

## VERSATILE AGENT BASED MULTI-LAYER SECURITY FRAMEWORK FOR CLOUD DATA CENTER

D.Vimala<sup>1</sup>, I. Mary Linda<sup>2</sup>

<sup>1,2</sup>Assistant Professor, Dept of CSE,

BIST, BIHER, Bharath University, Chennai – 73

<sup>1</sup>vimala.cse@bharathuniv.ac.in, <sup>2</sup>marylinda.cse@bharathuniv.ac.in

**Abstract:** This paper proposes another versatile operator based cloud security structure involving four diverse security and verification layers to set up the trust connection between two substances before utilizing cloud administrations. The proposed system is partitioned into four layers with each layer performing confirmation, check and trustworthiness at various levels of correspondence between two substances. A calculation is utilized to check and examine the legitimacy and usefulness of each layer.

The structure utilizes verified versatile specialists from both customers and cloud specialist organization to play out the errands for the benefit of clients to set up reliable computing relationship. The proposed system viably guarantees protection and security of customer information and offers control to customer over his information utilizing the security specialists.

**Keywords:** Cloud Computing, Cloud Security, Cloud Security Framework, Mobile Agents and Trust Relationship

### 1. Introduction

Distributed computing worldview is dynamically making huge force in the current advancement of IT framework to give distinctive administrations to end clients on request with negligible expenses and less over-head. Administrations gave by cloud have as of late progressed toward becoming pervasive administration conveyance display, hiding a wide scope of administrations and applications from individual record sharing to being an endeavour information warehouse. It significantly improves coordinated effort; responsiveness, agility and scaling of extensive variety of advances empowering a genuinely worldwide processing model over the Internet. Cloud stage powerfully apportions, conveys, redeploys and crosses out various administrations as client necessities change with entry of time. Distributed computing, the long-held dream of "registering as an utility", has open up another time of future on request registering, changing and reshaping vast some portion of IT industry, to buy and utilize IT assets with impressive consideration from worldwide and nearby IT players,

national governments, and universal agencies. Cloud innovation utilizes diverse qualities like area free asset pooling, universal arrange access, on-request self-benefit, fast versatility what's more, measured administrations, alongside different components to expert vide consistent and straightforward administrations to all clients furthermore, clients. The cloud foundation spins around three major useful segments to make this innovation advances with another fantasy vision of registering as utility to be utilized on request when required and required[7]. These segments are:

#### Cloud Service Provider

A cloud specialist co-op is an organization or endeavor that offers diverse administrations in cloud as components ordinarily alluded to as Infrastructure as a Service (IaaS), Software as a Service (SaaS) and Platform as a Service habit (PaaS) to organizations or individual clients on request with most astounding velocity, accessibility and uptime. This substance likewise oversees Cloud Storage Server (CSS) for putting away information what's a more, different asset to safeguard clients and customer's information with high calculation control[1-3].

#### Client/Owner

End clients or clients who need to utilize distinctive cloud benefits by putting away their information and depend intensely on cloud for information upkeep and calculation exercises, these can be either singular customers or associations[4].

#### User

An association or venture has a great deal of representatives or clients who utilize cloud administrations of that association, these clients enrol themselves with the cloud administrations and information put away on that cloud being given by that association, here and there these clients can be a proprietor itself. Individuals depend on PC systems to get news, stock costs, email and web based shopping. The respectability and accessibility of every one of

these frameworks require to be safeguarded against various dangers. A huge crevice exists between seller cases and client perspectives of the cloud security[5], protection and straightforwardness, while cloud industry's reaction has been: Clouds are more secure than whatever you're utilizing now. In any case, numerous clients and associations do not concede to this claim. Organizations and buyers are mindful in utilizing cloud administrations to store high-esteem or delicate information furthermore, data. "One of the significant impediment of distributed computing spins around security and confidentiality of information being stores". This paper investigates the barricades and answers for give a reliable distributed computing

### Security Challenges in Cloud Condition

The cloud boisterous processing model is quickly changing the IT scene. It is another processing worldview that conveys processing assets as an arrangement of solid and versatile web based administrations permitting clients to remotely run and deal with these administrations. Be that as it may, as additional what's more, more data on people and organizations is set in the cloud, concerns are starting to become about exactly how safe a situation it is. In this way cloud security turns into a noteworthy issue and new classifications of dangers are to be presented. These dangers are a consequence of the cloud virtual foundation many-sided quality made by the reception of the virtualization innovation[6]. Rupturing the security of any segment in the cloud virtual foundation significantly impacts on the security of different segments and thusly influences the general framework security. Security challenges in a distributed computing condition might be delegated:

- Protection of information towards client's side
- Protection of information towards specialist co-op's end
- Protection of information away server or Cloud Data Focus (CDC)

One of the real worries in cloud condition is to shield client's touchy data from different clients and programmers that may bring about information spillage in cloud storage[11].

### Literature survey conducted by conducted/ released in major findings

IDC October 2008-Security October 2008 Security concern was the most concern was the most serious Serious barrier to cloud adoption barrier to cloud adoption Information week 2009 and 31% of companies in 2010 viewed SaaS Apps as less secure than the Internal IDC (conducted in Asia-Pacific) April 2010 Less than 10% of respondents were

structure with secure administration level understandings to be concurred by both vendors and clients. It proposes a protected cloud structure for both clients and specialist organizations to safely store and exchange information and apply distinctive security strategies on virtual servers to ensure private and touchy data and concede to certain administration level assertions. The system requires[8-10]:

- Actual presence of distributed computing condition
- Proper security of data in the cloud
- Trustworthiness of the frameworks in distributed computing condition

Confident about cloud security Harris Interactive survey for Novell October 2010 90% were concerned about cloud Security50 viewed security concerns as the primary barrier to cloud adoption76% thought private data more secure when stored in premises.81%were worried about regulatory Compliance IDC2011 A third of IT executives feel the benefits of cloud exceed risks .About a quarter did not fully understand the regulatory & compliance 47% concerned about a security threat. Cisco's cloud watch 2011 76% of respondents cited security & privacy a top barrier to cloud adoption.64% of respondents concerned about location of data

### Related Security Models

In spite of all the build up encompassing the cloud, endeavour clients are as yet hesitant to convey their business in the cloud. Security is one of the real issues which lessens the development of distributed computing and complications with information security and information insurance keep on torment the market[12]. Conventional system security techniques and approaches are insufficient for securing cloud assets as they wind up plainly out of date with regularly evolving what's more, expanding security dangers and to keep away from information misfortune in cloud condition. Retrieval (POR) display proposed by Juels for guaranteeing the trustworthiness of remote information on mists combines spot-checking and mistake rectifying code to guarantee both ownership and recuperation of records on file benefit systems. Wang proposed homomorphism distributed check conspire utilizing pseudorandom information to check the capacity accuracy of client information in cloud. This plan accomplishes the insurance of information availability, unwavering quality and respectability. Kamara and Lauter proposed a security display for open mists for protecting trustworthiness with the assistance of cryptographic primitives. This system is absolutely based on cryptographic stockpiling administrations. In this system, at the point when a client needs to send information to other client, they first create an ace key that encodes their message[13]. Popa proposed a technique called Cloud Proof, a safe

stockpiling framework for expanding security over cloud. In this model clients can identify infringement of uprightness, secrecy, compose serial capacity and eshness. This model uses cryptographic devices and building endeavours to acquire a proficient and versatile framework, which permit clients to recognize and demonstrate cloud misbehaviour. Li and Ping took a shot at setting up a trust-based connection between specialists co-ops furthermore, end clients to build up a safe cloud infrastructure. Jin-Song proposed another system which, isolates contain and design from archives, before taking care of furthermore, putting away of information into the remote cloud server farm to shield cloud assets from unapproved clients or hackers[14-16].

### Proposed Security Framework

Distributed computing is a looming change in Data Technology (IT) industry as it gives a more up to date form of processing in which diverse applications, software's, administrations, stages and different offices are given on request insignificant costs, most elevated accessibility and availability, most extreme limit and capacity and enthusiastic execution. This paper proposes a multi-layer portable specialist based structure for performing distinctive exercises in the cloud concurred by both customer and cloud specialist organizations. Portable specialists are utilized for performing assignments for the sake of customers on virtual machines in cloud server farms. This procedure helps both elements to construct trust and certainty on each other to utilize cloud administrations effectively. This paper proposes a multi-layer versatile operator based system for performing diverse exercises in the cloud concurred by both customer and cloud specialist organizations. Portable specialists are utilized for performing undertakings for the sake of customers on virtual machines in cloud server While the greater part of the cloud processing stages as of now utilize virtual machines where Java is completely bolstered and deals with the mechanism of "compose once, run anyplace", so versatile specialists can keep running on the JVMs with any working framework introduced. The portable specialist can relocate from one MAP to another amid its lifecycle, the outcome is sent back specifically to the customer. These layers are portrayed beneath.

1. Client to Cloud Service Provider Layer
2. Customer Authentication Layer
3. Versatile Agent Integrity and Authenticity Verification Layer
4. Asset Allocation Layer

#### Client to cloud service provider layer

This is the main layer in proposed system, which depicts the connection amongst customers and their

cloud specialist co-ops. There can be one customer or different clients and there can be one cloud specialist co-op or there can be numerous, so its pre essential to have a relationship between these both substances keeping in mind the end goal to concede to administrations required and gave by cloud stage. The connection transport amongst customer and cloud specialist co-op is straightforwardly relative to each different as customer demand an administration through versatile operator, the specialist co-op gives its virtual stage for versatile operators to execute and perform their undertakings utilizing errand directors[17].

#### Client Authentication Layer

The taking after system is taken after to build up a safe association amongst customer and cloud specialist organization the steps are portrayed beneath.

Step 1: The customer makes an association with cloud benefit supplier on a SSL port, typically 443, SSL association is indicated by HTTPS rather than HTTP.

Step 2: The cloud specialist organization answers back with its open key to the customer. When customer gets the key, program of customer checks the general population key and chooses whether to continue with association or not in view of the accompanying data.

Step 3: Public key of customer should be sent to CSP if customer believes the CSP and chooses to continue with association.

Step 4: Cloud specialist co-op makes a novel hash encoded key from both customers open key and CSP's private key. Hash (Key) is then sent back to the customer.

Step 5: Browser of customer will decode the hash key; this handle suggests that specific customer can just read the hash key sent by CSP[18-20].

Step 6: Client and CSP can now safely trade information.

The calculation used to set up hash key between customer what's more, CSP is given underneath.

#### Calculation 1: Hash Key Algorithm

Client Hello →

CSP Server Hello

Endorsement

CSP Server Key Exchange

Certificate Request← CSP Server Hello Done

Certificate

Client Key Exchange  
 Verify Certificate  
 [Cipher Spec Changed Client]  
 Finished →  
 [Cipher Spec Changed CSP]  
 ← Finished  
 Application Data ↔ Application Data

### Mobile Agent Integrity and Authenticity Check Layer

After the confirmation strategy amongst customer and CSP, Mobile Agent (MA1) will be made on customer and exchanged to CSP site. The servers introduced on both entities must check the legitimacy and trustworthiness of Mobile Operator (MA1) as appeared in Figure 4. MA1 is enacted and sets up another session key with customer. This key is kept mystery from CSP, and is utilized for secure correspondence furthermore, conceals information from CSP. This procedure guarantees customer about the security of versatile operator and assignments performed by MA1 without sharing the information and other mystery information with CSP.

### Resource Allocation Layer

MA1 asks for assets from CSP for the benefit of customer as indicated by prerequisite and assignments stack on virtual machines oversight by assignment administrator. MA1 additionally screens asset use and post a keep an eye on CPS for bogus employments of administrations. CSP apportions VM's and different assets according to the demand. Another versatile operator MA2 will be generated if required and sent to he some stage where new assets are given to play out the outlined undertakings all the more productively and vivaciously. A few versatile operators can be made in same way and introduced in various VM designated to customer. This portable specialist registers itself registers itself to portable specialist to assignment supervisor. The algorithm for entire process is portrayed beneath[21-22].

Calculation 2: Algorithm for Proposed Cloud Security system

Validation

Customer Enter Username and Password

Utilize SSL for security

CSP check Authenticity of customer

Validation Granted

Respectability Verification MA1

Send MA1 to CSP

CSP check the Authenticity uprightness of MA1

CSP sends MA1 credibility Integrity to Client

MA1 Activated at CSP Server

Session Established Between Client and MA1

CSP superseded

Asset Allocation

MA1 Act as Client

MA1 Checks Resource Requirement of customer

MA1 Request assets from CSP

CSP gifts assets to MA1

MA1 Monitor Resource Usage

MA1 Generate Alert on Misuse of Resource

## 2. Conclusion

Distributed computing is still in its early stages and security difficulties are deferring its appropriation and acknowledgment around the world. This paper proposes an extensive portable specialist based cloud security structure for cloud computing situations to build up dependable relationship amongst customers and cloud specialist organizations. The master postured structure is separated into four layers with each layer performing confirmation, check and uprightness at various levels of correspondence between two substances. We have proposed versatile specialists as principle parts for performing diverse errands allocated and asked by customers and concurred by both customers and cloud benefit suppliers. This method serves to powerfully include and design benefits on the virtual bunches in cloud information focuses. The principle commitment of our proposed work is without a doubt the understanding of reliable relationship between two elements to concur on security benefit level assentions to powerfully arrange and include portable specialists on virtual machines took care of by errand supervisors in their particular portable specialist stages. This makes the entire process straightforward and clearer as per clients furthermore, cloud specialist co-ops point of view. The proposed system viably guarantees protection and security of customer information and offers control to customer over his information utilizing the security operators. It likewise guarantees the usage of security strategies by cloud specialist co-ops to stay away from assaults on virtual machines.

### References

- [1]. Foster I, Zhao Y, Raicu I, Lu S. Cloud computing and grid computing 360-degree compared. Proceedings of the Grid Computing Environments Workshop, GCE 2008; IEEE Press; 2008. p. 1–10.
- [2]. Buyya R, Chee SY, Venugopal S, Broberg J, Brandic I. Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems*. 2009; 25(6):599–16.
- [3]. Armbrust M, Fox A, Griffith R, Joseph AD, Katz R, Kon-winski A, Lee G, Patterson D, Rabkin A, Stoica I, Zaharia M. A view of cloud computing. *Communications of the ACM*. 2010; 53(4):50–8.
- [4]. Mell P, Grance T. The NIST definition of cloud computing. *Communications of the ACM*. 2010; 53(6):50.
- [5]. Clavister. Security in the cloud. Clavister White Paper. 2009. Available from: [http://www.itwire.nu/members/cla69/attachments/CLA\\_WP\\_SECURITY\\_IN\\_THE\\_CLOUD.pdf](http://www.itwire.nu/members/cla69/attachments/CLA_WP_SECURITY_IN_THE_CLOUD.pdf)
- [6]. Brintha RS, Nalini C. An efficient cost model for data storage with horizontal layout in the cloud. *Indian Journal of Science and Technology*. 2014 Mar; 7(3S):45–6.
- [7]. Ghosal S, Chaturvedi S, Taywade A, Jaisankar N. Android application for ticket booking and ticket checking in sub-urban railways. *Indian Journal of Science and Technology*. 2015 Jan; 8(S2):171–8.
- [8]. Udayakumar R., Kaliyamurthie K.P., Khanaa, Thooyamani K.P., Data mining a boon: Predictive system for university topper women in academia, *World Applied Sciences Journal*, v-29, i-14, pp-86-90, 2014.
- [9]. Kaliyamurthie K.P., Parameswari D., Udayakumar R., QOS aware privacy preserving location monitoring in wireless sensor network, *Indian Journal of Science and Technology*, v-6, i-SUPPL5, pp-4648-4652, 2013.
- [10]. Brintha Rajakumari S., Nalini C., An efficient cost model for data storage with horizontal layout in the cloud, *Indian Journal of Science and Technology*, v-7, i-, pp-45-46, 2014.
- [11]. Brintha Rajakumari S., Nalini C., An efficient data mining dataset preparation using aggregation in relational database, *Indian Journal of Science and Technology*, v-7, i-, pp-44-46, 2014.
- [12]. Khanna V., Mohanta K., Saravanan T., Recovery of link quality degradation in wireless mesh networks, *Indian Journal of Science and Technology*, v-6, i-SUPPL.6, pp-4837-4843, 2013.
- [13]. Khanaa V., Thooyamani K.P., Udayakumar R., A secure and efficient authentication system for distributed wireless sensor network, *World Applied Sciences Journal*, v-29, i-14, pp-304-308, 2014.
- [14]. Udayakumar R., Khanaa V., Saravanan T., Saritha G., Retinal image analysis using curvelet transform and multistructure elements morphology by reconstruction, *Middle - East Journal of Scientific Research*, v-16, i-12, pp-1781-1785, 2013.
- [15]. Khanaa V., Mohanta K., Saravanan. T., Performance analysis of FTTH using GEAPON in direct and external modulation, *Indian Journal of Science and Technology*, v-6, i-SUPPL.6, pp-4848-4852, 2013.
- [16]. Kaliyamurthie K.P., Udayakumar R., Parameswari D., Mugunthan S.N., Highly secured online voting system over network, *Indian Journal of Science and Technology*, v-6, i-SUPPL.6, pp-4831-4836, 2013.
- [17]. Thooyamani K.P., Khanaa V., Udayakumar R., Efficiently measuring denial of service attacks using appropriate metrics, *Middle - East Journal of Scientific Research*, v-20, i-12, pp-2464-2470, 2014.
- [18]. T. Padmapriya and V. Saminadan, "Improving Throughput for Downlink Multi user MIMO-LTE Advanced Networks using SINR approximation and Hierarchical CSI feedback", *International Journal of Mobile Design Network and Innovation- Inderscience Publisher*, ISSN : 1744-2850 vol. 6, no.1, pp. 14-23, May 2015.

