International Journal of Trend in Scientific Research and Development (IJTSRD)

International Open Access Journal

ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 3

Maintaining Secure Cloud by Continuous Auditing

M. Kanimozhi, A. Aishwarya, S. Triumal
Department of Computer Science and Engineering,
G.K.M. College of Engineering and Technology, Chennai, Tamil Nadu, India

ABSTRACT

Increases in cloud computing capacity, as well as decreases in the cost of processing, are moving at a fast pace. These patterns make it incumbent upon organizations to keep pace with changes in technology that significantly influence security. Cloud security auditing depends upon the environment, and the rapid growth of cloud computing is an important new context in world economics. The small price of entry, bandwidth, and processing power capability means that individuals and organizations of all sizes have more capacity and agility to exercise shifts in computation and to disrupt industry in cyberspace than more traditional domains of business economics worldwide. An analysis of prevalent cloud security issues and the utilization of cloud audit methods can mitigate security concerns. This verification methodology indicates how to use frameworks to review cloud service providers (CSPs). The key barrier to widespread uptake of cloud computing is the lack of trust in clouds by potential customers. While preventive controls for security and privacy are actively researched, there is still little focus on detective controls related to cloud accountability and auditability. The complexity resulting from large-scale virtualization and data distribution carried out in current clouds has revealed an urgent research agenda for cloud accountability, as has the shift in focus of customer concerns from servers to data.

Keywords: *trust in cloud computing, cloud service providers (CSPs), logging, auditability, accountability, data provenance, continuous auditing and monitoring, governance*

Introduction

Cloud computing is the term used to share the resources globally with less cost .we can also called as "IT ON DEMAND". It provides 3 varieties of services i.e., Infrastructure as a service (IaaS), Platform as a service (PaaS) and package as a service(SaaS)[3]. The ever cheaper and additional powerful processors, along with the software as a service (SaaS) computing design, square measure reworking knowledge centers into pools of computing service on a large scale. End users access the cloud based applications through the web browsers with internet connection. Moving knowledge to clouds makes more convenient and reduce to manage hardware complexities. Knowledge stored at clouds are maintained by Cloud service providers (CSP) with various incentives for different levels of services [2]. However it deletes the responsibility of local machines to maintain knowledge, there is a chance to lose information or it effects from external or internal attacks [1]. Our contribution can be summarized as the following three aspects:

1) Compared to several of its predecessors, that only give binary results concerning the storage standing across the distributed servers, the planned theme achieves the combination of storage correctness insurance and knowledge error localization, i.e., the identification of misbehaving server(s).

2) Unlike most previous works for ensuring remote knowledge integrity, the new scheme further supports secure and convenient dynamic operations on data blocks, including: update, delete, append and insert.

3) The experiment results demonstrate the proposed scheme is highly convenient. Extensive security analysis shows our scheme is resilient against Byzantine failure, malicious information

modification attack, and also server colluding attacks.

Related works

A. *Governance, Risk Management and Compliance (GRC) Stack of the Cloud Security Alliance (CSA)*

The Cloud Security Alliance (CSA), comprised of many subject matter experts from academia and leading organizations, is a non-profit organization formed to promote best practices for providing security assurance within Cloud Computing, and provide education on Cloud Computing. Two projects from the CSA's Governance, Risk Management and Compliance (GRC) Stack are relevant: *CloudAudit* [19] and the *Trusted Cloud Initiative* [20].

B. *HP Labs – Cloud and Security Lab*

Pearson and Mowbray have done research on technical and procedural methods for promoting cloud privacy [21, 22]. Recently, Ko, Lee and Pearson established the case for accountability in [10], via a short paper covering scenarios and concerns of accountability within the cloud.

C. *University of Pennsylvania/ Max Planck Institute for Software Systems*

Haeberlen et al. were one of the first researchers to call for awareness in an accountable cloud [23]. In [23], they assumed a primitive *AUDIT* with considerations of *agreement*, *service* and *timestamps*. However, *AUDIT* did not have a clear explanation of the scope, scale, phases and layers of abstraction of accountability. It is our aim to complement their work. They also proposed an approach for accountable VMs [24], and discussed a case study on the application to detect cheats in an online multi-player game Counterstrike. This non-cloud based game was not a practical business scenario for accountability, and did not address the needs of logging virtual-to-physical mapping.

D. ***HyTrust Appliance*** *[8]* Recently, HyTrust, a startup focusing on cloud auditing and accountability, has released a hypervisor consolidated log report and policy enforcement tool for VM accountability management. HyTrust Appliance addresses the *System layer* (recall Section IV) of cloud accountability. It focuses on the virtual layers and does not log virtual-to physical complexities. It also views accountability from a system perspective and not a file-centric perspective.

E. ***Accountability of Services by CSIRO*** Chen and Wang of CSIRO currently have a team looking at "accountability as a service" for the cloud [25, 26]. Their work presented a prototype which enforces accountability of service providers whose services are deployed in the cloud. This is achieved by making the service providers responsible for faulty services and a technique which allows identification of the cause of faults in binding Web services.

F. ***Provenance in Clouds*** Muniswamy-Reddy et al. [27] discuss the main challenges of provenance adoption for cloud computing and suggest four properties (data coupling, multi-object casual ordering, data-independent persistence, and efficient querying) that make provenance systems truly useful. Secure provenance [28] and privacy-aware provenance [29] have also been proposed for cloud computing systems, as provenance information may contain or expose sensitive, confidential or proprietary information directly or indirectly.

Proposed System

Finally, we propose architecture to continuously audit cloud services in a practically and economically feasible manner. Our conceptual architecture highlights important components (i.e., various interfaces and auditing management modules) as well as processes that have to be implemented. 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.

Continuous Auditing:

When you hear the word "audit," you probably don't think about an ongoing, regular process. Instead, your stomach might drop a little at the thought of an examination by the IRS, or maybe you've established a periodic internal assessment. Continuous auditing, however, can be an ally in keeping your system secure, and with advancements in technology, it's not that intimidating to take advantage of it. In fact, some managed service providers take care of the details, tailoring a continuous audit system to your organization's unique needs.

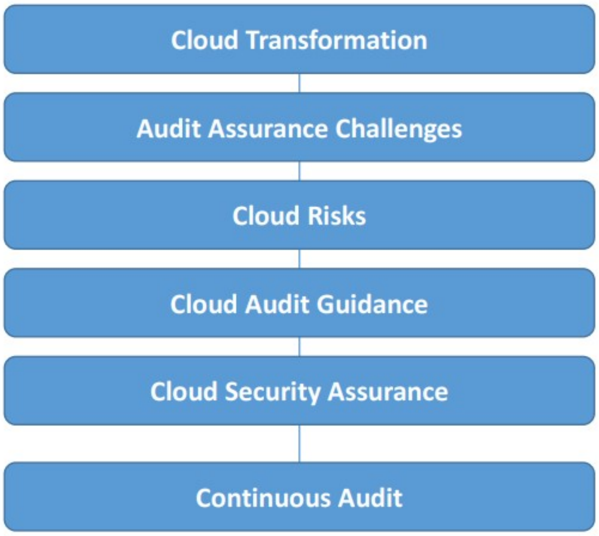


Fig. 1 Continuous Auditing in cloud

- **Process of Continuous Auditing:**

According to a white paper by the American Institute of CPAs (AICPA), companies have successfully used continuous auditing and continuous monitoring (CA/CM) processes to make better decisions about risk by analyzing key business data and metrics, giving them an important competitive advantage. By constantly tracking your data system, you can evaluate it against industry regulations, such as PCI, and identify deviations or risks faster. Because breaches in compliance or information security can quickly spiral out of control, it's a huge advantage to be able to recognize and respond to any issues before much time elapses.

- **Advantage of continuous auditing services**

When working with a cloud service provider, you should inquire into their continuous auditing offerings, such as Tripwire Configuration Assessment. You can partner with your provider to track your system according to your own custom rules, ensuring that the monitoring process addresses your specific infrastructure setup and the metrics that are important to your business.

Continuous auditing services can give you peace of mind knowing that any deviations from a trusted system state will trigger alerts in real-time. Real-time reporting makes it possible to react to system changes without compromising performance or compliance, helping to keep your solution secure.

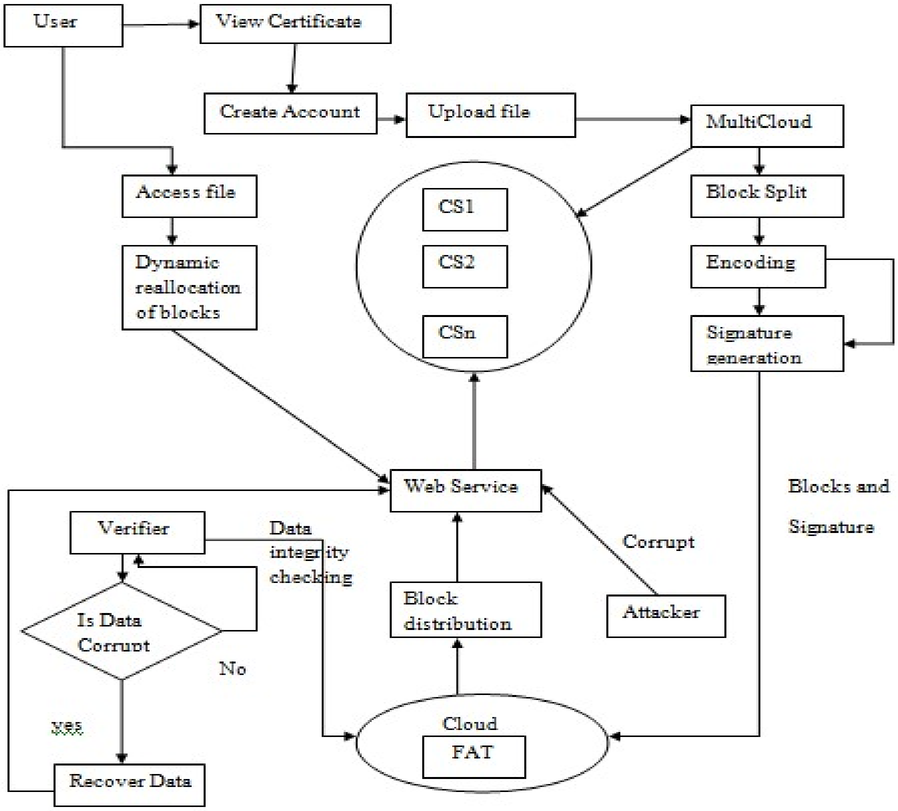
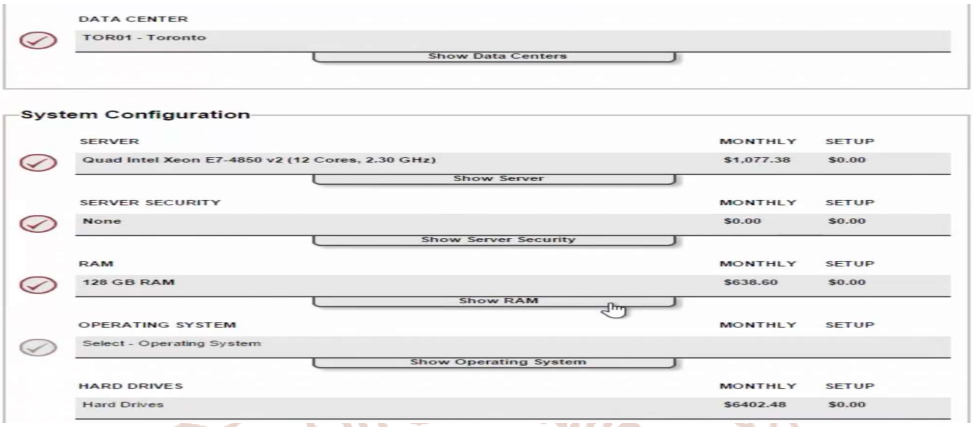


Fig. 2 Architecture

A. Server Configuration

During server configuration and setup, you can select the operating system, memory and storage. These selections should be based on application workload and technical requirements. You can also select the location of the data centre where the high-performance computing instance will be hosted. If the workload requires higher throughput with low latency, you should add InfiniBand, which can support up to 56 GB per second of throughput for your HPC on Soft Layer compute instance.



DATA CENTER
TOR01 - Toronto

System Configuration

SERVER — MONTHLY — SETUP
Quad Intel Xeon E7-4850 v2 (12 Cores, 2.30 GHz) — $1,077.38 — $0.00

SERVER SECURITY — MONTHLY — SETUP
None — $0.00 — $0.00

RAM — MONTHLY — SETUP
128 GB RAM — $638.60 — $0.00

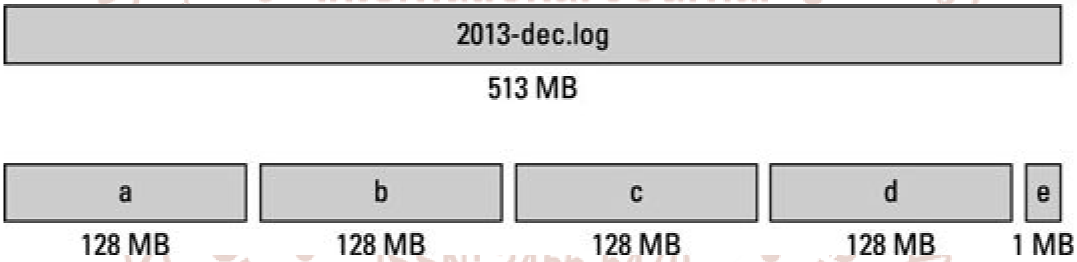
OPERATING SYSTEM — MONTHLY — SETUP
Select - Operating System

HARD DRIVES — MONTHLY — SETUP
Hard Drives — $6402.48 — $0.00

Fig. 3 *Server* and System Configuration

B. Data Upload and Block Split:

When you store a file in HDFS, the system breaks it down into a set of individual blocks and stores these blocks in various slave nodes in the Hadoop cluster. This is an entirely normal thing to do, as all file systems break files down into blocks before storing them to disk.



HDFS has no idea (and doesn't care) what's stored inside the file, so raw files are not split in accordance with rules that we humans would understand. Humans, for example, would want record boundaries — the lines showing where a record begins and ends — to be respected. HDFS is often blissfully unaware that the final record in one block may be only a partial record, with the rest of its content shunted off to the following block. HDFS only wants to make sure that files are split into evenly sized blocks that match the predefined block size for the Hadoop instance (unless a custom value was entered for the file being stored). In the preceding figure, that block size is 128MB. The concept of storing a file as a collection of blocks is entirely consistent with how file systems normally work. But what's different about HDFS is the scale. A typical block size that you'd see in a file system under Linux is 4KB, whereas a typical block size in Hadoop is 128MB. This value is configurable, and it can be customized, as both a new system default and a custom value for individual files. Hadoop was designed to store data at the petabyte scale, where any potential limitations to scaling out are minimized. The high block size is a direct consequence of this need to store data on a massive scale.

C. Data Integrity Checking

The basic idea of the project applies only to static storage of data. It cannot handle to case when the data need to be dynamically changed. This dynamic data integrity is used to support for data dynamics via the most general forms of data operation, such as block modification, insertion, and deletion, is also a significant step toward practicality. While prior work on ensuring remote data integrity often lacks the support of either public auditability or dynamic data operations. The project first identify the difficulties and potential security problems of direct extensions with fully dynamic data updates from prior works and then show how to construct an elegant verification scheme for the seamless integration. To achieve efficient data dynamics, we improve the existing proof of storage models by manipulating the classic Merkle Hash Tree construction for block tag authentication.

D. Experimental evaluation

A digital signature or digital signature scheme is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit. Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering. Digital signatures employ a type of asymmetric cryptography. For messages sent through a non secure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender. Digital signatures are equivalent to traditional handwritten signatures in many respects; properly implemented digital signatures are more difficult to forge than the handwritten type. Digital signature schemes in the sense used here are cryptographically based, and must be implemented properly to be effective. Digital signatures can also provide non-repudiation, meaning that the signer cannot successfully claim they did not sign a message, while also claiming their private key remains secret; further, some non-repudiation schemes offer a time stamp for the digital signature, so that even if the private key is exposed, the signature is valid nonetheless.

CONCLUSIONS

In this paper, we establish the urgent need for research in cloud accountability. We propose detective rather than preventive approaches to increasing accountability. Detective approaches complement preventive approaches as they are non-invasive, and enable the investigation not only of external risks, but also risks from within the CSP. With the shift in end-users' concerns from system health and performance to the integrity and accountability of data stored in the cloud, we require a file-centric perspective, on top of the usual system-centric perspective for logging. Using the abstraction layers defined via the TrustCloud framework, we were able to list several cloud accountability issues previously not mentioned in cloud computing literature. We intend to develop a system based on the TrustCloud framework that gives cloud users a single point of view for accountability of the CSP. We are currently researching and developing solutions for each accountability layer, with one example being a logging mechanism for the system layer.

REFERENCES

1. Juels, A. and Oprea, A., 2013. New approaches to security and availability for cloud data. *Communications of the ACM*, *56*(2), pp.64-73.
2. Chatterjee, R., Roy, S. and Scholar, U.G., 2017. Cryptography in Cloud Computing: A Basic Approach to Ensure Security in Cloud. *International Journal of Engineering Science*, *11818*.
3. Ganesh, A., 2017. Security Capabilities Of Fine Grained Two Factor Access Control In Web Based Cloud Computing Services.
4. Subashini, S. and Kavitha, V., 2011. A survey on security issues in service delivery models of cloud computing. *Journal of network and computer applications*, *34*(1), pp.1-11.
5. Sah, B.K., Yadav, D. and Rain, C.K., 2017. Cloud Computing Using AES.
6. Pancholi, V.R. and Patel, B.P., 2016. Enhancement of cloud computing security with secure data storage using AES. *International Journal for Innovative Research in Science and Technology*, *2*(9), pp.18-21.
7. Lins, S., Schneider, S. and Sunyaev, A., 2016. Trust is good, control is better: Creating secure clouds by continuous auditing. *IEEE Transactions on Cloud Computing*.
8. Wang, C., Wang, Q., Ren, K., Cao, N. and Lou, W., 2012. Toward secure and dependable storage services in cloud computing. *IEEE transactions on Services Computing*, *5*(2), pp.220-232.