American Journal of Data Mining and Knowledge Discovery
2016; 1(1): 1-6
http://www.sciencepublishinggroup.com/j/ajdmkd
doi: 10.11648/j.ajdmkd.20160101.11

A Scheme for Improving the Performance of User Authenticity Through Client Validation Process Using Fuzzy Associative Memory (FAM) in Cloud Computing

R. Poorvadevi, S. Rajalakshmi

SCSVMV University, Kanchipuram, Tamilnadu, India

Email address:
poorvadevi@gmail.com (R. Poorvadevi), srajalakshmi@kanchiuniv.ac.in (S. Rajalakshmi)

To cite this article:
R. Poorvadevi, S. Rajalakshmi. A Scheme for Improving the Performance of User Authenticity Through Client Validation Process Using Fuzzy Associative Memory (FAM) in Cloud Computing. *American Journal of Data Mining and Knowledge Discovery.* Vol. 1, No. 1, 2016, pp. 1-6. doi: 10.11648/j.ajdmkd.20160101.11

Received: October 27, 2016; **Accepted**: November 14, 2016; **Published**: December 17, 2016

Abstract: So far, in cloud computing lots of services are consumed by the distinct clients. However, cloud is providing all kind of services (everything as a service - Xaas) to its dependent users. Still, there will be efficient security procedures and parameters are needed in the client end. Cloud service providers are offering the service with proper security perimeter control. After receiving the service from the CSP, users are losing the security control over their confidential data. So, protecting the user secret data is essential. The proposed approach will be used for securing the data by authenticating the registered user through the fuzzy associative memory (FAM) technique. This approach mainly focuses on one / two dimensional data access point might be considered for user authenticity computational process in order to increase the performance level of data security. This can be achieved by using the green cloud simulator tool in cloud environment.

Keywords: Cloud Vendor, Fuzzy Associative Memory (FAM), Cloud Service Provider (CSP), Cloud Clients, Data Security and Green Cloud Sim

1. Introduction

Cloud computing is the buzzword will explicitly offers tremendous information as a form of resources to the requested users. Anything can be given as a service to the web clients. So, cloud is also referred as utility computing. There are lots of services are offered to the various cloud clients in order to improve the business agility and easy way accessing unlimited services. Initially cloud computing was introduced for the enterprise level applications and increasing the business strategic process between the end users.

Security aspect will be a major factor in cloud service access environment. Earlier computing mechanisms are not providing the sufficient security procedures to the web users.

Ensuring the security service reliability is the vital feature for the cloud customers. We need to analyze that, how far the security service is feasible in the client focal point for using the cloud services from the distinct cloud vendors. Cloud service providers are enabling the distinct features with the authorization and access privileges to the requested users. However service provider is providing the service to its dependent users, still sufficient security schemes and parameters are lacking in the client end.

1.1. Recent Security Issues in Cloud

Cloud computing is the business related functionality which applied into the business forums. In traditional approaches, most of the enterprises are included the cloud resource for the purpose of their easy way of adopting the user queries and managing the distinct activities. Although, there are major services and resources which is offered by the cloud, still there is some major cloud security related problems.

The most cloud issues are listed below:

- Interoperability

- Vendor lock-in
- Security
- Privacy
- Efficient Resource management

So, from these issues, we are mainly concentrating on the security problem in order to safeguard the user confidential information.

1.2. Significance of Cloud Security and Privacy

In the scientific computing era, all the web resources and user services are encrypted and hidden in the unreadable format due to the problem of security and privacy factor. Protecting the confidential information such as, the user log history, service usage report, Secret data usage, sharing the resources to other web user, finding the resource monitoring and management services is mandatory in the client level computing mechanism. So, it is needed to increase the performance of security and privacy is the major concern in the client access cloud environment.

2. Literature Survey Analysis

As per an author Barsoum, A.F., San Antonio, Hasan paper titled as, "Provable Multi copy dynamic data possession in cloud computing systems". In this paper an authors stated that, for the authentication feature and data possession analysis feature customers prefer the multi copy identical values for preventing the authenticity for each cloud user. [1]

To automate the services and providing the consistency kind of service utilization between the CSP and cloud user this strategy was proved by an author Phansalkar S, Dani A, "Tunable consistency guarantees of selective data consistency model" this approach mainly focuses on the service guarantee and consistency services from the cloud service provider. How to improve the service utility segment value from the end user by improving the consistency value it was achieved by this model [2].

From the survey study report shows that, security is ranked as a first challenge in cloud computing. It's a major concern to safeguard all kind of transactions which is happening in the cloud environment.

3. Proposed Work

The proposed model will focus on, how to secure the cloud client information and their confidential data in cloud atmosphere. It emphasizes the various kinds of security parameters are taken in to an account of cloud security and privacy concern. This method will concentrates on applying the cloud user activities and other important information's into the fuzzy logic forum in order to get the desired security outcome.

The new idea is, applying the security credentials into a fuzzy logic and does certain computational process over the input dataset. With the help of above information it is specifically added as a new feature for the web users for an easy way of resource/service protection from the distinct types of attacks. The following security controls are considered into the proposed work.

- User service request type
- Kind of access privileges
- Service provisioning ID
- Security segment value

(By referring SLA report)

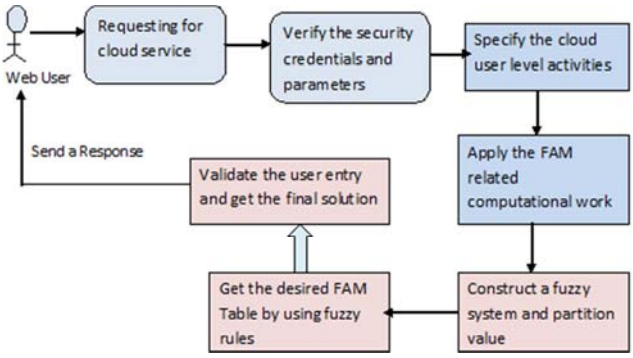
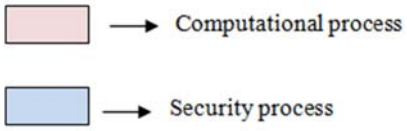


Fig. 1. *System Architecture Design.*

In the above process, all the proposed functionalities are depicted in pictorial form. This model will be an iterative process of validating cloud user in order to prove the uniqueness feature of the requested users.

In an above figure majorly two symbols are used:



All these kinds of information are processed in to the SecSDLC (Secured software development life cycle) environment. This computed result set would be an effective strategic solution for cloud security issue.

3.1. Significance of FAM

The new method of, Fuzzy associative memory is the one implication model for the cloud user for using n canonical (or) non-interactive kind of inputs and only one output (solution). Form the n distinct input parameters we may able to pass number of security perimeters, values, access control for the cloud user.

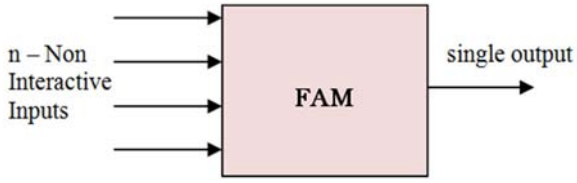


Fig. 2. *Illustration of Input and Output relationship.*

An important factor of FAM is, using or considering n-different set of inputs and do the computational process hence the desired outcome will be obtained as a single output.

Initially, for the computation process will have the following series:

- Get the service request from the user
- Analyze the input parameter for the concern person by CSP
- Group the different set of inputs(n – Non interactive inputs)
- Send it to the computational block.
- Design the fuzzy rules(Using canonical forms)
- From the fuzzy rule we need to govern the MF value
- Construct a FAM table
- Construct a FAM graph for the specified request

3.2. Process of Fuzzy Associative Memory

In FAM principle, the cumulative set of n inputs are processed and the processing block will be computed then finally, only one desired output will be obtained for the corresponding policy. The heterogeneous kind of inputs is considered and creations of fuzzy rules are mandatory to construct the FAM table.

Let, consider a fuzzy system with the set of n – non interactive inputs and a single output, and also assume each input universe of discourse will be considered.

That is,

$$X = X_1, X_2, X_3 \ldots\ldots\ldots X_n; \text{ // Fuzzy inputs} \quad (1)$$

$$K\text{- Partitions; // Fuzzy partition} \quad (2)$$

Based on the input elements create the fuzzy canonical model. By using the non linear system, the total numbers of possible rules are decided. It is given below as an expression form

$$l = k_n; \text{ // Partitioned values} \quad (3)$$

$$l = (K+1)_n; \text{ //ordered set of fuzzy values} \quad (4)$$

Here, l – is the maximum possible number of canonical rules for the various cloud services or request from the cloud user. It is majorly used as a one factor for fuzzy partition.

4. Implementation Work

In cloud environment, restricting the unauthorized user entry is somehow difficult in the client end service process. Because hackers are applying the intelligent kind of attacking mechanism and different set of illegal access during the client service processing and service exchange time.

To rectify these problems we need to find out the suitable solution for improving the credibility of user entry level data access. For that concern, the FAM can be used in this proposed model. In this case, FAM will be functioned as a processed segment of following computations:

Cloud users are specified as,

$$C_1, C_2, C_3 \ldots\ldots C_n; \text{ // cloud clients}$$

Smaller set of inputs are n=1, 2, 3…

FAM table can be generated by using the non linear mapping from input space and output space of the fuzzy system. The general model of FAM table has been given below:

I/P set	Process		
	X1	X2	X3
	X3	X2	X1
	X2	X2	X3

Fig. 3. *Partitioning the Fuzzy inputs.*

The input sets are accounted as X1, X2 and X3.

The various possible set of fuzzy system entities are specified as a non linear set of input identical values.

The user needs to specify the input credentials for their own privacy data access.

The non linear mapping fuzzy set need to specify the information sequences and other set of values in the mid range value of input space and output space of the fuzzy system.

Table 1. *Dataset used.*

Protocol type	Service flag	Service request	IP address
https	S0	Enabled	192.168.10.250
http	SF	Enabled	192.168.25.021
Smtp	S0	Enabled	192.168.28.876
Icmp	SF	Disabled	192.162.24.201
Tcp	SF	Enabled	192.163.62.103
https	S0	Enabled	192.169.02.361
http	S0	Enabled	192.167.04.832

Where,

S0 – service originate; SF – service Finish

An above dataset is used a major input set of entries for FAM method process. The resultant set value will be shown for the consecutive process of canonical form and fuzzy table derivation for the various input segment values. From this process segments we need to analyze the output region boundary state constraints as in the mentioned form which is represented below:

$$r << l; \quad (5)$$

r = canonical rules, l= fuzzy rules

From the process implications are included as a major part of the fuzzy based results and that can be configured as a fuzzy rule system along with the FAM table.

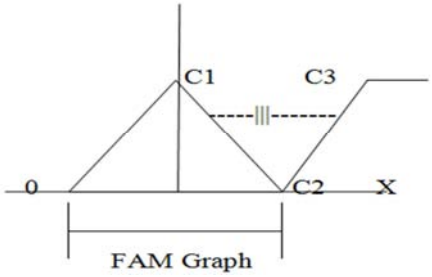


Fig. 4. *Process of FAM Components.*

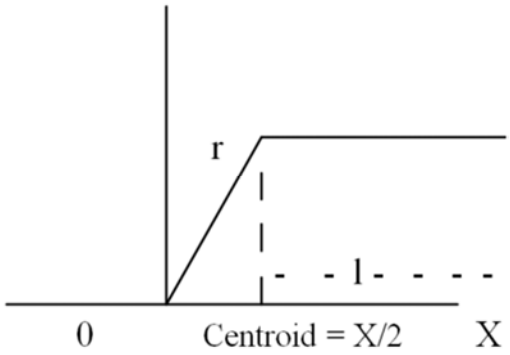


Fig. 5. *Process of FAM Segment Values.*

Above figures shows that, increasing of fuzzy rules (r) must be computed with the canonical form of implication result. These set of values will be applied into the common security service environment.

Table 2. *FAM Table set values.*

User service type	IP address matching	Fuzzy rule	Non linear set entries X = 0 >1	FAM segment Value for user Credentials
Public	YES	TRUE	X = 0.9	T
private	YES	TRUE	X= 1.5	T
private	NO	FALSE	X= 0.2	F
private	YES	TRUE	X = 0.9	T
private	NO	FALSE	X=0.01	F

The tables which is given below is the various set of input identical elements and therefore security value has been identified and also the results are discovered to the authorized cloud users in order to verify the security credential values.

5. Implementation Work

The results which can be obtained will be iterated for 3 more items in order to validate the security parameters well manner. To secure the client service access and keeping the data confidentially is not easy thing. We need to develop a strong user authentication system and then checking the requirements of system access and access control over the data.

The absolute value function = FAM outcome + cloud service access rate + fuzzy rule process output

In cloud environment, the process and the services are migrated from the cloud service provider to the end user location. It is necessary to verify the user level access. Will they are authorized and authenticated to use the cloud services or not. It's a greatest challenge in cloud service access environment. Protecting the virtual machine and segregating the VMM level constraints and also specify the access to the user by the way of keeping the hypervisor will be in safe manner.

5.1. Simulation Setup

Simulation IDE: netbeansIDE
Platform Used: Java Jdk 1.6.0
Simulator tool: cloud sim 2.0
Cloud_service_Provisioning: Enabled
IP address Detector: Enabled
Security Perimeter control: Active state

Above mentioned parameters are used in the cloud service platform to validate the user level access in the public and private domain. The fuzzy level implications have been proved in the new model to cross check the attributes which can be transferred between the CSP and cloud user.

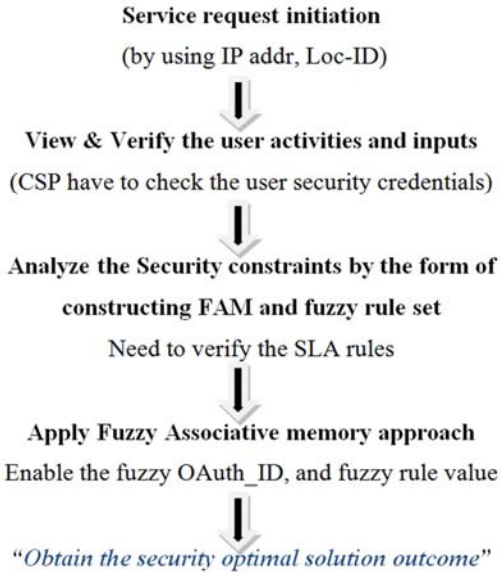


Fig. 6. *User Authenticity Provenance Process.*

The FAM approach can be specified as authorized information and various level information segments. In order to improve the client level confidence on the secret data the proposed approach has been activated as an emulator for user authenticity. The various client level processes also to be secured in the cloud environment.

5.2. Simulation Implication

In cloud environment all the services are processed and computed with the support of cloud service provisioning control level. This methodology has comprising the solution for cloud user level security issues and how to reduce the occurrences of hacking that also considered by using the authenticity protocol such OAuth, OpenID. This can be used to validate the client level security parameters.

6. Simulated Result Set &Validation

User authentication tasks can be already proved in the various domains. However while considering, cloud user authentication so far, 79.21% security result set only proved. When, the user is having strong bandwidth connectivity with the cloud applications they can consume and use boundless

services. The following table has depicting the authentication value which was obtained during the execution time.

Table 3. *Fuzzy Associative Memory Process Validation.*

Service Type	User Control segment value (b/w 0 and 1)	FAM process value(Satisfied)	Security solution value(% 10)
SAAS	0.31	YES	6.78
PAAS	0.72	NO	7.09
PAAS	0.23	YES	8.93
IAAS	0.72	YES	8.032
NAAS	0.37	YES	9.5
SEC-AAS	0.97	YES	9.87
MAAS	0.821	YES	9.02
DAAS	0.432	NO	9.045
XAAS	0.91	YES	9.53

SEC – AAS = Security as a service

So, from this simulated results it is proved that, security results are obtained as a high ratio outcome. By using the fuzzy associative memory (FAM) the user related information and activities are protected in order to safeguard the cloud user confidential data.

Cloud clients are can able to prefer the best security mechanism by the way of applying the fuzzy logic and its techniques. User control segment is classified with an interval range between 0 and 1 that can be implied as a one of the major factor for cloud security and privacy task. From this an operational efficiency has been proved for cloud user authenticity process.

Table 4. *User Authenticity Process.*

User Service Request	Cloud simulator process value (0 < x < 0.5)	Operational Efficiency (%100)
192.168.10.259	X = 0.35	83.1%
192.163.19.268	X = 0.21	97.2%
197.162.92.29	X = 0.49	96.39%
193.183.2.61	X=0.348	89.03%
198.163.83.71	X=0.292	93.28%
192.162.25.96	X=0.341	95.07%

From an above table results (Table 3 &4) shows that how the various security components are involved and processed in the cloud environment. There by security analysis and user authenticity process has been done with the help of cloud sim simulator tool.

7. Experimental Results

From the analytical results, we have been proved that, user authenticity has been specified as a major security challenge in cloud service process environment. So, this issue has been solved by using the fuzzy associative memory technique.

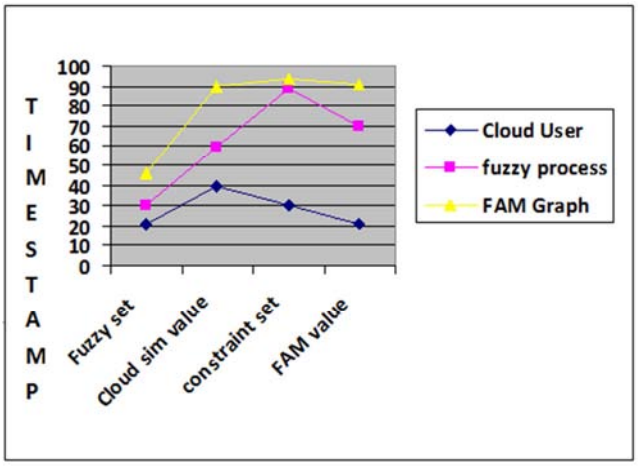


Fig. 7. *FAM Process Result set.*

The process that has been illustrated in the table is, as an identical process of user authenticity process. The following graph has been sustained as a user authenticity process for the client validation system.

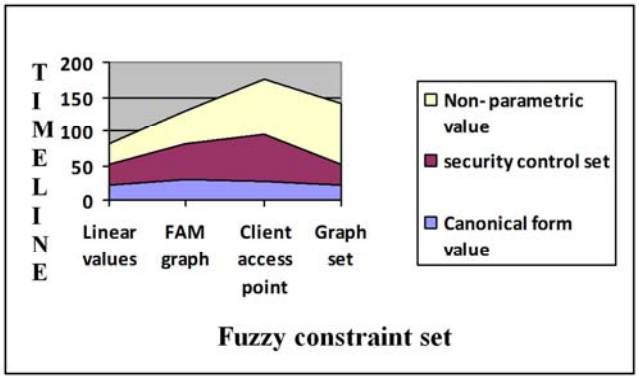


Fig. 8. *Fuzzy Optimization Process.*

From the simulated results, it proved that various security controls set and parameters are applied in the proposed model in order to get an efficient security solution.

8. Conclusion

Fuzzy logic set and its techniques to be enhanced in the various application domains. In cloud computing environment, the security solutions have been obtained in an effective manner by used the technique of fuzzy associative memory. This kind of security procedures will be useful for the various threats based systems. Likewise, this kind of security system / security model based on fuzzy logic computations also to be applied in the data analytics domain.

9. Future Enhancement

In upcoming cases, the security solution has been applied into all necessary platforms. Eradicating the hackers entry will be the most expected process in the web computing. Fuzzy logic and constraint set will be applied in all application process environments.

References

[1] Miyoung jang; Min Yoon; Jae-Woo Chang, paper entitled as "A Privacy-aware query authentication index for database outsourcing" IEEE conference publications 2014.

[2] Confidentiality-Preserving Image Search: A Comparative Study between Homomorphic Encryption and Distance-Preserving Randomization author: Wenjun Lu; Google, Mountain View, CA, USA; Varna, A.L.; Min Wu IEEE transactions on volume 2 – 2014.

[3] Bio-cryptographic authentication in cloud storage sharing author: Velciu, M.; Comput. Sci. Dept, Mil. Tech. Acad., Bucharest, Romania; Patrascu, A.; Patrice, V. IEEE 9th International symposium on Applied Computational Intelligence and Informatics (SACI), 2014.

[4] Improving Cloud Security by Enhanced HASBE Using Hybrid Encryption Scheme author: Poornima, B.; Rajendran, T. World Congress on Computing and Communication Technologies (WCCCT), 2014 march-14.

[5] Analysis and prevention of vulnerabilities in cloud applications domains Durrani, IEEE Conference on Information Assurance and Cyber Security (CIACS), 2014.

[6] Authorized Public Auditing of Dynamic Big Data Storage on Cloud with Efficient Verifiable Fine Grained Updates Chang Liu; Fac. of Eng. & IT, Univ. of Tech., Sydney, NSW, Australia and more authors Parallel and Distributed Systems, IEEE Transactions on cloud computing- 2014.

[7] Effective Third Party Auditing in Cloud Computing Hussain, M.; Dept. of Interdiscipl. Studies, Zayed Univ. Dubai, Advanced Information Networking and Applications Workshops (WAINA), 28th International Conference on13-16 May 2014.

[8] Implementation of a secure genome sequence search platform on public cloud leveraging open source solutions authors: VikasSaxena, et al. Journal of Cloud Computing: Advances, Systems and Applications-2014.

[9] A multi level security model for partitioning workflows over federated clouds authors: Paul Watson journal of cloud computing 2014.

[10] Scalable transactions in cloud data stores author: Ahirrao S, Ingle R, Springer series. Journal of Cloud Computing: Advances, Systems and Applications, November–2015. Virtual machine introspection: towards bridging the semantic gap MoreA, Tapaswi S, Journal of Cloud Computing-2014.

[11] Clustering based fragmentation and data replication for flexible query answering in distributed databases, WieseL, Journal of Cloud Computing- 2014.