ISSN No. 0976-5697

Volume 4, No. 8, May-June 2013

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Security Enhancement For Reliable Computing In Cloud

Akshaya.V
Dept. of Information Technology
Vel Tech High Tech Dr. RR Dr.SR Engg. College,
Chennai, India.
akshaya.vaidhyanathan@gmail.com

Vignesh.R.C.
Dept. of Computer Science and Engineering
Rajalakshmi Institute of Technology,
Chennai, India.
v950217@gmail.com

Jhansi Lakshmi.D.V
Dept. of Information Technology
Vel Tech High Tech Dr. RR Dr.SR Engg. College,
Chennai, India.
jhanujhan@gmail.com

M.Infanto hearty Shamirna
Dept. of Information Technology
Vel Tech High Tech Dr. RR Dr.SR Engg. College,
Chennai, India.
heartisharmi@gmail.com

K.Subala M.E.,
Assistant professor, Dept. of Information Technology
Vel Tech High Tech Dr. RR Dr.SR Engg. College,
Chennai, India.
subalamathi@gmail.com

Abstract:Cloud computing has become the long dreamed vision of computing as a utility in IT enterprise, where users remotely store and access data from a shared pool of configurable computing resources today. Data outsourcing relieves the burden of user from local data storage and maintenance whereas the management of the data and services on the centralized large data centres may not be full trustworthy. The privacy and security of data is at stake by the prevalence of intruders and other faults in cloud. This paper reveals the enhancement in security by introducing the intrusion detection along with increased privacy over the data. The privacy of data in cloud is preserved by enabling the public auditability and data dynamics. The performance of the proposed method is analysed using the simulator tool cloudsim.

Keywords:Cloud computing, Privacy preservation, intrusion detection, public auditing, data dynamics.

I. INTRODUCTION

Cloud computing is believed to bring a new change to the way we access technology similar to that of the commercialization of the internet over decades. Cloud computing enables innovations and it alleviates the innovators to focus on the innovation. Cloud computing on the whole is a combination of distributed and parallel systems. Cloud computing has 3 basic abstraction layer namely system layer (which is a virtual machine abstraction of a server), the platform layer (a virtualized operating system of a server), and application layer (that includes web applications)[1]. Hardware layer is not included as it does not offer any services to the users directly. Amazon, salesforce.com and Google are the leading cloud services providers for storage, application and computing on pay as you use basis. When this is implemented users worry about who will supervise the providers and control their behaviors. Here the security is at stake when the intruders access others data(figure 1). This can be prevented by the use of intrusion detection system and security can be enhanced by using privacy preservation.

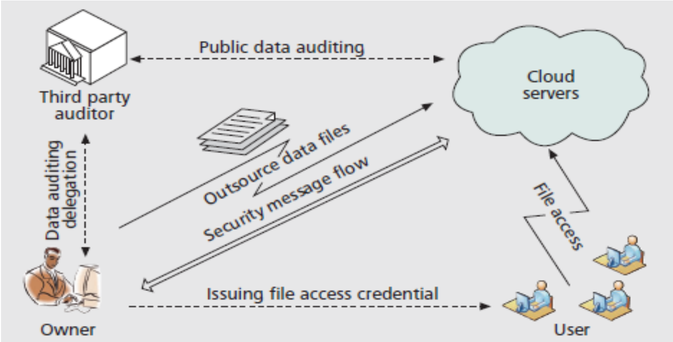

Figure1. Architecture of cloud storage service

There are several Instruction Detection System(IDS), such as Host based IDS(HIDS), monitor specification host machines, Networks based IDS, etc., These IDS generates alerts to providers when true intrusion takes place by detecting intrusion patterns by critically inspecting the network packets, applying signatures and these providers instruct the user that their system is under attack. There are two methods of intrusion detection namely anomaly detection- works on user behavior patterns and misuse detection- works through port scan.

In this paper, we focus on increasing the security of data by motivating the public auditing system of data storage in cloud [2][3] and propose a protocol that supports dynamic data operations[4] and also an intrusion detection system[5] using multi-threaded IDS approach.

II. RELATED WORKS

A. Cloud Computing Architecture:

The cloud has become the metaphor for internet and is an abstraction for complex infrastructure it conceals. Cloud computing is an internet based development and is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable resources such as networks, servers, storage, applications and services which can be provisioned and released with minimal management effort or service provider interaction. Cloud computing is classified into three service models based on the type of services provided namely Software as a service (SaaS), Platform as a service (PaaS), Infrastructure as a service (IaaS). Cloud computing is fully enabled by virtualization technology (hypervisors) and virtual appliance (application that is bundled with all the components that it needs to run, along with a streamlined operating system)[6]. In cloud computing environment, a virtual appliance can be instantly provisioned and decommissioned as needed, without the complex configuration of operating environment. This flexibility is the key advantage to cloud computing and makes cloud computing unique from other forms of grid, utility and SaaS. Cloud computing applications are scaled by maximizing concurrency and utilizing computer resources more efficiently. To provide scaling services to a large number of users certain steps such as optimize locking duration, stableness, sharing pooled resources like task thread, network connection bus, cache reference data and partition large databases Figure 2. Cloud computing architecture and management comprises of various managers like information manager, transfer manager, execution manager and scheduler manager.

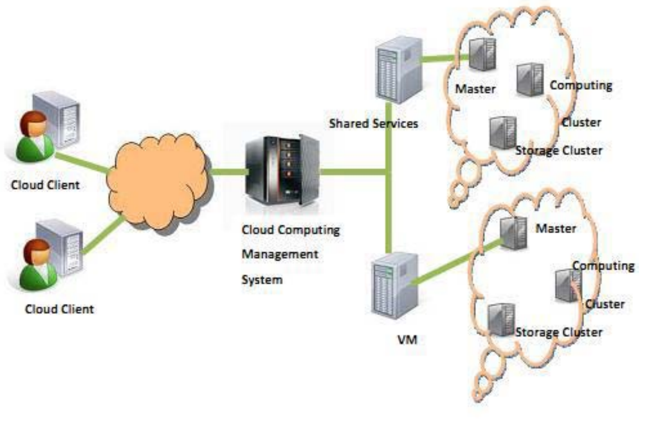

Figure 2. Cloud Computing Architecture

Cloud computing involves all applications that use large data center and powerful servers that host web applications and web services which can be accessed by anybody holding a suitable internet connection or a standard browser.

B. Security Enhancement in Cloud:

Ateniese et al [7] was first to consider the public auditability on cloud and define provable data possession model for ensuring possession on untrusted storage. They utilized RSA based homomorphic tags for auditing the outsourced data and public auditability was achieved and dynamic operations were not considered. In later works, the author proposed a proposed a PDP scheme which considered the basic block operations [12]. Many researches were taken on dynamic operations. Erway et al explored the constructions for dynamic provable data possession by extending the PDP model to support provable updates and storage [8].

C. Intrusion Detection in Cloud:

Intrusion detection system plays a major role in security and acts as an active defense system against intruders in all organizations. The cloud service providers are remote servers and it has limited control over data and resources. So, the administration of IDS is a must for the cloud providers.

Roschke and Cheng et al [1] have proposed an integration solution for central IDS management that can combine and integrate various renowned IDS sensor output reports on a single interface. The authors have suggested the deployment model of IDS in various layers such as application layer, system layer and platform layer. Alerts generated are sent to a program called event gatherer which receives and converts alert messages in a standard format (IDMEF) and store in event data repository that could be monitored and used by user.

III. SECURITY FACTORS IN CLOUD

There are many security factors in cloud computing [6] [9] as follows.

a. Secure data transfer
b. Secure software interfaces
c. Secured data storage
d. Separation of data
e. User access control
f. Data location
g. Data recovery

IV. DESIGN GOALS

A. Public auditability for storage correctness assurance: to enable the capability of all not only the clients to verify the correctness of the stored data [2] [3].
B. Dynamic data operation support: to perform block level operation on data files dynamically and maintain the same level of data correctness [4].
C. Effective intrusion detection system: to detect the intruders and communicate the alert logs to the user [5].

V. PROPOSED MODEL

In our proposed model we consider two ways to improvise the cloud computing. One way is to increase the security system and the other is to make the strategy based on the statistical model for the security system. This idea enables us to construct a flexible computing with increased security. We use PKC-based homomorphic authenticator using BLS signature [10] to increase the public auditability and BLS-based scheme to illustrate our design with data dynamics support as of the system proposed by Wang et al. We use Merkle hash tree [11] constructed similarly as a binary tree to study the authenticated signature. We introduce the efficient multi-threaded IDS system to identify intruders and improve the performance.

A. *To increase the public auditability:*

The client's public and private key are generated by invoking KeyGen() and it is signed and preprocessed by running SignGen(), and the homomorphic authenticators along with the metadata are produced. Then the public auditability is performed as follows

a. To generate a message the TPA (verifier) selects a random set from a subset of that element and sent to the provider (server).
b. In server both the data blocks and signature blocks are aggregated into a single block. The provider responds to the verifier with proof (GenProof()).
c. By receiving the response, the verifier generates root and authenticates it by checking sign (VerifyProof()).
d. If the authentication fails, the verifier rejects by emitting FALSE else it checks for integrity and gives the output TRUE.

B. *To handle dynamic data operation with integrity check:*

The basic data operations involve replacement of specified blocks with new ones or update or insert a new data block.

a. If the client wants a block to be modified or updated or inserted, it generates the corresponding signature and sends specific operation request to the server.
b. The server on receiving the request replaces or inserts the new block at the specified location and generates new root based on the new block.
c. The server sends response to the client with a proof for the specific operation.
d. After receiving the response the client generates the root and authenticates by checking the sign.
e. If authentication fails, it outputs FALSE else it can check whether the server has performed specific operation by computing the root and compares with the root that was created by the server.
f. If the output is TRUE, the client sends the new authenticated and verified root to the server for update and executes default integrity check protocol.

C. *To detect the intruders effectively:*

Cloud model works on the concept of virtualization of resources. With the rapid flow of high volume of data in the cloud, many issues like overloading of VM, hosting of IDS, dropping packets would be raised. We use multi-threaded IDS approach to handle this case. The multi-threaded IDS would process large volume of data with less packet loss. This IDS system monitors and alerts the TPA regarding misconfigurations and intrusion loop holes in the system and the TPA alerts the user regarding the same (figure 3).

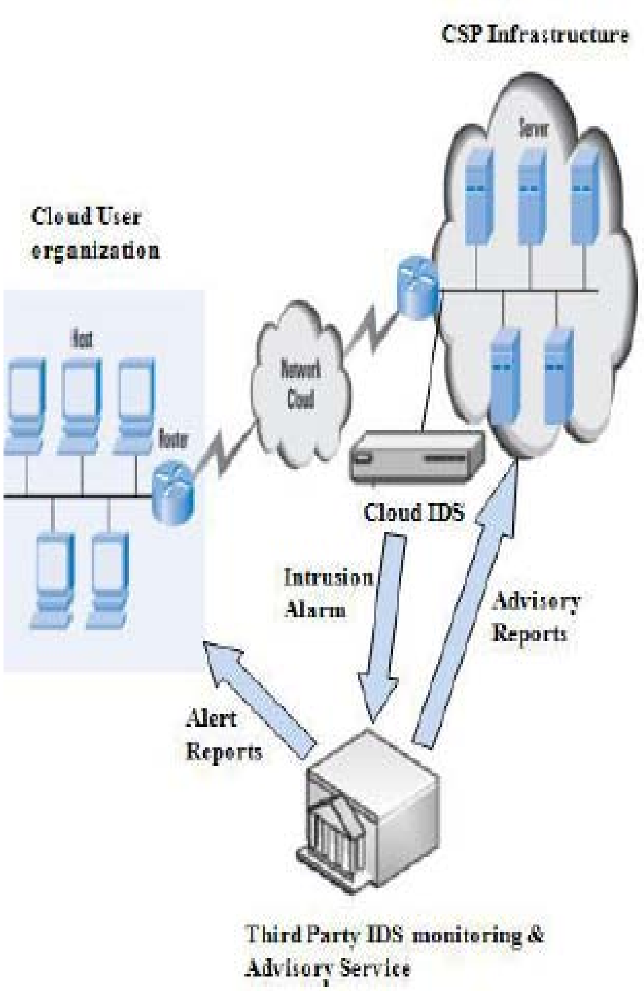

Figure 3. Intrusion detection system

Requests and actions of user are monitored and logged through multi-threaded NIDS which involves three phases.

a. The in-bound and out-bound data packets for accessing the specific encrypted data blocks are captured and sent to shared queue for analysis.
b. The analysis phase analyze the data packets against signature base and a pre-defined rule set based on the Public key authentication technique with a digest signature. Each process can have multiple threads to improve system performance.
c. Through the efficient matching and analyzing phase the bad packets are identified and alerts are generated.
d. The reporting phase captures the alert from the shared queue and report about it to the TPA and the TPA immediately generates alert to the user.

VI. PERFORMANCE ANALYSIS

The proposed model was simulated using cloudsim and the performance was analyzed with various existing techniques. The proposed technique showed higher performance and reduced cost than other techniques for public auditability and intrusion detection system.

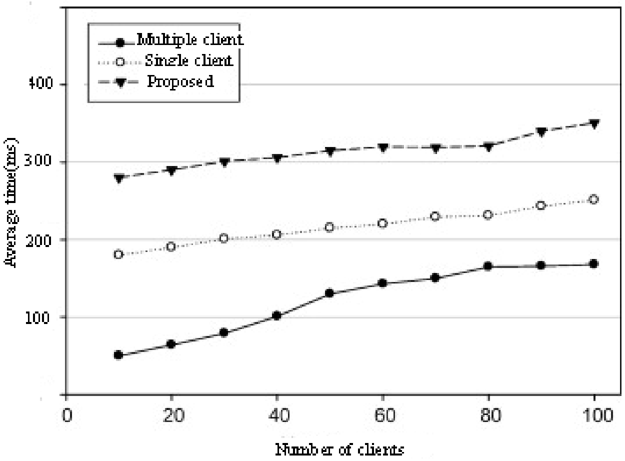

Figure 4. Performance comparison using simulation

VII. REFERENCES

[1] Sebastian Roschke, Feng Cheng, Christoph Meinel,“ Intrusion Detection in the Cloud", Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, 2009. J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[2] Cong Wang, Sherman S.M. Chow, Qian Wang, Kui Ren”Privacy-preserving public auditing for secure cloud storage”, *IEEE transactions on computers.*

[3] Cong Wang and Kui Ren, Illinois Institute of Technology Wenjing Lou, Worcester Polytechnic Institute Jin Li, Illinois Institute of Technology, “Toward Publicly Auditable Secure Cloud Data Storage Services*”, IEEE networks July, august 2010.*

[4] Qian Wang, Kui Ren, Wenjing Lou, “Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing”, *IEEE transactions on parallel and distributed systems*, vol.22.

[5] Ms.Parang.K.Shelke, Ms.Sneha Sonatakke, “Intrusion detection system for cloud computing”, *International journal of scientific and tech research*, vol.1.

[6] Wikipedia, “http://en.wikipedia.org/wiki/Cloud_computing”.

[7] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z.Peterson, and D. Song, “Provable Data Possession at UntrustedStores,” Proc. 14th ACM Conf. Computer and Comm. Security (CCS’07), pp. 598-609, 2007.

[8] C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia,“Dynamic Provable Data Possession,” Proc. 16th ACM Conf.Computer and Comm. Security (CCS ’09), 2009.

[9] Richard Chow, Philippe Golle, Markus Jakobsson, “Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control”, ACM Computer and Communications Security Workshop, CCSW 09, November 13, 2009.

[10] H. Shacham and B. Waters, “Compact Proofs of Retrievability,”Proc. 14th Int’l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT ’08), pp. 90-107, 2008.

[11] R.C. Merkle, “Protocols for Public Key Cryptosystems,” Proc. IEEE Symp. Security and Privacy, pp. 122-133, 1980.

[12] G. Ateniese, R.D. Pietro, L.V. Mancini, and G. Tsudik, “Scalable and Efficient Provable Data Possession,” Proc. Fourth Int’l Conf.Security and Privacy in Comm. Networks (SecureComm ’08), pp. 1-10, 2008.