Indian Journal of Science and Technology, *Vol 8(12), DOI: 10.17485/ijst/2015/v8i12/52923, June 2015*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Mobile Agent based Multi-layer Security Framework for Cloud Data Centers

Mueen Uddin[1*], Jamshed Memon[2], Raed Alsaqour[3], Asadullah Shah[4] and Mohd Zaidi Abdul Rozan[2]

[1]Faculty of Computer Systems and Software Engineering, University Malaysia Pahang, Malaysia; mueenmalik9516@gmail.com
[2]Department of Information Systems, Faculty of Computing, Universiti Teknologi Malaysia, Malaysia
[3]School of Computer Science, Faculty of Information Science and Technology, University Kebangsaan Malaysia, Bangi, 43600, Selangor, Malaysia
[4]Kulliah of Information and Communication Technology, International Islamic University Malaysia, Malaysia

Abstract

Objectives: This paper proposes a new mobile agent based cloud security framework comprising four different security and authentication layers to establish the trust relationship between two entities before using cloud services. **Methods/Analysis**: The proposed framework is divided into four layers with each layer performing authentication, verification and integrity at different levels of communication between two entities. An algorithm is used to check and analyze the validity and functionality of each layer. Mobile agents are used as main components for performing different tasks assigned and requested by clients from cloud service providers. **Findings**: The framework uses authenticated mobile agents from both clients and cloud service provider to perform the tasks on behalf of users to establish trustworthy computing relationship. This makes the whole process transparent and clear according to users and cloud service providers' perspective. The proposed framework effectively ensures privacy and security of client data and gives control to client over his data using the security agents. **Conclusion/Application**: The main contribution of this paper is undoubtedly the agreement of trustworthy relationship between two entities to agree on security service level agreements to dynamically configure and add mobile agents on virtual machines handled by task managers in their respective mobile agent platforms.

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

1. Introduction

Cloud computing paradigm is progressively making tremendous momentum in the recent development of IT infrastructure to provide different services to end users on demand with minimal costs and less overhead. Services provided by cloud have recently become ubiquitous service delivery model, concealing a wide range of services and applications from personal file sharing to being an enterprise data warehouse[1]. It significantly enhances collaboration; responsiveness, agility and scaling of wide range of technologies enabling a truly global computing model over the Internet. Cloud platform dynamically allocates, deploys, redeploys and cancels different services as user requirements change with passage of time[2]. Cloud computing, the long-held dream of "computing as a utility", has open up a new era of future on demand computing, transforming and reshaping large part of IT industry, to purchase and use IT resources with considerable attention from global and local IT players, national governments, and international agencies[3]. Cloud computing services are inherently provided by large scale tier level data centers, in which a pool of abstracted, virtualized, dynamically-scalable, highly available and configurable and reconfigurable computing resources are rapidly provisioned and released with minimal management effort[4].

According to a recent IDCI survey, 74 percent of IT executives and CIO's cited security as the top challenge

*Author for correspondence

preventing their adoption of the cloud services model[5]. Analysts' estimate that within the next five years, the global market for cloud computing will grow to $95 billion and that 12 percent of the worldwide software market will move to the cloud in that period. Cloud computing architecture offers on demand services and facilities with high speed Internet as "X as a Service (XaaS)" including applications platforms and infrastructure. Cloud technology employs different characteristics like location-independent resource pooling, ubiquitous network access, on-demand self-service, rapid elasticity and measured services, along with other features to provide seamless and transparent services to all customers and users. The cloud infrastructure revolves around three major functional components to make this technology progresses with a new dream vision of computing as utility to be used on demand when required and needed. These components are:

1.1 Cloud Service Provider

A cloud service provider is a company or enterprise that offers different services in cloud in the form of components typically referred to as Infrastructure as a Service (IaaS), Software as a Service (SaaS) and Platform as a Service (PaaS) to businesses or individual users on demand with highest speed, availability and uptime. This entity also manages Cloud Storage Server (CSS) for storing data and other resources to preserve users and client's information with high computation power.

1.2 Client/Owner

End users or customers who want to use different cloud services by storing their data and rely heavily on cloud for data maintenance and computation activities, these can be either individual consumers or organizations.

1.3 User

An organization or enterprise has a lot of employees or users who use cloud services of that organization, these users register themselves with the cloud services and data stored on that cloud being provided by that organization, sometimes these users can be an owner itself.

Over the last decade, our society has become technology dependent. People rely on computer networks to receive news, stock prices, email and online shopping. The integrity and availability of all these systems need to be defended against a number of threats. The distributed and open structure of cloud computing and services becomes an attractive target for potential cyber-attacks by intruders. Cloud computing is still in its infancy in spite of gaining incredible impetus recently; providing highest level of security to individuals and organizations is one of the major obstacles faced by today's clouds service providers and recently is the most discussed topic by academia and researchers. As sensitive applications and data are stored on cloud data centers, this poses many novel tangible and intangible security and privacy challenges to securely store the data and provide guarantee to users about the safely storage and transfer of their data and other vital information[6]. Security issues like accessibility, vulnerabilities, virtualization vulnerabilities, and web application vulnerabilities are the serious challenges faced by today's cloud enterprise data centers[7]. A significant gap exists between vendor claims and user views of the cloud security, privacy and transparency, while cloud industry's response has been: Clouds are more secure than whatever you're using now[8]. But many users and organizations do not agree on this claim. Issues such as security, privacy and availability are among the topmost concerns in organizations' cloud adoption decisions rather than the total cost of ownership[9]. Businesses and consumers are cautious in using cloud services to store high-value or sensitive data and information[10]. "One of the major disadvantage of cloud computing gyrates around security and confidentiality of data being stores"[11]. Cloud can ensure user's data security by implementing different security techniques like firewalls, virtual private networks and other security policies with in its own periphery or perimeter. But still the concept of cloud requires resource polling with other cloud owner's, hence, business critical or other important data is not only available to cloud but also to third party clouds[12]. Security is therefore a major element in any cloud-computing infrastructure, because it is essential to ensure that only authorized access is permitted and secure behavior is expected[13].

This paper explores the roadblocks and solutions to provide a trustworthy cloud-computing framework with secure service level agreements to be agreed by both vendors and users. It proposes a secure cloud framework for both users and service providers to securely store and transfer data and apply different security policies on virtual

servers to protect private and sensitive information and agree on certain service level agreements. The framework requires:

- Actual existence of cloud computing environment
- Proper security of information in the cloud
- Trustworthiness of the systems in cloud computing environment

2. Security Challenges in Cloud Environment

The cloud loud computing model is rapidly transforming the IT landscape. It is a new computing paradigm that delivers computing resources as a set of reliable and scalable internet-based services allowing customers to remotely run and manage these services. But as more and more information on individuals and companies is placed in the cloud, concerns are beginning to grow about just how safe an environment it is[30]. Thus cloud security becomes a major issue and new categories of threats are to be introduced. These threats are a result of the cloud virtual infrastructure complexity created by the adoption of the virtualization technology. Breaching the security of any component in the cloud virtual infrastructure significantly impacts on the security of other components and consequently affects the overall system security. Security challenges in a cloud-computing environment may be classified as:

- Protection of data towards user's side
- Protection of data towards service provider's end
- Protection of data in storage server or Cloud Data Center (CDC)

One of the major concerns in cloud environment is to protect user's sensitive information from other users and hackers that may cause data leakage in cloud storage[29]. The other inherent challenge with these cloud data centers is that data stored is unencrypted on machines owned and operated by different vendors from the data owner of the cloud. There are threats of unauthorized uses of data by service providers and theft of data from machines in a cloud data center. This is causing serious apprehension and fear in the minds of users for leaking sensitive data in the adoption of cloud as a service in their organizations. A report released in 2008 by Gartner on cloud security states that, there are serious threats to data integrity, recovery and privacy while adopting and implementing cloud services[14]. These security threats and attacks are the biggest concern towards the improvement of a more secure cloud infrastructure. Different critics perceive and agree that concerns related to security, privacy and confidentiality of cloud servers having physical control of data, identity and credential management responsible for storing data securely and data verification, tempering, integrity, confidentiality, data loss and theft might outweigh other benefits provided by clouds. Table 1 shows Organizations' perceptions of the cloud's security through different surveys and clearly demonstrates that there is a major gap exists between users and vendors on security breaches or lawsuits tied to data breach while providing security facilities.

A cloud-computing platform is exposed to several threats including threats to the integrity, confidentiality and availability of its resources, data and the virtualized infrastructure, which can be used as a launching pad for new attacks[15]. Around last year 2011, a hacker used Amazon's Elastic Computer Cloud service to attack Sony's online entertainment systems by registering and opening an Amazon account and using it anonymously[16]. Cloud services are as cheap and convenient for hackers as are for clients. This malicious incidental attack on Sony compromised more than 100 million customer accounts, the largest data breach in the U.S[17]. The cloud challenges differ according to different cloud scenario, but most of the research currently focuses on:

- How to make and increase users control over their data when stored and processed in cloud to avoid theft, nefarious use and unauthorized resale.
- How to guarantee data replications in a jurisdiction and consistent state, where replicating user data to multiple suitable locations is a usually choice, and avoid data loss, leakage and unauthorized modification or fabrication.
- Which party is responsible for ensuring legal requirements for personal information?
- What extent cloud sub-contractors involved in processing can be properly identified, checked and ascertained.
- How to establish a trustworthy relationship between client and cloud service provider to agree on different security service level agreements.

Table 1. Organizational perception of cloud's security

Survey Conducted by	Conducted/ Released in	Major Findings
IDC October 2008 - Security concern was the most serious barrier to cloud adoption	October 2008	Security concern was the most serious barrier to cloud adoption for
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 confident about cloud security measures.
Harris Interactive survey for Novell	October 2010	• 90% were concerned about cloud security. • 50 viewed security concerns as the primary barrier to cloud adoption. • 76% thought private data more secure when stored on the premises. • 81% were worried about regulatory compliance.
IDC	IDC 2011	• A third of IT executives feel the benefits of cloud exceed risks. • About a quarter did not fully understand the regulatory and compliance issues in cloud computing, • 47% concerned about a security threat.
Cisco's CloudWatch	2011	• 76% of respondents cited security and privacy a top barrier to cloud adoption. • 64% of respondents concerned about location of data.

3. Related Security Models

Despite of all the hype surrounding the cloud, enterprise customers are still reluctant to deploy their business in the cloud. Security is one of the major issues which reduces the growth of cloud computing and complications with data privacy and data protection continue to plague the market. Traditional network security techniques and policies are not enough for protecting cloud resources as they become obsolete with ever-changing and increasing security threats and to avoid data loss in cloud environment. A lot of research is going on to develop strategies for implementing secure clouds. Retrievability (POR) model proposed by Juels for ensuring the integrity of remote data on clouds combines spot-checking and error-correcting code to ensure both possession and recovery of files on archive service systems[18]. Wang proposed homomorphism distributed verification scheme using pseudorandom data to verify the storage correctness of user data in cloud. This scheme achieves the guaranty of data availability, reliability and integrity. However, this scheme was also not providing complete protection to user data in cloud computing, since pseudorandom data would not cover the entire information[19].

Kamara and Lauter proposed a security model for public clouds for preserving integrity with the help of cryptographic primitives. This technique is purely based on cryptographic storage services. In this technique, when a user wants to send data to other user, they first generate a master key that encrypts their message. The secret key for decryption is stored on receivers' system for decrypting the same message[20]. Popa proposed a technique called Cloud Proof, a secure storage system for increasing security over cloud. In this model users can detect violations of integrity, confidentiality, write serial ability and freshness. This model uses cryptographic tools and engineering efforts to obtain an efficient and scalable system, which allow users to detect and prove cloud misbehavior[21]. Li and Ping worked on establishing a trust-based relationship between service providers and end users to develop a secure cloud infrastructure[22]. Jin-Song proposed another technique which, separates contain and format from documents, before handling

and storing of data in to the remote cloud data center to protect cloud resources from unauthorized users or hackers[23]. An optimized authorization method (using encryption functions) is used for accessing database for trusted CSUs. Many works, which deal with design of agent based Grid platforms, use mobile agent's technology in order to implement basic services addressing some topics such as load balancing, fault masking and service discovery[24]. Mobile agents are utilized in order to manage and assign resources and to distribute applications and data. A mobile agent's based approach will allow moving services through different virtual machines and in different cloud contexts. A set of specialized agents will enrich the platform with a set of facilities for performing measures about the user-perceived performances and to dynamically adapt the allocation of resources on the basis of the effective load and the actual service level offered by a cloud[32].

Krugel point out the value of filtering a packet sniffer output to specific services as an effective way to address security issues shown by anomalous packets directed to specific ports or services. An often-ignored solution to accessibility vulnerabilities is to shutdown unused services, keep patches updated, and reduce permissions and access rights of applications and users[25,26]. Raj suggests resource isolation to ensure security of data during processing, by isolating the processor caches in virtual machines, and isolating those virtual caches from the hypervisor cache[26]. Hayes points out that there is no way to know if the cloud providers properly deleted a client's purged data, or whether they saved it for some unknown reason[27]. Basta and Halton suggested a way to avoid IP spoofing by using encrypted protocols wherever possible. They also suggest avoiding ARP poisoning by requiring root access to change ARP tables; using static, rather than dynamic ARP tables; or at least make sure changes to the ARP tables is logged[28]. Hayes points out an interesting issue of allowing a third-party service to take custody of personal documents raises awkward questions about control and ownership: if you move to a competing service provider, can you take a data with you? Could you lose access to documents if you fail to pay a bill? The issues of privacy and control can't be solved, but merely assured with tight Service-Level Agreements (SLAs) or by keeping the cloud itself private[27].

4. Proposed Security Framework

Cloud computing is an impending transformation in Information Technology (IT) industry as it provides a newer version of computing in which different applications, software's, services, platforms and other facilities are provided on demand with minimal costs, highest availability and accessibility, maximum capacity and capability and vigorous performance. It provides all these facilities without investing in new infrastructures, developing new personnel or licensing new software's. Cloud service providers use large tier level data centers for providing gigantic data storage and faster computing to customers over the Internet. A data center is a repository for storage, backups, availability and dissemination of data and services in a more robust and effective way. These data centers are associated with all multinational organizations like Amazon, Microsoft, Dell, IBM, Google and many others use them either for their own users requirements or for outsourcing purposes. As different services, databases, and application software's are being shifted to these large cloud data centers, the management of data and services becomes the critical issue between customers and service providers to provide trustworthy computing[31]. A lot of research is currently being conducted to develop security techniques and solutions to make agreements between customers and service providers to agree on certain security measures for securely transfer and store data and services.

This paper proposes a multi-layer mobile agent based framework for performing different activities in the cloud agreed by both client and cloud service providers. Mobile agents are used for performing tasks on the behalf of clients on virtual machines in cloud data centers. Clients and cloud service providers authenticate and verify these mobile agents to agree on specific rules to achieve security in order to perform all activities to create a trustworthy platform. This process helps both entities to build trust and confidence on each other to use cloud services efficiently.

A Mobile Agent (MA) is a piece of software used to design, implement, and maintain data and services in large scalable networks. They are used for their ability to operate asynchronously and autonomously of the process that created them. One of the major characteristics of

mobile agents is their ability to construct more robust and fault-tolerant systems and allow people to delegate work to them. This feature is used in the proposed framework to work on the behalf of clients. Cloud computing provides a substantial capability and provides best platform for these mobile agents to offer their services and capabilities to build secure cloud environment. Mobile agent based cloud computing framework is proposed because most of the mobile agent systems like Aglets and D' Agent are based on or support Java. While most of the cloud computing platforms currently use virtual machines where Java is fully supported and works on the mechanism of "write once, run anywhere", so mobile agents can run on the JVMs with any operating system installed. This feature helps to implement security framework without installing additional equipments and other hardware and software devices.

The mobile agent agreed and verified by both client and cloud service provider runs on a Mobile Agent Platform (MAP) installed on each virtual machine. These machines can have more than one mobile agent platform to support different types of mobile agents for performing different tasks from different clients simultaneously and to balance the load and resource requirements in large tier level data centers. The virtual machine or even physical machine acts as Task Manager (TM). The working of mobile agent and its task manager is shown in Figure 1. The user send an agreed, authenticated and verified mobile agent to the task manager, who reads the header of mobile agent to assess whether it's a mobile agent or other kind of data packages. The task manger matches the requirement with its resource index to decide which MAP the mobile agent should be sent to, or assign a new virtual machine with a MAP for that mobile agent. Once the MAP receives the mobile agent, it activates the mobile agent and executes the task included in the mobile agent and the process starts to execute and fulfill clients request in the virtual machine. The mobile agent monitors the execution of the task and the situation of the resources in the MAP, decide whether to leave the MAP, or clone some new mobile agents if required and send them to other MAPs in the same CSP or in a different CSP to accomplish the task. In simple case, clients' tasks are assigned to one or many mobile agents, if there are many mobile agents, these mobile agents don't interact with each other during the

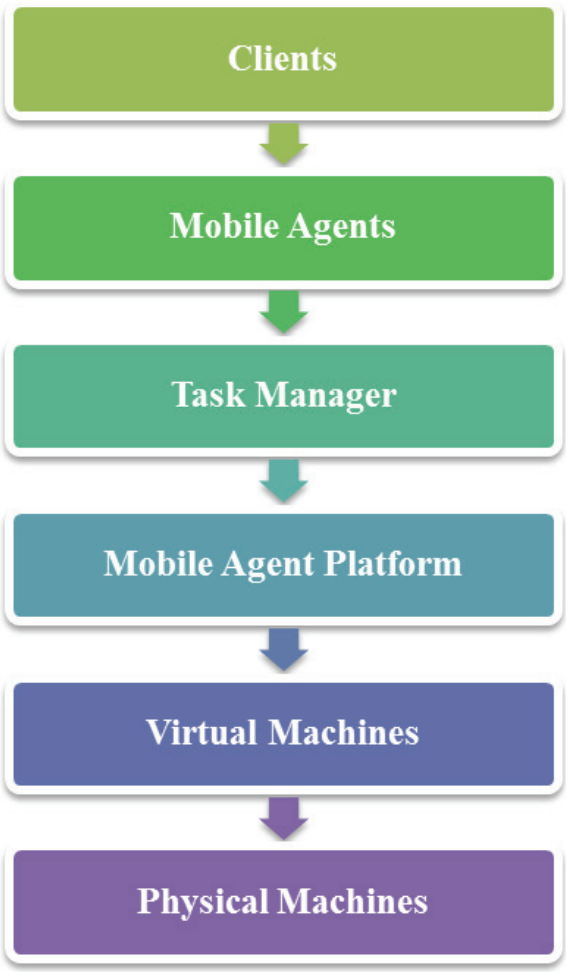

Figure 1. Mobile agent based execution of tasks.

execution of their tasks, but task manager can receive these mobile agents and sends them to their specific MAP for execution. The mobile agent can migrate from one MAP to another during its lifecycle, the result is sent back directly to the client. These mobile agents help in building the trust between various entities communicating with each other via a secure and reliable communication.

The proposed multi-layer security framework is divided into four layers. These layers are described below.

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

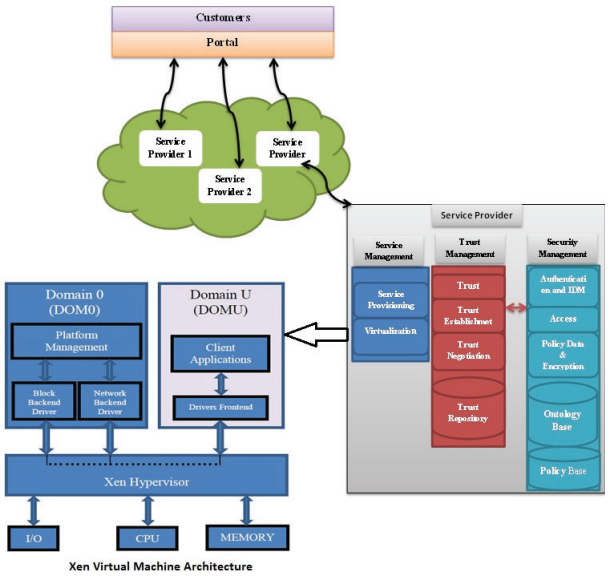

Figure 2. Customer to cloud service provider layer.

4.1 Customer to Cloud Service Provider Layer

This is the first layer in proposed framework, which describes the relationship between clients and their cloud service providers. There can be one client or multiple clients and there can be one cloud service provider or there can be many, so its pre requisite to have a relationship between these both entities in order to agree on services required and provided by cloud platform. The relationship between client and cloud service provider is directly proportional to each other as client request a service through mobile agent, the service provider provides its virtual platform for mobile agents to execute and perform their tasks using task managers as shown in Figure 2.

4.2 Client Authentication Layer

The second layer where cloud service provider and client must authenticate and verify each other in order to agree on certain service level agreements for achieving security to securely perform different services using mobile agents. The authentication is provided by using SSL key exchange mechanism to establish a trustworthy relationship between two entities as shown in Figure 3. The following mechanism is followed to establish a secure connection between client and cloud service provider the steps are described below.

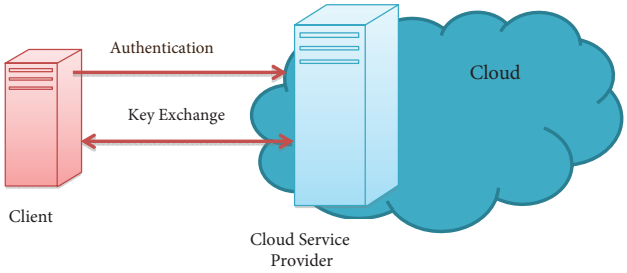

Figure 3. Client authentication layer.

Step 1: The client creates a connection to cloud service provider on an SSL port, normally 443, SSL connection is denoted by HTTPS instead of HTTP.

Step 2: The cloud service provider replies back with its public key to the client. Once client gets the key, browser of client checks the public key and decides whether to proceed with connection or not based on the following information.

a) The CSP public key need NOT be expired
b) The CSP public key must be for that particular client only
c) Trust wave must be installed on clients' browser certificate store. 99.9% of all modern browsers contain the Trust wave root certificate. Trust wave certificate indicates that they can trust the cloud service provider and that public key really belong to that particular cloud service provider with whom client want to connect.

Step 3: Public key of client needs to be sent to CSP if client trusts the CSP and decides to proceed with connection.

Step 4: Cloud service provider creates a unique hash encrypted key from both clients public key and CSP's private key. Hash (Key) is then sent back to the client.

Step 5: Browser of client will decrypt the hash key; this process implies that particular client can only read the hash key sent by CSP.

Step 6: Client and CSP can now securely exchange information.

The algorithm used to establish hash key between client and CSP is given below.

Algorithm 1: Hash Key Algorithm

ClientHello →
CSPServerHello
Certificate
CSPServerKeyExchange
CertificateRequest

← CSPServerHelloDone
Certificate
ClientKeyExchange
VerifyCertificate
[CipherSpecChangedClient]
Finished →
[CipherSpecChangedCSP]
← Finished
ApplicationData ←→ ApplicationData

4.3 Mobile Agent Integrity and Authenticity Verification Layer

After the authentication procedure between client and CSP, Mobile Agent (MA1) will be created on client and transferred to CSP site. The servers installed on both entities must check the authenticity and integrity of Mobile Agent (MA1) as shown in Figure 4. MA1 is activated and establishes a new session key with client. This key is kept secret from CSP, and is used for secure communication and hides data from CSP. This process ensures client about the security of mobile agent and tasks performed by MA1 without sharing the data and other secret information with CSP.

4.4 Resource Allocation Layer

MA1 requests for resources from CSP on behalf of client according to requirement and tasks load on virtual machines managed by task manager. MA1 also monitors resource usage and post a check on CPS for false uses of services. CSP allocates VM's and other resources according to the request. A new mobile agent MA2 will be generated if required and sent to the some platform where new resources are provided to perform the designed tasks more efficiently and vigorously. Several mobile agents can be created in same way and installed in different VM allocated to client. This mobile agent registers itself registers itself to mobile agent to task manager. These mobile agents can generate new pair of keys for communication with other mobile agents as shown in Figure 5. The algorithm for whole process is described below.

Algorithm 2: Algorithm for Proposed Cloud Security framework

Authentication
Client Enter Username & Password
Use SSL for security
CSP check Authenticity of client
Authentication Granted

Integrity Verification MA1
Send MA1 to CSP
CSP verify the Authenticity integrity of MA1
CSP sends MA1 authenticity Integrity to Client
MA1 Activated at CSP Server
Session Established Between Client and MA1
CSP overridden
Resource Allocation
MA1 Act as Client
MA1 Checks Resource Requirement of client
MA1 Request resources from CSP
CSP grants resources to MA1
MA1 Monitor Resource Usage
MA1 Generate Alert on Misuse of Resources
Resources Allocated to MA1

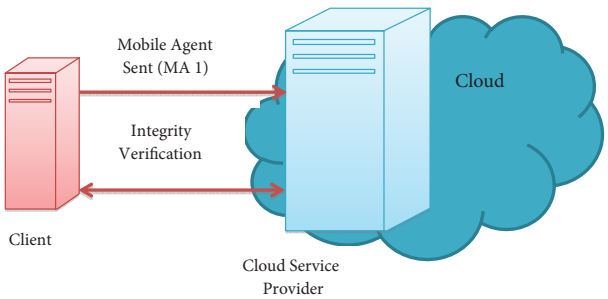

Figure 4. Mobile agent integrity and authenticity verification layer.

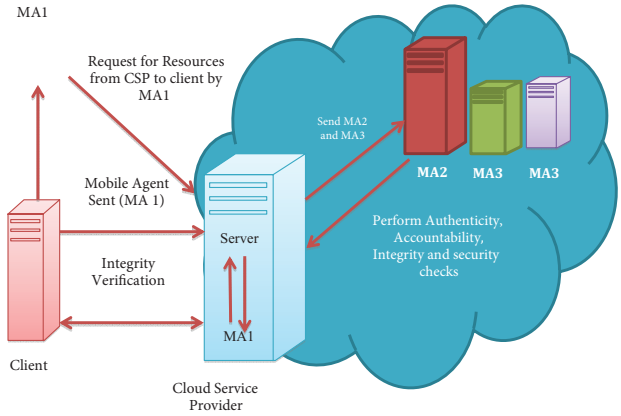

Figure 5. Resource allocation layer.

5. Conclusion

Cloud computing is still in its infancy and security challenges are delaying its adoption and acceptance worldwide. This paper proposes a comprehensive mobile agent based cloud security framework for cloud computing environments to establish trustworthy relationship between clients and cloud service providers. The proposed framework is divided into four layers with each layer performing authentication, verification and integrity at different levels of communication between two entities. We have proposed mobile agents as main components for performing different tasks assigned and requested by clients and agreed by both clients and cloud service providers. This technique helps to dynamically add and configure services on the virtual clusters in cloud data centers. The main contribution of our proposed work is undoubtedly the agreement of trustworthy relationship between two entities to agree on security service level agreements to dynamically configure and add mobile agents on virtual machines handled by task managers in their respective mobile agent platforms. This makes the whole process transparent and clearer according to users and cloud service providers perspective. The proposed framework effectively ensures privacy and security of client data and gives control to client over his data using the security agents. It also ensures the implementation of security policies by cloud service providers to avoid attacks on virtual machines.

6. 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, Konwinski 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.it-wire.nu/members/cla69/attachments/CLA_WP_SECURITY_IN_THE_CLOUD.pdf
6. Paquette S, Jaeger PT, Wilson SC. Identifying the security risks associated with governmental use of cloud computing. Government Information Quarterly. 2010; 27(3):245–53.
7. Subashini S, Kavitha VA. Survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications. 2011; 34(1):1–11.
8. Talbot D. Security in the ether. Technology Review. 2010; 113(1):36–42.
9. Brodkin JS. Problems with SaaS security. Network World. 2010; 27(18):1–27.
10. Goodburn MA, Hill S. The cloud transforms business. Financial Executive. 2011; 26(10):34–9.
11. Allen JM. Cloud computing: heavenly solution or pie in the sky? Pennsylvania. CPA Journal. 2011; 82(1):1–4.
12. Julisch K, Hall M. Security and control in the cloud. Information Security Journal: A Global Perspective. 2010; 19(6):299–309.
13. Overby E, Bharadwaj A, Sambamurthy V. Enterprise agility and the enabling role of information technology. European Journal of Information Systems. 2006; 15(3):120–31.
14. Heiser J, Nicolett M. Assessing the Security risks of cloud computing. 2008. Available from: http://www.gartner.com/DisplayDocument?id=685308,2008
15. Cloud-Security-Alliance, Top Threats to Cloud Computing V1.0. 2010. Available from: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf
16. Galante J, Kharif O, Alpeyev P. Sony network breach shows amazon cloud's appeal for hackers. 2011 May 17. Available from: http://www.bloomberg.com/news/2011-05-15/sony-attack-shows-amazon-s-cloud-service-lures-hackers-at pennies-an-hour.html
17. Pearson S, Benameur A. Privacy, security and trust issues arising from cloud computing. CloudCom 2010. Proceedings of the 2nd IEEE International Conference on Cloud Computing Technology and Science; IEEE Press; 2010 Nov. p. 693-02.
18. Juels A, Burton J, Kaliski S. PORs: proofs of retrievability for large files. Proceedings of CCS'07; 2007. p. 584–97.
19. Wang C, Wang Q, Ren K, Lou W. Ensuring data storage security in cloud computing, quality of service. 2009. IWQoS IEEE 17th international workshop; 2009. p. 1–9.
20. Kamara S, Lauter K. Cryptographic cloud storage. Lecture Notes in Computer Science. 2010; 6054:136–49.
21. Popa RA, lorch JR, Molnar D, Wang HJ, Zhuang L. Enabling security in cloud storage SLAs with cloudproof. Technical report Microsoft Research. 2010 May.
22. Li W, Ping L. Trust model to enhance security and interoperability of cloud environment. LNCS 5931. Proceedings of CloudCom 2009; Springer-Verlag Berlin Heidelberg; 2009. p. 69–79.
23. Xu J-S, Huang Ru C, Huang WM, Yang G. Secure document service for cloud computing. LNCS 5931. Proceedings of CloudCom 2009; Springer-Verlag Berlin Heidelberg; 2009. p. 541–6.
24. Algirdas A, Jean-Claude L, Brian R, Carl L. Basic concepts and taxonomy of dependable and secure computing. IEEE

Transactions on Dependable and Secure Computing. 2004; 1(1):11–33.
25. Krugel C, Toth T, Kirda E. Service specific anomaly detection for network intrusion detection. Proceedings of the 2002 ACM Symposium on Applied Computing; 2002. p. 201–8.
26. Raj H, Nathuji R, Singh A, England P. Resource management for isolation enhanced cloud services. Proceedings of the 2009 ACM Workshop on Cloud Computing Security; Chicago, USA: 2009. p. 77–84.
27. Hayes B. Cloud computing. Commun ACM. 2008; 51(7):9–11.
28. Basta A, Halton W. Computer security and penetration testing. Delmar Cengage Learning. 2007.
29. 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.
30. Ghosal S, Chaturvedi S, Taywade A, Jaisankar N. Android application for ticket booking and ticket checking in suburban railways. Indian Journal of Science and Technology. 2015 Jan; 8(S2):171–8.
31. Neela TJ, Saravanan N. Privacy preserving approaches in cloud: a survey. Indian Journal of Science and Technology. 2013 May; 6(5):4531–5.
32. Rajathi A, Saravanan N. A survey on secure storage in cloud computing. Indian Journal of Science and Technology. 2013 Apr; 6(4):4396–401.