RESEARCH ARTICLE OPEN ACCESS

# Trust is good Control is Better- Creating Secure Clouds by Continuous Auditing

S.Deepalakshmi[1], E.Dilipkumar[2]
[1]PG Student, [2]Associate Professor
[1,2,] Department of MCA, Dhanalakshmi Srinivasan College of Engineering and Technology

## Abstract:

Cloud service certifications (CSC) attempt to assure a high level of security and compliance. However, considering that cloud services are part of an ever-changing environment, multi-year validity periods may put in doubt reliability of such certifications. We argue that continuous auditing (CA) of selected certification criteria is required to assure continuously reliable and secure cloud services, and thereby increase trustworthiness of certifications. CA of cloud services is still in its infancy, thus, we conducted a thorough literature review, interviews, and workshops with practitioners to conceptualize architecture for continuous cloud service auditing. Our study shows that various criteria should be continuously audited. Yet, we reveal that most of existing methodologies are not applicable for third party auditing purposes. Therefore, we propose a conceptual CA architecture, and highlight important components and processes that have to be implemented. Finally, we discuss benefits and challenges that have to be tackled to diffuse the concept of continuous cloud service auditing. We contribute to knowledge and practice by providing applicable internal and third party auditing methodologies for auditors and providers, linked together in a conceptual architecture. Further on, we provide groundings for future research to implement CA in cloud service contexts

## 1. INTRODUCTION

An increasing number of organizations outsource their data, applications and business processes to the cloud, empowering them to achieve financial and technical benefits due to on-demand provisioning and pay-per-use pricing. However, organizations are stillhesitant to adopt cloud services because of security, privacy, and reliability concerns regarding provisioned cloud services as well as doubts about trustworthiness of their cloud service provider [1–3]. Cloud service certifications (CSC) are good means to address these concerns by establishing trust, and increasing transparency of the cloud market [2, 4]. Several CSC have evolved, such as *CSA STAR*or *EuroCloud Star Audit*. These CSC attempt to assure a high level of security, reliability, and legal compliance, for a validity period of one to three years. However, cloud services are part of an ever-changing environment, resulting from fast technology life cycles and inherent cloud computing (CC) characteristics, like on-demand provisioning and entangled sup-ply chains [5, 6]. Hence, such long validity periods may put in doubt reliability of issued certifications. CSC criteria may no longer be met throughout these periods, for in-stance, due to configuration changes or major security incidents. Thus, continuous auditing (CA) of certification criteria is required to assure transparent, continuously reliable, and secure cloud services and to establish a trustworthy CSC after the initial certification process is accomplished.Extant research has focused on implementing and evaluating CA of information systems since the early nineties. This progression has included the evolution of architecturally different methodologies, for instance, embedded audit modules [7]and independent monitoring control layers [8], which help to monitor and audit information systems. However, past research has mostly examined CA for internal purposes only. In the context of CC, researchers recently proposed the means to enable third party authorities to audit data integrity [9], data location compliance [10], and changes of cloud infrastructure [11] among others. Aside from these special purpose methodologies, re-search currently lacks a comprehensive architecture, enabling third party auditors to continuously audit a broad variety of CSC criteria.

## 2. LITERATURE SURVEY

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 [13]. 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 [6]. Therefrom, 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 [1].Extant research already proposes certifications and audits as detective controls and good means to assess quality and performance of IT services in procurement processes [2, 4, 14]. A certification is defined as a third party attestation of products, processes, systems, or persons that verifies conformity to specified criteria [15]. Several CSC (e.g., *CSA STAR*) and cloud certification schemes in particular (e.g., *ISO 27017*) 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 in-crease trustworthiness of CSC [6, 16, 17].

Continuous auditing is defined as a methodology that enables independent auditors to provide written assurance on a subject matter, using a series of auditors' reports issued virtually simultaneously with, or a short period of time after, the occurrence of events underlying the subject matter [18]. Thus, CA enables auditors to immediately re-act to changes or events concerning the subject matter and to adjust their auditing reports based on assessment of these changes and events.

## Disadvantages of existing System

1. Long validity periods may put in doubt reliability of issued certifications.
2. Data Integrity.

## 3. Proposed System

In MultiCloud environment, remote data integrity checking is required to secure user's data. User will upload file to Cloud. This file is split into blocks using Dynamic Block generation Algorithm and stored in a Multi Cloud environment. File Allocation Table (FAT) File System has proper Indexing and Metadata's for the different Chunks of the Cloud Storage.Herethe auditor agrees to inspect logs, which are routinely 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. Cloud provides random blocks to Verifier for Integrity Checking which is to protect user privacy from Verifier (Third Party). File recovery is done by the Verifier automatically if the data gets corrupted during checking. Users can complaint cloud for file recovery.

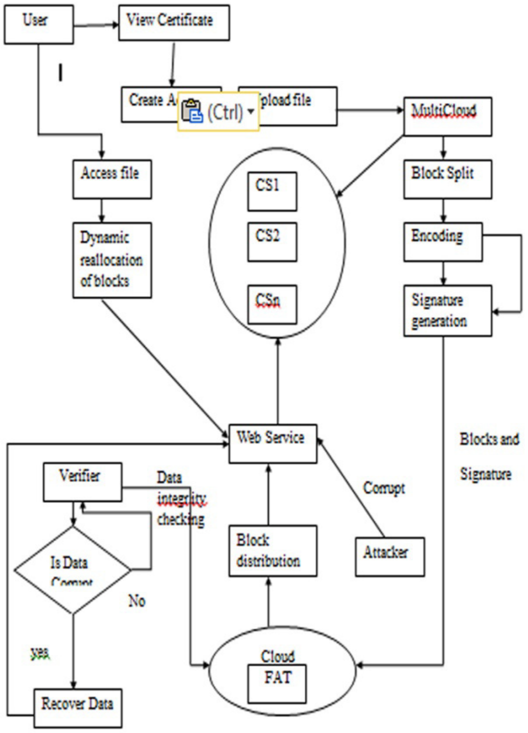


Fig.1 Overall System Architecture

## Modules

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

## 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 MultiCloud Storage. If the admin has to reconfigure the old MultiCloud 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.

## 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 split 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.

## Data Integrity Checking

FATFS has proper Indexing and Metadata's for the different Chunks of the Data that is being uploaded by User. 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.

## File Recovery and Certificate Generation

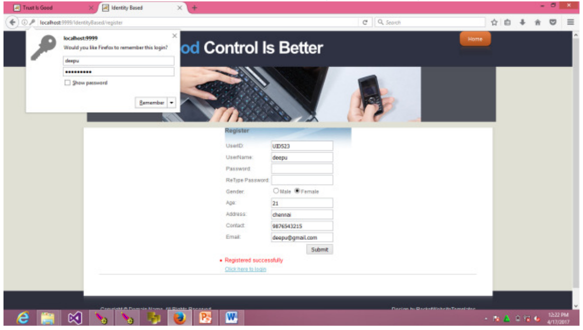
Attacker can corrupt data in any one of the cloud servers. On Data Integrity Checking done by the Verifier, Verifier informs Corrupted blocks to the Cloud. Recovery Process will be done by the verifier automatically when data gets corrupted. User can complaint to the Cloud if the user file get corrupted (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 joins in the cloud they will read the certificate and then they can create an account in the cloud.

### Advantages of the proposed system

1. User data is split in multiple blocks.
2. Continuous auditing process helps the verifier to perform.
3. Users can complaint cloud for file recovery.

## 4. RESULTS

The proposed system is implemented in java. Frist we need to register with the user details as shown in the figure Fig.2.



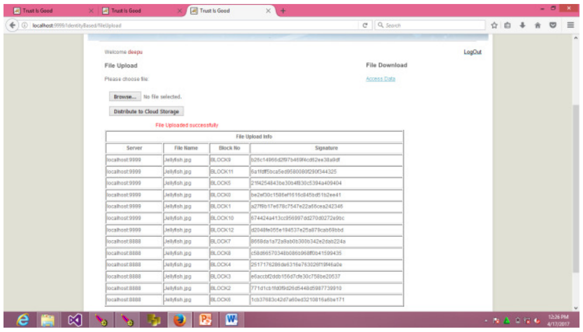
localhost:9999
Would you like Firefox to remember this login?
deepu
••••••••••
□ Show password

Register

| | |
|---|---|
| UserID: | UID523 |
| UserName: | deepu |
| Password: | |
| ReType Password: | |
| Gender: | ○ Male ● Female |
| Age: | 21 |
| Address: | chennai |
| Contact: | 9876543215 |
| Email: | deepu@gmail.com |

• Registered successfully
Click here to login

Fig.2 Registration Page


Trust Is Good
Trust Is Good
Trust Is Good
localhost:9999/IdentityBased/FileUpload
LogOut
Browse...
Distribute to Cloud Storage
Access Data

Welcome deepu

File Upload

Please choose file:

No file selected.

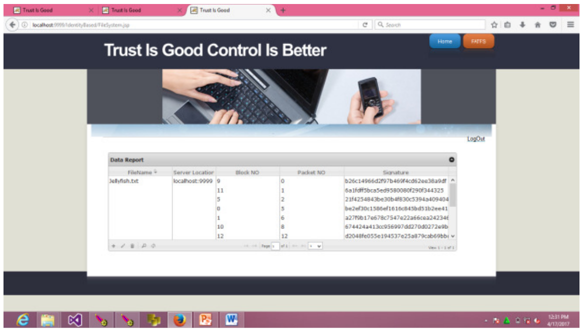
File Download

File Uploaded successfully

File Upload Info

| Server | File Name | Block No | Signature |
|---|---|---|---|
| localhost:9999 | Jellyfish.jpg | BLOCK9 | b26c14966d2f97b469f4cd62ee38a9df |
| localhost:9999 | Jellyfish.jpg | BLOCK11 | 6a1fdff5bca5ed9580080f290f344325 |
| localhost:9999 | Jellyfish.jpg | BLOCK5 | 21f4254843be30b4f830c5394a409404 |
| localhost:9999 | Jellyfish.jpg | BLOCK0 | be2ef30c1586ef1616c845bd51b2ee41 |
| localhost:9999 | Jellyfish.jpg | BLOCK1 | a27f9b17e678c7547e22a66cea242346 |
| localhost:9999 | Jellyfish.jpg | BLOCK10 | 674424a413cc956997dd270d0272e9bc |
| localhost:9999 | Jellyfish.jpg | BLOCK12 | d2048fe055e194537e25a879cab69bbd |
| localhost:8888 | Jellyfish.jpg | BLOCK7 | 8668da1a72a9ab0b300b342e2dab224a |
| localhost:8888 | Jellyfish.jpg | BLOCK8 | c58d66570348b086b968ff0b41599435 |
| localhost:8888 | Jellyfish.jpg | BLOCK4 | 2517176286de6316e763028f19f46a0e |
| localhost:8888 | Jellyfish.jpg | BLOCK3 | e6accbf2ddb156d7cfe30c758be20537 |
| localhost:8888 | Jellyfish.jpg | BLOCK2 | 771d1cb1fd0f9d26d5448d5987739910 |
| localhost:8888 | Jellyfish.jpg | BLOCK6 | 1cb37683c42d7a60ed3210816a6be171 |

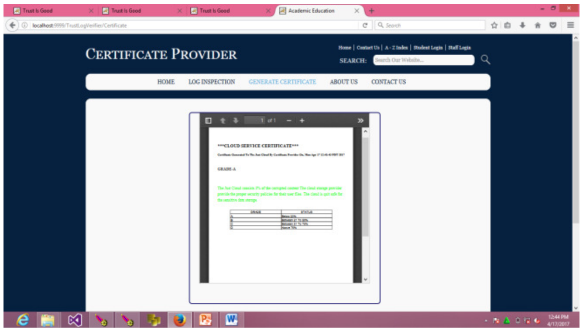
Fig.3 Data Upload and Block Split



Data Report

| FileName | Server Location | Block NO | Packet NO | Signature |
|---|---|---|---|---|
| Jellyfish.txt | localhost:9999 | 9 | 0 | b26c14966d2f97b469f4cd62ee38a9df |
| | | 11 | 1 | 6a1fdff5bca5ed9580080f290f344325 |
| | | 5 | 2 | 21f4254843be30b4f830c5394a409404 |
| | | 0 | 5 | be2ef30c1586ef1616c845bd51b2ee41 |
| | | 1 | 6 | a27f9b17e678c7547e22a66cea242346 |
| | | 10 | 8 | 674424a413cc956997dd270d0272e9b |
| | | 12 | 12 | d2048fe055e194537e25a879cab69bb |

Fig.4 Data integrity checking



***CLOUD SERVICE CERTIFICATE***

Certificate Generated To The Just Cloud By Certificate Provider On, Mon Apr 17 12:43:43 IST 2017

GRADE-A

The Just Cloud consists 0% of the corrupted content The cloud storage provider provide the proper security policies for their user files. The cloud is quit safe for the sensitive data storage

| GRADE | STATUS |
|---|---|
| A | Below 20% |
| B | Between 21 To 50% |
| C | Between 51 To 70% |
| D | Above 70% |

Fig.5 Certificate generation

## 5.CONCLUSION AND FUTURE ENHANCEMENT

The ever-changing cloud environment, fast update cycles, and the increasing adoption of business-critical applications from cloud service providers demand for highly reliable cloud services. Continuously auditing such cloud services can assure a high level of security and reliability to (potential) cloud service adopters. However, methodologies to efficiently and continuously audit cloud services are still in their infancy. With our study, a first step to increase trustworthiness of CSC is provided by conceptualizing architecture to continuously audit cloud services.

As the discussion of challengesreveals, there is still plenty of research to do. Further research should focus on developing auditing methodologiesadjusted to the CC context, especially concerning validation of security measures and adherence to critical cloud