ISSN: 2229-6956 (ONLINE)
DOI: 10.21917/ijsc.2016.0164

AN QUALITY BASED ENHANCEMENT OF USER DATA PROTECTION VIA FUZZY RULE BASED SYSTEMS IN CLOUD ENVIRONMENT

R. Poorva Devi[1] and S. Rajalakshmi[2]
[1,2]*Department of Computer Science and Engineering, Sri Chandrasekharendra Saraswathi Viswa Mahavidyalaya, India*
E-mail: [1]poorvadevi@gmail.com, [2]srajalakshmi@kanchiuniv.ac.in

Abstract

So far, in cloud computing distinct customer is accessed and consumed enormous amount of services through web, offered by cloud service provider (CSP). However cloud is providing one of the services is, security-as-a-service to its clients, still people are terrified to use the service from cloud vendor. Number of solutions, security components and measurements are coming with the new scope for the cloud security issue, but 79.2% security outcome only obtained from the different scientists, researchers and other cloud based academy community. To overcome the problem of cloud security the proposed model that is, "Quality based Enhancing the user data protection via fuzzy rule based systems in cloud environment", will helps to the cloud clients by the way of accessing the cloud resources through remote monitoring management (RMMM) and what are all the services are currently requesting and consuming by the cloud users that can be well analyzed with Managed service provider (MSP) rather than a traditional CSP. Normally, people are trying to secure their own private data by applying some key management and cryptographic based computations again it will direct to the security problem. In order to provide good quality of security target result by making use of fuzzy rule based systems (Constraint & Conclusion segments) in cloud environment. By using this technique, users may obtain an efficient security outcome through the cloud simulation tool of Apache cloud stack simulator.

Keywords:

Cloud Service Provider, Cloud Vendor, RMMM, Fuzzy Rule Systems, Managed Service Provider, Cloud Clients, Cloud Security, Apache Cloud Stack Simulator Tool.

1. INTRODUCTION

Day by day huge service request and maximized resource consumption are coming as a wider range of service access to the web clients in cloud environment. End users are primarily focusing on cost-cutting and time saving service schemes. Distinct set of services and resources are handled by Cloud service provider (CSP) across several data centers. Virtual machine monitor (VMM) is mainly focusing on massive applications that are processed in guest OS platforms. Even though, enormous amount of resources that are offered by various cloud vendors still cloud security problem is not entirely eradicated in client's focal point. Typical kind of hacking techniques is taking place in all domains. However people are applying the intelligent methods, techniques, tools and security schemes for protecting their own set of private data still, some of the cloud vendors are not coming forward to guarantee the confidential data to its dependent users. Because of client service usage level and mode of running services it will prompt into various level of security related problem. Cloud vendors could not provide the sufficient security ideals for client's service/ data usability aspects.

1.1 RECENT CLOUD SECURITY CHALLENGES

The various challenges are newly found in the literature analysis and it needs to be overcome by considering the various input parameters and packages.

- Client authentication and authorization
- Security shortcomings of hardware virtualization
- Flooding attacks and DOS
- Cloud Accountability of capture the wrong activity
- Service traffic hijacking
- Challenges over the storage protection
- Protection of outsourced computation

Monitoring of cloud services is most important task in cloud environment. To ensure the quality of security result we need to analyze the SLA constraints, user service package and other factors.

1.2 SECURITY IMPLICATIONS OF CLOUD SECURITY

Before processing any function in cloud area we need to analyze the suitable application which was requested by the cloud users. If any user is selecting the cloud service then it combines the resource package selection, platform selection and choosing the outsourced provider for each application is an essential factor in security environment.

2. RELATED WORK

In the traditional approaches, number of security solutions and security related methodologies are derived in all the aspects. However, Xu Wu [2] proposed fuzzy reputation based trust model based on the fuzzy logic inferences. The fuzzy logic inferences will generate the fuzzy inference rules to set the integrity of the user who access the data from the cloud. Fuzzy inference rules are still unable to produce quantified results using aggregated inference rules. The proposed model adds more fuzzification rules to improve the security aspects.

Supriya et al. [3] highlighted the experimental results which improves the cloud access trust management under the various data centre resources. This approach allows the user to set various levels of security parameters to implement the secured cloud access trust boundary model in cloud using fuzzy.

Kawser et al. [4] set the probabilistic trust model including user behavioural probability to improve the trust model under the cloud user authentication process. The proposed model will combine the probabilistic values of user behaviour and fuzzy logic

rule implementation to ensure the trusted cloud based access framework developments.

Manish Kumar Aery et al. [6], Comparative study of security parameters by Cloud Providers discussed about the various security authentication model implemented in the public cloud domain to prevent the cloud security access management issues. all the solutions are implemented using the cryptographic techniques which encompasses the various key management issues .The proposed fuzzy based security trust model will eliminate the key management issues.

As per Sood [13], combined security approach in cloud access management issues resolved using Message Authentication Check (MAC) to identify the integrity of the cloud user and data. User name and passwords will be supplied along with the encrypted data access will motivate the proposed model to implement the multifactor authentication trust model using fuzzy logic.

So, from the study reports, user need to protect their applications, services by finding the suitable solution for the cloud security issue. The proposed model will brings the adequate results for securing the user confidential information and their resources in the cloud service access platform.

3. PROPOSED WORK

This proposed phenomenon, will focuses on how to improve the data security value for user private contents. Quality must be enhanced in user level data protection. Through this method, this proposed model will increase the security performance rate for cloud applications.

All the cloud user applications are processed into the virtual machine it's also call it as, "Pseudo-machine". All the application or service creation and management of VM's have been processed in the platform virtualization. It needs to be addressed and directed into the cloud environment in the security portal access group. If a cloud user, need any kind of services or resources in their utilization at that time, the cloud vendor can provide VOIP (voice over IP services). It is purely relies on the SOA constraints.

3.1 IMPLICATIONS ON SOC (SECURITY OPERATION CENTER)

Normally, the data owners are deploying their applications/ service packages into the cloud environment into order to perform the web content retrieval task. There is a one major mechanism in cloud is, SOC it can process the task in following two different modes:

- By knowing the service TOC values (Total cost of ownership) to ensure the service consumption cost which is requested by the user.
- Also another focuses goes on to the high end security result by considering the operational cost of cloud services, achieving the user confident level about their stored data in cloud database.

Early detection (ED) will used to detect the service and find the new security vulnerabilities.

3.2 REAL-TIME LOG MONITORING

This feature is mainly enabled for security monitoring services to the distinct clients. It can also help to customers, business peoples to regulate their events and free from the hackers by providing the control set is called, log-in-failures.

The following picture shows that how far the security service is to operate in cloud vendor locations in order to provide an outcome for data safety.

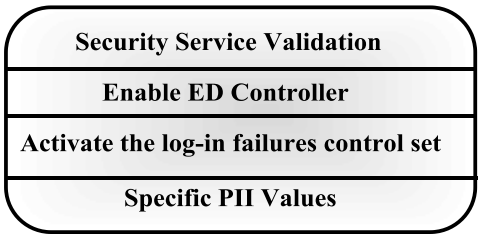


Fig.1. Illustration of service validation

Depends on, ED and log-in failures values we may able to identify the various vulnerabilities in customer end. There will be an approach is called, personally identifiable information (PII) will be used as an Information security service optimizer.

The following components are used and specified as a, user input level field parameters such filed names are given below:

- Finding the privileged user access
- Verifying the regulatory compliance
- Identify the data location
- CIA value set
- Levels of data segregation

Above mentioned components are processed as a client level validation factors to sustain the security outcomes. By using these input entity sets we may trying to obtain efficient data security value.

4. SIGNIFICANCE OF FUZZY RULE BASED SYSTEMS

Fuzzy rule based systems is the most powerful technique in modeling some complex systems that can be used and observed by individual because they make use of linguistic variables as their antecedents and consequents form in nature. The restriction statements are usually connected by linguistic connectives variable set such as, "and", "or", "else" connectives. These linguistic restrictions R^1, R^2, R^3,…., R^r apply to the output actions, or consequents of the rules.

The canonical form for a fuzzy rule based system is given below:

Rule 1: IF Condition C^1, THEN restriction R^1
Rule 2: IF Condition C^2, THEN restriction R^2
…….. … …… …….. ……. …
Rule r: IF Condition C^r, THEN restriction R^r

With the help of fuzzy rule based systems, cloud applications and user tasks to be processed in fuzzy rule based constraints.

4.1 AGGREGATION OF FUZZY RULES

Most of the rule based systems involve more than one rule to bring out the suitable solution for any kind of problem.

The process of obtaining the overall consequent (conclusion) is to be derived from the individual constraints of input parameters and source finder values.

Determining an aggregation strategy, two simple extreme cases are existing to prove the optimal value. It may be two types of evaluation strategies:

- Conjunctive system of rules
- Disjunctive system of rules

For conjunctive membership function is represented by,

$$\mu_y(Y) = \min\left(\mu_y^1(Y), \mu_y^2(Y).....\mu_y^r(Y)\right); \quad \text{for } y \in Y$$

If the task outcome is focusing on maximal set of output value then, disjunctive values to be specified and used.

In disjunctive membership function should be processed by using at least one rule is required by using "or" connectives.

$$Y = y^1 \text{ or } y^2 \text{ or } ..... \text{ or } y^r$$

(or)

$$Y = y^1 \cup y^2 \cup ..... \cup y^r$$

In disjunctive membership function is represented by,

$$\mu_y(Y) = \max\left(\mu_y^1(Y), \mu_y^2(Y).....\mu_y^r(Y)\right); \quad \text{for } y \in Y$$

Through these result set parameters we may apply the fuzzy min value and max value utility output for an optimal value specifier.

4.2 FUNCTIONS OF FUZZY RULES IN CLOUD ENVIRONMENT

IF – THEN propositions rules are considered for cloud applications.

A = Application for cloud user (A_1, A_2…)

X = input parameter variable set

Y = action flow or output

IF x_1 is A_1^k and x_2 is A_2^k, THEN Y^k is B^k, for k = 1,2,...,r

where,

A_1^k and A_2^k = cloud user applications and fuzzy sets representing the k^{th} antecedent pairs;

B^k = is the fuzzy set representing the k^{th} consequent pair

An above mentioned computation formulas are used into the cloud environment in order to verify the cloud user authenticated result value.

5. SIMULATION WORK

In this approach, cloud user resource and services are get processed in to an appropriate cloud vendor by using the mechanism of RMMM. With the help of constraints and segments (from fuzzy rule based systems) IF-THEN rules premises can be used to verify the min and Max threshold values.

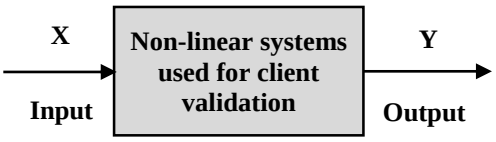
In this work, two different cases of input and output processing systems are considered.

System 1: The Inputs to the system are scalar values

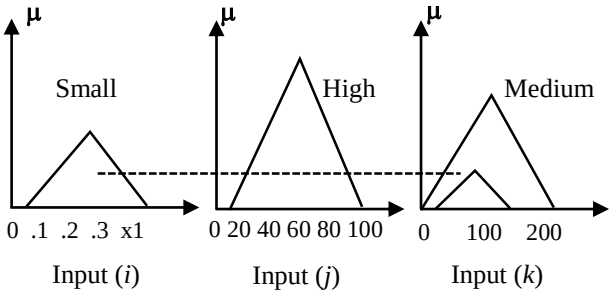
This method can enables the approaches like we may get any input parameter for cloud clients and that inputs can be validated through the reference of cloud database and log table values. (Max-min inference method)

System 2: The Inputs to the systems are scalar product values

To eliminate the unauthorized person access and finding the vulnerabilities over the cloud service access, there will be enabling approaches of maximal threshold value from cloud vendor metadata and cloud database values. (Max-product inference method)

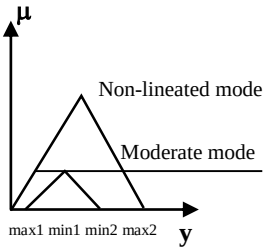


Rule 1:



From an above rule based systems we are deriving the non-linear system modeling values by considering the three main parametrical components of i, j and k and the service access ranges are small, medium and high rates.

Rule 2:



To obtain the moderate values as an aggregate result set of min and max elements rule 2 can be used.

A fuzzy rule based systems consists of following factors:

i) A set of rules that represent the decision makers understanding of the behavior of the system.

ii) The system inputs and outputs can be either a vector set, scalar, scalar product values.

In this proposed model,

Cloud client level input fields:

- Service request initiation field
- Login entry value
- Type of service access
- Selection of security images

- Service or application host on to the cloud
- Validation of authorized control value
- Access fee package

Fuzzy rule based constraints:

- Ensure the service access policy
- Monitoring the frequent events
- Specify the access limit for each user by getting an access rights from cloud vendor
- Implement the fuzzy model IF-THEN rules simulator
- Secure the access via fuzzy rule set indicator
- Validate the service rate for secured user

This proposed concept wills purely, works on the similarity measures of cloud users for already registered security parameters by compared with the cloud database.

This system will accept inputs from cloud users in the form of vector quantified one.

Let,

x_1 – be a consideration of client input products

x_2 – be an another set of client input perimeter control

Y – be a data rules for given X input entries.

The computation will be defined as,

$$X = x_1 * x_2 * \ldots x_n;\ Y = y_1 * y_2 * \ldots y_m$$

$$f(X, Y) = f(\text{All set of } x \text{ values}) + f(\text{all set of } y \text{ values})$$

The input data, rules, and output actions or consequents are generally fuzzy sets. It is expressed by means of appropriate membership functions (MF) defined on a user application appropriate universe of discourse.

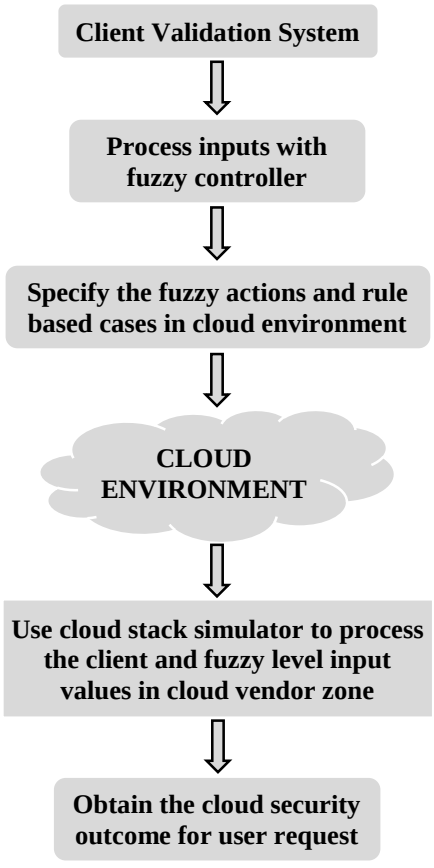


Fig.2. Illustration of Simulation work

The user level authenticity process has been proved in the various parameters in the clod environment. The following diagram will specify the Fuzzy rule based implications in the cloud security domain.

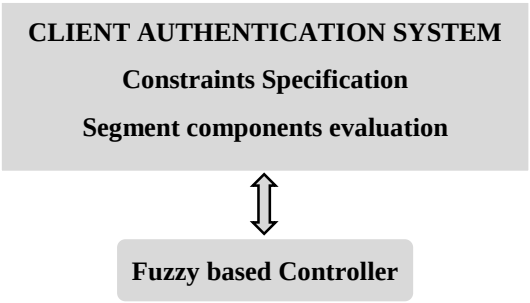


Fig.3. Depicting the process of user authentication

All the cloud user applications are processed in the suitable cloud environment, to get the service in a quick-response manner. To eliminate the problem of resource or data stealing then get the secure components from the various user zones.

5.1 CLIENT ENTRY AUTHENTICATION IN FUZZY FORUM

To specify the user access credentials and application deployment in the cloud environment that can be processed initially. Client level security parameters can be implemented into the constraints and segments manner with respect to the user validation control.

Constraints Used:

- User login values
- Security image finding
- Service access time span
- Protection of user content based on their request IP address

Segments Used:

- Specification of distinct user parameter
- Implementing the Fuzzy-rule access systems
- Process the IP and OP system specification
- Make use of Fuzzy membership function

Based on the above mentioned security parameters all the cloud user related information's are derived from the cloud environment.

Time complexity has been evaluated as a set of user constraint segments and the fuzzy rule implications.

$$\text{Time complexity rate} = \frac{\text{Total services consumed}}{\text{Fuzzy rule value + security result}}$$

5.2 SIMULATED RESULT TABLE (RESULT SET-1)

In this result set entry all the user parameters are processed into the validation access control into the cloud service provider access rights all the security credentials are supervised by the cloud administrator. To enhance the quality based content protection is achieved.

Table.1. Result set 1

User input parameter	Service type	Constraints Segments value (%10)	Fuzzy rule based values (%100)	Security outcome (%100)
Alpha-numeric	SAAS	8.051	88.53	89.43
Text	PAAS	8.903	80.03	90.54
Pixel	IAAS	9.781	94.561	95.83
Nominal	CAAS	9.047	98.04	97.03
String	MAAS	8.906	95.83	96.81

5.3 SIMULATED RESULT TABLE (RESULT SET-2)

In this result set, analyzing the user login details are considered as a one of the major input value. The various user level input parameters are processed into the apache cloud stack simulator tool with an essential cloud user input package and cloud vendor built in package set.

Table.2. Result set 2

User input values	Fuzzy min values (0.5)	Fuzzy max values (0.5 to 1)	Client security values
Image	0.35	0.683	Authenticated
Audio	0.459	0.790	Authenticated
Text	0.327	0.931	Authenticated
Video	0.341	0.960	Authenticated
Pattern	0.468	0.95	Authenticated

From an above result sets (Table.1 and Table.2), user input values are processed in to the cloud environment. Various computation approaches are used and simulated in the proposed client validation system. Use of eclipse IDE and java jdk 1.7.0 version software tools are used and manipulated in the user level security perimeter control.

6. EXPERIMENTAL RESULTS

With respect to the user level input constraints and segments form of process user will get a quality security result for cloud client private data. This proposed model will evaluates a user validation control and needs to be used free from the hackers.

This mechanism is used for any cloud user to protect their confidential information. By using the fuzzy rule based system some sort of computation process has taken place into the cloud environment.

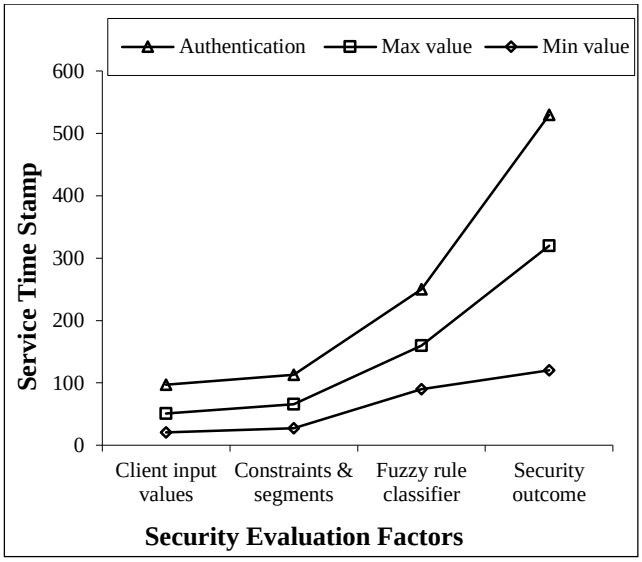


Fig.4.

From an experimental result set, four major different parameters are considered as an input values for X- axis, and 100 point scales is used in Y- axis as a value based factors in timescale or timeline.

From the result obtained we are trying to obtain the quality and enhancement of cloud used data protection.

7. CONCLUSION

From the proposed approach, a client level security target result has proven for trustworthy for client level resource and service which is consumed from the cloud vendor. This result set can apply into the various cloud applications in order to prove an authenticity for cloud clients. So, this result can be used for many applications to secure and safeguard the user content protection.

8. FUTURE ENHANCEMENT

All application environment, the service package and security implementation strategy have been proved for the distinct cloud user services. Need to analyze the various security peripherals around the cloud application platform. In upcoming cases, we may apply this kind of rule based systems in any security service domains.

REFERENCES

[1] Tram Truong- Huu and Chen Khong Tham, "A Novel Model for Competition and Cooperation among Cloud Providers", *IEEE Transactions on Cloud Computing*, Vol. 2, No. 3, pp. 251-265, 2014.

[2] Xu Wu, "A Fuzzy Reputation-based Trust Management Scheme for Cloud Computing", *International Journal of Digital Content Technology and its Applications*, Vol. 6, No. 17, pp. 437-445, 2012.

[3] M. Supriya, L. Venkataramana, K. Sangeeta and G.K. Patra, "Estimating Trust Value for Cloud Service Providers using Fuzzy Logic", *International Journal of Computer Applications*, Vol. 48, No. 19, pp. 28-34, 2012.

[4] K.W. Nafi, A. Hossain and M.M. Hashem, "An Advanced Certain Trust Model using Fuzzy Logic and Probabilistic Logic Theory", *International Journal of Advanced Computer Science and Applications*, Vol. 3, No. 12, pp. 164-173, 2012.

[5] Bei Guan, Jingzheng Wu, Yongji Wang and Samee U. Khan, "CIVSched: A Communication-Aware Inter-VM Scheduling Technique for Decreased Network Latency between Co-Located VMs", *IEEE Transactions on Cloud Computing*, Vol. 2, No. 3, pp. 320-332, 2014.

[6] Manish Kumar Aery and Sumti Gupta, "Comparative Study of Security Parameters by Cloud Providers", *Indian Journal of Computer Science and Engineering*, Vol. 4, No. 2, pp. 132-137, 2013.

[7] K. Konstanteli, T. Cucinotta, K. Psychas and T. Varvarigou, "Elastic Admission Control for Federated Cloud Services", *IEEE Transactions on Cloud Computing*, Vol. 2, No. 3, pp. 348-361, 2014.

[8] Sheng Di, Cho-Li Wang, and Franck Cappello, "Adaptive Algorithm for Minimizing Cloud Task Length with Prediction Errors", *IEEE Transactions on Cloud Computing*, Vol. 2, No. 2, pp. 194-207, 2014.

[9] Sudip Misra, Snighda Das, Manas Khatua and Mohammad S. Obaidat, "QoS-Guaranteed Bandwidth Shifting and Redistribution in Mobile Cloud Environment", *IEEE Transactions on Cloud Computing*, Vol. 2, No. 2, pp. 181-193, 2014.

[10] Amir Vahid Dastjerdi and Rajkumar Buyya, "Compatibility-Aware Cloud Service Composition under Fuzzy Preferences of Users", *IEEE Transactions on Cloud Computing*, Vol. 2, No. 1, pp. 1-13, 2014.

[11] Hossein Morshedlou and Mohammad Reza Meybodi, "Decreasing Impact of SLA Violations: A Proactive Resource Allocation Approach for Cloud Computing environments", *IEEE Transactions on Cloud Computing*, Vol. 2, No. 2, pp. 156-167, 2014.

[12] Luca Ferretti, Fabio Pierazzi, Michele Colajanni and Mirco Marchetti, "Performance and Cost Evaluation of an Adaptive Encryption Architecture for Cloud Databases", *IEEE Transactions on Cloud Computing*, Vol. 2, No. 2, pp. 143-155, 2014.

[13] Sandeep K. Sood, "A Combined Approach to Ensure the Data Security in Cloud Computing", *Journal of Network and Computer Applications*, Vol. 35, No. 2, pp. 1831-1838, 2012.

[14] Chun-Wei Tsai, Wei-Cheng Huang, Meng-Hsiu Chiang, Ming-Chao Chiang and Chu-Sing Yang, "A Hyper-Heuristic Scheduling Algorithm for Cloud", *IEEE Transactions on Cloud Computing*, Vol. 2, No. 2, pp. 236-250, 2014.