Journal of Applied Information Science
Volume 05 Issue 01, 2017
ISSN.: 2321-6115

An Advanced Mechanism of Cloud Resource Security Process in Client Location by Using Soft Computing Approach

R. Poorvadevi1, S. Rajalakshmi2,
[1]Assistant Professor (CSE), SCSVMV University, Kanchipuram, Tamil Nadu, India.
Email: poorvadevi@gmail.com
[2]Director of SJCAC, SCSVMV University, Kanchipuram, Tamil Nadu, India.
Email: srajalakshmi@kanchiuniv.ac.in

Abstract: Cloud computing is providing the distinct set of services by the form of cloud resources to the client end location. It needs to be iterated and operated on the secured cloud platform. It will increase the lots of security controls, function elements to be protected in the in the cloud client end. Though numerous security procedures, components, data security options are exist, but still we need to improve the cloud resources. Whenever the clients will perform some set of cloud service transactions, it is mandatory to secure the login, security, attribute credentials for the concern users. It will be evaluated on the cloud user service access platform and also it increases the security rate of cloud services. The proposed approach will be the betterment of cloud service operations and the securing aspect of cloud service components in an effective way by making use of soft computing applications. Fuzzy based operational sequences, authentication techniques are adopted in the cloud security process.

Keywords: Cloud vendor, Fuzzy technique, Cloud server, Cloud clients, Cloud service provider, Data centre.

I. Introduction

Cloud computing presently focuses on, a new approach to enhance the modern consumption and delivery model for IT services based on the internet. The major problems which is facing by the customer is, losing control over their confidential data. Even though, many security mechanisms and frameworks are deriving from

Distinguished developers still, there is a lack of consumer trust in cloud service providers. Many Approaches will focus on cloud service providers are attempted to overcome the data safety problem due to compliance across the geographic boundaries. So, as an end user perception emphasizing the data protection is most important with the privacy control. Cloud security is, the security principles applied to protect data, applications and infrastructure.

Cloud security is, the security principles applied to protect data, applications and infrastructure associated within the cloud computing technology. Rising the joint venture between cloud service providers and security solution providers are mostly expected. Growing the emergence of cloud services are specifically focused on the security content solution providers. One of the major components in cloud security service is identity and Access management principles that can be used as an authenticity validation or recognition system.

A. Challenges of Cloud Security Process

In the cloud service access environment, lots of cloud services can be optimized in the distinct cloud vendor location. Data centre will process all the client level information, type of security approaches, security policies, security based cloud service measurements will be considered in the different aspect of cloud resource optimization and identification process. The following lists of challenges are faced by both cloud user and cloud service provider which is given below:

- Cloud based vendor lock – in issue
- Security API's & GUI's
- Security control segments
- Multi tenancy issue
- Service based Software configuration and updates controls
- User level security policy exchanges

II. Related Work

The various client level transactions are performed in the different security time spans and it also considers the set of authentication parameters which enables the function of user level secure resource sharing process. Another technique is, authorized public auditing of dynamic big data storage on cloud with efficient verifiable fine grained updates, this approach deals with the storage as a service as a big data storage phenomenon for proving the authorization of public auditing scheme [1]. Preventing anomaly based intrusion detection systems can also

be applied for security solution in order to improve the security provenance rate between cloud service provider and clients [2].

Another approach is a secure cloud computing based framework for big data information management of smart grid. It was defined and developed a framework model designed for evaluating the huge data content management for smart grid services [3].

III. Proposed Work

In cloud environment, all the services and processes can be migrated and processed on the various virtual machines. It will interpret the values of security process control under the specific organizational units. In the processing location of data centre it will prompt and redirect the user resources from the actual location to VMM location analyzer zone. The various security based parameters can be executed on the cloud based platform access oriented applications.

The service based resource modeling has been enabled in the functionalities of user level service access security process can be initiated on the secure platform based cloud resource migration. There is a migration time will be taken into the consideration of service based resource pooling warehouses. It will provides the security functions, components, authentication policies will be structured into the evaluation oriented on the security level classifications will be in infrastructure security, physical security, operational security. The following system architecture shows the proposed work.

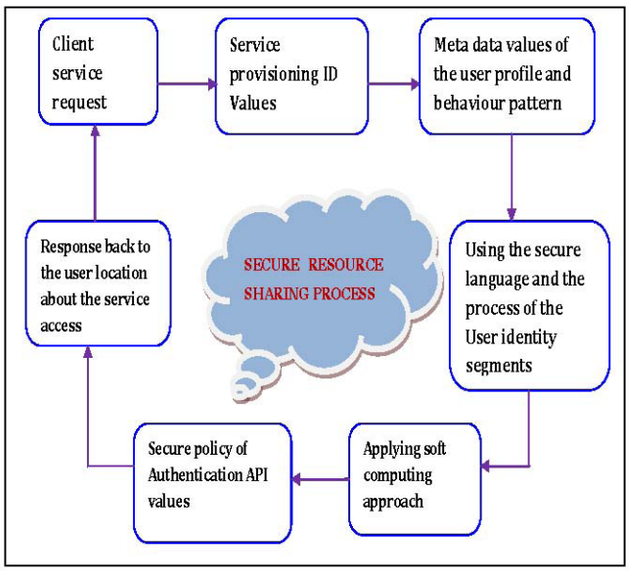


Fig. 1: Proposed System Architecture

The system architecture depicts the functional operations of secure access platform for providing the data protection in a well secured environment. The following security components were used in the proposed system modeling to enhance the client level security process. Components are given below:

- User service provisioning ID
- SAML and SPML ID values
- User service request location
- Determine the process runs on VM
- Use the data analysis to process the client values
- Specify the user service access API's
- Meta data values process ID segments.

The various references can be indicated in the service based platform through which user may share the resources and the security components are evaluated based on the user level segmented input process.

IV. Simulation Work

The security process can be indicated on the service based access location. They need to specify to enable about what are the securities functions, components can be evaluated in the security block and security engine. It may be processed in the cloud service provider access locations. The major security process can be specified and the levels of security and privacy components and additional tools can be identified in the various segmented values.

The following security parameters are evaluated during the service enhancement time. The fuzzy level operations can be involved in the indicating the operational performances in the public cloud infrastructure model. The various security based assertions and implications can be running on the source component of security platform which can be specify the security value of the input level considerations

A. Use of Soft Computing Technique

Soft computing or fuzzy computing will operates on the certainty and uncertainty values. On the boundary values range it will compute the values in the rationale format. Fuzzy set and its rules will gives the possibility of all the occurrences value which can be specifies in the security environment client level access predictions.

The set of fuzzy rule classifiers, segment values, operational elements can be processes and execute don the service implications based access privileges contents. It will externally specify the transactional reports could be effectively optimized in the cloud vendor.

The following computational formula is used in the simulation process.

User Security Evaluation Rate = set of attribute evaluated values + security procedures / 100

Resource sharing Security Process = Fuzzy application resultant value + operational outcomes.

The following flowchart has been used to specify and determine the values of soft computing based secure resource sharing

applications. In this strategy, the security applications can be runs on the specific cloud platform to enhance the security level applications.

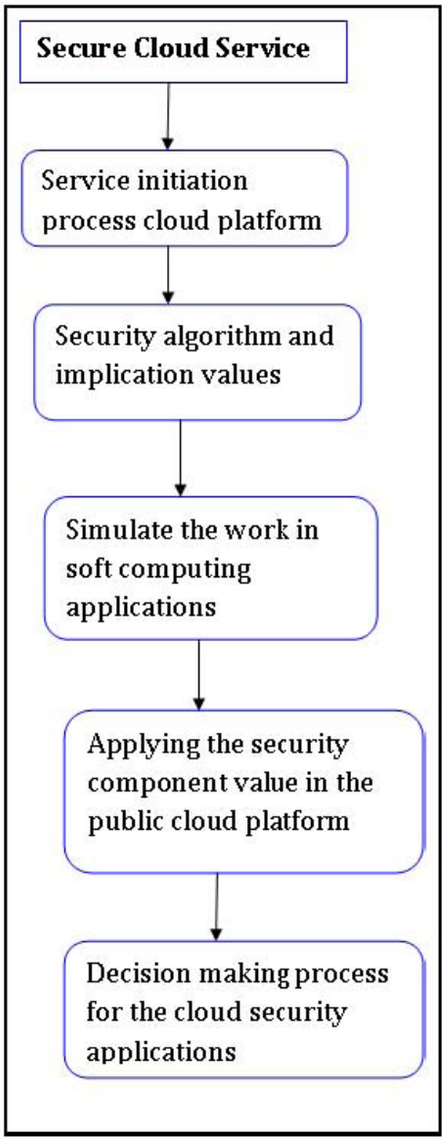


Fig. 2: Illustration of Proposed Work Flowchart

To implement the cloud security offering services people may consider the different action flow and workflow in cloud environment service portals.

V. Implementation Work

In cloud computing environment the various securities based operations are implemented and executed under the common cloud platform. To enable service access in the cloud service access region, then it's very significant to know the legitimacy of the user access privileges. The various security controlling features has been adapted to the distinct type of cloud resources via the form of data centre.

Nowadays, lots of security mechanism will come into the practical implementation to solve the problem of data leakage/ data loss due to insufficient techniques of security operational performance. In the client location, it will be prompt into the concern cloud user whoever, heavily depending on the cloud services. It is the most specific focus is, how to secure the client level process in the security portal and security based environment system.

The following security components are used in the proposed approach to enable the functionality of the security based service operational values which is listed below:

- User ID
- Access input pattern
- Security mode and the security key pair value
- Specification of I/O segment value
- Optimized security component value
- Frequent type of service access location
- Access permission and the controlled elements

With an above elements it will be validated the various controlling features with the help of adequate set of soft computing approaches. Specifically, in this proposed mechanism fuzzy clustering has been used to optimize the secure cloud resources sharing should be iterated between the client and CSP location.

The following table values will shows the result set of implementation outcome in the cloud security process function. The different security parameters will be optimized in the security portal access region in order to specify the qualitative process of secure resource distribution over the cloud.

Table I: Security Outcome Values

User IP address	Service access	Service Request region	Security outcome (% 100)
192.168.10.32	SaaS	DC - 4	85.92
187.3.023.20	SaaS	DC - 32	84.923
193.27.754.98	Iaas	DC - 509	67.02
184.92.04.93	Paas	DC - 764	89.54
191.05.853.138	SecaaS	DC - 31	98.943
195.168.10.42	Caas	DC- 076	92.19
198.843.15.94	Maas	DC - 964	94.873

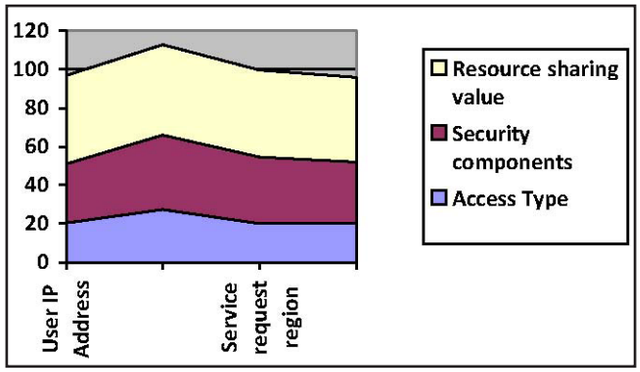
VI. Experimental Result Set

In the service access environment, the various type of service can be iterated and optimized in the different service access region as the form of DC (data centre) location. The service provisioning model can be specifies the controlling aspect of the user security services and resource sharing functionalities.

So, from the implementation results and study reports, in SecaaS (Security as a Service) better security value has been obtained.

The implementation strategy results will be incorporated in to the user legitimacy process for comparing different security elements and that execution procedure. The following diagram will shows the outcome of proposed model which is depicted below:

Result Graph Comparison



From an graphical illustration, it will be showing that the various implementation strategies solutions can be optimized with the different components which was involved in the specification of process of identifying and implementing the process over the secured platform and the communication channel should be operated on the client level security process. It will isolate all the controlling components, security elements, and other resource sharing processes are operated in the security portal environment.

VII. Conclusion

From the implementation results all the components, security process can be operated on the different data centre location to optimize the controlling component value. It will be identified with advanced techniques of security, data protection, information retrieval process and other security based applications. This component will be merged with the security domain with the concern CSP to give the solutions of the cloud users.

VIII. Future Enhancement

In future cases, the various security based operations can be involved in the process of enhancing the common portal and security infrastructure for all the domain specific applications.

References

[1] T. Truong-Huu, "A novel model for competition and cooperation among cloud providers," *IEEE Transactions on Cloud Computing*, vol. 2, no. 3, pp. 251-265, 2014.

[2] A. Tchana, B. Dilenseger, N. De palma, J. Salmi, and A. Harbaoui, "A self-scalable and auto regulated request injection benchmarking tool for automatic saturation detection," *IEEE Transactions on Cloud Computing*, vol. 2, no. 3, pp. 279-291, 2014.

[3] L. Toma's, and J. Tordsson, "An automatic approach to risk-aware data center overbooking," *IEEE Transactions on Cloud Computing*, vol. 2, no. 3, 2014.

[4] Y. Wang, and W. Shi, "Budget-driven scheduling algorithms for batches of map reduce jobs in heterogeneous clouds," *IEEE Transactions on Cloud Computing*, vol. 2, no. 3, pp. 306-319, 2014.

[5] B. Guan, J. Wu, Y. Wang, and S. U. Khan, "CIV scheduled communication-aware inter-VM scheduling technique for decreased network latency between co-located VM's," *IEEE Transactions on Cloud Computing*, vol. 2, no. 3, 2014.

[6] S. Tang, B. Lee, and B. He, "Dynamic MR: A dynamic slot allocation optimization framework for Map reduce clusters" *IEEE Transactions on Cloud Computing*, vol. 2, no. 3, 2014.

[7] K. Konstanteli, T. Cucinotta, K. A. Psyches', and T. Varvarigou, "Elastic admission control for federated cloud services," *IEEE Transactions on Cloud Computing*, vol. 2, no. 3, pp. 348-361, July, 2014.

[8] S. Kailasam, P. Dhawalia, S. J. Balaji, G. Iyer, and J. Dharanipragada, "Extending Map-reduce across clouds with B-stream," *IEEE Transactions on Cloud Computing*, vol. 2, no. 3, 362-376, July, 2014.

[9] S. Di, C. L. Wang, and F. Cappello, "Adaptive Algorithm for Minimizing Cloud Task Length with Prediction Errors," *IEEE Transactions on Cloud Computing*, vol. 2, no. 2, April-June, 2014.

[10] S. Misra, S. Das, M. Khatua, S, and M. S. Obaidat, "Qos-guaranteed bandwidth shifting and redistribution in mobile cloud environment," *IEEE Transactions on Cloud Computing*, vol. 2, no. 2, April-June, 2014.

[11] A. V. Dastjerdi, and R. Buyya, "Compatibility-Aware cloud service composition under fuzzy preferences of users," *IEEE Transactions on Cloud Computing*, vol. 2, no. 1, January-March, 2014.

[12] H. Morshedlou, and M. R. Meybodi, "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.