A Review on Continuous Public Auditing Scheme for Regenerating Code Based Secure Cloud Storage

[1]R.N.Boob, [2]Prof. S.M.Rokade
[1]PG student, [2]Head of Department
[1]Computer Engineering Department, SVIT, Chincholi, Sinner, Nashik, India

***Abstract* - 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. The continuous auditing of selected certification criteria is required to assure continuously reliable and secure cloud services 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. From this work we have to encourage auditors to implement CA techniques to create trustworthy certifications as well as practitioners to develop business models, for instance, auditing as a service in the context of cloud. For better and efficient auditing, proxy can be introduced for regenerating code based cloud storage.**

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

I.INTRODUCTION

In this modern era, many large organization, business firms and even individual person outsourced their data to the cloud to avoid the hectic task of data management. Cloud provides the beneficial features for end user i.e. low storage cost, increasing capacity. Many business and applications processes get extra financial benefits as cloud permits them for pay-per-use mechanism. Cloud assures high level of security service while storing customer's data. As every-one is aware of ever changing environment of cloud also multi-year validity periods may arises the service reliability issues. Due the concerns of security, privacy and reliability organizations unsure to utilize cloud services. Initial step of CSC i.e. cloud service certification is good to addressed these issues by establishing trust and increasing the clarity of cloud market. There is multiple of CSC evolved like CSA STAR or EuroCloud star Audit. These give the assurance of high level of security, reliability and legal concurrences for validity period of one to three years. Due to configuration changes or major security issues previously defined CSC criteria may no longer be met over all these periods.
Cloud computing faces many challenging issues which storing and managing user's data in it. These issues are accessibility, liability, privacy and control issues related to data confidentiality and privacy. Therefore, continuous auditing for cloud certification is required to established trustworthy CSC after initial certification process get completed. To construct a bridge between conceptualizing architecture for continuous auditing of cloud services CSC criteria should be continuously audited. Further, how to these criteria can be increasing audited to identify main auditing component which get evaluated. In trustworthiness of CSP, CA required dealing with the ever-changing cloud environment. In 1980's C. L.-y. Chou et al[35], developed different computer based tools of auditing as well as technology which supports the CA.
Continuous auditing is a process that enables independent auditor to provide declaration on subject matter using the sequence of audit report issued in short period of time after existence of the events hidden in subject matter. Therefore, CA approves auditor to react to modify events with respect to the subject matter to adjust their auditing reports. CSC criteria have to audit continuously, to identify which kind of CA mechanism is applicable for continuous cloud service auditing and finally how to integrate methodologies to build architecture that enables CA. CA is transfer to the new concept for further more research to demonstrate benefits, issues, disadvantages and limitations etc. of CA of cloud services. A 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. Trustworthiness of CSC is provided by gestate architecture for continuously audit cloud services. Certain limitations have been addressed in this paper such as, within this CA architecture there does not exist any kind of technical implementations. Another limitation is an unavailability of security validations and scalability of services. CA can incorporate with the various text, data and mining process that performed on daily basis for audit evidence extraction.

II. RELATED WORK

P. Stephanow, M. Gall [1], introduced language classes for cloud service certification to facilitate the research in design and implementation of CA systems. They have used language classes developed for signature based intrusion detection systems and applied them to cloud service certification systems. Author did detailed study of similarities between signatures based IDS and cloud service certification translated to reusable concepts for certification system. Furthermore, they derived six languages classes such as, event, response, and reporting, correlation, and detection policy as well as detection mechanism. Furthermore, six language

classes were derived (event, response, reporting, correlation, detection (policy), as well as detection (mechanism)) whose concepts are applicable to cloud service certification, and another two classes (cloud service description, certification model description) are proposed to address remaining classes of the conceptual model introduced by Cimato et al.

Philipp Stephanow, Niels Fallenbeck [2], proposed a bottom-up approach which uses low-level metrics available through widely delivered implementation of IaaS. This metrics support validation of universal requirements from previous certificates such as, CSA STAR and ECSA etc. it is corresponds to complex metrics construction. In their future work they defined to construct complex metrics similar to existing certificate requirements. This term can be used for continuous certification. In future work author planned to evaluate our activities with industry partners participating in NGCert.

Authors M. Alles, G. Brennan [3], identified the management of audit alarms and the prevention of alarms floods as it is critical task in CMBPS implementation process. In this paper they construct an approach to solve the problem of implementation of hierarchical structure of alarms. In this paper, only diverse practical experience will provide the facts necessary for identifying trade-offs between effectiveness, efficiency and timeliness of audit procedures and determining how to make CMBPC implementations worthwhile.

J. Woodroof and D. Searcy [4], proposed a novel technique for continuous audit implications. Electronic Data Interchange (EDI) brought a significant efficiencies and reductions in cost to supply chains. A leading web application known as, "Cold fusion" is utilized to design and demonstrated a system that uses agents and alarm triggers that sent over internet to sequentially to observe actual values of clients variable. In this paper, stringent criteria must require a web based CA system to be feasible.

Shams Zawoad, A.K. Dutta et al.[5], introduced Secure-Logging-as-a-Service (SecLaaS) system. It stores virtual machine's logs and provides access to forensic investigators by ensuring the confidentiality of cloud users. This system preserves the proofs of previous logs therefore; it can protect the integrity of logs from dishonest investigators. In this paper, author evaluates the feasibility of the scheme by implementing SecLaas for network access logs in open stack.

J. Ramya Rajalakshmi, M.Rathinraj, et al.[6], proposed homomorphic encryption scheme to identify the challenges for secure cloud-based management. The process of anonymization is used to remove or replaces the identity information from communication or record. This communication and records may be pseudonymous that same subject always have the replacement identity but it cannot be identified as seperatly.In future work they were planning to evaluate the performance overhead using alternative option such as, pair of partial homorphic algorithm. Also performance of system planned to calculate using anonymzing networks like, Ultra surf, Freegate etc.

H. Ye, Y. He. [7], proposed a continuous auditing model that utilizes web service technology. It leverages the power of XML and their related technologies. XML and web services can be utilized for the process of CA. XML web services include SOAP, WSDL, UDDI protocols those are discussed in this paper. Web services technology stay in auditee's accounting system.

In future research work author looks towards a security mechanism. It automatically audit new risks faced in providing on-demand, real-time assurance.

Stephan Schneider, Ali Sunyaev [8] concentrating on CC and ITO context. To identify determinant factors of sourcing decision in CC context they were concentrating on rich body of research on ITO. In this paper, authors inherits then set of determinant factors of cloud sourcing.

John R. Kuhn, Jr.[9][10], proposed a continuous auditing ERP system. Development in ERP system provides critical infrastructure which required for effective evaluation of the assurance functions from periodic event to ongoing process through the merging of auditing process. An embedded auditing methodology is developed for combining continuous auditing functionality internally.

Author Carol E. Brown, Jeffrey A. Wong and Amelia A. Baldwin [11], introduced Continuous auditing is based on multiple research streams. They state that is made in this paper is that continuous auditing requires more than changes in hardware and software, it requires changes in the control environment and in the behavior of management and auditors. Vasarhelyi and Halper (1991) outline the key concepts and components of a continuous process auditing system.

N. Mahzan[12], discussed about the use of computer-assisted audit techniques and tools (CAATTs) is a part of many professionally recommended audit procedures. This paper aims to argue that obtaining a better understanding of the factors underlying successful CAATTs adoptions would be helpful to aid wider development of these technologies in internal audit functions. In this paper author explores the successful adoption of GAS in ten cases to draw out the general factors that appear to be essential elements that lead to successful adoptions. From this basis, the paper proposes an initial model, built on existing theories of IT adoption more generally, as a theoretical basis for GAS adoption by decision-makers in an internal audit setting to better understand what may be essential factors to their adoption decisions to be likewise successful. Results suggest that two constructs from UTAUT (performance expectancy and facilitating conditions) appear to be particularly important factors influencing successful adoptions of GAS in this domain.

R. Nithiavathy [13], proposed rCloud computing technique. It gains the promotion in I.T. cloud computing world. It considered as the second thing after internet. They have proposed a mechanism of distributed integrity auditing that utilises homomorphic token and erasure coded data for dynamically storing data. It allows TPA to audit cloud storage at very low computation cost. An efficient and dynamic operations i.e. update & delete are provided on block of data. Byzantine failure, malicious data modification attack, and even server colluding attacks the proposed technique is highly efficient and resilient. They to aim to achieve the goals like: Storage accuracy, data error in fast localisation and dynamic data support, lightweight etc. The proposed scheme accomplishes the integration of correctness of storage and corruption of data. For auditing procedure TPA allows cloud storage without expecting probability and time.

K. Yang, et al. [14], proposed efficient and privacy preserving protocol of auditing. It supports to data dynamic operations. They have extended their work to support batch auditing. The proposd approach generates the proof to solve the problem of data privacy. The proof is generated with challenge stamp and it utilises the bilinear property such that auditor can only verify the correctness of

proof without decrypting it. At the time of batch auditing process for multiple clouds proposed method does not required trusted orgniser. The generated proof is serve as intermediate value of verification. In the process of auditing protocal containts the two-way communication such as : challenge and proof.
S. Lins, et al [15], enables data auditor to verify integrity of data, complicance in data and the dynamic infrastructure of cloud. To address the gap between continuous auditing a conceptualise architecture of CA has been introduced. It supports data auditor to to classify whether or not a high frequency auditing of their CSC criteria is needed. From the proposed approach CA, high level security as well as realiability is achieve in the cloud environment. But the methodologies to efficiently and continuously audit cloud services are remains immatur.

III. PROBLEM DEFINITION

Continuous auditing of cloud services is an infancy task. Due to legal requirements third party auditor has limited access to data as well as system. Hence to develop such system that enables reliable cloud services to cloud customer and also to solve the regeneration problem.

IV. SYSTEM ARCHITECTURE

Following Figure 1 represents the system architecture.

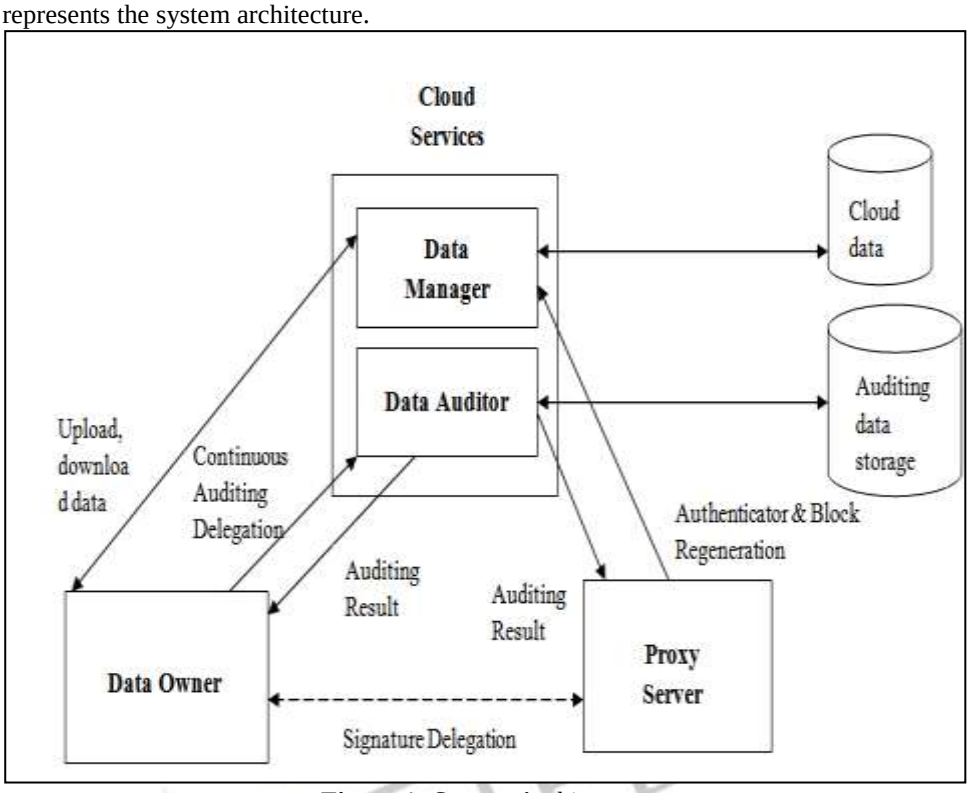

Figure 1: System Architecture

The proposed method can be implemented in following sequence:

1. Key Generation
2. Delegation
3. Signature and Block generation
4. Auditing
5. Challenge and Proof generation
6. Verification
7. Repair
8. Block and Signature ReGeneration

V. CONCLUSION

In this review paper, we did study of existing techniques of continuous auditing of cloud services. There are some limitations which we have been determined from section II. The limitations of existing system are, data dynamic updates, elegant verification of data, some difficulties and potential security problems etc. From overall literature survey there is need of efficient cloud service auditing system. According our analysis CA can be better solution to address the problem of cloud service auditing.

VI. ACKNOWLEDGMENT

This research was supported by SVIT clollege, chincoli, nashik. I would like to thank our project guide Prof. S. M. Rokade for their helpful assisistance for our proposed research work. Also I heartly thanks to principal of SVIT college, chincholi, Dr. S.A.Patil as well as other staff members of computer department for sharing their piece of advise with us during the course of this research.

REFERENCES

[1] P. Stephanow and M. Gall, “Language Classes for Cloud Service Certification Systems”, in 2015 IEEE 11th World Congress on Services (SERVICES), 2015.

[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] K. 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

[4] J. Woodroof and D. Searcy, “Continuous audit implications of internet technology”, in Proc. HICSS, Outrigger Wailea Resort, Island of Maui, 2001, pp. 1–8.

[5] S. Zawoad, A. K. Dutta, and R. Hasan, “SecLaaS”, in Proc. ASIA CCS, Hangzhou, China, 2013, pp. 219–230.

[6] J. R. Rajalakshmi, M. Rathinraj, and M. Braveen, “Anonymizing log management process for secure logging in the cloud”, in Proc. ICCPCT, India, 2014, pp. 1559–1564.

[7] U. S. Murthy and S. M. Groomer, "A continuous auditing web services model for XML-based accounting systems", International Journal of Accounting Information Systems, vol. 5, no. 2, 2004.

[8] A.Sunyaev and S. Schneider, "Cloud services certification", Commun ACM, vol. 56, no. 2, pp. 33–36, 2013.

[9] 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.

[10] K. 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.

[11] C. E. Brown, J. A. Wong, and A. A. Baldwin, "A review and analysis of the existing research streams in continuous auditing", Journal of Emerging Technologies in Accounting, vol. 4, no. 1, 2007.

[12] N. Mahzan and A. Lymer, "Examining the adoption of computer-assisted audit tools and techniques", Managerial Auditing Journal, vol. 29, no. 4, pp. 327–349, 2014.

[13] R. Nithiavathy, “Data integrity and data dynamics with secure storage service in cloud”, in Proc. PRIME, Salem, Germany, 2013

[14] K. 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.

[15] S. Lins ,S. Schneider, A. Sunyaev, "Trust is Good, Control is Better: Creating Secure Clouds by Continuous Auditing ", IEEE Trans. On cloud computing, vol. 27, no. 9, pp. 1717–1726, Jan 2016.