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

STRENGTHENING THE PROCESS OF USER LEGITIMACY IN CLOUD ENVIRONMENT USING FUZZIFICATION APPROACH

R. Poorvadevi*, S. Rajalakshmi**

**Assistant Professor, CSE Department, SCSVMV University, Kanchipuram, Tamil Nadu, India*
Email: poorvadevi@gmail.com
***Director of SJCAC, SCSVMV University, Enathur, Kanchipuram, Tamil Nadu, India.*

Abstract *In cloud computing lots of resources are consumed by the distinct end users whoever are strongly connected with the web. CSP is providing enormous amount of services to its requested clients. However service provider is offering plenty of services, still there is a lack in security and privacy factors at the client end. Whatever transaction and operations are performed by the cloud users those are safely maintained on the cloud database. Once the resources /services are transferred from CSP to the customer's location at that instance, hackers get the loophole from the customers based on the way they use the service. So, securing the user data is the essential task in the cloud service access platform. So, this proposed work is mainly used to authenticate cloud users and also protect the client data from the attackers as well as restricting the attacker's entry in the cloud environment. This can be achieved by using the fuzzy computational process, that is called fuzzification process to find the security solution which is optimal to the user focal point. The targeted result can be processed on the cloud apache stack tools.*

Keywords: *Cloud Vendor, Fuzzy Computations, Fuzzification, Cloud Service Provider, Cloud Clients, Authenticity*

Introduction

Cloud computing is an emerging commercial infrastructure and Internet based cost-efficient computing where information can be accessed from a web browser by customers according to their requirement. Cloud computing in a generic term is defined for anything that involves delivering hosted services over the Internet. It is based on the concepts of shared computational, storage, network and application resources provided by third party in Cloud.

There are different kinds of clouds that can be developed like private, public, and hybrid clouds. In the private cloud the infrastructure is operated solely for an organisation and managed by the organisation or a third party and it may be exists on- premise or off-premise. A private cloud is supposed as a data centre that supplies hosted services to a limited number of people or group of people.

When a service provider uses public cloud resources to create their private cloud, the result is called a virtual private cloud. A hybrid cloud is a cloud computing environment which combines the benefits of different types of cloud. An organisation provides and manages some resources in-house and has others provided externally in hybrid cloud.

You can create a fuzzy system to match any set of input-output data. The Fuzzy Logic Toolbox makes this particularly easy by supplying adaptive techniques such as adaptive neuro-fuzzy inference systems (ANFIS) and fuzzy subtractive clustering.

Fuzzy logic models, called fuzzy inference systems, consist of a number of conditional "if-then" rules. For the designer who understands the system, these rules are easy to write, and as many rules as necessary can be supplied to describe the system adequately (although typically only a moderate number of rules are needed).

Related Work

In the technique given in "An approach to unified cloud service access, manipulation and dynamic orchestration via semantic cloud service operation specification framework" by Fang, Liu, Romdhani and Pahl (n.d.), the unified cloud service value can be optimised and monitored at various levels of cloud related service information. It improves the performance and throughput values of the cloud vendor service operations. It also emphasizes that the various set of cloud service related manipulation can be found in the cloud service based specification framework approach (Tsar & Lo, 2015).

To implement the operational efficiency of performing data consistency approach. This technique can be mainly applied onto the various platforms and also ensure the cloud service with the data consistency value. This has been proved in the strategy by Phansalkar and Dani (n.d.), in "Tuneable consistency guarantees of selective data consistency model". How to improve the service utility segment value from the end user by improving the consistency value was achieved by this model (Samanthula, Elmehdwi, & Jiang, 2015).

So, this set of results implications will specify the cloud services and guarantee for various cloud resources to enable the functionality. Whenever cloud vendor is providing the service from that part to end-user delivery notifications, preventing the secured transactions between the user and CSP is the vital task.

Proposed Work

In cloud era, all kind of applications have different kind of entities and component values. How to process the requested user service and delivered into the user location is the much important aspect. This will be properly happening at the service provider end. Once, user has obtained the service from the CSP, they start to adopt and access it. During that time only, the security issue can be initiated by the attackers. So, the most challenging part of security issue has been solved up to the end user level satisfaction.

Latest Cloud Security Issues

In the recent study reports of cloud computing, it's proved that security is challenged as the top most issue in cloud environment. The important security issues are listed below:

- User Authentication
- Vendor lock-in
- Data loss
- Data Privacy

Focusing on the cloud security issue may increase the rate of cloud service usage among the cloud clients. Proving the authenticity of cloud user is most essential.

Significance of Fuzzification

Fuzzification is the major process of making a crisp quantity of fuzzy values. We will perform this operation by recognising many quantities of deterministic values from the operational sequences. In fuzzy approach, uncertainty, imprecision, ambiguity values will be considered as the better fuzzy probability functions. The data considered for fuzzy based membership function will be taken to an account of rule implication system in order to provide the qualitative result.

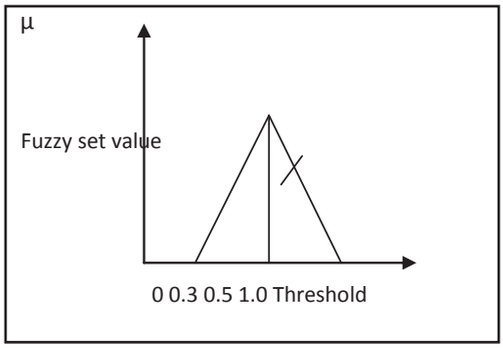
In other cases, the sampling rate will be translated into the fuzzy membership functions to prove the optimal result set value.

Implementation Work

In cloud service access environment, all the resources can be specified across the service provisioning segment. The various levels of authenticity parameters can be considered to provide the better result to the dependent clients.

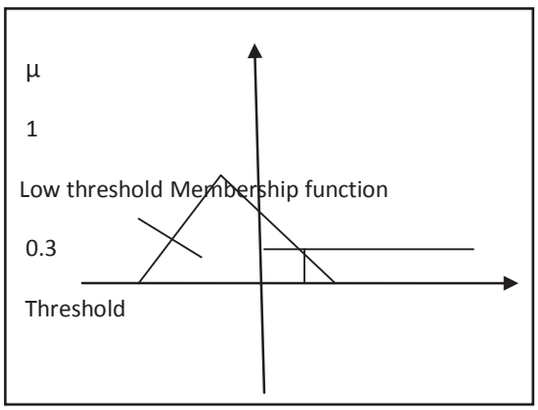
User authorisation and authentication will be proved in the cloud platforms to ensure the uniqueness feature of cloud user. It is also recommended to have such approaches to secure the user level secret data and also protect the data security. The major services of cloud resources are mainly concentrating on improving the business agility and service utilisation among the service providers.

Fig. 1: Illustrates the Fuzzification Process by Considering the Threshold and Membership Function Value



From Figs. 1 and 2 it has been proved that the various threshold values will be find out during the fuzzification process. It also emphasizes that the different level of threshold values will be noted.

Fig. 2: Finding Low Threshold Value



Simulation Process in Cloud

Research and evaluation of wide environments are usually associated with simulation. Also cloud computing is no exception of this rule, because research on total context of internet is too difficult and involves interaction with multiple computing and network elements, which may not be under control of developers. Moreover, network conditions may not be controllable and predictable and this will affect evaluation.

This approach will cover evaluation and simulation of cloud environment. For simulation, we will use Cloud Analyst tool which is a graphical design based on cloud sim. It is necessary to note that scenarios in Cloud Analyst are controllable and repeatable and do not require programming.

Simulation Components

In simulation with Cloud Analyst tools, there are two main components which are introduced below. It should be noted that each of these two components is configurable. Data centres or DC, show the hardware configuration, which include processors, storage, internal memory, bandwidth etc.

These data centres can be defined in different geographic areas. Besides the number of processors in data centres, VM's speed is also configurable. Cloud users have been distributed geographically as user groups. The requests are configurable for users such as geographical area, number of requests per hour, etc. It should be noted that each user can symbolise a person, an organisation, or a group. There are different policies for scheduling these tools, such as nearest data centre, optimising, response time, and dynamic configuration.

The assumptions used in the simulation are described as following. Type of requests based on data size is assumed as data centre and also 6 geographical regions are defined as shown in Table 1. Maximum number of users is 50, simulation time is 24 hours, and data centres policy is based on the closest connection to the to the data centre.

The various set of information process should be analysed and optimised in following sections:

Table 1: Data Size Assumptions

Data size Assumptions	Request types
100 – 500 Byte	Hybrid requests (computing, networking, I/O, memory)
500 – 1000 Byte	Requests related to memory
1000 – 1500 Byte	Requests related to CPUs and computing
1500 – 2000 Byte	Requests related to transmission and network
2000 – 2500 Byte	Requests related to storage and retrieval and data access

Table 2: Cloud Service Access Geographic Regions

Region Number	Region	Time Zone
0	N. America	GMT - 6.00
1	S. America	GMT - 4.00
2	Europe	GMT + 1.00
3	Asia	GMT + 6.00
4	Africa	GMT + 2.00
5	Oceania	GMT + 10.00

The various set of information process should be analysed and optimised in the following sections.

Simulation Metrics

Table 3: Simulation Metrics

Type of service	FV Value	FCM outcome (% 100)
Monitoring	8.532	90.543
Security	7.094	98.547
Platform	8.921	90.736
Compliance	9.032	96.048
Privacy	8.281	95.095
Data	7.973	94.865
Network	7.628	90.541
Identity	8.940	96.732

The following metrics of Cloud Analyst are used in this simulation to prove the user authenticity task:

- Minimum, maximum and average overall response time
- Minimum, maximum and average processing time in the overall data centre
- Minimum, maximum and average response time per user
- Minimum, maximum and average time per data centre
- The total cost of the virtual machine
- Cost per VM of Data Centre
- Cost of data in each data centre
- Total cost in each data centre

Simulation Category

There are three categories in this simulation and evaluation to prove the user authenticity process. It should be mentioned that this category has been selected based on major components in cloud environment. Specific metrics are used in each section and reviewed in chart. These categories have been selected because data centres, users, and geographic region are important in cloud computing environments.

This process is based on data centres, in which evaluation is done by modifying the virtual machine, memory, and bandwidth. In the section of simulation and evaluation based

on users, we evaluate the results with change in number of users and volume of work.

In the section of simulation and evaluation based on geographical region, we study geographical location of users and data centres and want to determine how effective they will be on criteria if the data centres and users are in the same region or are far from each other in different regions. It should be mentioned that only results of some metrics are studied and mentioned for each case of simulation scenario.

Simulation Evaluation Based on Data Centres

Scenario: In this scenario, the number of users is assumed to be constant and equal to 50. They are distributed in different regions, and requests are hybrid. All settings related to the data centres are fixed and only the number of data centres is changed from 1 to 20 centres. The simulation time is 24 hours.

The simulated outcome has been given in Tables 4 and 5.

Tables 4 and 5 have shown the outcome value of the proposed work by using feature recognition system. This implication of results shows that, security service has been improved as 98.547%. So, this kind of fuzzy based approach can be used to solve the computational problems. Table 6 implies the comparative study or comparative analysis report.

Table 4: FCM Process Outcome

User IP address	CSP process ID and value set	Feature vector (FV) process value (% 10)
192.168.10.261	A102.98	8.532
191.164.09.209	AF029	7.094
192.184.32.028	AE281.02	8.921
192.163.29.463	BH0.43	9.032
192.162.10.372	AF93.92	8.281
193.24.837.033	BFA.102	7.973

Table 5: Simulated Security Value through FCM Quality Check Constraints

User Service type	FCM outcome (0 to 1)	Authenticity value (%10)
SAAS	0.09	89.2
PAAS	0.46	94.10
PAAS	0.8	89.024
MAAS	0.76	96.39
IAAS	0.92	93.2
DAAS	0.63	95.2
SEC-AAS	0.84	98.32

The resultant value which we obtained from the proposed approach can be compared with the existing security method values in order to show the efficiency/performance rate of the proposed process.

Table 6: Analysis of Comparative Study

Service type	Authentication parameters	Compared outcome
Security	Multifactor	86.437
Monitoring	Image consideration	92.03
Privacy	Encryption technique	93.872

The simulated result shows that proposed security approach has been proved as an efficient process than the existing approaches by comparing with the existing survey and analysis report.

Experimental Results

The targeted result sets are applied in the cloud environment to ensure the performance rate of the newly developed technique. This technique has undergone with the help of FCM value set. This can be specified through Fig. 3.

Fig. 3: FCM Process Illustration

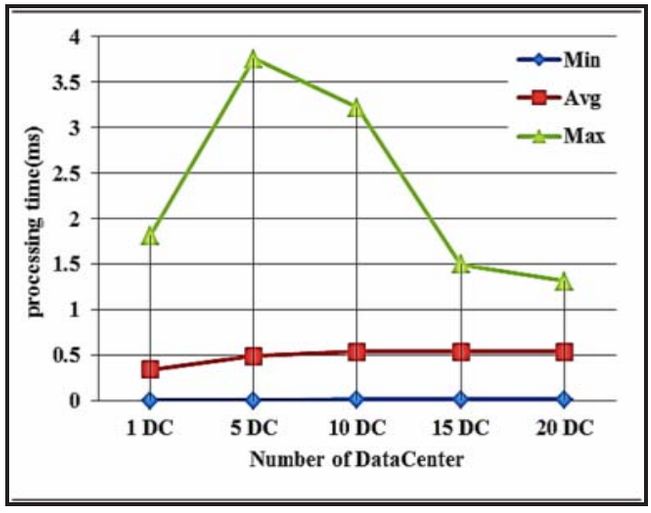


Fig. 3 illustrates that how the proposed work has been achieved through FRS process by using the various components and parameters. The rates have been fixed in maximum and average state. After 10 data centres the rate is fixed which will not have positive impact and will only increase cost. It should be mentioned that interaction between 5 data centres is due to the chart level rise for this state, as can be shown in Fig. 3.

Conclusion

User level data security is the major challenge in service access environment. End users are required to protect their own secret data from the various vulnerable. This approach could be a more effective method to safeguard the user information by using the fuzzy based mathematical computation model.

Future Enhancement

In upcoming cases, fuzzy based computational approaches can be used in any security domains. Even in data analytics domain we could able to analyse the large volume applications with the help of feature/ fuzzy based input recognition system.

References

Baek, J., Vu, Q. H., Liu, J. K., Huang, X., & Xiang, Y. (2015). *A Secure Cloud Computing Based Framework for Big Data Information Management of Smart Grid*. IEEE Transactions on Cloud Computing, 3(2), 233-244.

Barsoum, A. F., & Hasan, M. A. (2015). *Provable Multi-copy Dynamic Data possession in cloud computing systems*. IEEE Transactions on Information Forensics and Security, 10(3), 485-497.

Fang, D., Liu, X., Romdhani, I., & Pahl, C. (2015). An approach to unified cloud service access, manipulation and dynamic orchestration via semantic cloud service operation specification framework. *Journal of Cloud Computing*, December, 4(1), 1.

Hongbing, C., Chunming, R., Kai, H., Weihong, W., & Li, Y. (2015). *Secure big data storage and sharing scheme for cloud tenants*. IEEE Transactions on Communication Systems, June, 12(6), 106-115.

Juliadotter, N. V., & Choo, K. K. R. (2015). *Cloud Attack and Risk Assessment Taxonomy*. IEEE Transactions on Cloud Computing, 2(1), 14-20.

Liu, H., Ning, H., Xiong, Q., & Yang, L. T. (2015). *Shared Authority Based Privacy-Preserving Authentication Protocol in Cloud Computing*. IEEE Transactions on Systems, 26(1), 241-251.

Liu, J., Huang, K., Rong, H., Wang, H., & Xian, M. (2015). *Privacy-Preserving Public Auditing for Regenerating code-based Cloud service*. IEEE Transactions on system security.

Phansalkar, S. P., & Dani, A. R. (2015). Tunable consistency guarantees of selective data consistency model. *Journal of Cloud Computing Advances, Systems and Applications*, December, 4(1), 1.

Samanthula, B. K, Elmehdwi, Y., & Jiang, W. (2015). *K-Nearest neighbor classification over Semantically secure encrypted relational data*. IEEE Transactions on Knowledge and Data Engineering, 27(5), 1261-1273.

Tari, Z., Yi, X., Premarathne, U. S., Bertok, P., & Khalil, I. (2015). Security and Privacy in Cloud Computing: Vision, Trends, and Challenges. IEEE Transactions on Cloud Computing, 2(2), 30-38.

Tsar, J., & Lo, N. (2015). *A Privacy-Aware authentication scheme for Distributed Mobile cloud computing services.* IEEE Transactions on System Engineering, 9(3), 805-815.

Wu, Z., Xu, Z., & Wang, H. (2015). *Whispers in the Hyper-space: High-Bandwidth and Reliable covert channel Attacks inside the cloud*. ACM transactions on Networking, April, 23(2), 603-614.

Yao, X., Liu, H., Ning, H., Yang, L. T., & Xiang, Y. (2015). Anonymous Credential-based Access Control Scheme for Clouds. IEEE Transactions on Cloud Computing, 2(4), 34-43.