Creating Secure Clouds by Continuous Auditing

Abhishek H V[1] Roshan Baig[2] Prashanth Kumar N[3] Vineet Kumar[4]
[1,2,3,4]Department of Computer Science & Engineering
[1,2,3,4]SVIT, Bangalore India

Abstract— Using cloud storage user can remotely store their data and enjoy on demand high quality application without the burden of local data storage and maintains cloud computing security or more simply cloud security refers to a broad set of policies, controls deployed to protect database attempts to assure high level of security and compliances but considering the fact cloud services are part of ever-changing environment multiyear validity periods may put in doubt reliability certifications. our research shows that criteria should be continuously audited most of exiting methodology are not applicable for third party auditing purposes therefore we propose conceptual ca architecture and process that have to implement we discuss benefits and challenges that have to be taken to diffuse the concept of continuous cloud service auditing.

Key words: Cloud Computing, Security, CA, CSC

I. 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 still hesitant 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. 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. 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.

Researchers recently proposed the means to enable third party authorities to audit data integrity, data location compliance, and changes of cloud infrastructure among others.

We focus on the following objectives within this study:

1) Which CSC criteria should be continuously audited?
2) Which CA methodologies exist and are applicable in the context of continuous cloud service auditing?
3) How can methodologies be linked together to form an architectecture.
4) Architecture which enables CA?

Finally, our conceptual architecture highlights important components (i.e., various interfaces and auditing management modules) as well as processes that have to be implemented. We thereby con- tribute to practice and research in several ways:

- We support cloud auditors to classify whether or not a high frequency auditing of their CSC criteria is required. Further on, we illustrate methodologies which can be used by auditors to perform (external) auditing of cloud services as well as by cloud service providers to set up an internal auditing department.
- We transfer the concept of CA in a new context, pro- vide means and foundations for further research, and demonstrated benefits, challenges, and limitations of CA of cloud services.
- By providing a first conceptual architecture, we want to encourage auditors and cloud service providers to implement CA techniques, consequently creating trustworthy certifications and services.

II. LITERATURE SURVEY

In the last few years, cloud computing has grown from being a promising business concept to one of the fast growing segments of the IT industry. But as more and more information on individuals and companies are placed in the cloud, concerns are beginning to grow about just how safe an environment it is. Despite of all the hype surrounding the cloud, enterprise customers are still reluctant to deploy their business in the cloud. Security is one of the major issues which reduces the growth of cloud computing and complications with data privacy and data protection continue to plague the market. The advent of an advanced model should not negotiate with the required functionalities and capabilities present in the current model. A new model targeting at improving features of an existing model must not risk or threaten other important features of the current model. The architecture of cloud poses such a threat to the security of the existing technologies when deployed in a cloud environment. In this paper, a survey of the different security risks that pose a threat to the cloud is presented. This paper is a survey more specific to the different security issues that has emanated due to the nature of the service delivery models of a cloud computing system.

A. Continuous Auditing Criteria

Existing CSC represent only a retrospective look at the fulfillment of technical and organizational measures at the time of their issuing. CSC criteria may no longer be met throughout certification validity periods. Current CSC are facing several drawbacks when assuring ongoing certification adherence, including:

1) Inherent cloud computing characteristics

Cloud services are part of an ever-changing environment, resulting from inherent CC characteristics, like on-demand pro-visioning and entangled supply chains. Furthermore, cloud services are characterized by fast technology life cycles compared to other industries.

2) Ongoing architectural changes

Hardware or software configuration changes as well as changing sub service providers might lead to certification violations or security vulnerabilities. Environmental threats.

Changes in the CC and IT environment, for example emergence of new vulnerabilities, require providers to adapt their services to cope with emerging challenges. Major security incidents may threaten the service or reveal harmful vulnerabilities, which in turn void a certification.

3) Changes in legal and regulatory landscape.

The legal and regulatory landscape of cloud services is highly dynamic since existing laws are currently adjusted, and new laws are being proposed to cope with challenges resulting from the digital transformation of society and continuous changes in IT. Just recently, the Safe Harbor data sharing agreement between the European Union and the United States was questioned. These dynamics might change responsibilities of both cloud service customers and providers as well as require certification criteria to be successively updated.

4) Deliberate discontinuance.

A cloud service provider might deliberately discontinue adherence to CSC criteria

III. SYSTEM DESIGN

A. Modules

– Cloud service provider
– Continuous auditing
– Cloud service customer

1) Cloud Service Provider

Providers have already equipped their service centers with sophisticated monitoring technologies to gather service data and quickly detect malicious attacks, failures, and outages. Leveraging collected data for the purpose of CA as well is beneficial. Yet, participating in CA requires providers to use comprehensive (continuous) monitoring systems to ensure that all audit-relevant data is up-to-date, accurate, and available.

2) Continuous Auditing

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 is-sued virtually simultaneously with, or a short period of time after, the occurrence of events underlying the subject matter. 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.

3) Cloud Service Customer

Cloud service customers confirm that especially criteria ensuring service availability, data integrity and location, a secure access management, and data encryption should be continuously audited.

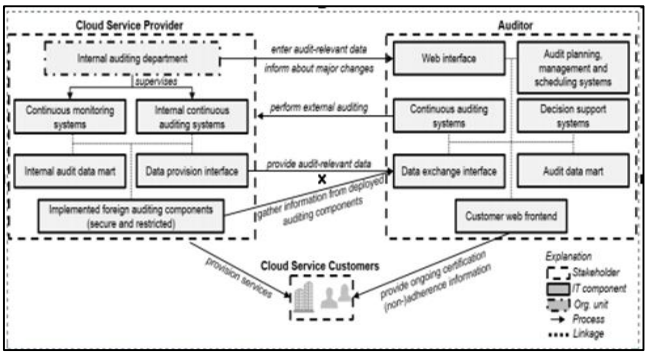

Fig. 1: Conceptual Architecture

IV. IMPLEMENTATION

A. Admin Page

First, admin login with valid user name and password. Here admin provides and update the space according to the customer requirement.

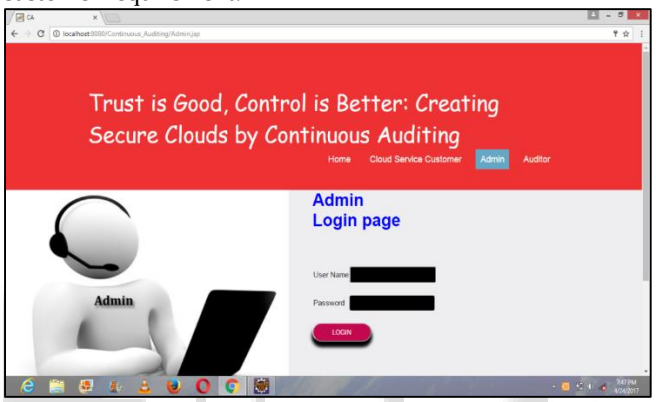

Fig. 2: Admin login page

B. Customer Page

Here customer login with valid username and password. User can upload file or download file to the server provided by the cloud service provider.

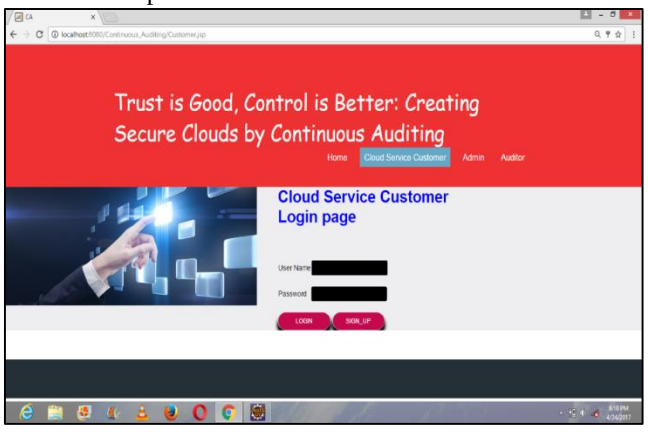

Fig. 3: Customer Login Page

1) Auditor Page

Here auditor login, auditor activates the valid user and file respectively.

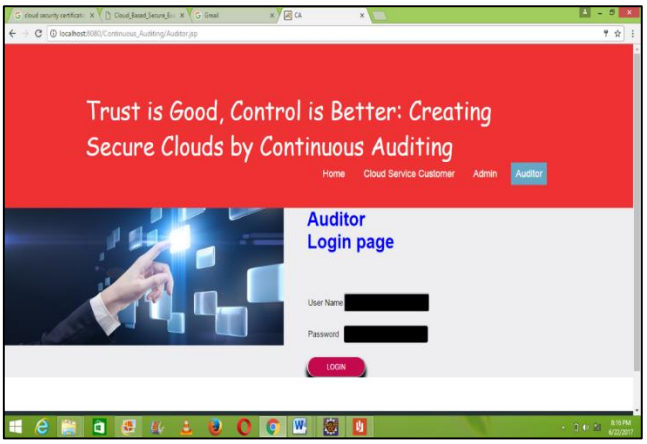

Fig. 4: Auditor Login Page

C. Once user logins to upload or download he/she receives an alert through mail (OTP)

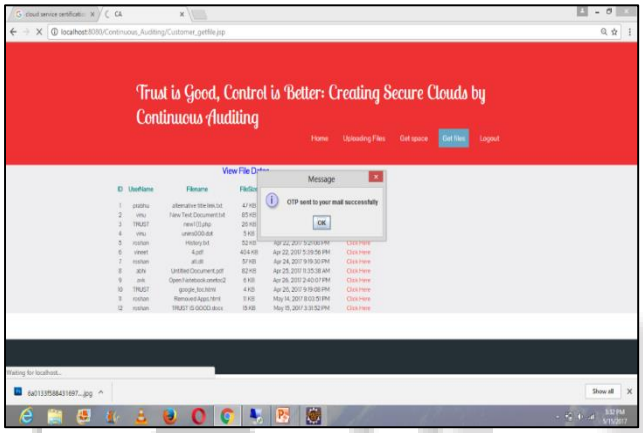

Fig. 5: File uploading and downloading

D. Web interface to enter OTP

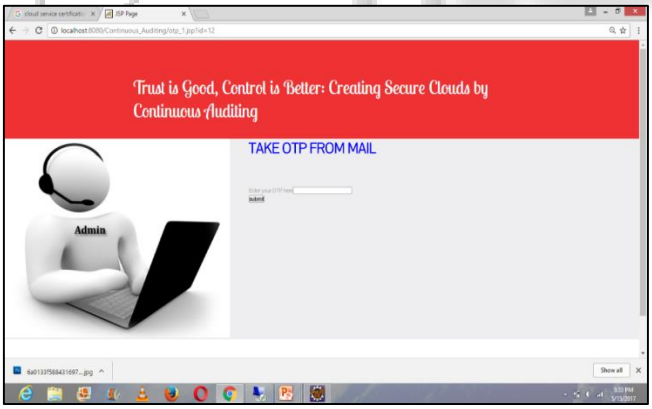

Fig. 6: Enter otp

V. TEST CASE

A. Test case for Admin

Test case id/input	Expected output	Result
TC1: Enter Username & password	Admin has to login	Invalid UserName and Password
TC2: Enter Username only	Display message saying Fields are Empty	Message displayed stating that Fields are Empty
TC3: Enter Valid UserName and Password	Admin has to login	Admin logged in Inappropriate data notification
TC4: Upload data	Data has to be stored	Data stored to database

Table 1: Test case for admin

B. Test case for Customer

Test case id/input	Expected output	Result
TC1: Enter Username & password	Customer has to login	Invalid UserName and Password
TC2: Enter Username only	Display message saying Fields are Empty	Message displayed stating that Fields are Empty
TC3: Enter Valid UserName and Password	customer has to login	Customer logged in
TC4: Upload file	File has to be Uploaded	Data stored to database
TC5:Upload User Activated File	File has to be Uploaded	User Not Activated
TC6:Download File		User Not Activated
TC7:File Activated		File Downloaded

Table 2: Test case for Customer

C. Test case for Auditor

Test case ID/ Input	Expected output	Result
TC1:Enter Username & password	Auditor has to login	Invalid UserName and Password
TC2:Enter Username only	Display message saying Fields are Empty	Message displayed stating that Fields are Empty
TC3:Enter Valid UserName and Password	Auditor has to login Activated	Auditor logged in
TC4:User and File Activate	File and User has to Activate	No Request File and User Activated

Table 3: Test case for auditor

D. Advantage

- It assures high level of security and reliability.
- By providing a first conceptual architecture, we want to encourage auditors and cloud service providers to implement CA techniques, consequently creating trustworthy certifications and services.

E. Disadvantage

- It makes hectic for the user to enter the otp
- Every time when user upload or download the file.

VI. CONCLUSION

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 an architecture to continuously audit cloud services.

REFERENCES

[1] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", J Netw Compute App, vol. 34, no. 1, pp. 1–11, 2011.
[2] K. M. Khan and Q. Malluhi, "Trust in Cloud Services: Providing More Controls to Clients", Computer, vol. 46, no. 7, pp. 94– 96, 2013.
[3] S. Schneider and A. Sunyaev, "Determinant factors of cloudsourcing decisions", Journal of Information Technology, 2014.
[4] A. Sunyaev and S. Schneider, "Cloud services certification", Commun ACM, vol. 56, no. 2, pp. 33–36, 2013.
[5] S. Cimato, E. Damiani, R. Menicocci, and F. Zavatarelli, "Towards the certification of cloud services", in Proc. SERVICES, Santa Clara, California, USA, 2013, pp. 100–105.
[6] I. Windhorst and A. Sunyaev, "Dynamic certification of cloud services", in Proc. ARES, Regensburg, Germany, 2013.

