An Empirical and Efficient Auditing over cloud Services

Prakash Palika[1], K Ravi Kumar[2]
M.Tech Scholar[1], Associate Professor[2]
[1,2]Dept of Computer Science, KIET Korangi, Andhra Pradesh

Abstract: Auditing is an important research issue in the field of cloud computing, we are proposing an empirical model of auditing protocol for auditing the data component over the cloud architecture with a protocol by a third party auditor. Data component security can be maintained by the Rijandael and authentication can be maintained by the random challenges and our efficiently maintains the integrity of the data component efficiently.

I.NTRODUCTION

Cloud computing has several advantages of their resource specification as Infrastructure as service, Software as service and operating system as service ,Wide range of applications available with cloud services, various roles involved in the cloud architectures Data owner, Auditor and user

Data owner outsources the data to the cloud service ti efficient usage for end user through service provider with an authentication from the owner end. Data owner does not know where the data has been uploaded and How it is being maintained on the hard disks of the server, So many interesting issues raised during the confidentiality and sensitivity of data

Where the data is going to be stored?

How the service provider provides security to our data?

What are the access rights(Auditor, Data preprocesser,End user) to our data?

So Data owners uses auditor for monitor the data which is stored over the cloud servers, whether data has been stored properly without losing data integrity and confidentiality.

In order to ensure, compliance of security policies mechanisms and to verify whether these policies and procedures are implemented in true letter and spirit, auditing can be employed as a verification tool. Auditing is the process of tracing and logging significant events that could take place during a system run-time. It can be used for analysis, verification and validation of security measures to achieve overall security objectives in a system. Since advantages of cloud computing are obvious, but the security risks associated with each cloud service model hinder its widespread adoption [1]. The externalized aspect of outsourcing makes it difficult to maintain data integrity, privacy, availability and above all compliance check of security measures taken by the service provider. According to a survey in 2009, cloud security was revealed as the top most challenge/ issue of cloud computing among others like availability of services, performance, lack of interoperability standards and so on.From the data owners' perspective , a flexible on-demand manner brings appealing benefits:

1. Relief of the burden of storage management.
2. Universal data access with independent geographical locations.
3. Avoidance of capital expenditure on hardware, software, personnel maintenance.

Since cloud service providers (CSP) are separate administrative entities, data outsourcing actually relinquishes the owner's ultimate control over the fate of their data. To fully ensure data security and save data owners' computation resources, researchers propose to enable publicly auditable cloud storage services TPA(Third Party Auditor).

TPA provides a transparent yet cost-effective method for establishing trust between data owner and cloud server Traditional cryptographic primitives for the purpose of data security protection cannot be directly adopted. It is often insufficient to detect data corruption only when accessing the data. The tasks of auditing the data correctness in a cloud environment can be formidable and expensive for data owners

II.RELATED WORK

Out sourcing of data over cloud services economically feasible than the traditional approaches of data storage or service, So many legislation issues involved in the cloud service architectures

- Data protection Law
- Data transfer over abroad
- Third party or data preprocessor Monitor
- End user agreement

© 2013 IJAIR. ALL RIGHTS RESERVED

So many auditing protocols introduced for secure auditing of data over cloud services, but the main objective of the monitor in to check the data integrity, it obviously involving the auditor to check our confidential or sensitive Data.

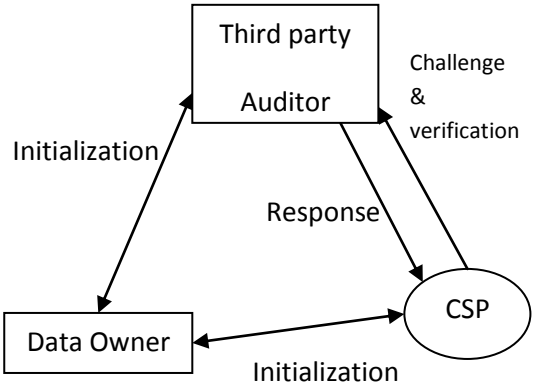
Our paper Works on this approach, by designing an efficient auditing protocol without revealing the content or data component to the cloud by forwarding the authentication parameters to the Auditor and Cloud service provider,various cryptographic mechanism implemented for the secure data transmission over the network,for data integrity segment the data into number of components and generates the tag keys for the individual data components and encrypt the data components with their respective keys before uploading the data uploading to the server.

Various Symmetric and asymmetric approaches released for secure data transmission .However, the authors did not discuss the audit authentication of TPA for a cloud server to respond. Also no details are discussed for authentication handshake between User, Cloud Server or Cloud Service Provider (CSP) and the TPA. B. Big IT giants such as Google, Yahoo and Microsoft are earning a lot of money by providing storage services like online backups, video hosting and photo sharing to their customers. A customer has to rely on storage service providers to maintain their data integrity. Unluckily, no data storage service is fully reliable as large scale storage systems are complicated and prone to multiple threats that cause data corruption. At present there are no proper mechanisms for policy compliance that leads to protect data by the service providers.

In this paper, Shah and Baker et al.[3] have proposed some efficient challenge-response auditing protocols by a third party auditor, not only to check data integrity from service provider but also fraudulent customers who claim loss to get paid. Privacy preservation is achieved through zero-knowledge, concealing data Contents from the auditor. The suggested protocol has mainly three stages: initialization, audit and extraction. During initialization, user and the service provider enter into an agreement on the stored data object. The auditor confirms both customer & service agree on contents of encrypted data or encryption key, else it would be difficult to resolve future conflicts. In audit stage, auditor can effectively verify the proof of data possession by the service provider through a challenge-response protocol. During extraction phase, the auditor verifies data integrity of data returned to the customer through the auditor. The encrypted data and a "blinded" version of encryption key are forwarded to the auditor. The auditor checks its completeness and passes it to the customer who then recovers the actual data

III. PROPOSED WORK

In this paper we proposed an efficient dynamic auditing protocol between data owner, auditor and cloud server. The following dynamic auditing protocol contains the following implementations like File segmentation and distribution, Tag generations, Challenge generation and verification, architecture of the system is shown below.



Auditing protocol

Data owner fragment the entire content in to number of blocks and generates the tags for individual block and uploads the data in to the server and forwards the hash code and a random challenge. Abstract information, tag generation keys and random challenge are forwarded to the third part auditor

Dynamic auditing protocol:

Before describing the auditing protocol, we first define some notations

Symbol	Meaning
M	Data component
T	Set of tag generation keys
R_A	Random challenge to Auditor(Large Prime Number)
R_B	Random Challenge to Cloud server(Large Prime Number)
$H(R_A \text{ XOR } R_B)$	Hash code after XOR Over R_A and R_B
M_{info}	Meta or abstract information of M
n	Number of blocks in the each component

Data Owner Initialization:

Suppose a file F has m data components as F = (F1, · · · ,Fm). Each data component has its physical meanings and can be updated dynamically by the data owners, data owner needs to encrypt it with its corresponding key. Each

© 2013 IJAIR. ALL RIGHTS RESERVED

data component F_k is divided into n_k data blocks denoted as $Fk = (m_{k1}, m_{k2}, \cdots, m_{knk})$.

After dividing the file in to number of blocks and encrypts the blocks with key that can be considered as tag key $T_{i,\ encrypt}$ the all file until the data component is encrypted with tag keys, now data owner generates a random challenge R_A and forwards to the cloud service provider along with data component $(m_1, m_2, \ldots m_n)$ and hash code ,which is generated by the two random challenges which are distributed by the data owner,for encryption process we used Rijndael algorithm .

B. Rijandael algorithm

Our paper uses an advanced cryptographic algorithm for secure data transmission and it uses the key, which is generated from the multikey exchange group key protocol and the brief structure of the novel cryptographic algorithm as shown below, the system mainly works on substitution and affine transformation techniques. KeyExpansion—round keys are derived from the cipher key using key schedule. Initial Round: AddRoundKey—each byte of the state is combined with the round key using bitwise xor Rounds. SubBytes—a non-linear substitution step where each byte is replaced with another according to a lookup table. ShiftRows—a transposition step where each row of the state is shifted cyclically a certain number of steps. MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column. AddRoundKey

Novel Dynamic Auditing Protocol:

1. Final Round (no MixColumns)
    1. SubBytes
    2. ShiftRows
    3. AddRoundKey

Complete implemention of the subbytes,shiftrows,mix columns and add round key as follows[16], for implementation details we had used builtin algorithm from the dotnet namespaces.

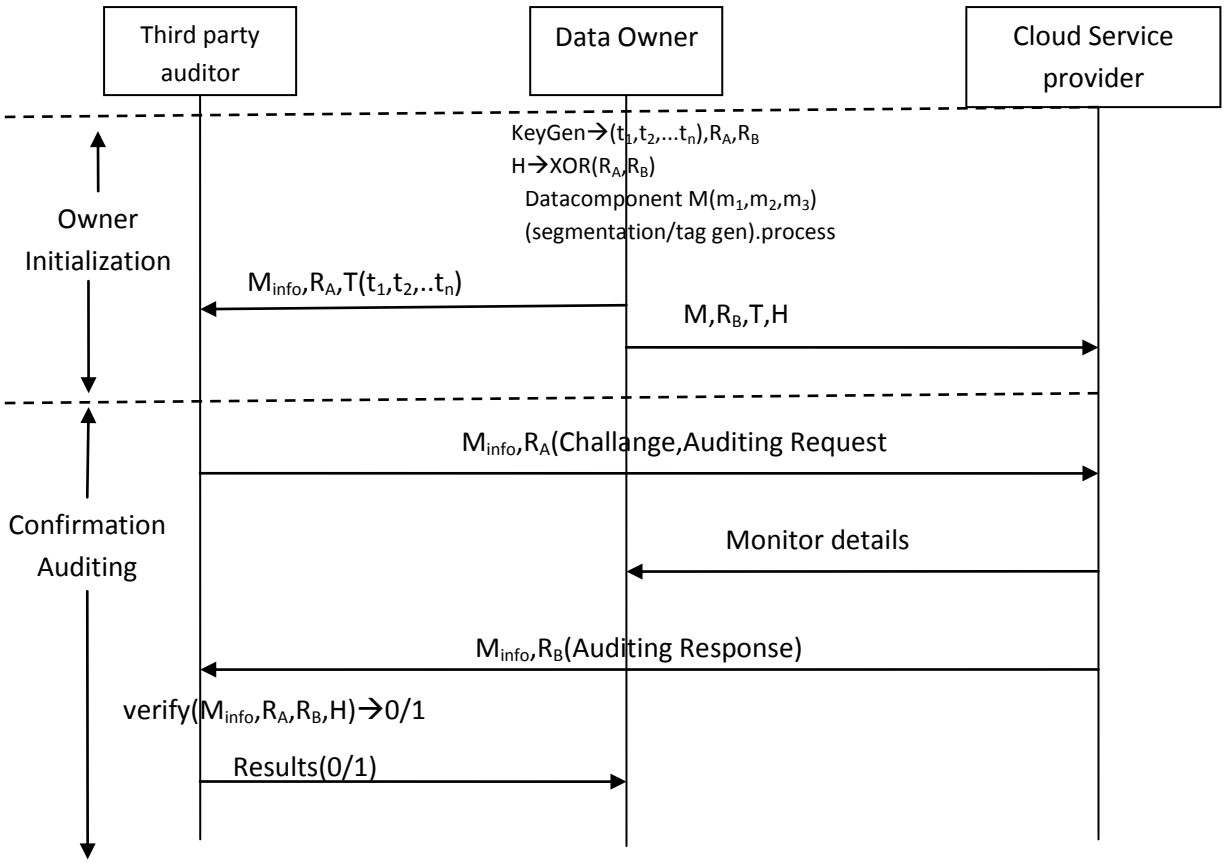
Auditor Implementation:

Auditor monitors the manipulations between the data owner and cloud service provider, receives the meta information of the data component, tag generation key and random challenge from the data owner, now by making a request to the cloud server auditor gets the meta information of the data component, before processing the request checks for authentication the and checks with the meta information which is received from the data owner.

Service Provider:

Data owner hosts the data over cloud servers. Here the data which is fragmented and encrypted by the data owner, data owner can access the information when ever required from the cloud server. Auditor access the information for auditing purpose if he is authenticated, Submits the access process to the data owner when ever required

© 2013 IJAIR. ALL RIGHTS RESERVED



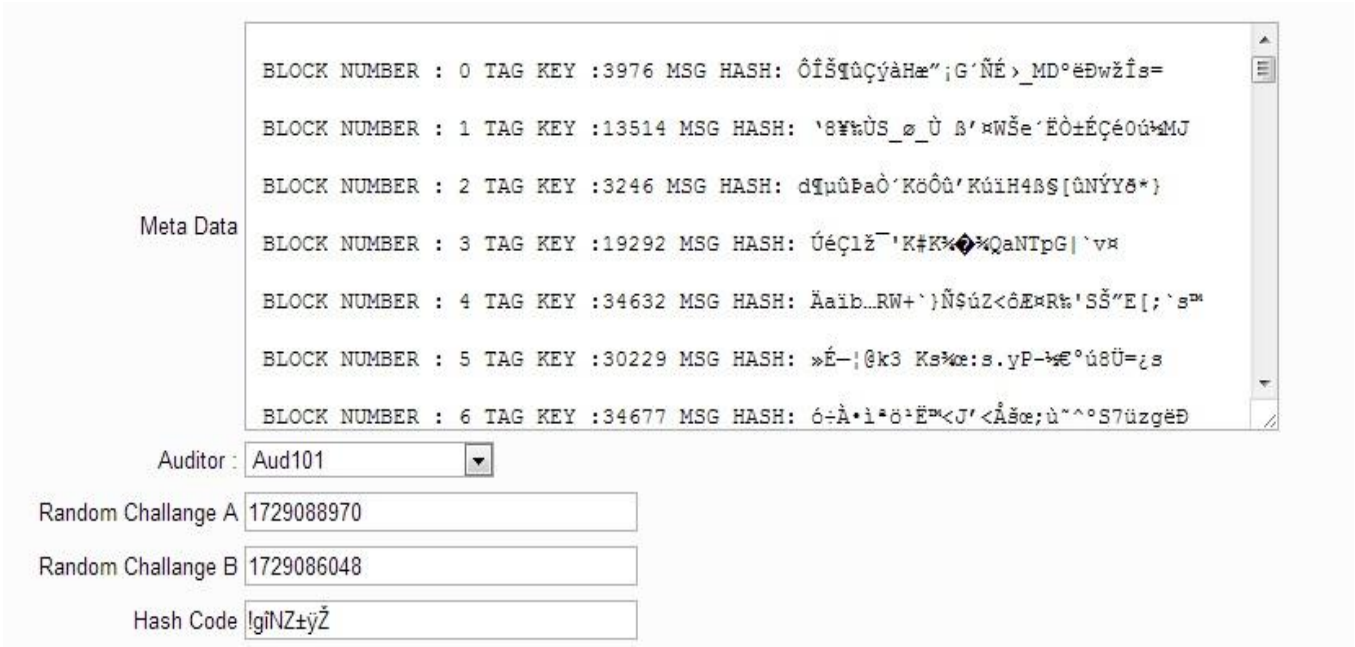
Data owner initializes the data component by fragmentation, encryption and by forwarding the Meta information about the data component and random challenge and data can be hosted in to the server and hash/authentication code forwarded to the cloud server for authenticated monitor

Auditor receives the Random challenge (a large prime number) and (M_{info}) meta information and makes a monitor request to the cloud server. Cloud service provider authenticates the auditor and forward the meta information to the Auditor, CSP forwards the monitor details when ever requested.

Experimental Analysis:

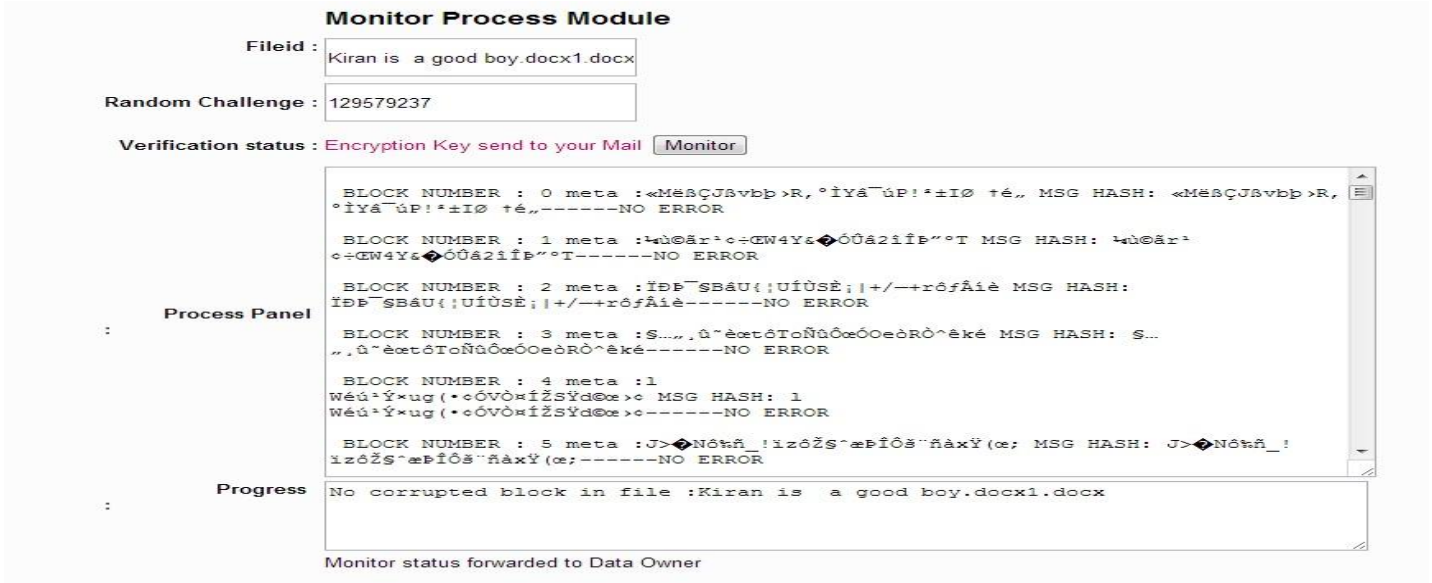
For implementation purpose we are using C#.net and asp.net .Initially Data owner can Initially Segments the data component in to number of blocks and encrypts the individual blocks by Rijandael algorithm with tag keys for individual bocks and genets the hash codes and random challenges for auditor and cloud service provider as follows

© 2013 IJAIR. ALL RIGHTS RESERVED



Data components can be uploaded to the service provider then auditor receives the random challenge and authenticate himself with random challenge at service provider. Service provider checks the authentication of auditor by his random challenge which is received by the data owner, if Authentication is reliable ,csp forwards the auditor details to Data owner through mail(smtp implementation).

Third party auditor monitor the data components after authentication and forwards the monitor details to data owner as follows



IV. CONCLUSION AND FUTURE WORK

We conclude our research work with an efficient auditing protocol without losing its data integrity, In our approach we need not forward the data components to the auditor directly in our approach, but auditing can be done efficiently. We can enhance our approach by increasing the authentication approach rather than simple random challenges and we can minimize the time complexity of our cryptographic algorithm and minimize the computational complexity in Rijandael by in changing the traditional GPU

© 2013 IJAIR. ALL RIGHTS RESERVED

References:

[1] Xuan Zhang, Nattapong Wuwong, Hao Li, Xuejie Zhang,“ Information Security Risk Management Framework for the Cloud Computing Environments", 10th IEEE International Conference on
Computer and Information Technology, 29 June, 2010.

[7] Wang, Sherman, Kui, Lou, “Privacy-Preserving Public Auditing for
Secure Cloud Storage", INFOCOM, 2010 Proceedings IEEE, 14-19

[2] G. R. Goodson, J. J. Wylie, G. R. Ganger, and M. K. Reiter, “Efficient byzantine-tolerant erasure-coded storage,” in DSN. IEEE Computer Society, 2004, pp. 135–144.

[3] V. Kher and Y. Kim, “Securing distributed storage: challenges,
techniques, and systems,” in StorageSS, V. Atluri, P. Samarati, W. Yurcik, L. Brumbaugh, and Y. Zhou, Eds. ACM, 2005, pp. 9–25.

[4] L. N. Bairavasundaram, G. R. Goodson, S. Pasupathy, and J. Schindler, “An analysis of latent sector errors in disk drives,” in SIGMETRICS, L. Golubchik, M. H. Ammar, and M. Harchol-Balter, Eds. ACM, 2007, pp. 289–300

[5] B. Schroeder and G. A. Gibson, “Disk failures in the real world: What does an mttf of 1, 000, 000 hours mean to you?” in FAST. USENIX, 2007, pp. 1–16.

[6] M. Lillibridge, S. Elnikety, A. Birrell, M. Burrows, and M. Isard, “A cooperative internet backup scheme,” in USENIX Annual Technical Conference, General Track. USENIX, 2003, pp. 29–41.

[11] Y. Deswarte, J. Quisquater, and A. Saidane, “Remote integrity checking,” in The Sixth Working Conference on Integrity and Internal Control in Information Systems (IICIS). Springer Netherlands, November 2004.

[12] M. Naor and G. N. Rothblum, “The complexity of online memory checking,” J. ACM, vol. 56, no. 1, 2009.

[13] A. Juels and B. S. K. Jr., “Pors: proofs of retrievability for large files,” in ACM Conference on Computer and Communications Security, P. Ning, S. D. C. di Vimercati, and P. F. Syverson, Eds. ACM, 2007, pp. 584–597.

[14] T. J. E. Schwarz and E. L. Miller, “Store, forget, and check: Using algebraic signatures to check remotely administered storage,” in ICDCS. IEEE Computer Society, 2006, p. 12.

[15] D. L. G. Filho and P. S. L. M. Barreto, “Demonstrating data possession and uncheatable data transfer,” IACR Cryptology ePrint Archive, vol. 2006, p. 150, 2006.

[16] F. Seb´e, J. Domingo-Ferrer, A. Mart´ınez-Ballest´e, Y. Deswarte, and J.-J. Quisquater, “Efficient remote data possession checking incritical information

[17]http://en.wikipedia.org/wiki/Advanced_Encryption_Standard.

March, 2010.

[8] Mehul, Ram, Baker, “Privacy-Preserving Audit and Extraction of
Digital Contents”, HP Lab Technical Report No. HPL-2008-32, 25
April, 2008

[9] J. Li, M. N. Krohn, D. Mazi`eres, and D. Shasha, “Secure untrusted data repository (sundr),” in Proceedings of the 6th conference on Symposium on Operating Systems

© 2013 IJAIR. ALL RIGHTS RESERVED

BIOGRAPHIES

Sri.K.Ravi Kumar,Recieved his M.Tech from Pragati Engg.College Surampalem. He has working as Assoc. Professor&Head of the Dept of CSE,He has 7 years of experience in teaching and he has been guided 13 projects for M.Tech Students and more than 30 projects for B.Tech students. He has published 13 papers in National and International Journals.

Mr. P.Prakash is a student of, Kakinada Institute of Engineering and Technology, Korangi, Kakinada. Presently he is pursuing his M.Tech (C.S.E) from JNTUK and he received his Faculty of Engineering in Degree of Master of Computer Applications. Passed First Division from St.Mary's College for P.G Coureses ,Surampalem Affiliated to Andhra University, in the year 2005. His area of interest includes Networking and Cloud computing.

© 2013 IJAIR. ALL RIGHTS RESERVED