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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

Trust and Reliability Control by Continuous Auditing: Ensuring Cloud Security

Nagorav Kolhe, Harshad Khanekar, Vishal Jawadwar, Priyanka Dhere, Prof. Moholkar K.P.

Department of Computer Engineering, JSPM's Rajashri Shahu College of Engineering, Tathawade, Pune, India

ABSTRACT: In the cloud computing context, trust is based on several factors such as reputation, reliance, degree of control, scope of influence, and predictability. It means you can rely on something to behave or deliver as expected. In particular, control influences trust significantly: how much control a client holds in a service that processes and stores valuable data assets affects how much trust that client has in the provider. "Control" implies that, the client is in the owner of data and decides what exactly to protect. Cloud service certifications (CSC) are used to attempt reliability of any service provider and gaining customers trust. The paper presents a model for continuous auditing (CA) of selected certification criteria which make cloud service reliable and secure cloud services, and increases trustworthiness of certifications. Such auditing of cloud certification is carried out depends on criteria's. Like literature review, interviews, and workshops with practitioners to conceptualize architecture for continuous cloud service auditing.

KEYWORDS: Certification, cloud computing, continuous auditing, security.

I. INTRODUCTION

Cloud computing is emerging technology which enables universal, adoptable, on demand access to shared data. Cloud increases its storage capacity and decreases the cost of processing. During the process of data outsourcing cloud service certification provides guarantee of high level security measures as well as the better solution for upcoming complications and gives security assurance to customer [9], [10]. Many customers' select service providers with cloud service certification. But service providers are not fully trusted; they are semi-trusted [5]. They may behave dishonestly and can misuse or alter customer's private data. Continuous auditing of certificates provided to service provider is required to assure reliability of services provided by cloud and to ensure security in cloud which can increase trustworthiness of certifications.

The third party auditing strategies for auditors and providers, linked together in a conceptual architecture to diffuse the concept of continuous cloud service auditing. The paper presents an online continuous auditing of cloud certificates by applying some criteria's from customer prospective to store data securely on cloud and to have control over these data to protect important data. For instance, auditing as a service in the context of cloud. Continuous auditing is a process that enables independent auditor to provide trust in cloud and continuously checking the reliability of all certificates provided to service providers in short period of time after existence of the events hidden in subject matter. Such auditing of cloud certification is carried out by some criteria's. Like customers review, ratings key policies, data integrity to conceptualize architecture for continuous cloud service auditing [7], [8]. Cloud service certifications (CSC) criteria have to audit continuously, to identify the reliability of certificates and service quality cloud. A continuous auditing (CA) technique enables CSP with reasonable trustworthy certifications and services. Continuous auditing from which cloud can assures high level of security as well as reliability to CSP.

Objective and Goal:

Cloud service certification assures high level trust among user but, such long validity periods may put in doubt reliability of issued certifications. CSC criteria may no longer be met throughout these periods, for instance, due to configuration changes or major security incidents. Thus, continuous auditing (CA) of certification criteria is required for:

- To check the reliability of Cloud Service Provider and to provide more trustworthiness.
- To provide the security and integrity to user's data.

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

- Detection of dishonest behavior of service provider.
- Managing Cloud Service Certification validity period and its quality of service.
- To assure transparent, continuously reliable, and secure cloud services.

II. LITERATURE SURVEY

P. Stephanow, C. Banse, and J. Schütte, "Generating Threat Profiles for Cloud Service Certification Systems", in *17th IEEE High Assurance Systems Engineering Symposium (HASE)*, 2016.
Authors propose a method to model different architecture variants of cloud service certification systems and analyze threats these systems face. By applying our method to a specific cloud service certification system, authors show how threats to such systems can be derived in a standardized way that allows us to evaluate different architecture configurations.

P. Stephanow and N. Fallenbeck, "Towards continuous certification of Infrastructure-as-a-service using low-level metrics", in *Proc. ATC*, Beijing, China, 2015.
Continuous cloud service certification describes the process of continuously validating whether a service adheres to a set of requirements. However, most requirements derived from existing standards such as ISO-27001:2013 are generic, often times inherently ambiguous and thus cannot be validated automatically. In this paper, authors address this gap by presenting a bottom-up approach using low-level metrics available through widely deployed implementations of infrastructure-as-a-service (IaaS) components. They further present examples how these low-level metrics can serve to construct complex metrics to support validation of generic requirements.

P. Stephanow and M. Gall, "Language Classes for Cloud Service Certification Systems", in *2015 IEEE 11th World Congress on Services (SERVICES)*, 2015.
Certification of cloud services aims at increasing the trust of customers towards cloud services and providing comparability between cloud services. Applying the concept of certification to cloud services requires systems which continuously detect ongoing changes of the service and assess their impact on customer requirements. In this paper, authors propose eight language classes for cloud service certification systems to facilitate research in design and implementation of these systems.

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.
Authors focus on the definition of a unifying meta-model to provide representational guidelines for (i) the definition of the security properties to be certified, (ii) the types of evidence underlying them, (iii) the phases of the certificate life cycle, as well as of all mechanisms for generating supporting evidence.

Windhorst and A. Sunyaev, "Dynamic certification of cloud services", in *Proc. ARES*, Regensburg, Germany, 2013.
Authors proposed dynamic certification approach which adopts the common certification process to the increased flexibility and dynamics of cloud computing environments through using of automation potential of security controls and continuous proof of the certification status. Dynamic certification is based on a new semi-automated certification process and the continuous monitoring of critical parameters of cloud services.

Singh, P. J. Best, M. Bojilov, and C. Blunt, "Continuous auditing and continuous monitoring in ERP environments", *Inf. Syst. J*,vol. 28, no. 1, pp. 287–310, 2013.
The need for continuous auditing and continuous monitoring (CA/CM) has increased in the global digital economy. Modern computer-based systems make it possible to measure and monitor business processes at an unprecedented level of detail in a real- or near real-time basis. This empowers auditors to become increasingly dependent on computer technology and software tools. While there is a growing body of literature related to this domain, there is a need for empirical evidence from actual implementations that document these systems in detail. In this research, authors perform such an investigation on three CA/CM systems, namely SAPSECURE, CAMAP, and Bagheera-S.

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing", *IEEE Trans. Parallel Distrib. Syst,*vol. 24, no. 9, pp. 1717–1726, 2013.
In this paper, authors first design an auditing framework for cloud storage systems and propose an efficient and privacy-preserving auditing protocol. Then, they extend this auditing protocol to support the data dynamic operations, which is efficient and provably secure in the random oracle model.

C. Liu, J. Chen, L. Yang, X. Zhang, C. Yang, R. Ranjan, and K. Ramamohanarao, "Authorized public auditing of dynamic big data storage on cloud with efficient verifiable fine grained updates", *IEEE Trans. Parallel Distrib. Syst,*vol. 25, no. 9, 2013.
In this paper, authors provide a formal analysis for possible types of fine-grained data updates and propose a scheme that can fully support authorized auditing and fine-grained update requests. Based on our scheme, they also propose an enhancement that can dramatically reduce communication overheads for verifying small updates.

Kuhn Jr, John R. and S. G. Sutton, "Continuous auditing in ERP system environments", *Inf. Syst. J,*vol. 24, no. 1, pp. 91–112, 2010.
In this paper, authors explore the alternative architectures for continuous auditing that have been proposed in both the research and practice environments. They blend a focus on the practical realities of the current technological options and ERP structures with the emerging theory and research on continuous assurance models. The focus is on identifying the strengths and weaknesses of each architectural form as a basis for forming a research agenda that could allow researchers to contribute to the future evolution of both ERP system designs and auditor implementation strategies.

G. Alles, A. Kogan, and M. A. Vasarhelyi, "Audit automation for implementing continuous auditing", 2008.
In this paper, not only must audit automation be undertaken systematically, it also has to incorporate reengineering in the more limited sense of first transforming manual audit processes to facilitate their automation. This is not full blown reengineering of the clean sheet sort, but this hybrid approach is one that is more manageable—and marketable— from a change management perspective, and more likely to lead to a positive outcome.

III. SOFTWARE REQUIREMENT SPECIFICATION

Software Requirements

- Operating System - Windows XP/7
- Programming Language - Java/J2EE
- Software Version - JDK 1.7 or above
- Tools - Eclipse
- Front End - JSP
- Database - Mysql

Hardware Requirements

- Processor - Pentium IV/Intel I3 core
- Speed - 1.1 GHz
- RAM - 512 MB (min)
- Hard Disk - 20GB
- Keyboard - Standard Keyboard
- Mouse - Two or Three Button Mouse
- Monitor - LED Monitor

IV. COMPARISON BETWEEN EXISTING SYSTEM AND PROPOSED SYSTEM

Disadvantage of Existing System

1) Not much reliable and less secure.
2) Not accurate cloud certification auditing criteria's are provided.

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

3) Multi-year-validity period creates the reliability issues.

Advantages of proposed system:

1) Provides Trustworthiness.
2) Provide Security and integrity to user's data.
3) The multiyear validity issue of cloud service certificates is handled by continuous auditing.
4) User can control way to protection of data stored on cloud.
5) More accurate and easy criteria's are applied for auditing.

V. ALGORITHM FOR RELEVANT FEATURE DISCOVERY

- Secrete Key Generation Algorithm
- AES Encryption Algorithm
- AES Decryption Algorithm

VI. SYSTEM ARCHITECTURE

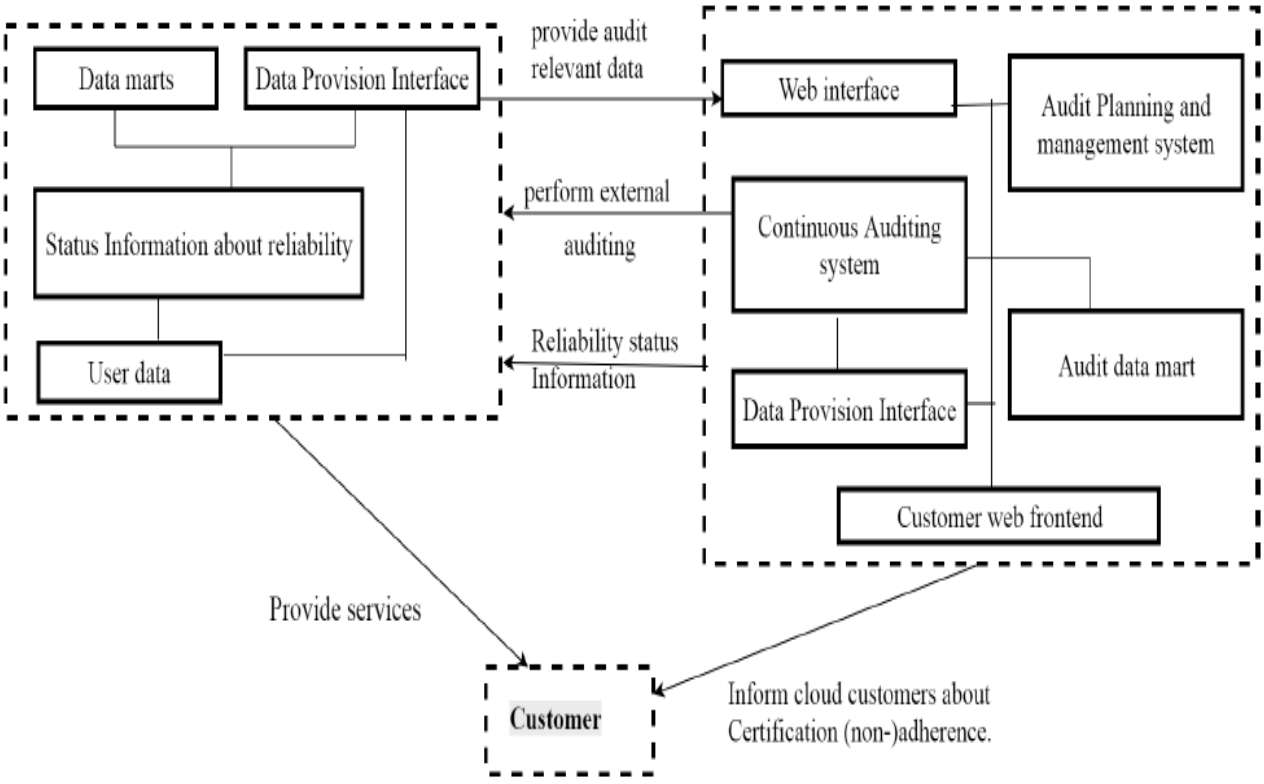

Figure 1: System Architecture

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

VII. EXPERIMENTAL SET UP AND RESULT TABLE

1. Result Table

File Id	File Length (Kilobytes)	Time(ms)
1	118.784	300
2	118.668	190
3	118.54	120
4	335.777	250
5	270.938	800
6	10.308	60

Table 1: File Downloading Time

Above table shows that time required for merging all fragments related to a file and downloads the particular file.

2. Result Graph

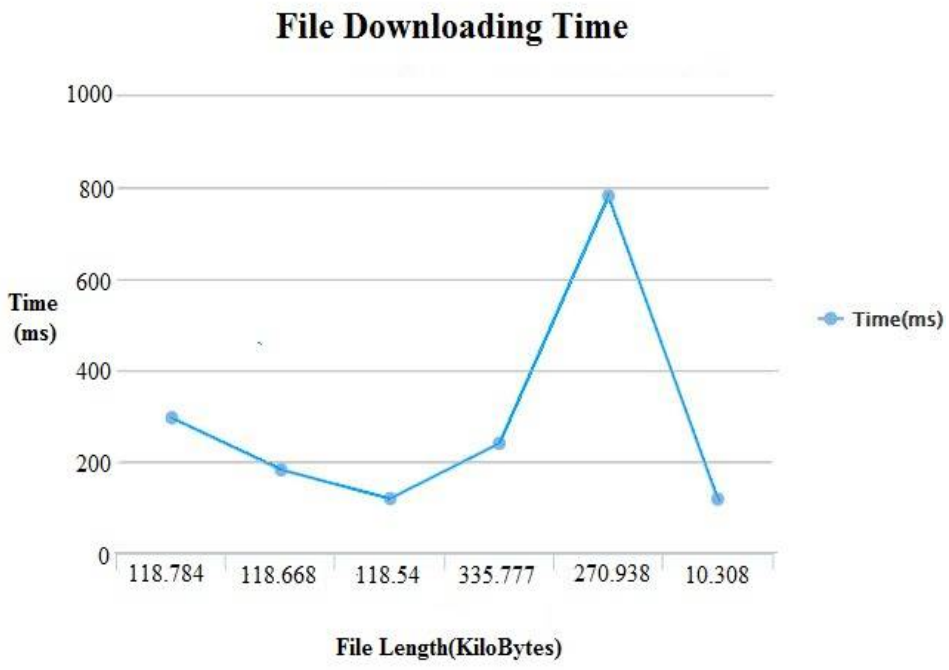

Figure 2: Result Graph of File Downloading Time

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

The above figure shows the graph of file downloading time and of proposed system. Our result shows the minimum time required to download the file as compare to other state-of-art systems.

VIII. 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 of cloud services can assure a high level of security and reliability to (potential) cloud service adopters. However, a methodology employed for efficiently and continuously auditing cloud services are still in their infancy. With our study, a first step to increase trustworthiness of cloud service certifications (CSC) is provided by conceptualizing architecture to continuously audit cloud services.

REFERENCES

[1] P. Stephanow, C. Banse, and J. Schütte, “Generating Threat Profiles for Cloud Service Certification Systems”, in *17th IEEE High Assurance Systems Engineering Symposium (HASE)*, 2016.
[2] P. Stephanow and N. Fallenbeck, “Towards continuous certification of Infrastructure-as-a-service using low-level metrics”, in *Proc. ATC*, Beijing, China, 2015.
[3] P. Stephanow and M. Gall, “Language Classes for Cloud Service Certification Systems”, in *2015 IEEE 11th World Congress on Services (SERVICES)*, 2015.
[4] K. M. Khan and Q. Malluhi, "Trust in Cloud Services: Providing More Controls to Clients", *Computer*, vol. 46, no. 7, pp. 94–96, 2013.
[5] A. Sunyaev and S. Schneider, "Cloud services certification", *Commun ACM*, vol. 56, no. 2, pp. 33–36, 2013.
[6] 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.
[7] Windhorst and A. Sunyaev, “Dynamic certification of cloud services”, in *Proc. ARES*, Regensburg, Germany, 2013.
[8] Singh, P. J. Best, M. Bojilov, and C. Blunt, "Continuous auditing and continuous monitoring in ERP environments", *Inf. Syst. J*,vol. 28, no. 1, pp. 287–310, 2013.
[9] M. Jans, M. Alles, and M. Vasarhelyi, "The case for process mining in auditing", *Methodologies in AIS Research*, vol. 14, no. 1, pp. 1–20, 2013.
[10] Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing", *IEEE Trans. Parallel Distrib. Syst*,vol. 24, no. 9, pp. 1717–1726, 2013.
[11] C. Liu, J. Chen, L. Yang, X. Zhang, C. Yang, R. Ranjan, and K. Ramamohanarao, "Authorized public auditing of dynamic big data storage on cloud with efficient verifiable fine grained updates", *IEEE Trans. Parallel Distrib. Syst*,vol. 25, no. 9, 2013.
[12] Kuhn Jr, John R. and S. G. Sutton, "Continuous auditing in ERP system environments", *Inf. Syst. J*,vol. 24, no. 1, pp. 91–112, 2010.
[13] G. Alles, A. Kogan, and M. A. Vasarhelyi, “Audit automation for implementing continuous auditing”, 2008.
[14] Y. Chen, "Continuous auditing using a strategic systems approach", *Internal Auditing*, vol. 19, no. 3, pp. 31–36, 2004.