. Inter cloud data transfer security. Proceeding of the 4th International Conference on Communication Systems and Network Technologies.

Sanjay, P., S. Rajeev and T. Udai-Bhan, 2014. Cloud-computing challenges, security and solutions: Using SaaS. Int. J. Innov. Adv. Comput. Sci., 3(5): 1-10.

Sathyendrasingh, S.R. and S. Niresh, 2012. A survey of various techniques to secure cloud storage. Int. J. Comput. Sci. Netw. Secur., 12(3).

Schwarz, T.J.E. and E.L. Miller, 2006. Store, forget, and check: Using algebraic signatures to check remotely administered storage. Proceeding of the 26th IEEE International Conference on Distributed Computing Systems (ICDCS, 2006), pp: 12.

Sebe, F., J. Domingo-Ferrer, A. Martinez-Balleste, Y. Deswarte and J.J. Quisquater, 2008. Efficient remote data possession checking in critical information infrastructures. IEEE T. Knowl. Data En., 20(8): 1034-1038.

Shah, M.A., M. Baker, J.C. Mogul and R. Swaminathan, 2007. Auditing to keep online storage services honest. In: Hunt, G.C. (Ed.), Proceeding of the 11th USENIX Workshop Hot Topics in Operating Systems (HOTOS).

Shikha, C., 2014. Comparative study on authentication schemes for cloud computing. Int. J. Eng. Dev. Res., 2(2).

Ugale Santosh, A., 2014. Survey paper on integrity auditing of storage. Int. J. Comput. Eng. Res., 4(3).

Vijay, G.R. and A.R. Mohan Reddy, 2014. Investigational analysis of security measures effectiveness in cloud computing: A study. Comput. Eng. Intell. Syst., 5(7).

Visu, P., J. Janet, E. Kannan and S. Koteeswaran, 2012b. Optimal energy management in wireless adhoc network using Artificial Bee Colony based routing protocol. Eur. J. Sci. Res., 74(2): 301-307.

Visu, P., S. Koteeswaran and J. Janet, 2012a. Artificial bee colony based energy aware and energy efficient routing protocol. J. Comput. Sci., 8(2): 227-231.

Wang, C., Q. Wang, K. Ren and W. Lou, 2010. Privacy-preserving public auditing for data storage security in cloud computing. Proceeding of the IEEE INFOCOM, 2010. San Diego, CA, pp: 1-9.

Wang, Q., C. Wang, K. Ren, W. Lou and J. Li, 2011. Enabling public auditability and data dynamics for storage security in cloud computing. IEEE T. Parall. Distr., 22(5): 847-859.

XiaoChun, Y., L. ZengGuang and L. Hoon Jae, 2014. An efficient and secured data storage scheme in cloud computing using ECC-based PKI. Proceeding of the 16th International Conference on Advanced Communication Technology (ICACT, 2014). Pyeongchang, pp: 523-527.

Yamamoto, G., S. Oda and K. Aoki, 2007. Fast integrity for large data. Proceeding of the ECRYPT Workshop on Software Performance Enhancement for Encryption and Decryption. Amsterdam, The Netherlands, pp: 21-32.

Zhu, Y., H. Hu, G. Ahn and M. Yu, 2011b. Cooperative provable data possession for integrity verification in multicloud storage. IEEE T. Parall. Distr., 23(12): 2231-2244.

Zhu, Y., H. Wang, Z. Hu, G.J. Ahn, H. Hu and S.S. Yau, 2011a. Dynamic audit services for integrity verification of outsourced storages in clouds. Proceeding of the ACM Symposium on Applied Computing (SAC'11), pp: 1550-1557.