Article can be accessed online at http://www.publishingindia.com

A Security Aware User Access Privileges in Cloud through Fuzzy Reasoning Approach

Ms. R. Poorvadevi*, S. Rajalakshmi**

Abstract

So far, the web browsers act as a major cloud client, used to access the computational resources from the public cloud with online connectivity. In these cases, there is a possibility of security issues related to the resources which are shared through online, untrusted public channel service access, in secured protocol usages on cloud services. So to eliminate these problems, a new on-demand security service needs to be introduced in the cloud computing environment. Cloud computing is a forum which offers massive amount of resources to its end users. As cloud providers offer tremendous services to the stakeholders, still there is a security lacking in cloud. Even though cloud is offering security-as-a-service, still customers are afraid to use that service which is offered by the cloud service provider itself, because they are maintaining and storing lots of confidential information on cloud database. Number of security solutions and measurements are coming with the new scope to prevent the customer owning data in cloud. Still, we are getting the security solution up to 79% only. So, this proposed model will be a suitable approach for cloud users to safeguard their data. Using this, we can obtain the efficient security outcomes by getting the distinguished kind of input values from the users and justifying identity of users by setting access parameter values to prove the authenticity through the fuzzy reasoning technique.

Keywords: Cloud Vendor, Fuzzy Reasoning, Cloud Service Provider, Input Recognizer, Hytrust Data Control

Introduction

Cloud computing focuses on enhancing the features of web services and resources in boundless range, to online users. To make use of cloud services, users must have a strong network bandwidth connectivity. Cloud server provides enormous amount of services to users who may request for cloud service from anywhere in the globe.

Without protecting the transaction details, maintaining the partial level of secrecy data, governing the regulatory compliance service in non-secured manner will not satisfy the user expectations. So, information security and privacy are the most important factors. Majorly, considering the security feature in the cloud environment will lead the customer in a better secured atmosphere.

Several efforts are taken by the cloud service providers to overcome the data safety issue because of increasing the compliance rate across the geographic boundaries. So, as an end user's perception, emphasizing the data protection with user control is the most important aspect.

Cloud security is the security principles applied to protect data, applications, and infrastructure associated within the cloud computing technology. Growing the cooperative endeavour between cloud service providers and security solution providers are mostly expected. Increasing the emergence of cloud services are specifically focused on the security based content solution providers.

Importance of Cloud Security

- Increasing usage of cloud services in non-traditional sectors.
- Increase in cloud service-specific attacks.

* Assistant Professor (CSE), SCSVMV University, Kanchipuram, Tamil Nadu, India. Email: poorvadevi@gmail.com
** Director of Sjcac, Scsvmv University, Kanchipuram, Tamil Nadu, India. Email: srajalakshmi@kanchiuniv.ac.in

- Growing usage of cloud services for critical data storage.
- To overcome the problem of performance issue
- Rise in employee mobility.
- Non- secure content delivery to the clients.

Related Work

In traditional feature, consumers perform all their activities through shared, distributed approaches. There was a trade-off control between scalability and granularity components. Other approach is scalable and secure key updating mechanism for access hierarchies and attribute based signature scheme, it is described about the authentication process and its outcome sets through attribute dependency values. However, cryptographic access control protocols are applied for existing untrusted cloud services with high scalability feature, still lack of proper implementation should be avoided.

Another technique is through big data mechanism user can prevent their data in cloud environment. That is, tremendous applications and services are predicted and processed in big data platforms based on the outcome from big data predicted output sequences; user input layered values are applied into the cloud server area for evaluating the authenticity of each cloud client (Huu, 2014). Preventing anomaly based intrusion detection systems can also be applied for security solution (Tchana *et al*., 2014). Another approach is a secure cloud computing based framework for big data information management of smart grid. It was defined and developed as a framework model designed for evaluating the huge data content management for smart grid services (Toma's & Tordsson, 2014).

Proposed Work

The latest approach could be more effective than using the traditional encryption, key exchange management scenarios, and secure system workings. However, in this proposed model by using the mechanism of fuzzy reasoning, we will get the user input elements and values that can be passed to the secure CSP environment then process the unique access parametric segments through fuzzy reasoning control to protect the secure information from the hackers.

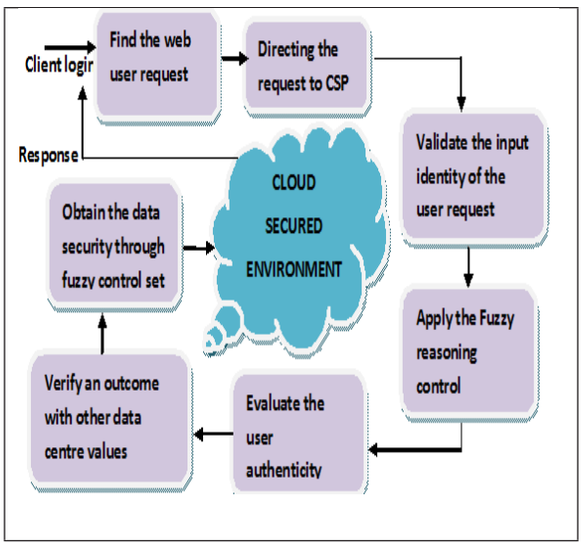
In this proposed model, firstly directing the user request to cloud service provider, secondly we will apply our own secure strategy to predict and examine the user access credentials to prove the authenticated control. Once, user has been evaluated or found as an authenticated, authorised user then only requested services and resource will be offered to him.

The following security components are considered during the authentication process.

- Receive the input elements from the user
- Find out the type of input ranges
- Manipulate the input with the fuzzy reasoning controlled variables
- Examine the input values should be matches to the cloud database.
- Obtain the fuzzy based input reasoning sequences to know the access privileges
- Use the open cloud simulator to process and compare this input set during the simulation response time

This approach is mainly used to ensure the unique features of each customer who belongs to the service in cloud platforms.

Figure 1: System Architecture



The system architecture depicts that the various functionalities will perform in cloud environment. The major target is before giving the service to the clients,

we must ensure that whether they are an authorised and authenticated person to get the service or not. After identifying the authenticated outcome only, cloud will offer the service to the requested users.

Levels of Security

Depending on the access permission and privileges, there will be two different security mechanisms available in cloud environment.

- Security on Vendor level
- Security on User level

Normally, as a developer or an end user we don't have access rights to protect the data at vendor level, because cloud vendors are providing all kind of service (Everything-as-a-service) to its dependent users. Vendors have the sufficient security mechanism at their end. People do not have the confidence on the vendor level security approaches.

So, user confidential information must be embedded with the specific security approaches. At user level we may use any feasible security technique to prevent the customer data from the hackers.

The following functions are carried out during the implementation of proposed method.

- User request type (IP, Private Access point)
- Analyse the request and pass it to CSP
- While registration time, user attributes, input elements, key identity, image segment values are collected
- Validate those input parameters with fuzzy controller module
- Apply the fuzzy reasoning technique to ensure the appropriate user conditions and access level
- Hytrust data control is entrenched for the purpose of encrypting the data from VM level.
- Verify the same attribute value with matches in any other data centre or not.
- Finally, all the collaborated values are sending to the cloud server to make final decision.

Importance of Fuzzy Reasoning Technique

Fuzzy logic and techniques are approximate reasoning values based on the certainty principles. In this state, fuzzy reasoning will act as an analyser and difficulty finder from the user request. It also perhaps invokes the several functions that will lead to the good computation model to the distinct kind of domain.

Fuzzy reasoning will analyse the various functions by using the controlled variable. The process and computation of fuzzy reasoning is given below

i) **Fuzzy reasoning set**: User Attribute level + user request location

ii) **Fuzzy reasoning control** = Comparing the data centre values + user entry level authentication

iii) **Fuzzy reasoning evaluator** => Verifying the access credential in processing time

Fuzzy reasoned segment will analyse and check the user entry level authentication value. Minimal amount of authenticated values must be satisfied for the user service provisioning control.

Implementation Work

During the application or service deployment time in cloud at that state, we need to analyse the number of constraints. While performing the SLA (service level agreement) we must ensure about all the security related agreements.

Cloud customers must know what kind of security perimeter available in traditional cases and how to improve the security measuring components to obtain the efficient results.

Security will concern in the following categories:

- Operational Security
- Infrastructure Security
- Data Security

Recently, one security has been newly launched to the market that is 'Virtualisation admin control' which protects the hacking issue in software level services.

Cloud services are processed and computed through the cloud vendor control to ensure the access mode will be

in private user, public user, and hybrid user type. It will direct the cloud clients to make use of suitable access type.

Simulation Work

Cloud user authenticity has to be proved in cloud environment to be free from the hacking problem. Number of simulator and simulating parameters are identified based on the service type.

The following components and factors are used in this work:

- Cloud let tool has been used
- By using open cloud simulator we will process the proposed mechanism to find out the security solution
- Input values and its request origin must be identified
- Processing the fuzzy reasoning set entry values to each and every cloud users.

Simulation work outcomes are obtained based on the input collection segment and estimation procedure that will processed in the suitable data centre location and authenticated outcome will be derived based on the given formula

Total outcome = Input validation result set+ Data center response + threshold value – encrypted or hidden information rate * 100

Efficiency (%)

Fuzzy reasoning control set = user request identifier + cloud admin response+ attribute finder sequence+ fuzzy certainty value

Security perimeter control boundary

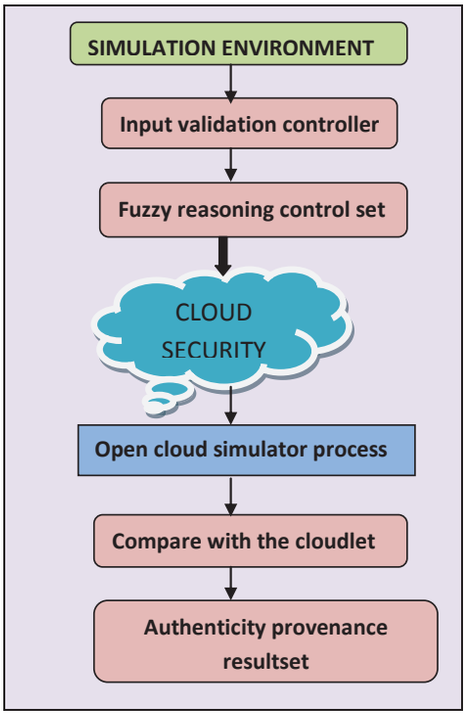
Simulated environment illustrates the various tasks that can be carried out in the cloud let and open cloud tools. The various elements are used in the simulation work as a dataset that is given below:

Table 1: Simulation Data Set

IP Address	*Data elements, Input node selector*
192.168.10.251	.bmp , .txt, pixel node selection
192.132.18.02	.imp , .xls, jpeg node selection
192. 179.10.45	.pxt, .tiff, .rtf, track play node

Figure 1 illustrates the operation in cloud environment during the simulation time.

Figure 1: Work Set Process in Simulation



In above process, users try to achieve the authenticity outcome based on the level or layer approach.

The result set has been obtained after the process computation of authenticity task.

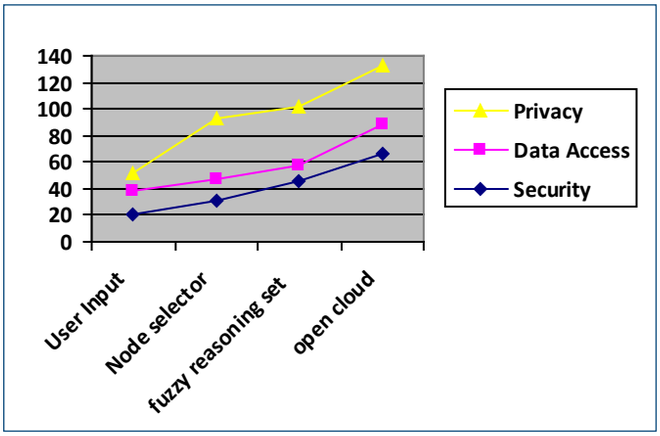
Table 2: Result Set

IP address	*Service type*	*Security outcome (%)*
192.163.10.35	Communication	78.34
187.234.56.10	Monitoring	89.02
191.163.17.89	Software	81.92
189.161.36.71	Security	98.03
192.167.18.02	Data privacy	98.45

Experimental Results

Cloud security is the most important phenomenon to the cloud users. Distinct kind of attributes are used and verified in the open cloud simulator that can be well suitable for user access service and resource provisioning. The following values (Figure 2) are obtained during an implementation time.

Figure 2: Data During Implementation Time



From this graphical outcome, we are ensuring the security feature and security data access rate to sustain the cloud user confident level about data safety.

Conclusion

Cloud is the best mechanism, to provide boundless services. From this implemented result, the major security problem will be eradicated and users can perform any confidential transaction without any worries about the hackers. This can be a better model to limit and create an access boundary for authenticated users.

Future Enhancement

In future cases, users may know their distinct kind access parameter and privileges to make use of any service. Likewise, we can create some level of boundary to restrict the unauthorised entry into the cloud environment. In future cases, we can apply this kind of security mechanism in all the domains.

References

Guan, B., Wu, J., Wang, Y., & Khan, S. U. (2014). *CIV Scheduled Communication- Aware Inter-VM Scheduling Technique for Decreased Network Latency between Co-located VM's.* IEEE Transactions on Cloud Computing, 2(3), 320-323.

Huu, T. T. (2014). *A Novel Model for Competition and Cooperation among Cloud Providers*. IEEE Transactions on Cloud Computing, 2(3), 251-265.

Kailasam, S., Dhawalia, P., Balaji, S. J., Iyer, G., & Dharanipragada, J. (2014). *Extending Map-reduce across Clouds with B-stream*. IEEE Transactions on Cloud Computing, 2(3), 362-376.

Konstanteli, K., Cucinotta, T., Psyches, K. A., & Varvarigou, T. (2014). *Elastic Admission Control for Federated Cloud Services.* IEEE Transactions on Cloud Computing, 2(3), 348-361.

Sheng, D., Wang, C. L., & Cappello, F. (2014). *Adaptive Algorithm for Minimizing Cloud Task Length with Prediction Errors*. IEEE Transactions on Cloud Computing, April-June, 2(2), 194-207.

Tang, S., Lee, B., & He, B. (2014). *Dynamic MR: A Dynamic Slot Allocation Optimization Framework for Map Reduce Clusters*. IEEE Transactions on Cloud Computing, 2(3), 1-14.

Tchana, A., Dilenseger, B., De palma, N., Salmi, J., & Harbaoui, A. (2014). *A Self-scalable and Auto Regulated Request Injection Benchmarking Tool for Automatic Saturation Detection*. IEEE Transactions on Cloud Computing, 2(3), 279-291.

Toma's, L., & Tordsson, J. (2014). *An Automatic Approach to Risk-aware Data Center Overbooking*. IEEE Transactions on Cloud Computing, 2(3).

Wang, S., & Shi, W. (2014). *Budget-driven Scheduling Algorithms for Batches of Map Reduce Jobs in Heterogeneous Clouds*. IEEE Transactions on Cloud Computing, 2(3), 306-319.