**A Study of Cloud Computing and Security Reinforcement with Anticipated Protocol Framework**

Akhilesh Kumar Bhardwaj **[1]** Dr. Rajiv Mahajan **[2]** Dr. Surinder **[3]**

Research Scholar Professor & Principal Associate Professor

Punjab Technical University C.T.I.T., Jalandhar H.C.T.M, Kaithal

INDIA INDIA INDIA

Corresponding E-mail: [akhilesh.akhand@gmail.com](mailto:akhilesh.akhand@gmail.com) [1]

**ABSTRACT**

Cloud computing allows users to store data and access it on demand with less resources in client system. At present, there has been an escalating inclination in outsourcing data to remote cloud, where the community outsource their data at cloud service provider who offers substantial storage liberty with little cost. Thus users can trim down the maintenance and burden of local data storage. Proficient and confidential methods are desirable to ensure the data verification and effectual load supervision of outsource data on un-trusted cloud servers. This paper exhibits an overview of fundamental mechanisms of cloud computing in opening segment and illustrates consideration of new protection enrichment protocol in the later one. The foundation of the projected design is the permutation of firefly algorithm and merkle hash tree together with n-th degree truncated polynomial ring unit algorithm and LZW string compression technique. Our method makes use of third party auditor to periodically verify the stored data.

**Key-words:** Cloud Computing, Third Party Auditor, AES, Firefly, MHT

**1. INTRODUCTION**

Cloud is something, which is present at remote location. Cloud can provide services over public and private networks. Cloud computing refers to manipulating, configuring and accessing the hardware and software resources remotely. It offers online data storage, infrastructure and application. Cloud computing offers platform independency, as the software is not required to be installed locally on the PC. Hence, the Cloud computing is making our business applications mobile and collaborative. The initiative at the back of cloud computing (CC) has been introduced after the development of distributed computing, parallel computing and grid computing [1]. Some of the texture of cloud computing take account of ubiquity, increased reliability, being virtual, adaptability, scalability, quick suppleness, abundant tendency, planned service, increased intelligence, autonomic efficient control and high quality of service “QoS” [2].

More recently, it is highly essential to learn and examine the way the cloud computing and its applications operate on clouds. In addition, it is also necessary to observe the level of privacy offered by the cloud computing services and the determination of the kind of cloud computing service to be used by the users becomes more vital. Of the serious challenges posed in cloud computing, mutual authentication is more important. Several authentication methods can be used for authenticating the user. Few authentication methods like, plain password authentication can be implemented without much difficulty. But, they are commonly feeble and primitive [3]. Making use of a reliable third party auditor, who serves as the user for evaluating and revealing the risk of cloud storage services as per user request, can be a better way of assuring data security [4].

**1.1 Cloud Computing Architecture**

Cloud computing structure contains two core layers: a management layer and a virtualization layer [5]. In the Management layer, we come across the modules liable for enabling the complete operations detailed for the cloud.

These modules are

1. Security (answerable with all security concerns associated to the cloud system like intrusion detection and alarming module)
2. Validation engine (receives requests to add new jobs to be processed)
3. Virtual jobs (creates an abstraction between the data requested by the user and the payload that must be delivered to the cloud system)
4. Scheduler (schedules the jobs to the virtualization layer)
5. Hypervisor interface (acts like a translation layer that is specific to a virtualization software vendor)
6. Load distribution (responsible with horizontal and vertical scaling of the requests received from the scheduler)
7. Internal cloud API (projected as a link between the virtualization layer and the cloud system)
8. External cloud API (offers a way to the user for interacting with the system).

In the Virtualization layer, we catch the actual platforms and servers that host the virtual machines and have virtualization enabled hardware.

……….

**Management layer**

**Scheduler**

**Virtual**

**Jobs**

**Validation**

**Engine**

**Security**

**External Cloud API**

**Internal Cloud API**

**Load Distribution**

**Hypervisor**

**Interface**

**Virtualization layer**

**Hypervisor N** …

**Hypervisor 2** …

**Hypervisor 1** …

VM

N

VM

2

VM

1

VM

N

VM

2

VM

2

VM

1

VM

1

VM

N

**Figure 1: General Cloud Computing Architecture**

**1.2 Infrastructural Constraints**

Fundamental constraints that cloud infrastructure should implement are

* **Transparency**

Virtualization is the key to share resources in cloud environment. But it is not possible to satisfy the demand with single resource or server. Therefore, there must be transparency in resources, load balancing and application, so that we can scale them on demand.

* **Scalability**

Scaling up an application delivery solution is not that easy as scaling up an application because it involves configuration overhead or even re-architecting the network. So, application delivery solution is needed to be scalable which will require the virtual infrastructure such that resource can be provisioned and de-provisioned easily.

* **Intelligent Monitoring**

To achieve transparency and scalability, application solution delivery will need to be capable of intelligent monitoring.

* **Security**

The mega data center in the cloud should be securely architected. Also the control node, an entry point in mega data center, also needs to be secure.

**Scalability**

**Monitoring**

**Security**

**Transparency**

**Figure 2: Fundamental Constraints for Cloud Infrastructure**

**1.3 Basic Concepts in cloud computing**

There are certain services and models working behind the scene making the cloud computing feasible and accessible to end users. Following are the working models for cloud computing:

* Deployment Models
* Service Models

**Deployment Models**

Deployment models characterize the type of access to the cloud, i.e., how the cloud is located? Cloud can have any of the four types of access: Public, Private, Hybrid, and Community. The public cloud allows systems and services to be easily accessible to the general public. Public cloud may be less secure because of its openness. The private cloud allows systems and services to be accessible within an organization. It is more secured because of its private nature. The community cloud allows systems and services to be accessible by a group of organizations. The hybrid cloud is a mixture of public and private cloud, in which the critical activities are performed using private cloud while the non-critical activities are performed using public cloud.

**Service Models**

Cloud computing is based on service models. These are categorized into three basic service models which are

* Infrastructure-as–a-Service (IaaS)
* Platform-as-a-Service (PaaS)
* Software-as-a-Service (SaaS)

**IaaS**

Infrastructure-as-a-Service provides access to fundamental resources such as physical machines, virtual machines, virtual storage, etc. Apart from these resources, the IaaS also offers:

* Virtual machine disk storage
* Virtual local area network (VLANs)
* Load balancers
* IP addresses
* Software bundles

**PaaS**

Platform-as-a-Service offers the runtime environment for applications. It also offers development and deployment tools required to develop applications. PaaS has a feature of point-and-click tools that enables non-developers to create web applications.

**SaaS**

Software-as–a-Service (SaaS) model allows providing software application as a service to the end users. It refers to software that is deployed on a host service and is accessible via Internet.

**1.4 Characteristics of Cloud Computing**

There are five key characteristics of cloud computing.

* **On Demand Self Service**: allows the users to use web services and resources on demand. One can logon to a website at any time and use them.
* **Broad Network Access**: Since cloud computing is completely web based, it can be accessed from anywhere and at any time.
* **Resource Pooling:** Cloud computing allows multiple tenants to share a pool of resources. One can share single physical instance of hardware, database and basic infrastructure.
* **Rapid Elasticity:** It is very easy to scale the resources vertically or horizontally at any time. Scaling of resources means the ability of resources to deal with increasing or decreasing demand.The resources being used by customers at any given point of time are automatically monitored.
* **Measured Service:** In this service, the cloud provider controls and monitors all the aspects of cloud service. Resource optimization, billing, and capacity planning etc. depend on it.

**1.5 Technologies behind the Cloud Computing**

There are certain technologies working behind the cloud computing platforms making cloud computing flexible, reliable, and usable. These technologies are

* Virtualization
* Service-Oriented Architecture (SOA)
* Grid Computing
* Utility Computing

Utility Computing

Grid Computing

SOA

Virtualization

**Figure 3: Technologies supporting Cloud Computing Platforms**

**Virtualization**

Virtualization is a technique, which allows sharing single physical instance of an application or resource among multiple organizations or tenants (customers). It does this by assigning a logical name to a physical resource and providing a pointer to that physical resource when demanded.

**Service-Oriented Architecture (SOA)**

Service-Oriented Architecture helps to use applications as a service for other applications regardless the type of vendor, product or technology. Therefore, it is possible to exchange the data between applications of different vendors without additional programming or making changes to services.

**Grid Computing**

Grid Computing refers to distributed computing, in which a group of computers from multiple locations are connected with each other to achieve a common objective. These computer resources are heterogeneous and geographically dispersed. Grid Computing breaks complex task into smaller pieces, which are distributed to CPUs that reside within the grid.

**Utility Computing**

Utility computing is based on Pay-per-Use model. It offers computational resources on demand as a metered service. Cloud computing, grid computing, and managed IT services are based on the concept of utility computing. Cloud Computing architecture comprises of many cloud components, which are loosely coupled. We can broadly divide the cloud architecture into two parts:

* Front End
* Back End

Each of the ends is connected through a network, usually Internet. The front end refers to the client part of cloud computing system. It consists of interfaces and applications that are required to access the cloud computing platforms, Example - Web Browser. The back End refers to the cloud itself. It consists of all the resources required to provide cloud computing services. It comprises of huge data storage, virtual machines, security mechanism, services, deployment models, servers, etc. It is the responsibility of the back end to provide built-in security mechanism, traffic control and protocols. The server employs certain protocols known as middleware, which help the connected devices to communicate with each other.

**1.6 Types of Cloud**

Four types of clouds are considered in cloud computing.

**Private cloud**

**Public cloud**

**Cloud**

**Community**

**Cloud**

**Hybrid cloud**

**Figure 4: Types of Cloud**

**Public cloud**

Public Cloud allows systems and services to be easily accessible to general public. The IT giants such as Google, Amazon and Microsoft offer cloud services via Internet.

**Private cloud**

Private Cloud allows systems and services to be accessible within an organization. The Private Cloud is operated only within a single organization. However, it may be managed internally by the organization itself or by third-party.

**Hybrid cloud**

Hybrid Cloud is a mixture of public and private cloud. Non-critical activities are performed using public cloud while the critical activities are performed using private cloud.

**Community cloud**

Community Cloud allows system and services to be accessible by group of organizations. It shares the infrastructure between several organizations from a specific community. It may be managed internally by organizations or by the third-party.

**2. LITRATURE SURVEY**

**Zhifeng Xiao and Yang Xiao *et al*. [6]** have recommended plenty of methodologies for third party authentication that assist in handling storage and data transaction in a secure way. They have exposed significant security and privacy parameters. **Cong Wang *et al.* [7]** have put forward a additional protective cloud storage system that supports public auditing with privacy-preserving ability. They have also broadened their outcomes in a way that the TPA is rendered with the power to carry out audits for multiple users at the same time in an effective manner. **Hsiao-Ying Lin *et al*. [8]** have presented a threshold proxy re-encryption scheme, which is integrated with a decentralized erasure code for developing a secure distributed storage system. **Yang Tang *et al.* [9]** have dealt with the design and implementation of a protected overlay cloud storage system that is capable of realizing fine-grained, policy-based access control and file assured deletion. **Assad Abbas *et al.* [10]** have proposed a cloud service in the health sector, wherein, the cloud serves as a medical record storage center along with the ability to perform the transfer of electronic medical records between various hospitals and health centers. **Ching-Nung Yang *et al.* [11]** have proposed a cloud security services, which incorporates key agreement and authentication. Here, the secure cloud computing (SCC) has been developed with the utilization of Elliptic Curve Diffie-Hellman (ECDH) and symmetric bivariate polynomial based secret sharing. **Jingxin K. Wang *et al.* [12]** have put forth a number of methods for providing user data security that comprises of single encryption, multi-level virtualization and authentication interface. Authentication inter cloud was yet another concept dealt chiefly in their work. In addition, an authentication inter-cloud model that relies on CA and PKI model have been described**Faraz Fatemi et *al*. [13]** have offered an efficient and scalable user authentication scheme for cloud computing environment. A client-based user authentication agent has been introduced to confirm identity of the user in client-side. **G. Jai Arul Jose et *al*. [14]** have offered an security system providing authentication, confidentiality and data integrity of user’s data by joining the cloud computing framework with cluster load balancing, SSL over AES and secure session. **E.M. Mohamad et *al*. [15]** have provided on-demand security options by making selection from different encryption. Algorithm performance is calculated by testing encryption speed. Comparisons among algorithms done are based on P-value and rejection rate. **V. Nirmala et *al*. [16]** have proposed user authentication scheme in which data is divided into blocks and applied with AES encryption after the generation of hash value for each block. Further, the hash code is also implemented to check the data integrity. The cloud here is used to storing encrypted data and generating hash while rest of work takes place at user side. . A two layer encryption based approach has been suggested by **Mohamed Nabeel and Elisa Bertino [17]** in order to work out the problem by delegating as much of the access control enforcement responsibilities as feasible to the cloud while decreasing the information exposure risks due to colluding users and cloud.

**3. The Proposed Architecture**

In the proposed work, an improved protocol construction technique with superior authentication has been presented. Here, a third party auditor (TPA) would assist in the cloud participation. The objective is alienated into several modules including design and implementation of the proposed protocol, evaluation of various threats on the security of cloud environment, analysis of security and performance parameter like encryption time, decryption time, throughput and network delay and to ensure appropriate load balancing with metrics like throughput, response time, migration time, scalability and fault tolerance.

**Cloud Environment**

**Firefly Decryption**

**TPA Registration**

**Decompression**

Client

**MHT -LZW compression**

**Master server login**

**MHT -Concurrency mgt.**

**Firefly –NTRU encryption**

**Data input**

**File sharing**

**AES –FH encryption**

**Figure 5: Secure Cloud System Storage using Firefly and Merkle Hash Tree Protocol**

Steps of the working of proposed system are as follows:

* **Step 1:** Establishment of Validation: TPA Registration - Master Server Login
* **Step 2:** Read the input file
* **Step 3:** Authentication using AES and Full Homomorphic Technique
* **Step 4:** File Sharing
* **Step 5:** Firefly Encryption with NTRU Key Generation
* **Step 6:** MHT Block Division followed by LZW String Compression
* **Step 7:** Decompression using LZW
* **Step 8:** Decryption using Firefly
* **Step 9:** Concurrency Management by MHT

**Figure 6: Steps of the Proposed System**

**4. Conclusion**

In cloud environment, ensuring the security of client’s data is the prime focus. In this paper, the cloud computing key issues are discussed and new code of behavior for protecting the data and concurrency supervision has been suggested. The proposed cloud computing model could fix the serious problems, namely public authentication, load balancing and dynamic data integrity.

**5. References**

[1]WANG En Dong WU Nan, LI Xu, "**QoS-oriented Monitoring Model of Cloud Computing Resources Availability**", In the Proceeding of *IEEE International Conference on Computational and Information Sciences*, pp. 1537-1540, June 2013.

[2]Maha Attia Hana, "**E-Government Cloud Computing Proposed Model: Egyptian E\_Government Cloud Computing**", In the Proceeding of *IEEE International Conference on Advanced in Computing Communication*

*and Information (ICACCI)*, pp. 847-852, Aug 2013.

[3]Nimmy K., M. Sethumadhavan, "**Novel Mutual Authentication Protocol for Cloud Computing using Secret Sharing and Steganography**", In the Proceeding of *IEEE fifth International Conference on Application of Digital Information and Web Technologies (ICADIWT)*, pp.101-106, Feb 2014.

[4]Shuai Han, Jianchuan Xing, "**Ensuring Data Storage Security Through a Novel Third Party Auditor Scheme in Cloud Computing**", In the Proceeding of *IEEE International Conference on Cloud Computing and Intelligence System (CCIS)*, pp. 264-268, Sept 2011.

[5]. Patrascu, V.V. Patriciu, **“Logging for Cloud Computing Forensic Systems”,** *International Journal of Computer Communication and Control*, ISSN 1841-9836, 10(2):222-229, April, 2015.

[6]Zhifeng Xiao and Yang Xiao, "**Security and Privacy in Cloud Computing**" In the Proceeding of *IEEE Conference on Communication Surveys & Tutorials*, Vol. 15, No. 2, pp. 843-859, May 2013.

[7]Cong Wang, Sherman S.M. Chow, and Qian Wang, “**Privacy-Preserving Public Auditing for Secure Cloud Storage**”, In the Proceeding of *IEEE Transaction on Computers*, Vol. 62, No. 2, pp. 362-375, Feb 2013.

[8]Hsiao-Ying Lin, and Wen-Guey Tzeng, “**A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding**”, In the Proceeding of *IEEE Transaction on Parallel and Distributed Systems*, Vol. 23, No. 6, pp. 995-1003, June 2012.

[9]Yang Tang, Patrick P.C. Lee, and John C.S. Lui, “**Secure Overlay Cloud Storage with Access Control and Assured Deletion**”, In the Proceeding of *IEEE Transaction on Dependable and Secure Computing*, Vol. 9, No. 6, pp. 903-916, Nov 2012.

[10]Assad Abbas and Samee U. Khan, "**A Review on the State-of-the-Art Privacy-Preserving Approaches in the e-Health Clouds"**, *Journal of Biomedical and Health Information*, Vol. 18, No. 4, pp. 1431-1441, July 2014.

[11]Ching-Nung Yang, and Jia-Bin Lai, “**Protecting Data Privacy and Security for Cloud Computing Based on Secret Sharing**”, In the Proceeding of *IEEE Transaction on Biometrics and Security Technologies (ISBAST)*, pp. 259-266, July 2013.

[12]Jingxin K. Wang, Xinpei Jia, "**Data Security and Authentication in Hybrid Cloud Computing Model**" In the Proceeding of *IEEE International Conference on Global High Tech Congress on Electronic (GHTCE)*, pp. 117-120, Nov 2012.

[13] Moghaddam, Faraz Fatemi, Shiva Gerayeli ; Rouzbeh, Sohrab ; Araghi, Sagheb Kohpayeh ; Alibeigi, Nima Morad ; Varnosfaderani, Shirin Dabbaghi, "**A Scalable and Efficient User Authentication Scheme for Cloud Computing Environments**", *IEEE symposium*, Kuala Lumpur, Malaysia, pp. 508-513, 2014.

[14]. G. Jai Arul Jose, C. Sajeev, Dr. C. Suyambulingom, **“Implementation of Data Security in Cloud Computing*”,*** *International Journal of P2P Network Trends and Technology*, volume 1, issue 1, pp 18-22, 2011.

[15]. E. M. Mohamed, H.S. Abdelkadar, S.E. Etriby, **“Enhanced Data Security Model for Cloud Computing”,** *International Conference on Informatics and Systems*, 2012.

[16]. V. Nirmala, R. K. Shivanadhan, R. S..Lakshmi, **“Data Confidentiality and Integrity Verification using User Authentication Scheme in Cloud”,** *International Conference on Green High Computing, IEEE*, pp 1-5, 2013.

[17]Mohamed Nabeel and Elisa Bertino, "**Privacy Preserving Delegated Access Control in Public Clouds**", *IEEE Transaction on Knowledge and Data Engineering*, Vol. 26, No. 9, pp. 2268-2280, Sep 2014.