Security Framework for Federated Cloud Environment

Ghulam Mudassir
School of Information Technology, University of Lahore, Pakistan.
&
S.T. Rehman
Faculty of Technology, Preston University, Islamabad, Pakistan.

Abstract:
Recently emergence of cloud computing drastically brought a revolution in the field of Information technology as well as in the perception of user about software delivery, development and architecture of infrastructure. Cloud computing architecture consisted on the element of grid computing, autonomic computing and utility computing. The fast pace of cloud computing utilization indulge the user of these systems into critical issue like security of the data. For this purpose cloud computing environment required an efficient mechanism or technique because it contains different kinds of private data, business transaction and different resources as well. In this paper we have proposed a unique model to solve the security issues especially regarding the security of storage data. Actually this model consisted on four layers two types of agents (CSU agents, CSP agents) and trust management layer have two modules (Security management module, trust management module) for checking the identification and trust of accessing user.

Keywords: Cloud Service User, Cloud, Service Provider, Secure System, Development Life Cycle

1-Introduction
In the last few years cloud computing have got immense attraction in the field of information technology, actually it is not a new innovation it is the mixture of existing technologies gives advanced computational power and also improved storage capabilities as well but due to some issues regarding security and trust it can’t fully prevailed its business to customer with full fledged confidence [1, 2]. But in the same way Cloud computing provides unlimited resources to client or user on request with fault tolerance, scalability and high performance [3].

Cloud computing accumulate different services to provide main services to user such as Data-as-a-Service(DAAS), Infrastructure as a Service(IAAS), Platform-as-a-Service(PAAS) and Software-as-a-Service(SAAS). However security of data in all these services is most important but now days it has become more critical as compared to past [4]. According to recent research still cloud computing has security problems regarding data storage because trend of shifting data to cloud computing increasing rapidly but processing and storage of data is somewhere on centralized location called “Data Centers”. In this prospect client always expect provider will give availability as well as security to their data. Moving private and confidential data between public and shared cloud environment is the major role of provider to keep the security over network. But verifying the security of cloud data storage is even more challenging regarding confidentiality, correctness, availability and integrity [5]. As we know this paper described federated security frame work for cloud computing for this purpose here is following the secure system development life cycle (SecSDLC) which has to be adopted for any secure framework.
1.1- Cloud Computing Goals:

1.1.1- Availability
Goal of availability in cloud computing means to ensure the user every kind of application of cloud available at any time, at any place. Cloud computing system allows the user to access the system from anywhere. This is the basic principle for all cloud system. Basically hardening and redundancy are the two basic properties used to enhance the availability of cloud computing systems. Mostly vendors which provide cloud computing systems their application and infrastructures are base on virtual machines e.g. Amazon totally based virtual machines which are called Xen [6] and similarly all the other system used different kind of virtual machines. For this purpose all the service provider take resources from Amazon and pay them according to services which are used. Basically virtual machine has capability to provide resources on demand to individual user on requirement. Here is following described the figure of virtual machine.

![Figure 2: Infrastructure of virtual machine][2]

Prominent vendors of cloud computing system such as Amazon and Google also provide geographic redundancy in heir system, and might be availability will be high for single provider. According one of the researches Google has 1 million machines across the world which is distributed in 36 data centers.

1.1.2- Confidentiality:
In confidentiality goal means cloud system should keep the privacy of user data. As it known cloud systems offers public networks for this purpose keeping all the data of the user confidential is the fundamental requirement of cloud system, in this way more people will be attracted towards this new concept. Basically there are two approaches in cloud system which are currently using for the privacy of confidential data of the user which are (i) physical location, (ii) cryptography, and these approaches are successfully practiced by TC3[8].

1.1.3- Privacy:
Privacy is one of the most important goals of cloud computing, both in the term of trust as well as legal acquiescence and it has great value in each stage. Maintaining privacy is always a critical issue for...
software engineer who build cloud services for user to uphold their trust. Here are following some point for developers, engineer and testers regarding maintaining the privacy of users [9].

(i) Minimum personal information should be stored on cloud
(ii) Permission of choice to clients
(iii) Personal information protection should be maximum
(iv) User control should be maximum
(v) Specification of the purpose for data use.
(vi) Provide feedback.

1.1.4 - Data Integrity:
Data integrity in cloud computing system is the basic requirement from user; it means no one unauthorized user allows to make changing or modification in data. As we know data is the basic thing for cloud computing services like DAAS, SAAS and PAAS. And responsibility of all these service to keep the integrity of data. Usually cloud computing have massive capacity in storing data.

In cloud system there are different technique using for data integrity, but most commonly technique which is used called Digital signature. The distributed file system in cloud system like GFS and HDFS divide large data into set of blocks and each block has default size of 64MB and 128MB. Each block assigned a digital signature for data integrity which recovers private and confidential data form corruption. So data integrity is the basic requirement for cloud computing and hopefully in near future other techniques like RAID-liked strategies will also be implemented for this purpose [10, 11].

1.1.5 - Control:
In cloud computing system control means to adjust the system including infrastructure, application and data. Cloud computing system always consist on distributed file system which store stat with the help of millions of machines. And every cloud use can access the data and use it through internet form different location e.g. Google search web pages and Amazon book store. So quality controls in computing system enhance the security of overall cloud computing system as well.

1.1.6 - Audit:
In cloud computing system Audit goal is used to monitor the overall what kind of activities running in the entire system, it is considered as an additional layer over virtual applications which are hosted on virtual machine. This additional layer is much securing than software contains itself. In most of the countries it is rule the cloud computing provides should not give access to customer data from other country to maintain the security for this purpose audit goal is used.

1.1.7 - Security-as-a Service:
Security-as-a Service is looking very much important in future prospect, because the way shifting information security work from internal to subcontract or outsourced and other security prospective are required form the organization which are using cloud system[12].

1.2 - Security Threats and Challenges of Cloud Computing
Cloud system is the new phenomena in field of information technology as it is provide very cheap resources according the requirement in the same way it’s facing some threats and challenges in the prospect of security. Here some of the following threats which are mentioned by “Cloud Security Alliance [13]”.

1.2.1 - Insecure Interface:
In cloud system the software interface through which user interacts should be secure especially when third party uses it regarding access control, authentication, and encryption and monitoring.
1.2.2- Data Losing or Leakage:
Deletion of data without any backup or deletion action perform by an unauthorized user always very dangerous. This think shake the confidence of user on cloud service provider and this is also violation of law to keep the data safe.

1.2.3- Hijacking:
In cloud system hijacking of account and services is another big issue for the cloud user and this thing performed by hacker’s fort the problems like denial of service attacks.

1.2.4- Multi-location of data:
In cloud computing data stored in multi location, it might be quite dangerous if it is stored on third part devices. In this way many things can be happen, firstly cloud service provider may finish the service or business and secondly the company should know in which country its data hosted.

1.2.5- Service provider Multi-location:
Service provider is also on multi-location so clients also want to know how the CSP is providing declared services. Through this way client will keep update about private data and also able to maintain direct relationship with CSP.

1.2.6- Data Commingling:
Clients of Cloud system want to ensure whether it private data stored separately or combined with other users. If it is commingled with the data of other clients then it might be quite dangerous regarding virus attacks from other data or there might be a chance of hijacking of confidential data as well.

1.2.7- Sniffer attacks:
These are attacks which are launched by detaining the packet of data flowing through network and it these packets are not encrypted or in readable form then these can be read.

1.2.8- IP Address Reusability:
In cloud computing system when user logout from the network then assigned IP of earlier user will be given new one, in this way there is a chance that new user might access the old one data because the earlier address may exist in DNS cache. So this may violate the privacy of old user.

1.2.9- SQL Injection Attacks:
In this attack malicious code is inserted into standard SQL statement. After that attackers can get unauthorized access to database and can change or delete the sensitive data.

1.2.10- Denial of Service Attacks:
In this attack service of cloud system make unavailable for authorized user. Through this attack server might be overloaded by request and in this way server might not respond to authorized users as well and when any customer try to access the site it gives error.

1.2.11- Poisoning of Cookies:
In this kind of attack contents of cookies changes by unauthorized user to have an access to WebPages. Basically cookies contain information of legal user once they make an access to cloud application after that using those information illegal user try to access the applications of cloud. Here following is the figure of Cookies poisoning.
1.3- **Agent Technology:** Agent technology is the combination of Artificial Intelligence and Network technology. It is more useful in dynamic and distributed applications, and now days it is using in many sectors of computer science.

**Definition:** Still it has not exact and clear definition usually call it intelligent agent or simple agent. Each researcher define it, in their own context of research but two researchers Wooldridge and Jennings defines it by two way “weak definition and strong definition”[21][20] according to its usage also these definition accepted more authentic by most of the academia.

**Weak definition:** Agent is the kind of computer hardware that has following features: autonomy, sociality, reactivity, procreativity, temporal continuity and goal orientedness.

**Strong Definition:** An agent that satisfies the weak definition features as well as more features of strong definition like mobility, adaptivity and collaboration.

1.3.1- **Types of Agents:**
Agents can be divided into several types on the behalf of usage and functionality; here we will describe the CSU Agent and CSP Agent which are currently using in our proposed framework.

**CSU Agent:** Cloud Service User agent is used for authentication from database whether the requested user is authorized or not.

**CSP Agent:** Cloud Service Provider Agent take information from A.I Agent before accessing to data storage layer, whether requesting user is authorized or not.

In this paper, in section II contain literature review III proposed methodology IV performance analysis V Experiment & Results VI conclusion.

2- **Literature Review**
There are many research has to done in the area of security of clouds. Many organization groups and research institute working for cloud security standards and in this regard many experiments analysis as well security frameworks has been proposed [15].

As it is obvious all the big vendors of clouds system like Google, Yahoo and Microsoft give the facility of data storage to customer. In this way customer also dependent on CSP for their data integrity but unfortunately still no CSP is reliable there exists many threats and also a chance of data corruption. Shah and Bakers et al [17] proposed an efficient auditing protocol which not ensure data integrity but also counterfeit to unauthorized customer who might involve in the corruption of data. Privacy of data achieved through zero-knowledge and obscurin...
data through auditor. This protocol exists on three stages: Initialization, extraction and audit. In initialization phase the customer and service provider access the stored data object under the agreement and auditor confirms that both parties are agreed on content of encrypted data. After that protocol enter into Audit stage auditor use challenge-response protocol to authenticate the confirmation of data possession by the cloud service provider. And in final stage of extraction, auditor confirms the integrity of data and returned to the customer by using auditor. The encrypted form of data and other version of encryption are passing to auditor. The auditor again confirms its comprehensiveness and handed over to the customer or user who convalesce the actual data. So the proposed protocol provides effectiveness of data and possibly divides data into encryption key and encryption data.

Wang and Sherman et al [16] proposed a public auditing system by using a privacy preserving protocol for the data storage security. This auditor having capability to audit the user data contents without having knowledge. This auditing method consist on almost for algorithm (VerifyProof, SigGen, KeyGen,GenProof ).TPA run VerifyProof and audit the proof from cloud server, SignGen algorithm is used for the verification of metadata, KeyGen algorithm is used by the user to set up the scheme and GenProof is used by CSP to assure the data storage accuracy. This proposed auditing scheme is considered among one of the leading work which support a proficient and scalable public auditing for cloud storage security.

Takabi et al [19] formulated a security frame work to secure cloud data storage environment. This frame work deal with current challenges which are facing by clouds system and it consist on different modules to control the challenges and problems and trust issue of cloud system as well. These modules control the issue from different clouds like policy integration, identity management, trust management and access control.

Venkkatesan and Vaish [18] presented an efficient frame work that is based on static and dynamic data reliability and frequently check the files stored on data storage. Actually this framework based on different multi agents because agent have potential of self-governing, social ability and perseverance. The proposed frame work has Multi agents to supervise the integrity of data and architecture as well. Architecture consists on service provider, customer and data owner.

(Bowers et al 2008) [21] Formulated an improved framework for “Proof of Retrievability” (POR) and extended it to distributed systems but all these mechanisms consist on static data. The most prominent thing in this framework it works on basic steps which user adopts before accessing the cloud data storage files. If there exist any sort of change in the content then must proliferate in error-correcting code. In this way it introduces a prominent working out and communication.

In data possession work (Curtmola et al, 2008) [17] purpose was to ensure multiple duplication of data across the network of distributed system. In this work “Provable
data possession” (PDP) is extended to ensure the multiple replicas of data are maintained without indoctrination each copy of data separately.

(Francisco et al 2002)[13] provide a mechanism to handle the security issues in one of the project named Dynamic on-LinEIntErnet Purchasing System based on Intelligent Agents (DEEPSIA) that is used for e commerce as a purchaser in this method very famous language named KQML is used for security functions and also formulated a new enhanced from of this language called S-KQML (Secure-Knowledge Query Manipulation Language) it contains properties of privacy, integrity and authentication.

(Lalanaet al 2002) [9] also formulated an approach for the security of multi-agent system, which make use of entrustment and trust management. So the main focus of this approach was verification and authorization.

(Ayesh&Bechkoum, 2000) [24] also proposed a framework for internet security using multi-agents and it composed on three different types of agents first intrusion detection, second encryption and decryption and third is combination of first two types, their classification is on the behalf of their functionalities. This frame work is very useful regarding security purpose but it has no concern about other security services like authentication, verification, digital signature and authorization as other approaches have. This approach is like (Gray et al , 1998) [24] focus on agents owner authentication ,endorsement to assign entrance restriction and enforcement that agents doesn’t infringe the restriction.

**Research Question**
The present research contributes to existing framework in two dimensions. Firstly it seamlessly integrate the security into existing framework thereby avoiding issues of integration, Secondly this research also provides adequate auditing facility.
3- Methodology
Here is following detail our propose methodology.

3.1- Proposed Cloud Security Framework
Our proposed security framework consists of four layers which are user agent layer, trust management layer, clouds service provider layer and data storage layer. In this model agent layer working as a bridge between user and the rest of the agents. The flow of information and other activities of proposed model discussed following step by step.

Step 1: Initially user interacts through agent layer.
Step 2: Cloud service user information sent to CSU Agent.
Step 3: CSU Agent communicate with CSU Agent database whether the correspondent user authorized or not.
Step 4: After checking the authorization CSU Agent acknowledge to CSU Agent.
Step 5: If authorized CSU Agent sent its information to security management. Security management identify the user, if it is trusted using security policies then forward it to trust management module. If there exist many user then stored in List “A” and check security individually.
Step 6: After receiving job from security management module, trust management module check the trusted value which user assigned from database, if this value greater then threshold then it’s confirmed that user is trusted and inform to security management module. And sent back to security management. And for the participant in the list checks the threshold of each user and create a list of...
threshold on the basis of local trust policy and current security policy. Every client which has trust value higher than threshold removes from List “A” and adds into List “T”.

**Step 7:** After that trust management module returns the list “T” to security management module.

**Step 8:** If client is not trusted then Security management module sent back to CSP agent.

**Step 9:** Then CSP Agent reject that specific client to user agent layer that it not trusted user or it is might be malicious.

**Step 10:** In the prospect of list after checking threshold security management compare List “A” with List “T”.

**Step 11:** If both lists are equal then security module allow for further process otherwise reject it.

**Step 12:** After verification of trusted user then forward it to cloud service provider.

**Step 13:** CSP communicate with CSP agent regarding new user.

**Step 14:** CSP agent communicate with security management module for verification that the requested user is authorized or not.

**Step 15:** SM Module acknowledge in this prospect.

**Step 16:** If CSP Agent acknowledge it is not authorized user, trying to access by illegal way or it’s a suspected user.

**Step 17:** So it request sent back to user agent layer.

**Step 18:** If CSP Agent authenticate that it’s a legal user then allow cloud data storage layer and getting the required data.

### 3.2- Architecture and System Design

It is a four tier architecture which is use for the security of proposed framework. User agent layer is used to control and communicate with other agents and users, trust management layer contain security policies and different kinds of modules to check identification and trust level of interacting users. CSP layer also contain agents for verification from previous two layers for the authentication of accessing clients and last data storage layer contain the actual data which user actually trying to access.
4- Performance Analysis

In cloud computing system different kinds of task has to carried out on the behalf of customers on hardware on which customer has no access easily. Typically the data is uploaded by the user on hard disk in an unencrypted form but it is encrypted by cloud system to make it secure [22]. Basically our proposed security framework consist on agents as well as on trust model. Trust degree is always increasing of customer by trusted communication and non-trusted communication decrease the trust. In this frame work trusted mechanism consisted on two modules (i) Security management module (ii) Trust management module.

Security management module received request from CSU Agent for checking the identity and trusted value by using security policies. After verification security module transfer it to the trust management for further confirmation regarding trusted value by using trusted policies. If trusted value is greater than threshold it’s considered to be authentic user and if not then considered it malicious user.

In another method if security management receives a list of user form CSP Agent then identification of listed element checked individually and sent it to trust management module for further verification. All verified element shifted to List “T” by trust management module, after this when list is received by security management it compares both lists if these are equal then allowed to CSP module otherwise rejected.

Here is an equation on the subject of trusted and non trusted user which calculates the behaviors of any CSU on the behalf of action performed.

\[ V_a = (1 - \frac{A_N}{Total_a}) \cdot W_a^{(m)} \] ........... (1) Where \( 0 \leq V_a \leq 1 \)

In this above mathematical equation range of 0 shows that behavior is negative and the range of 1 show behavior is positive. \( A_N \) is the number of negative or suspected actions and \( Total_a \) is the total number of action performed. Here “m” shows security level, the value of “m” effects the total value of \( V_a \) because the value of “m” is in exponential.
Here is following designed a sequence diagram for whole proposed model.

4.1- Security Management Diagram

5- Simulation Experiments and Results
The purpose of developing this whole proposed frame work to increase the privacy and security of client’s data. For simulation two type of CSU has been selected one is trusted and other is non-trusted and the total number of 2000 cloud clients taken into account to perform the experiments. To differentiate between trusted and non-trusted module proposed system take authentication form CSU database and pass through towards security management and trust management module to check the trust. Malicious or unauthorized nodes in the experiments are referred to those who try to cheat the framework security and trust policy. Experimental code is implemented in java tool and the performance of execution code was measured on the system having following configuration: 300 GB Hard disk, 4GB RAM with core i3 processor.

From equation (1) of parameter analysis we can find the trust value of different user have different behavior.

<table>
<thead>
<tr>
<th>Iteration</th>
<th>Action</th>
<th>$A_N$</th>
<th>Total$_a$</th>
<th>$V_A$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Positive</td>
<td>1</td>
<td>2</td>
<td>0.5</td>
</tr>
<tr>
<td>2</td>
<td>Malicious</td>
<td>2</td>
<td>4</td>
<td>0.4</td>
</tr>
<tr>
<td>3</td>
<td>Malicious</td>
<td>1</td>
<td>2</td>
<td>0.4</td>
</tr>
<tr>
<td>4</td>
<td>positive</td>
<td>1</td>
<td>3</td>
<td>0.7</td>
</tr>
<tr>
<td>5</td>
<td>positive</td>
<td>1</td>
<td>2</td>
<td>0.4</td>
</tr>
</tbody>
</table>
Here following is shown the graph two different lines for positive or authorized user and for malicious or unauthorized users.

As it is shown in graph X-axis shows malicious action and Y-axis represent trusted value in this regard, upper line representing the trusted or positive users and below line showing malicious or unauthorized user. Trusted line has value greater then thresholds therefore it is higher on graph and unauthorized line has less value the threshold for this reason it's steep.

So our proposed security framework is fundamentally is much secure as compared to others frameworks which are introduced because trust level is much higher of this model. It is distinguished by following advantages over other frameworks.
(i) Proposed model avoid security risks before operations.
(ii) Through agents every malicious or unauthorized user can be detected before any transactions.
(iii) For security there is established independent trust management module, which has ability to check every kind of traffic.
(iv) This model is comprehensive improvement in cross-clouds environment systems security and for other activities.

6- Conclusion
The proposed framework is about the cloud system security because now a day this is serious concern of cloud system user regarding their data on storage. Our model is about to ensure the appropriateness of user data. In this model we have used different types of agent like cloud service user agent (CSUA) and cloud service provider agent (CSPA) and it has four different layer from which user have to pass all those to access the data. These agents also have ability to of correctness and confidentiality to provide comprehensive defense to user data. In order to support more security to users there are two modules (security management module and trust management module) to check the identity and trust of the clients whether accessing user is authorized or unauthorized. Our future work is implementing this model on hybrid cloud environment.

References:


