ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

Augmented Security by TPA in Cloud Computing

Sashibala, Deepika Goyal

M-Tech(pursuing), Dept. of CSE, Advanced Institute of Technology and Management, Palwal, Haryana under the Affiliation of Maharshi Dayanand University at Rohtak, Haryana, India

Assistant Professor, Dept. of CSE, Advanced Institute of Technology and Management, Haryana under the Affiliation of Maharshi Dayanand University at Rohtak, Haryana, India

ABSTRACT: Cloud computing is the lengthy dreamed vision of computing as a utility, in which users can remotely access their information into the cloud with a purpose to experience the on-call for excessive quality programs and services from a shared pool of configurable computing resources, by way of facts outsourcing, users can be relieved from the weight of neighborhood records storage and maintenance, as a result, allowing public audit-ability for cloud records storage safety is of vital importance in order that customers transactions can audited to test the integrity of outsourced facts whilst wanted. To soundly introduce a powerful augmented security vide auditor (TPA), the subsequent essential necessities need to be met with the certain criteria i.e. TPA has to be capable of successfully audit the cloud records transactions without annoying the nearby reproduction of records, and introduce no extra online burden to the cloud sourcing, especially to data repositories and archives. However, under this scheme, motivation is to provide the augmented security technique using hashing algorithm for public auditing of information and cloud security in cloud computing and offer a privateers retaining auditing protocol, i.e., our scheme helps an external auditor to audit person's outsourced information in the cloud without studying know-how at the statistics content material. Consequently, this scheme ensures that in the intra cloud if two parties or resources communicate or perform any transactions the TPA is responsible to provide the digital signature copy to be associated for auditing purpose and to ensure no as such (mala-fide) mal-communication or mal-transactions is occurring.

KEYWORDS: Cloud computing; Hash service; encryption and decryption service; data protection and integrity, third part auditor (TPA).

I. INTRODUCTION

Cloud computing is reworking the character of however business and resources uses data technology these days. This computing paradigm shift provides a climbable atmosphere for growing amounts of knowledge and processes that employment on numerous applications and services by means of on demand self services. Notably, the outsourced storage in clouds could be a new profit generating space by providing a uniformly low value, scalable, geographically location-independent platform for managing users' knowledge, information, and data. The cloud storage services lighten the burden for storage management and maintenance. Nowadays it's a routine for many users to leverage cloud storage services to share knowledge with others in an exceedingly cluster, as knowledge sharing becomes a regular options in most cloud storage offerings as well as Google Drives, iClouds and Dropbox. However, the exciting benefits that ar provided by cloud storage services, storing knowledge in an exceedingly cloud doesn't provide any guarantee on knowledge integrity and accessibility. Users' knowledge is place in danger of losses or being incorrect throughout sharing because the cloud service suppliers ar separate body distance, out of the management of users. These security risks are often caused by: the interior and external threats in clouds infrastructures, for instance there are numerous motivations for cloud service suppliers to behave unreliably towards the clouds users yet because the dispute owing to lack of trust on Cloud storage service. Cloud users might not remember of this behaviour even though these disputes could results into users owns improper operation [4]. Following these and connected challenges, public auditing, especially privacy conserving one is usually recommended by researchers as trust worthy resolution to be increased in cloud storage service thus on check for correctness of users knowledge. In privacy conserving public auditing, the third

DOI: 10.15680/IJIRCCE.2017. 0505135

party auditor is resorted to in public verify the integrity of users' knowledge keep in clouds before being shared among multiple users while not knowing the info and users' identities privacy. A traditional approach provides only public auditing while preserving data privacy. This conventional approach will provide public auditing while keeping private users identities from third party auditor in a dynamic group data sharing environment using below mentioned techniques under the scheme.

Privacy-Preserving Public: Homomorphic authenticators are unforgeable verification metadata generated from individual data blocks, which can be securely aggregated in such a way to assure an auditor that a linear combination of data blocks is correctly computed by verifying only the aggregated authenticator. Overview to achieve privacy-preserving public auditing, we propose to uniquely integrate the homomorphic authenticator with random mask technique. In our protocol, the linear combination of sampled blocks in the server's response is masked with randomness generated by a pseudo random function (PRF).

Data Dynamics: Hence, supporting data dynamics for privacy-preserving public risk auditing is also of paramount importance. Now we show how our main scheme can be adapted to build upon the existing work to support data dynamics, including block level operations of modification, deletion and insertion. We can adopt this technique in our design to achieve privacy-preserving public risk auditing with support of data dynamics under the scheme.

Batch Auditing: With the establishment of privacy-preserving public auditing in Cloud Computing, TPA may concurrently handle multiple auditing delegations upon different users' requests. The individual auditing of these tasks for TPA can be tedious and very inefficient. Batch auditing not only allows TPA to perform the multiple auditing tasks simultaneously, but also greatly reduces the computation cost on the TPA side.

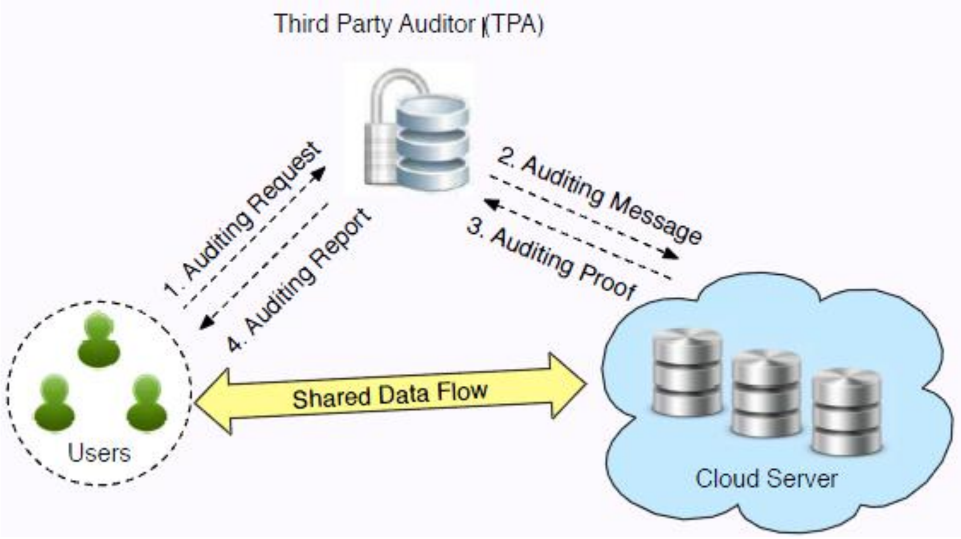

Figure 1: Depicting the Cloud Security and Auditing using Third Party Auditor

II. LITERATURE REVIEW

These days the use of cloud computing has become an attractive trend for organizations. Many organizations at the present use clouds to manage their business operations. However, there are several security issues attached with cloud computing. The purpose of this literature review is to outline some of the important security aspects which are discussed in other researches.

According to (Babar & Chauhan, 2011; Meng, Wang, Hu, & Li, 2011) [1], cloud computing is an up-and-coming paradigm, which guarantees to make the utility computing model broadly implemented by using Virtualization technologies. Additionally, an increasing number of business organizations have begun offering and utilizing cloud-enabled architectures and services. On the other hand, the progression of cloud computing creates a number of new challenges to existing techniques and approaches to build up and change software intensive systems (Babar & Chauhan, 2011; Meng, Wang, Hu, & Li, 2011).

In this regard, (Hamlen, Kantarcioglu, Khan, & Thuraisingham, 2010) [2] outline a number of security issues in a cloud computing environment. These problems and issues comprise physical security, data security, middleware safety, application security and network security. However, the key goal is to effectively store and administer data that is not managed by the owner of the data. In addition, the previous researches have focused on specific areas and aspects of cloud computing.

Especially, those researches have assessed such issues in a bottom-up approach to security where we are operating on little issues in the cloud computing arrangement that we hope will resolve the bigger issues and complexities of cloud security (Hamlen, Kantarcioglu, Khan, & Thuraisingham, 2010). Initially, they have shown that “how can we protect data, information and documents that can be published by a third party organization. After that, they have shown that how to protect co-processors and how they can be utilized to improve security. This research lastly discussed how XACML could be established in the Hadoop atmosphere and in protected federated query processing through SPARQL, Hadoop and MapReduce. Furthermore, there are many other security issues comprising security areas and features of Virtualization. Additionally, it is assumed that because of the issues and complexity of the cloud, it will be hard to attain an end-to-end security. [3]

Though, the problems this research outlined and solution proposed are able to make sure additional protected operations yet a number of parts of the cloud fail. For a lot of systems and applications, we don't simply require data and information assurance however as well attainment of objectives. Thus, even if a rival has come into the system, the intention is to prevent the challenger so that the corporation has time to perform the desired tasks (Hamlen, Kantarcioglu, Khan, & Thuraisingham, 2010)[3].

Moreover, (Chandran S. and Angepat M)[7] state that cloud computing is probable to have the similar impact on software that founders have had on the hardware manufacturing. They move on to advocate that technology developers would be intelligent to plan and develop their next and advanced generation of systems to be established into cloud computing. Seeing that many of the forecasts can be clouded advertise, it is assessed that the recent IT procurement model presented by cloud computing is here to stay. In addition, the acceptance of cloud computing has turned out to be common and deep thus a number of forecasts will rely mainly on overcoming doubts of the cloud (Chandran S. and Angepat M).

III. PROPOSED WORK & PSEUDO CODE

It is very common for users’ data in the cloud to be shared across multiple users in the group whereby a user digitally signs documents when making changes to data before resource can share again with other users in the same group. The unseen signatures tagged in data can possibly be learnt by auditor or cloud service provider during audit process. If that information gets to the knowledge of an authorized outsider, it is easy for kind of relationship and the roles placed by each user to be understood, which in turn can lead for an interested attacker to know which target to attack (keep in mind semi-trusted auditor can be easily manipulated for the sake of money or any other reason that can make him/her being interested). Think of market plan information for xyz company for instance, if competitors know exactly the major player by deducing his/her identities from that piece of shared information, the focused business will easily face stiff competition from their rivalry. Enforcing data privacy against publicly auditor does not keep him from learning users identities. This fact grabbed researchers’ attention to come up with some auditing scheme that addresses identity privacy. Identity privacy preserving auditing shared data in a cloud on dynamic groups’ environment where a new user is added into a group and an existing group member can be revoked has never been fully addressed. How to achieve an efficient and secure audit scheme that supports both public audit and data dynamics to the clouds is still an open challenging tasks in cloud computing. The proposed algorithm comprising of shift substitution along with XOR based crypt stem:

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

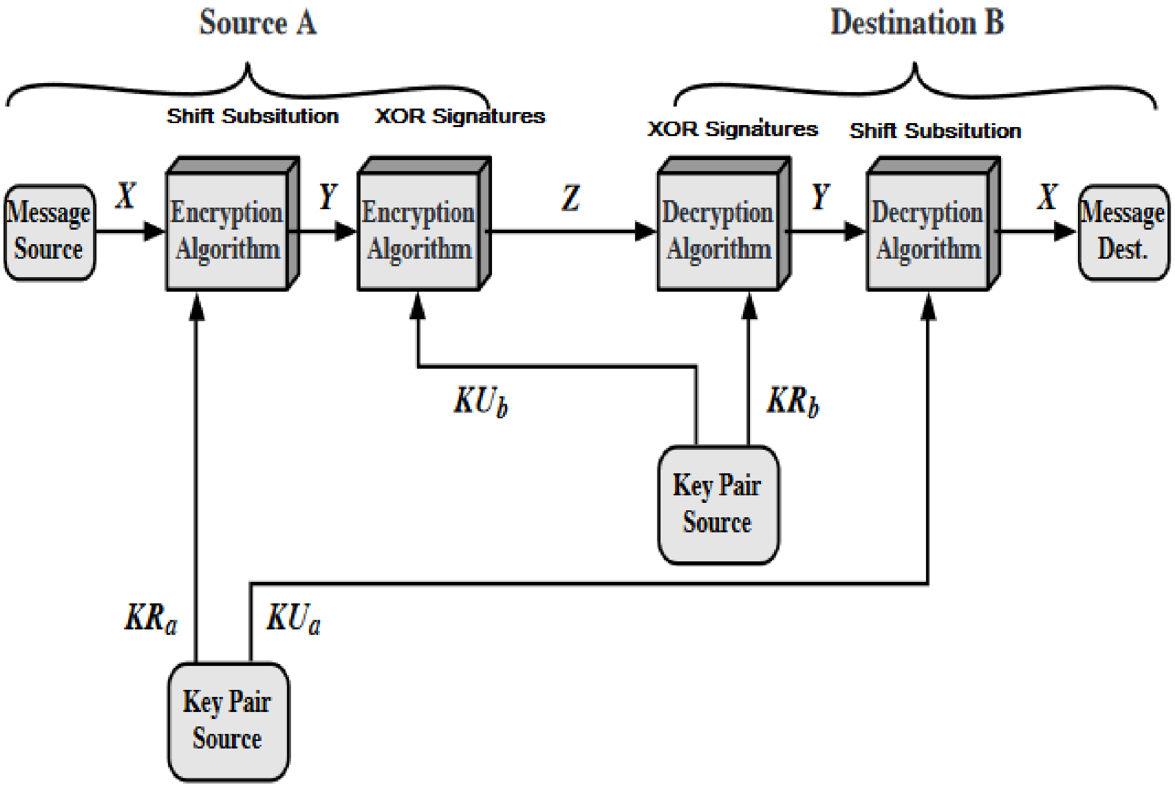

Figure 2: Proposed Architecture Security with Shift Substitution and XOR Crypt Stem

Pseudo Code:

```
Step 1 : [Forming Shift Substitution Structure]
1.  Accept Senders Signature
2.  Convert into ASCII value
3.  Add any Random Number
4.  Check Either the value is Less than 10 if Yes add two Zeros as Prefix
5.  Otherwise Check If Value is Less than 100 if Yes add one Zero as Prefix
6.  If the number is greater than 100 let it remain same
7.  Reverse The number
8.  Form one 10 bit sandbox with unique values
9.  Replace or substitute the numbers with the indices of the 10 bit sandbox
10. Shift the values as under
```

In this scheme, the key is first subjected to a permutation. Then a shift operation is performed. The output of the shift operation (left shift by 1 bit on the two halves of the input) then passes through a permutation function that produces an 10-bit out-put for the first subkey. The output of the shift operation also feeds into another shift left shift by 2 bits on the two halves of the data and another instance will produce the second subkey.

Step 2:

1. The input string is viewed as a sequence of n-byte blocks generated by shift and substitution.
2. The input is processed one block at a time in an iterative fashion to produce an n-bit hash function.

DOI: 10.15680/IJIRCCE.2017. 0505135

3. The hash function is the list-by-list XOR of every block, expressed as following:
   $C_i=b_{i1} \oplus b_{i2} \oplus \cdot \cdot \cdot \oplus b_{im}$
   Where
   C_i=i^{th} list of the hash code, 1≤i≤n
   M=number of n-bit blocks in the input
   B_{ij}=i^{th} list in j^{th} block
   ⊕=XOR operation.

160-bit buffer is used to hold intermediate and final results of the hash function. The buffer can be represented as five 32-bit registers (A,B,C,D,E). These registers are initialized to the following 32-bit integers (hexadecimal values):
A = 67452301
B = EFCDAB89
C = 98BADCFF
D = 10325476
E = C3D2E1F0

Below table depicts the scenario to transforming the substituted and shit number to hex numbers

Substituted numbers	Hexadecimal	Take integer part
0<= t <= 19	K_t = 5A827999	[2^{30} x 2 ^{½}]
20<= t <= 39	K_t = 6ED9EBA1	[2^{30} x 3 ^{½}]
40<= t <= 59	K_t = 8F1BBCDC	[2^{30} x 5 ^{½}]
60<= t <= 79	K_t = CA62C1D6	[2^{30} x $10^{½}$]

Table 1: substitution transformation using integer parts for hex decimal composition incorporating XOR encryption

The above algorithm has the property that every bit of the hash code is a function of every bit of the input. The complex repetition of the basic function of factors to produces results that are well mixed. It is unlikely that two messages chosen at random will have the same hash code. The difficulty of coming up with two messages having the same message digest is on the order of 2^{80} operations. The difficulty of finding a message with a given digest is on the order of 2^{160} operations even brute force cannot calculate the respective time.

IV. SIMULATION RESULTS

To test the two conjunctional algorithm i.e. Shift Substitution and XOR Hashing Transformation algorithms, we have conducted experiments that apply both algorithms to evaluate the performance.

Machine No.1	CPU Speed	L2 Cache	Cores	Bit	CPU Description	Virtual Machine	Memory
1	2.0 GHZ	2.4 MB	4	32	i3 Intel	YES	4 GB
2	2.4 GHZ	2.4 MB	4	64	i3 Intel		8 GB

Table 2: Infrastructure used for Measuring and evaluating the performance proposed algorithm in above scheme**.**

Machine	CPU Time in Seconds
1	1.227
2	0.743

Table 3: CPU time used to execute the proposed algorithm in seconds

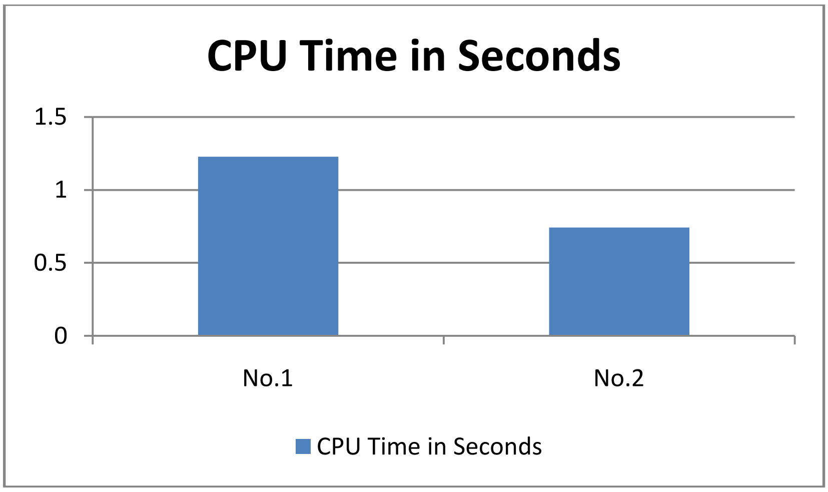

Chart 1: Bar graph depicting time utilized by proposed algorithm in two different virtual machines.

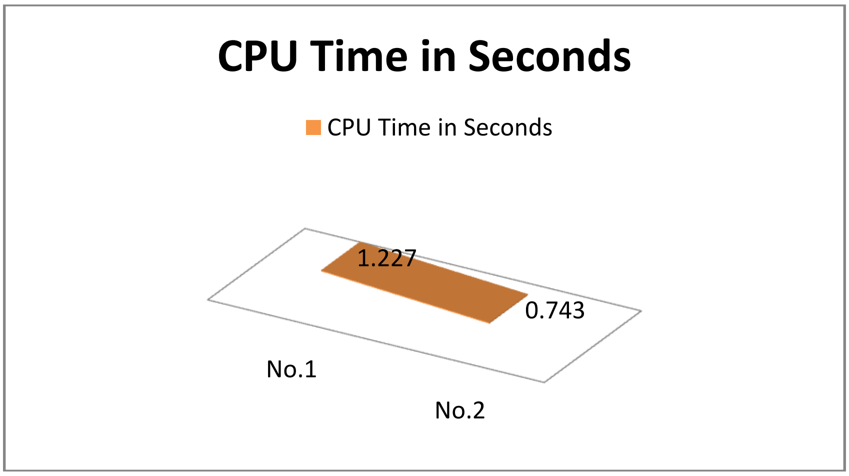

Chart 2: Surface Model depicting time utilized by proposed algorithm in two different virtual machines.

V. Conclusion and Future Work

This paper proposes a new Shift Substitution along with XOR algorithm to improve the encoding performance of TPA signatures. For these TPA signatures, the encoding performance is determined by two primary factors: the number of shift made and XOR operations with sandbox behavior. Consequently, this paper proposes a new scheduling algorithm which is able to efficiently utilize Virtual Machine resources and thus achieves much better encoding and decoding performance than the traditional algorithm. In a performance evaluation on some widely known codes on a variety of platforms, we show that the encoding performance obtained by our proposed algorithm significantly outperforms that of the traditional algorithm used in various scenarios.

Additional future work is to put our new proposed scheme algorithm into a real storage system. Although we have analyzed how proposed algorithm improves the whole performance of storage systems, the data used in our analysis is synthetic and may not be representative the real world scenarios. We plan to implement a reliable storage system and use various scheduling algorithms in it to find how our scheduling algorithm can improve this system's performance and proposed scheme can be used in firmware's as augmented security for TPA for auditing purpose.

REFERENCES

1. Babar, M. A., & Chauhan, M. A. (2011). A tale of migration to cloud computing for sharing experiences and observations. SECLOUD '11 Proceedings of the 2nd International Workshop on Software Engineering for Cloud Computing (pp. 50-56). New York: ACM.
2. Gregg, M. (2010). 10 Security Concerns for Cloud Computing. Retrieved February 28, 2012, from http://viewer.media.bitpipe.com/1078177630_947/1268847180_5/WP_VI_10SecurityConcernsCloudComputing.pdf Hamlen, K., Kantarcioglu, M., Khan, L., & Thuraisingham, B. (2010). Security Issues for Cloud Computing. International Journal of Information Security and Privacy, Volume 4 Issue 2 , 39-51.
3. Hamlen, K., Kantarcioglu, M., Khan, L., & Thuraisingham, B. (2010). Security issues for cloud computing. International Journal of Information Security and Privacy, 4(2), 36-48. DOI: 10.4018/jisp.2010040103
4. Bowers K.D, Juels A, and Oprea A, "Hail: A high-availability and integrity layer for cloud storage," in Proc. of CCS'09. Chicago, IL, USA: ACM, 2009, pp. 187–198.
5. M. Castro and B. Liskov, "Practical Byzantine Fault Tolerance and Proactive Recovery," ACM Trans. Computer Systems, vol. 20, no. 4,pp. 398-461,2002
6. Chang E.C, and Xu J, "Remote integrity check with dishonest storage server," in Proc. of ESORICS'08. Berlin, Heidelberg: Springer-Verlag, 2008, pp. 223–237.
7. Chandran S. and Angepat M., "Cloud Computing: Analyzing the risks involved in cloud computing environments," in Proceedings of Natural Sciences and Engineering, Sweden, pp. 2-4, 2010.
8. Cong Wang,Qian Wang,Kui Ren Ninig Cao and Wenjing Lou"Towards Secure and Dependable storage services in cloud computing",IEEE Transaction on service computing,vol 5,no 2,june 2012
9. Dalia Attas and Omar Batrafi " Efficient integrity checking technique for securing client data in cloud computing", October 2011
10. Jaison Vimalraj.T,M.Manoj"Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing", March2012
11. Kayalvizhi S,Jagadeeswari "Data Dynamics for Storage Security and Public Auditability in Cloud Computing", February 10, 2012
12. Metri P. and Sarote G., "Privacy Issues and Challenges in Cloud computing," International Journal of Advanced Engineering Sciences and Technologies, vol. 5, no. 1, pp. 5-6, 2011.
13. K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69-73,2012
14. D. Srinivas "Privacy-Preserving Public Auditing In Cloud Storage Security", November 2011
15. M. A. Shah, M. Baker, J. C. Mogul, and R. Swaminathan, "Auditing tokeep online storage services honest," in Proc. Of HotOS'07., CA USA: USENIX Association, 2007, pp. 1–6.
16. C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," Proc. 17th Int'l Workshop Quality ofService (IWQoS '09), pp. 1-9, July 2009