A Security Solution for Cloud Users to Protect the Private Data through Fuzzy Bayesian Decision Method (FBDM)

R.Poorvadev
Assistant Professor
CSE Department
SCSVMV University

S.Rajalakshmi, Ph.D
Director of SJCAC
Advanced computing center
SCSVMV University

G.Supraja Devi
PG Student
CSE Department
SCSVMV University

ABSTRACT

Fuzzy technique is a forum which provides the linguistic object sets and solutions in certainty and uncertainty based elements. Numbers of decisions were derived for various domains by using the fuzzy modeling method. In fuzzy there will be a one approach is, appropriate and approximate reasoning, this can be used to find the solution for critical problem which is happening in all platforms. Likewise, by using fuzzy Bayesian decision method we are trying to obtain the solution for cloud security and privacy issue. If user is consuming any resource or services from the cloud service provider such as, communication, monitoring services, instant transaction, verification of service availability, ensuring the service access privileges, however these applications and processing data sets are stored in the cloud database. Still, customers do not believe the security measurements and storage of secret information which is offered by the cloud vendors. Cloud users are in need of protecting the confidential or private data by embedding and applying their own security tools and parameters. This proposed model which helps to an end-users whoever in need of securing the individual data in cloud environment by using the certain sort of mathematical based derived functions and apply these outcomes into the fuzzy Bayesian decision block to eliminate and prohibit the hackers entry by setting the threshold log value in cloud environment to achieve an efficient security results

General Terms

Cloud security.

Keywords

Cloud vendor, Fuzzy Bayesian computation block, fuzzy threshold analyzer, Cloud service provider, and Apache cloud stack simulator tool.

1. INTRODUCTION

Cloud computing is trade-off between cloud developers and cloud user service level controller. It offers the massive amount of services to its dependent users. Number of research works is going on in cloud identity access boundary, reducing the government overhead by the form of access and maintain the web resources to its automation services. Nowadays all the educational institutions are evolutionarized as a cloud campus because to adopt the current services and automatic updating of future trends. To know a faithful value cloud services we may compare the outcome sets with distributed, collaborated, Information and soft computing.

Trend is changing based on the customer expectation. Cloud is providing the boundless services to its requested users via internet connectivity.

A web portal is initiated between the cloud vendor and cloud end-users with SLA (service level agreement) specification. All the resources are passed from the cloud vendor to user through web. The main limitation is, enough amount of internet bandwidth connectivity is needed to use any service which was obtained from the cloud service provider. Consuming the service is not a main focus. How far, user services, service details, usability transaction repots, confidential Meta-data are securely maintained in the storage location. Service reliability, security, privacy, access management services are protected from the distinguished attackers by making use of suitable security perimeter and controls.

To secure the schematic kind of information, individual user access policy, kind of access specified to protect the secrecy information. To ensure that what kind of security strategy exists in the cloud vendor end and how to maximize the security performance rate by applying the security procedure to enhance the data or content protection. To find out the gap between the existing security measurements and current security technological measurements and components, then only security related parameter can exactly allocated for the user processing applications.

1.1 Significance of Cloud Security

- Increasing usage of cloud services in all the ERP sectors.
- Increase the security performance rate to the cloud user’s applications.
- Growing usage of cloud services for decisive records storage.
- To eliminate the privacy and information management access problem.
- To make use of government regulatory services to carry out the huge service offering to the people.
- Ensure the high end data protection.
- Establish the client level security factors in order to obtain the authenticated results

2. RELATED WORK

To associate the existing work to the proposed model we need to analyze the work that was carried out in distinguished perspectives. Whenever the security problem is arising that moment, people are planning to apply cryptography based security mechanism in the form of key exchange, secret key generation, and key algorithmic computations.

Other approach is, processing the high-end data set through big data mechanism and its layered architectural principles. Creating the framework is used for processing and simulating the cloud applications to enhance the resources in all level to meet the user expectations. Data semantic information outcomes are applied into the cloud server for evaluating the authenticity of each cloud client [1]. Preventing anomaly based intrusion detection systems can also be applied for security solution [2]. 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 [3].

3. PROPOSED WORK

This proposed model will focuses on increasing the security performance rate for cloud applications. Although cloud security parameters are well investigated, still there is a lack in cloud security and privacy applications. This approach could be the effective phenomenon to prevent secure information from the hackers in the cloud environment.

The new paradigm will distinguish from the traditional approach because we are considering different level of authentication factors as listed below:

- ❖ Getting the user service request type
- ❖ Find out the alternative choices and attributes list
- ❖ For the user, previous usage frequency is to be notified
- ❖ There will be a clear identification of user entry details
- ❖ Apply an analytics principle based on the probabilistic event occurrence to know the current state values
- ❖ Use the predicted method to obtain the set of attribute segmented inputs
- ❖ Apply the fuzzy certainty elements to set the threshold for each and every authentication state principles.

Using these input entities to make a secured cloud environment to free from the hackers. Protecting the log details of user access, service offering vendor, the origin of service initiation should be hidden to third party users, all kind of input and processing segments should be visible only to the users and cloud app developers.

By setting the different forms of user access limit in terms of threshold value it is to be fixed according to the user concurrent input elements.

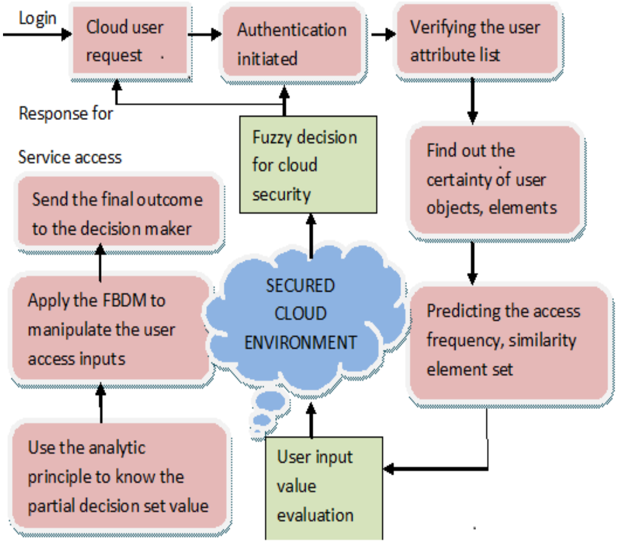
Login
Cloud user request
Authentication initiated
Verifying the user attribute list
Response for
Service access
Fuzzy decision for cloud security
Find out the certainty of user objects, elements
Send the final outcome to the decision maker
SECURED CLOUD ENVIRONMENT
Apply the FBDM to manipulate the user access inputs
Predicting the access frequency, similarity element set
Use the analytic principle to know the partial decision set value
User input value evaluation

Fig: 3.a) System Architecture

System architecture depicts the functionality of cloud application security. In this approach many input components are considered to reach and obtain the good quality of security results. Before providing the service to the requested users we need to analyze the authentication and authorization outcome based on multi factor input entities to ensure about the highly authenticated users. Initially gathering the choices, alternate attribute variables, predicting the certainty situation based object and attribute identical elements to prove the authenticity each cloud user.

The following security credentials should be considered before delivering the service to the users:

- ❖ Service request initiation
- ❖ Allow the users to select the security images and attributes during registration time
- ❖ Ensure that, whether user wants their secured data in encrypted form or not
- ❖ Denial of access service for third party user and unknown users
- ❖ Maximum of 5 to 7 security images and attributes should be chosen by the user and verification of authenticity based on the input parameters
- ❖ Create the access boundary by setting some threshold for each unique user
- ❖ There will be service access zone log details will be maintained properly

Above mentioned steps are to be carefully notified during the processing time. Based on the unique threshold value and attribute we will make decision whether users will get allowed to consume the resource or service in cloud environment.

The major security access rate and performance of utilization rate also to be calculated to get an efficient final outcome in cloud environment.

3.1 Importance of Fuzzy Bayesian Decision Method (FBDM)

Fuzzy will focuses on improving the problem solving result rate for any applications. In this paper, fuzzy playing a vital role for how to optimize the secured and privacy value for any individual data to be processed in a secured platform.

All the linguistic elements are considered as a following form of inputs:

(i) Object set

(ii) Attribute list segment

(iii) Alternate option / variable selection

(iv) Entity clustering set

(v) Image collection set

(vi) Service request origin

Depends on these access list each user action can be clearly notified. If they are doing any illegal kind of activities their access can be terminated permanently providing security for cloud vendor/ service provider end is very easiest process. But in the case security at the cloud user end is somehow difficult. Because there will be many attacks are possible in end-user perspective. So securing all the transaction, information passing, maintaining a confidential data will be processed on virtual machine.

If hypervisor and virtual machine is well secured then the attack is very less possibility. Because, all the applications, service rendering can be processed on virtual machine. Hypervisor is the controller for all kind process which is running on virtual machine sequence sector. So, process these mentioned security parameters and credentials on the VMware, XenWare control to achieve the good quality of security outcome.

All the security components can be processed and simulated through some kind of adaptability tool. That can be used to bring the solution for any type of problem which is facing by the user. Simulation is the main work to be carried out in any research work, processing the scientific related app engine, controlling the progression in the time span.

3.2 Processing of Fuzzy Bayesian Decision Method

Classical statistical decision making involves the notion that the uncertainty elements can be characterized as a probability values. Before making the decision we need to collect the following information to protect the user data.

- ♦ Collection of user alternative attributes
- ♦ Choice of cloud user service request
- ♦ Prediction of cloud customer access information
- ♦ Discretize the various authentication states
- ♦ Apply the analytics principle

→ **Analytic method**= assess the likelihood of an outcome* certainty states of nature

→ **Probability event**= chance of occurrences + future state predicted outcome

→ **Ensuring ambiguity** = {value of new information sequence + alternate variables – current state probability ratio}/100

These functions are computed with the processing metrics to obtain the quality results. Initially, we need to set the error rate is zero, and then only we will start our security performance operation.

Simulate this result set entity with an annotation fuzzy variable to avail the linguistic element set.

Fix an initial error rate = 0;

Find the probability event value

Set the threshold = between 0 to 1

Assume the marginal threshold value=0.5

Compute this result set entity = 10 user group

Let consider the formation of probabilistic decision analysis for cloud user content protection.

$$S = \{s1, s2. . . sn\} \qquad \text{-------- (1)}$$

S- Indicates set of possible states of cloud user nature, and the probabilities that these states will occur are listed in a vector,

$$\mathbf{P} = \{p(s1), p(s2), . . . , p(sn)\}, \qquad \text{-------- (2)}$$

Where, n=1

$p(si) = 1$

Assume that the decision maker can choose among *m* alternatives,

$$A = \{a1, a2, . . . , am\}, \qquad \text{-------- (3)}$$

For a given alternative *aj* we assign a utility value (data protection) *uji* , if the future state of nature.

$$aj = uji \qquad \text{--------- (4)}$$

These utility values should be determined by the decision maker. Since they express value, or cost, in terms of security outcome for each alternative-state pair, that is,

For each value of sate will be *aj* – *si* combination.

The most common decision criterion is the *maximum* expected utility (Security rate) among all the alternatives, that is,

$$E(u*) = \max jE(uj), \qquad \text{-------- (5)}$$

This leads to the selection of alternative

$$ak \text{ if } u* = E(uk) \qquad \text{--------- ((6)}$$

So, from this computation block;

$$\textbf{Security rate} = \frac{\text{cumulating the value of [state (s) +alternative (a) + utility (u)]}}{100}$$

Data protection = 10 user group attributes * fuzzy Bayesian state + utility value

Security Threshold = 0.5 to 1

Possibly achieving the user security credentials in all the applications forum by specifying the input parameters which is given by the cloud client during the service initiation time.

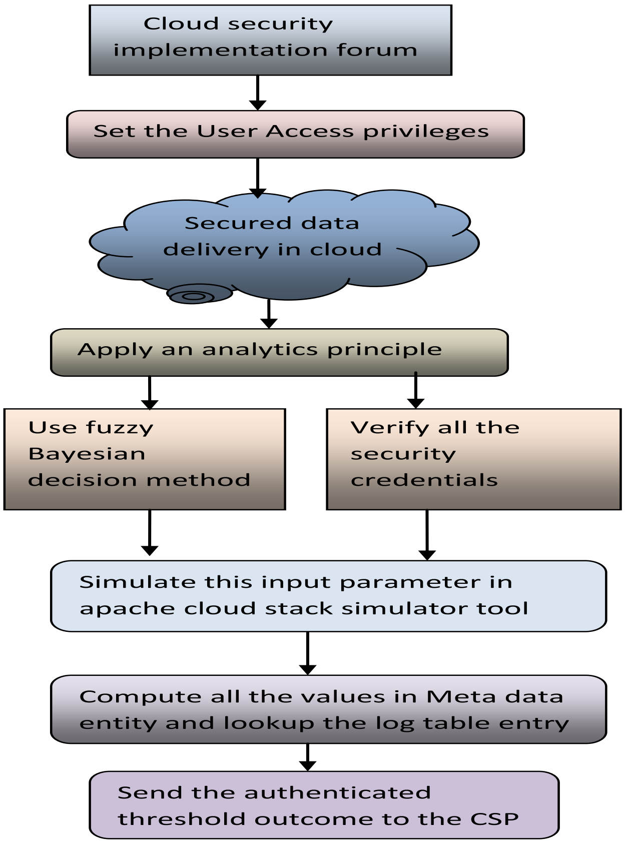
Cloud security implementation forum
Set the User Access privileges
Secured data delivery in cloud
Apply an analytics principle
Use fuzzy Bayesian decision method
Verify all the security credentials
Simulate this input parameter in apache cloud stack simulator tool
Compute all the values in Meta data entity and lookup the log table entry
Send the authenticated threshold outcome to the CSP

Fig: 3.2 a) Illustration of Simulation Work

4. SIMULATION WORK

To get an appropriate result for cloud user running applications, all the considered security parameters are deployed in to the cloud environment to simulate and compare the result set and Meta data entity to apply and process the value set entry can be calculated in cloud environment.

Apache cloud stack can be used in this approach. In this proposed work we are not using any algorithm. By making use of cloud simulator tool we are processing the security parameters in the desired sector to prove the security established work.

Normally, apache cloud stack is used to build large networks of VM's, console App's. This can be used to prove the target result will be highly available and scalable feature. It is mainly used to offer the cloud services (private) based on on-premises control. It is mainly considered about, user accounting management for web services and applications to execute the suitable VM control in their environment.

In this simulation work following factors are used for security provenance.

- User service request type
- Location of service request
- Selecting the input parameters
- Choosing the suitable cloud vendor
- Evaluate the FBDM value
- Set the correct threshold values in the cloud
- Apache cloud stack will process on VM.
- Use the log objects / log table content

The above mentioned parameters are used in the cloud stack simulator tool

Main Code

Cloud init (Data center, location, KVM);

Cloud service provisioning (minimal threshold=0.5);

Cloud service rendering (th_{ON}, th_{OFF}) =1;

Set error flag (EOF/ EF=1);

Cloud security service (INIT_ VM=2);

Cloud kernel virtual machine (HYPERV control (2.0); Access rights permission (R, W, and E));

Cloud fuzzy function (state, action, nature of cloud user, attribute, images, input values);

Cloud security prediction (Th=0 to 1);

Cloud execution (cloud stack version 3.1, init_services, service brokerages OFF);

4.1 Simulated Result Set and Validation

Initially, security threshold set it as, Th=0;

Process the cloud user parameter in different states (s1, s2…….sn);

All the input parameter values are computed as follows:

Security access rate = state + attribute- utility outcome

Security rate (100%) = 10 cloud user group *0.5

Security access privileges = fuzzy state outcome + analytic variable value

Evaluation of MAX_{Th} = 0.5 + maximum service offered + minimal security sequence set

Evaluation of MIN_{Th} = 0.5 + considering the minimal service access based on the attribute selection set / total service consumption time

Fuzzy Decision Maker = utilization of outcome + 95% access specified sequencer + probability occurrences.

Cloud security service rate = maximal threshold + attribute selection rate / total number of applications processed in the same domain.

4.1. a Log table –I for security Performance rate analysis

Service type	Service location	FBDM outcome (% 10)	Analytic outcome (% 100)
Security	Web user 192.168.10.251	9.21	92.1
Privacy	Web content miner 192.164.17.012	9.034	90.34
Data service	Web resource monitor 193.169.34.86	8.75	87.5
Identity access management	Web information container 192.165.10.45	8.931	89.31

4.1. b Log table –II for security Performance rate analysis

User security parameters	Fuzzy decision outcome	Cloud stack outcome (%)
Image set	Well security	Security (97.2)
Text attributes	frequently secured	Security (95.8)
User behavior	Moderate security	Security (89.6)
Object entity	Effective security	Security (98.3)

5. EXPERIMENTAL RESULTS

From the simulation work, we have obtained the efficient security value as a final outcome. Implemented parameters are simulated in cloud stack tool to enhance the security feature. The major phenomenon was used to exhibit the security based entity set. Fuzzy based decision can be proved to the cloud users to safeguard the individual and user private data in cloud environment.

The following graphical chart will shows the security outcome for protecting the each unique user data in the cloud environment.

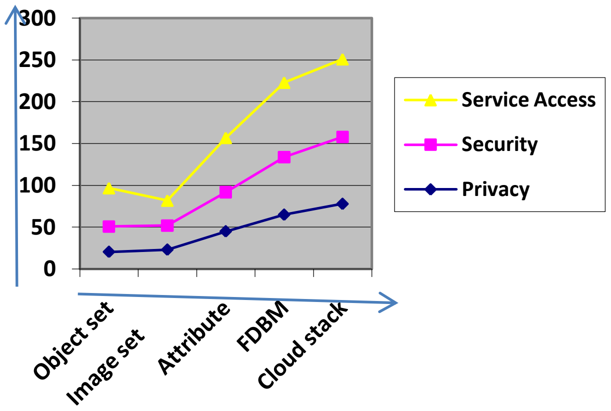

Fig: 5.1 depicting the experimentation value of cloud security result

Here, X-axis represents the major five cloud security components.

Y-axis indicates the number of user entry.

So, from this tabulated value we are monitoring that, gradually cloud authentication service is increasing based on the number of user which they are entered into the cloud vendor site.

6. 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.

7. FUTURE ENHANCEMENT

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

8. REFERENCES

[1] Truong- Huu. T “A novel model for competition and cooperation among cloud providers” IEEE transactions on cloud computing volume 2, issue 3, 2014.

[2] Tchana.A; Dilenseger.B; De palma.N; J, salmi; A. Harbaoui “A self-scalable and auto regulated request injection benchmarking tool for automatic saturation detection” IEEE transactions on cloud computing volume 2, issue 3, 2014.

[3] Toma’s.L; Tordsson.J “An automatic approach to risk-aware data center overbooking” IEEE transactions on cloud computing volume 2, issue 3, 2014.

[4] Wang’s; Shi.W; “Budget-driven scheduling algorithms for batches of map reduce jobs in heterogeneous clouds” IEEE transactions on cloud computing volume 2, issue 3.

[5] Guan. B; Wu. J; Wang. Y; Khan.S.U “CIV scheduled communication – aware inter-VM scheduling technique for decreased network latency between co-located VM’s”, IEEE transactions on cloud computing volume 2 , issue 3 , 2014

[6] Tang. S; Lee. B; He. B; “Dynamic MR: A dynamic slot allocation optimization framework for Map reduce clusters” IEEE transactions on cloud computing volume 2 , issue 3 , 2014

[7] Konstanteli. K; Cucinotta. T; Psyches’. K; A. Varvarigou. T “Elastic admission control for federated cloud services” IEEE transactions on cloud computing.

[8] Kailasam. S; Dhawalia. P; Balaji. S.J; Iyer. G; Dharanipragada. J “Extending Map-reduce across clouds with Bstream” IEEE transactions on cloud computing.

[9] Sheng Di, Member, IEEE, Cho-Li Wang, Member, IEEE, and Franck Cappello, IEEE Member, paper entitled as, “Adaptive Algorithm for Minimizing Cloud Task Length with Prediction Errors” IEEE transactions on cloud computing, vol. 2, no. 2, April-June 2014.

[10] Sudip Misra, Senior Member, IEEE, Snigdha Das, Manas Khatua, Student Member, IEEE, and Mohammad S. Obaidat, IEEE Fellow, paper entitled as, “Qos-Guaranteed Bandwidth Shifting and Redistribution in Mobile Cloud Environment” IEEE transactions on cloud computing, vol. 2, no. 2, April-June 2014

[11] Amir Vahid Dastjerdi, Member, IEEE and Rajkumar Buyya, Senior Member, paper entitled as, “Compatibility-Aware Cloud Service Composition under Fuzzy Preferences of Users” IEEE transactions on cloud computing, vol. 2, no. 1, January-March 2014.

[12] Hossein Morshedlou and Mohammad Reza Meybodi paper entitled as, “Decreasing Impact of SLA Violations: A Proactive Resource Allocation Approach for Cloud Computing environments” IEEE transactions on cloud computing, vol 2, no.2, April – June 2014.