CREATING SECURE CLOUD BY CONTINUOUS AUDITING USING DBM ALGORITHM

SWETHA M.
Department of Information Technology, Agni College of Technology, Chennai
swetha.mylife96@gmail.com

***ABSTRACT*--Cloud Service Certifications (CSC) is a good means to address a greater level of security. Keeping in viewthat, cloud services are part of continuously changing environment, doubt reliability of such certifications may occur in multi-year validity periods. To increase trustworthiness of certifications it is must to assure continuously reliable and secure cloud services. CA of cloud services is still in its immature state. Thus, we conducted a thorough workshops, interviews literature review with practitioners to finalize architecture for continuous cloud service auditing. Yet third party auditing methods are not available in existing methodologies. Therefore, we propose a possible ways of implementation that shows various benefits and changes that have to be managed to diffuse the concept of continuous cloud service auditing. Auditors and providers who are linked together in a conceptual architecture are getting benefit over applicable internal and third party auditing methodologies. Further on, we provide future research to implement CA in cloud service context.**

Index Terms - Certification, cloud computing, continuous, security auditing

I. INTRODUCTION

Many organizations upload their data, applications to the cloud, leading them to achieve financial and technical benefits. Organizations are indecisive to accept cloud services because of security, privacy, and reliability concerns. Cloud service certifications (CSC) are good means to address these concerns by establishing trust, and increasing transparency of the cloud market. Thus, to provide transparent, continuously reliable, and secure cloud services continuous auditing (CA) of certification criteria is required. Beyond these special purpose methodologies, research currently lacks a comprehensive architecture, enabling third party auditors to continuously audit a broad variety of CSC criteria. Before conceptualizing an architecture and defining how to perform CA, it has to be analyzed where CA is reasonable. Subsequently, we analyze which CSC criteria should be continuously audited to assure ongoing adherence by performing workshops with cloud service auditors first.

II. EXISTING SYSTEM

A major problem in cloud computing is about remote data integrity checking. The client's huge data is out of his control. To gain more benefits the hacker may corrupt the client's data. From fast technology life cycles and inherent cloud computing (CC) characteristics cloud services are part of an ever changing environment, like complicated supply chains. Issued certifications may lead to doubt in reliability for long validity periods. And also cloud service customers do not longer possess their data locally, assuring that their data is being correctly stored and integrity is maintained in cloud environments is of critical importance. Malicious insiders, data loss, technical failures and external attackers are the important cause for data integrity.

III. PROPOSED SYSTEM

Remote data integrity checking is demanded to secure user's data which is in Multi cloud environment,.The process starts with uploading a file to the cloud. The files splits into multiple blocks and stored in Multi cloud environmentusing Dynamic block generation Algorithm. Proper Metadata's for the different part of the Cloud Storage and indexing is afforded by File Allocation Table (FAT) File System. Here the auditor agrees to inspect logs, which are continuously created during monitoring operations by services providers to assess certification adherence. If Attacker corrupts data in MultiCloud, the continuous auditing process helps the verifier to perform Block level and File level checking for remote data Integrity Checking using Verifiable Data Integrity Checking Algorithm. To preserve user privacy from third party cloud provides random blocks to third party for integrity checking which is to protect user privacy from third party. If the data gets distorted during checking file recovery is done by the verifierautomatically before user complaintcloud for file recovery.

IV. BACKGROUND

Cloud computing enables ubiquitous, on-demand net-work access to a shared pool of configurable computing re-sources that can be rapidly provisioned and released with minimal management effort or service provider interaction These resources refer, for instance, to hardware, development platforms, and applications. CC entails five essential characteristics, that are: provision of (i) on-demand self-service access to (ii) virtualized, shared, and managed IT resources that are (iii) scalable on-demand, (iv) available over a network, and (v) priced on a pay per-use basis. These characteristics challenge current assessment processes There from, CC faces a broad range of security issues, including accessibility vulnerabilities, privacy, and control issues as well as issues related to data integrity and data confidentiality Extant research already proposes certifications and audits as detective controls and good means to assess quality and performance of IT services in procurement processes. A certification is defined as a third party attestation of products, processes, systems, or persons that verifies conformity to specified criteria. Several CSC have emerged to assure a high level of security, reliability, and legal compliance of cloud services. Recent research suggests that CA is required to deal with the ever-changing environment of cloud services and to increase trustworthiness of CSC\

A. Continuous Auditing

Continuous auditing is defined as a methodology that helps independent auditors to provide written assurance on a thesis or equivalent, using a series of auditor's reports issued virtually or in a limited time after the occurrence of events underlying the subject. Thus, CA enables auditors to immediately reply to changes or events regarding the subject and to adjust their auditing reports based on assessment of these changes and events.

V. NUMBER OF MODULES

After careful analysis the system has been identified to have the following modules:

- Server Configuration
- Data Upload and Block Split
- Data Integrity Checking
- File Recovery and Certificate Generation

A. Server Configuration

Admin configure Multi cloud server setup. Server IP Address and Port number is given by the admin for each Cloud. Now a Server Architecture is created for Multi Cloud Storage. If the admin has to reconfigure the old Multi Cloud server setup, it can be done. For old server setup, FAT file can be modified or remain same. Audit time will be set by the admin for Data Integrity checking process.

B. Data Upload and Block Split

User has an initial level Registration Process at the web end. The users provide their own personal information for this process. The server in turn stores the information in its database. After Registration, user can upload files to the server. Uploaded files will be stored in a Server. When the user upload the data to different cloud by the time it is splitted into different blocks using dynamic block generation Algorithm and each block will be appended with Signatures before storing the data in FATFS. Signature generated using MD5 Algorithm. Also the data gets encoded using for Base64 Algorithm.

C. Data Integrity Checking

FATFS has proper Indexing and Metadata's for the different Chunks of the Data that is being uploaded by User. Verifier performs Remote Integrity Checking on Cloud Data. Cloud allocates random combination of all the blocks to the Verifier, instead of the whole file is retrieved during integrity checking. This is to protect user privacy from a third party (Verifier). Verifiable Data Integrity Checking Algorithm is done in two steps: Block Checking and File Checking. In Block Checking step: Three signatures are generated for Block level Checking.

- A signature of a block retrieved from a FATFS
- A new signature is generated for block to be checked
- A Signature is retrieved from the block appended with the signature which is stored in the Cloud

The above three signatures are cross checked for Block level Integrity Checking. And the block contents are appended to verify with File level Integrity Checking.

D. File Recovery and Certificate Generation

Attacker can corrupt data in any one of the cloud servers. On Data Integrity Checking done by the Verifier, Verifier informs Corrupted blocks to the Cloud. Recovery Process will be done by the verifier automatically when data gets corrupted. User can complaint to the Cloud if the user file get corrupted (Verifier doesn't perform checking on this file).Whenever user access file, Blocks will be reallocated dynamically to provide access confidentiality in cloud and FAT File System will get updated.Auditor will monitor the cloud continuously and they provide the certificate based on the cloud performance.when new user join in the cloud they will read the certificate and then they can create an account in the cloud.

VI. ALGORITHM

A. MD5 ALGORITHM

The MD5 algorithm is a widely used hash function giving 16-byte hash value .Like most hash functions MD5 is neither encryption nor encoding.

Steps

- `Merge padded bits.

Message is stuffed such that its length is congruent to 448 modulo 512.

- Merge length i.e., A 64 bit representation of b is merged to the result of previous step. The resulting message has a length that is exact multiple of 8-byte.
- Initialize MD buffer

To compute the message digest 8-bit buffer (A, B, C, D) is used. Here each of (a , b ,c ,d) is a 4-byte register. It process message in 32 bit blocks

Four auxiliary functions that takes as input 3 32-bit words and produce as input 1 32-bit word.

F (B, C, D) = (B ∧C) ∨(¬ B ∧D)

G (B, C, D) = (B ∧D) ∨(C ∧¬D)

` H (B, C, D) = B □ C □ D

I (B, C, D) = C ⊕ (B ∨¬D).

- Output

The output A, B, C, D is derived from message digest. That is, output starts with low-order byte of A, and end with high-order byte of D.

B. BASE64 ALGORITHM

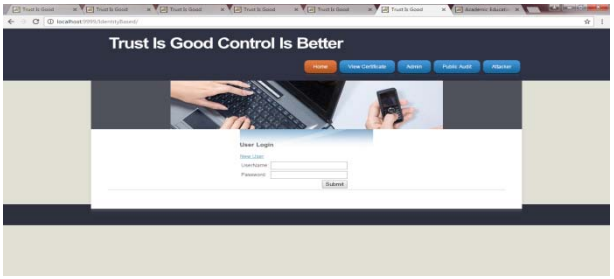
- Split the input bytes stream into 24 bit blocks
- Split24 bits of each 24-bit block into 4 groups of 6 bits.
- Using base-64 character set map, based on the 6-bit value map each group of 6 bits to 1 printable character.
- Attach 16-bit of zero (\x0000) after encoding it as a normal block, if last 3-byte block has only 8-bit of input data then override the last 2 characters with 2 equal signs (==), so the decoding process knows 16 bits of zero were padded.
- Attach 8-bit of zero (\x00) after encoding it as a normal block and override the last 1 character with 1 equal signs (=) if last 3-byte block has only 16- bits of input data, so the decoding process knows 1 byte of zero was padded.
- Carriage return (\r) and new line (\n) are attached into the output character stream. They will be rejected by the decoding process

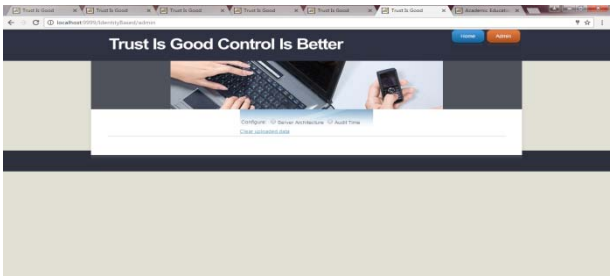
VII. IMPLEMENTATION

The system has been identified to have the following modules.

A. Server Configuration

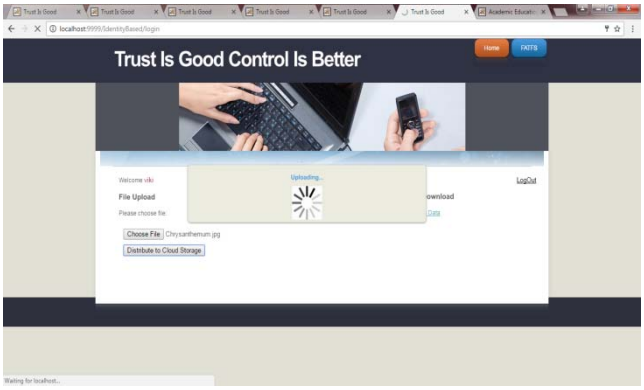
The Configuration is the process of connecting the servers to perform the auditing. The admin and user login is being designed at this stage. For new user, user registration is also available.

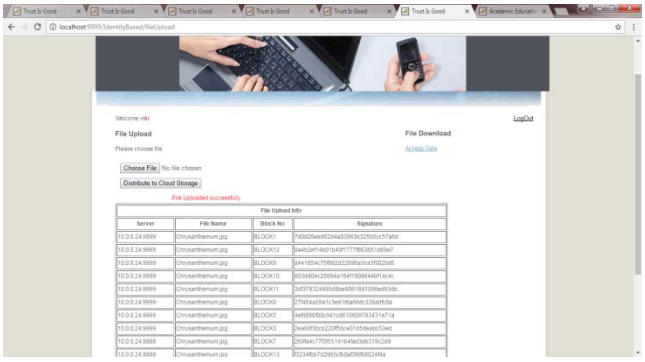




B. Data Upload and Block Split

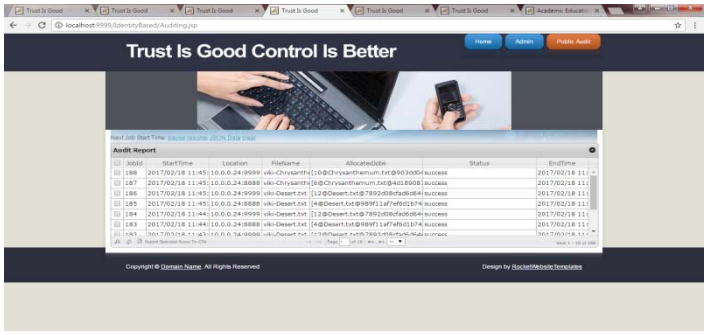
In this process, the uploaded files are splitted into multiple blocks and dynamically stored in cloud. For referencing further , FAT(file allocation table) file system is used.





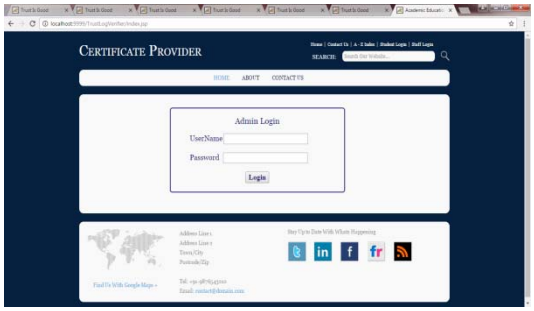
C. Data Integrity Checking

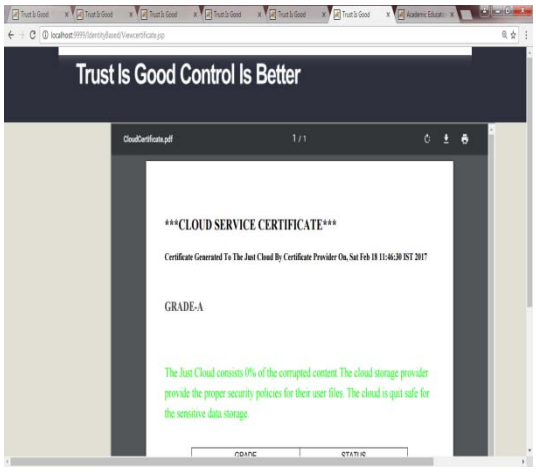
The data which are stored in multiple table are accessed when client requested. Hence signature is generated for each block andThe above signatures are cross checked for Block level Integrity Checking. And the block contents are appended to verify with File level Integrity Checking.



D. File Recovery and Certificate Generation

The encrypted file is then automatically retrieved by continuous auditing. Audit time is set for auditing. Finally a certificate is generated and shown to the client`





VIII. SUMMARY

Continuously auditing cloud services can provide a immense security and reliability to cloud service adopters as per our study. Continuous audit of cloud service can only increase trustworthiness of certificationswith our study, by conceptualizing an architecture interviews revealed that most of existing methodologies are not applicable for third party service auditing purposes. Therefore, service facilitatorsmustground an internal auditing department, which provides audit relevant data to auditors through secured and defined interfaces. Our conceptual architecture highlights important components as well as processes like sending reports, informing about major cloud changes and adjusting processes that have to be implemented. These findings are relevant for practitioners and researchers.Using a checklist that we provide to the auditors enables them to classify, after the initial certification process is accomplished whether or not a high frequency auditing of CSC criteria is required.

IX. FUTURE ENHANCEMENT

Further research is focused on developing auditing methodologies adjusted to the CC context, especially concerning validation of security measures and adherence to critical cloud service characteristics (e.g., availability and scalability of services). Likewise, future re-search should examine how unique cloud computing characteristics influence (continuous) auditing practices. Identified methodologies need to be implemented to prove their practical and economic applicability in cloud environments. Therefore, identified and future methodologies need to be linked to CSC criteria and corresponding metrics to measure criteria adherence. Furthermore, research should focus on evaluations regarding acceptance and benefits of cloud providers when participating in CA as well as drivers and inhibitors for cloud service customers' demand for CA. Besides future research should clarify how to manage certification violations, and if and how to inform cloud customers about certification adherence.

X. REFERENCES

[1] David G.Lowe,"Distinctive Image Features From Scale-Invariant Keypoints".
[2] NavneetDalal and Bill Triggs,"Histograms of Oriented Gradients for Human Detection."
[3] Herbert Bay,TinneTuytelaars and Luc Van Gool, "SURF:Speeded Up Robust Features."
[4] Johannes Bauer, NikoS¨underhauf, Peter Protzel,"COMPARING SEVERAL IMPLEMENTATIONS OF TWO RECENTLY PUBLISHED FEATURE DETECTORS".
[5] KrystianMikolajczyk and CordeliaSchmid."A performance evaluation of local descriptors