© 2016 IJSRSET | Volume 2 | Issue 2 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Evaluation of Service based Security Credentials for Resource Distribution Process in Cloud Environment Using Authorisation Management Approach

R. Poorvadevi, V. Bowshika, Mohana Priya, Bairavi. S

Department of Computer Science and Engineering, SCSVMV University, Kanchipuram, Tamilnadu, India

ABSTRACT

So far, in cloud computing people are accessing and consuming massive amount of services for their needs and improving the business agility. However, considering the factor of resource allocation / sharing in that instant, lots of security issues are raised with the unknown factor. So, Securing the data or confidential information of the cloud service is the vital task during the process of exchanging the resources among the cloud users. For avoiding such type of problem, the proposed model has come up with the new solution that is, authorization management. This technique will be mainly concentrates on, during the time of resource sharing between the user-to-user group, whatever the known and unknown malicious, threats and hackers entry will be identified based on the authorization features. This technique will have a key component of the function is, assigning the access privileges and entitlement of the cloud user. It also acts like a role-based access control (RBAC) policy for the user services. It will ensure the components of service provisioning, de-provisioning security parameters verification and other service based constraints. XACML standard is used for enforcing the authentication and authorization policies for the registered users. This approach could be an effective phenomenon to regulate the cloud services and secure those resources during service sharing moment. This could be achieving through the cloud simulator tool.

Keywords: Cloud user, Cloud service provider, cloud vendor, Cloud sim, Authorization policy, Resource sharing.

I. INTRODUCTION

In cloud computing environment a distinct set of services and resources are used by the cloud clients. A huge amount of services can be making use of cloud clients by sending the service request to the cloud vendor/cloud service provider in order to make use of some optimal services for their needs. A cloud environment is purely works on the different types of data centre and also perhaps the operations like VM allocation, Data centre allocation, verifying the client access credentials and also ensuring the SLA (service level information).This set of components are Explicitly Specify the security and access related privacy information. Whatever the services cloud service provider is offering, but still the data leakage (data security) and user authenticity is completely eradicated. In order to process the client level applications, software, programs, Files sharing in a secured platform, we need to analyse the most secured platform to the cloud user location. It will emphasise the various operations that will execute all type of cloud service provider tasks and also specifying the user based query segments and constraint set validations.

II. METHODS AND MATERIAL

A. Literature Survey Analysis

The various statistical reports are analysed in the cloud platform and specifying the result implications in the various service based access platforms. Paper entitled as, “Towards achieving data security with the cloud computing Adoption Framework” this paper has mainly concentrated on the data security feature and also

emphasizing the process based on the development of cloud computing adaptability framework level. This paper is not concentrated on the secure resource distribution process [1]. Another approach is, "The SDN and DDoS attacks in cloud computing environments" this mechanism has worked on the cloud and distributed environment. This approach is not for analysing the security based credentials policy [2]. The paper is, "An authorized identify authentication-based data access control scheme in cloud" This factor can specifies the identical parameters of authentication based access control and this approach could not be an effective mechanism for secure resource distribution process [3].
So an above approach is not met with the user requirements and also not proving the solution for secured resource/ service distribution process. So, for getting the desired result set of well secured access method for resource sharing process, we need to find out the suitable solution.

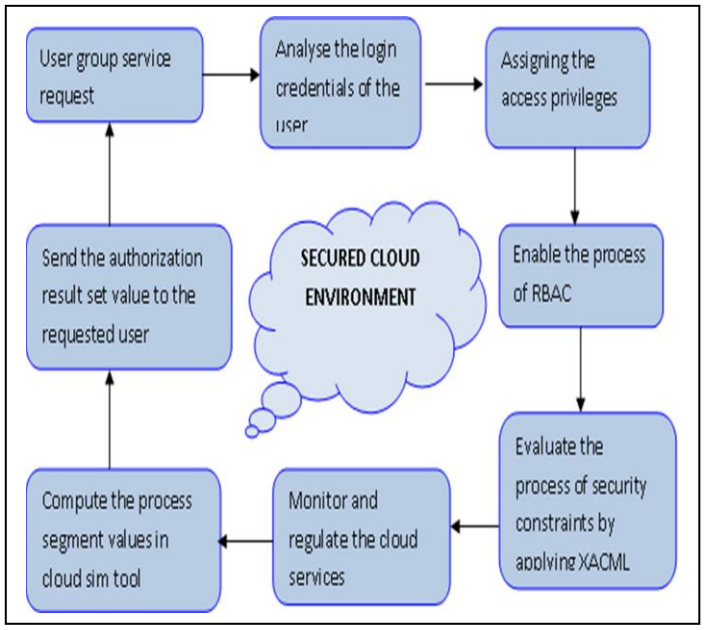

Figure : 1.a) Illustration of Proposed work

B. Proposed Work

The various types of services can be requested from the cloud service provider based on the request, cloud vendor needs to verify the service availability and also finding in which data centre location service is available. It will get a service from the desired cloud provider and offer the service to the requested user. The following parameters are used in this approach:

- Service Type requested
- Service based authorization ID value
- Specification of user access credentials
- Implementing the user level service access
- Finding the components of service offering
- Get the desired key value for authorisation process
- Analyse the security parameter available.

The huge amount of data will e processed in the cloud environment and also the result based implication values are optimistic in the cloud environment. It will suggest the various authorization and authentication based access techniques for the corresponding cloud user. The information and the result sets are maintained in the cloud database to secure the process of resource sharing among the cloud users. The following diagram will illustrate the process of proposed and the implementation process in cloud environment.

The proposed mechanism will specify the different set of constraints in order to secure the client level service. During the time of service sharing or exchanging process, at those instant users are suffering with the service reliability and resource security feature because of the hacker's entry.

The distinct set of access privileges can be allocated to the user in order to ensure the service login unique credential values. The optimal result set value can be obtained in the different environment access and also ensuring the service provision, optimizing the user accountability and other factors to improve the risk free service access zone.

C. Significance of Authorization Management Approach

The various set of authorization policies to be formed in the cloud service access environment and also perhaps the functionality of user service optimal solution set, then we need to specify the access control and the service level based information can be specifically notified and send the computed resultant value to the desired users. It increases the service utility rate and also emphasise the various set of user level service information and it is need to illustrate the various functionality feature in the dependent user locations.

4A's of Cloud Identity

There will be a different set of service consideration can be used in the cloud service environment it also uses the various factor like four parameters of users identity inputs.

1. Authentication
2. Authorization
3. Account Management
4. Audit logging

As per the user applications and the devices which can enable the scalable enterprises and maintaining the security and visibility and service control. Authorization management approach is used to determining the access rights of the cloud user and also it will explicitly specifies what user allowed to do and what does not do.. This will be like an application and infers the various approaches of how to securely perform the user level transactions and how to improve the client secure entity and identical components. Authorization can be determined based on the following factors.

- User identity value
- Additional information about
- Service based attributes values
- Type of service request
- Location of service imitation
- Access privileges
- User login credentials
- User service access details

So, all above components are used and processed in the cloud service access environment.

D. Implementation Work

In the proposed work, people need to work on the desired application and improve the service reliability component in order to use the service usage frequently without any interruption. It also facilitates the operation of how to improve the security factor for the cloud resources. The access policy management has been created the set of rules or rule list for finding the user location what type of virtual device they are using, how they are incorporating the virtual devices and servers including the external data source to determine whether user is allowed to access a service or not. It is a vital work to ensure the automated service provisioning has been enabled in the concern user location and how the applications are specified as a domain centric one or a service centric one. Generally, for authorization management and other tasks which are relevant to prove the authorization privileges we may use the SCIM protocol for increasing the service reliability nature.

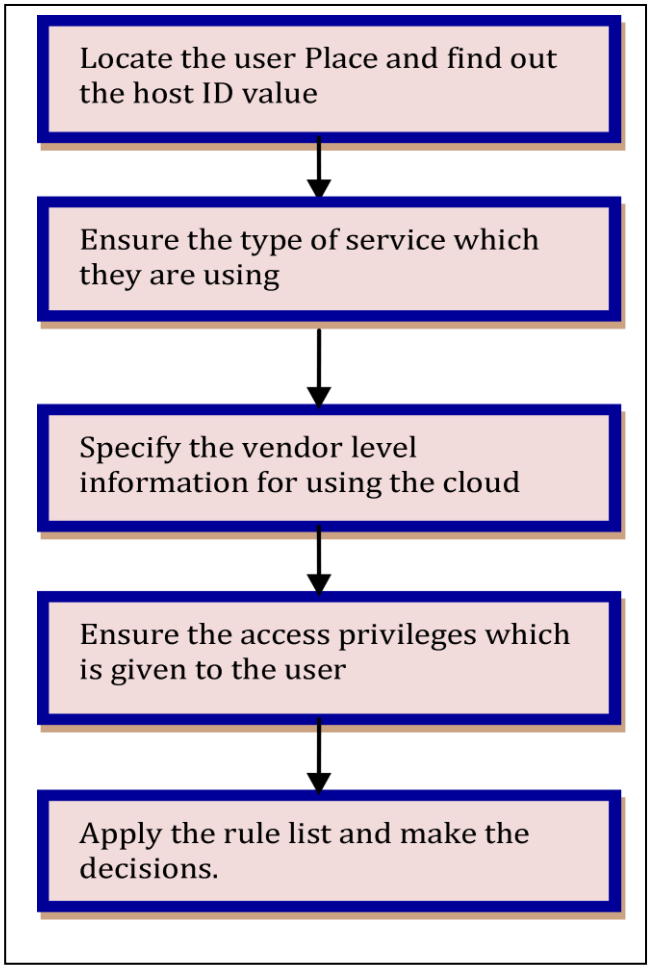

Figure 1.b) Depicting the proposed work in flow chart

An above flow chart will represents the proposed work that is carried out in the paper. A distinct set of security related parameters are used with the different boundary ranges. It also specify that, how to take a decision for allowing the registered and secured user to perform the task in the cloud environment**.** To determine the user location and from where the service request can be passed and find out the proper security controls and kind of cloud set-up is to be established among the cloud service provider and the cloud user. To specifically mention, for getting and securely verifying the cloud services we need to map our identical value with the NAT (Network Address Table). We need to analyse the

proper security controls for the cloud services. It also needs to optimize the following components:

1. Authorize requests
2. Identifying the user application
3. About authorization protocols
4. Acquiring and using an API key
5. Generating a token for the cloud service access

Above stated components are used in the cloud security access environment and it is need to specify the security related information among the cloud user.

E. Simulation Work

In cloud service access platforms, analysing the services and resources information is a major part of service distributing environment. It will explicitly specify, how the application, programs can be modified in order to satisfy the user needs. In the proposed work, we have considered authorization application in the form of user-centric OAuth flow protocol. It will functions on the Google cloud storage authentication and authorization access policy. The following key parameters are used in the proposed work to specify the security access platform.

- Storage authentication policy
  1. Authorization rule set
  2. Applying OAuth 2.0 protocol
  3. Discover the token ID
  4. Application API key

Need to specify the OAuth access endpoints between the clients and the cloud vendor. It will specifies that, how to determine the security policies and making the decision towards the user satisfaction and securing their resources.

Types of Data set Used:

Type	Services	Access location
Generic user	SAAS	Data centre 3
Abnormal user	IAAS	Data centre 11
Ideal user	CAAS	Data centre 7
Normal user	PAAS	Data centre 9

The distinct components can be specified as an authorization key controller which facilitates all the operational sequences that can be executed in the cloud user location.

III. RESULTS AND DISCUSSION

After the service processing in the cloud environment, we need to specifically mention the work flow that has been carried out in the proposed work. The work implications have been shown as a resultant value that has been given below:

Table – I Result set outcome

The following information and value can be obtained during the process of simulation work and these results are notified in the tabular values**.**

Service Request	Process segment	Authorization management values (%10)
192.168.30.2431	SEG - 12	8.023
192.168.03.62	SEG - 35	6.021
178.20.43.921	SEG - 17	9.032
163.73.03.15	SEG - 68	9.972
192.154.302	SEG - 19	9.875
194.160.10.251	SEG - 87	9.732

The various services based information are derived in the service regions and also need to specify the implication in the rule policy of an authorization management technique.

Table – II Result set outcome

Service level	RBAC / Authorization Process ID	Cloud sim 2.0 result (%100)
Generic service	192.168.10.34	89.03
Interrupted service	167.24.04.26	94.34

Normal service	178.37.02.94	98.18
Explicit boundary service	174.34.03.62	94.17

Experimental Results

In cloud computing environment all the service based access policies can be specified as a RBAC and it will regulate the user services to specifically use the cloud optimal resources. In an authorization management access privileges can be formed. The following flowchart will specify the obtained target value.

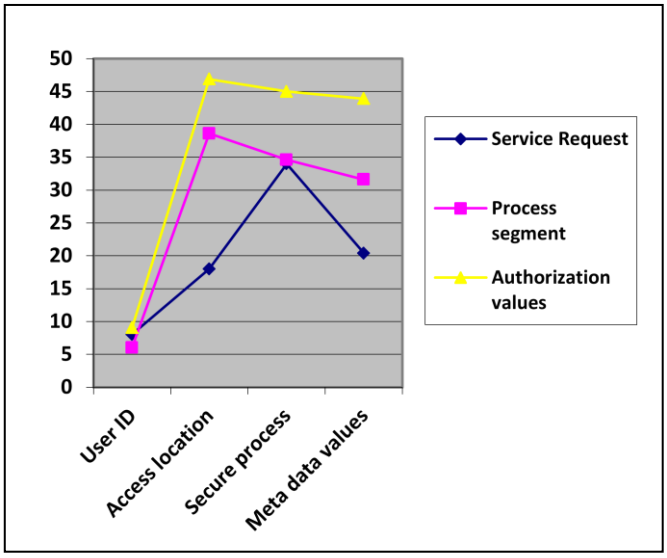

Figure 1. C) Illustration of resultant graph

The graph will show the ideal implementation of authorization management in the cloud service access platform to secure the user level resource transaction.

IV. CONCLUSION

In cloud computing environment, the web users are consuming enormous amount of services. We need to analyze what type of security setup has been configured for each and every user application. From this proposed work, the authorization management has specifically processed on the user and service level key parameters in order to make the suitable decision and also providing the key solution for the secure resource sharing process. This approach could be an effective mechanism for all clients based service transactions.

V. FUTURE ENHANCEMENT

In upcoming cases, users need to protect their secret data or confidential information from the hackers. It is the mandatory part of sustaining the cloud services and the application programs in a secured manner. The same approach of, authorization management can be applied to the data analytics platform and other security domains.

VI. REFERENCES

[1] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: State-of-the art and research challenges," Internet Services Appl., vol. 1, no. 1, pp. 7–18, 2010.

[2] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," Future Generat. Comput. Syst., vol. 25, no. 6, pp. 599–616, Jun. 2009.

[3] J. Baliga, R. W. A. Ayre, K. Hinton, and R. S. Tucker, "Green cloud computing: Balancing energy in processing, storage, and transport," Proc. IEEE, vol. 99, no. 1, pp. 149–167, Jan. 2011.Fourth Quarter 2012.

[4] K. M. Sim, "Agent-based cloud computing," IEEE Trans. Services Comput., vol. 5, no. 4, pp. 564–577, Fourth quarter.

[5] Mohammed Rashid Chowdhury, Mohammad Raihan, et.al, "Implementation and performance analysis of various VM placement strategies in cloud sim", Springer – Journal of cloud computing 2015.

[6] Samanthula, B.K; Elmehdwi.Y; Wei Jiang, "K-Nearest Neighbour classification over Semantically secure encrypted relational data, IEEE transactions on Knowledge and data engineering 2015.

[7] Barsoum, A.F; Hasan M.A., "Provable Multi copy Dynamic Data possession in cloud computing systems, IEEE transactions on Information Forensics and security 2015

[8] Jian Liu; Kun Huang; Hong Rong; Huimei Wang; Ming Xian, "Privacy-Preserving Public Auditing for Regenerating code-based Cloud service", IEEE Transactions on system security 2015.

[9] Zhenyu Wu; Zhang Xu; Haining Wang, "Whispers in the Hyper-space: High-Bandwidth and Reliable covert channel Attacks inside the cloud, ACM transactions on Networking 2015.

[10] Barsoum, A.F. ; Dept. of Comput. Sci., St. Mary's Univ. at Texas, San Antonio, TX, USA; Hasan, M.A., "Provable Multi copy Dynamic Data Possession in Cloud Computing Systems" IEEE Transactions on Information Forensics and Security, Volume: 10, Issue: 3 Year–2015.

[11] Samanthula, B.K. ; Dept. of Comput. Sci., Purdue Univ., West Lafayette, IN, USA Elmehdwi, Y. ; Wei Jiang, "K-Nearest Neighbor Classification over Semantically Secure Encrypted Relational Data" IEEE Transactions on Knowledge and Data Engineering, (Volume:27 , Issue: 5) year-2015.

[12] Tekeoglu, Ali; Tosun, Ali Saman, "Investigating Security and Privacy of a Cloud-Based Wireless IP Camera: NetCam", 24th International Conference on Computer Communication and Networks (ICCCN), 2015.

[13] Salvi, S. ; Dept. of Inf. Sci. & Eng., Nitte Meenakshi Inst. of Technol., Bangalore, India Sanjay, H.A. ; Deepika, K.M. ; Rangavittala, S.R."An encryption, compression and key(ECK) management based data security framework for infrastructure as a service in Cloud" IEEE International Conference on Advance Computing (IACC), 2015