Volume 4, Issue 2, February-2017, pp. 20-24 ISSN (O): 2349-7084

International Journal of Computer Engineering In Research Trends

Available online at: www.ijcert.org

An Enforcement of Guaranteed Client Level Defensive Mechanism in Public Cloud Services

Prof. R. Poorvadevi[1], S.Keerthana[2], V.S. Ghethalaxmipriya[3], K. Venkatasailokesh[4]

Assistant Professor[1], Department of computer science and engineering, SCSVMV University, Kanchipuram, India

Email ID: poorvadevi@gmail.com

UG Student[2], Department of computer science and engineering, SCSVMV University, Kanchipuram, India

Email ID: umail2keerthana@gmail.com

UG Student[3], Department of computer science and engineering, SCSVMV University, Kanchipuram, India

Email ID: ghethasrinivasan96@gmail.com

UG Student[4], Department of computer science and engineering, SCSVMV University, Kanchipuram, India

Email ID: venkatasailokesh@gmail.com

Abstract:-In the current era of cloud computing, the distinct enterprise information technology (IT) and business decision makers analyze the security implications of cloud computing to their business for the benefit of improving the business agility. Cloud has been playing a major role in the various multidisciplinary domains. Recent survey stated that 70% research issues are focusing on cloud security domain. Although, cloud is providing the huge amount of services to the users, still the client end level security problem is not completely eradicated. So, there is a major focus on improving and finding the solution for cloud security to know the various potential risks in the customer end. Several large cloud vendors have signaled practical implementations of the security mechanism, primarily to protect the cloud infrastructure from insider threats and advanced persistent threats. So, the proposed model brings the solution for giving the guaranteed type of cloud services in an attack free manner to the web clients. This could be achieved through the technique of client level guaranteed security system defensive approach. This mechanism will majorly operates on how to protect the user authentication procedures, security,policies, security layered approach from the client level transactions. The proposed work will be simulated on the cloud sim tool, through which end-users will obtain the better security solution in the public cloud environment.

Keywords: Cloud vendor, public cloud security, cloud service provider, cloud customer, defensive model, cloud sim, data centre, and virtual machine

---

1. Introduction

Nowadays, in the computing world all the tasks, user level service transactions are computed as a web based operations. So, it is mandatory to achieve the instant level of security operation for improving the user requirements and it's also important to satisfy the user in the service level usage. The Cloud will provide all types of resources as a form of cloud service. It will offer the services based on the mechanism of rapid provisioning or service provisioning model.

As cloud phenomenon, it will acts like an on-demand computing model, the various set of web services can be easily offered through the available public networks instantly. Cloud security also focusing the security mechanism of virtually partitioned data it will prompts the user level data segmentation on the storage component of cloud databases.

Based on the mechanism of metered service model users can pay only for the service consumption they need not to pay for owning the cloud service. The distinguished service group has been collaborated in the various entities level of cloud security application.

2. Related Work

As author Nelson Gonzalez et.al, stated that, "Quantitative analysis of current security concerns and solutions for cloud computing" this model majorly concentrated on knowing the various security ,vulnerable in a cloud computing environment and also how to improve the security solutions at the maximum end. [1]

As per an author Roland Schwarzkopf et.al, statement," Increasing virtual machine security in cloud environment" which will have the main focus on improving the success rate for attack free environment for cloud user. Whatever the applications hosted on the public network it process on the virtual machine layer with the help of VMM controller. Hackers are trying to hijack the entire VM instead of stealing the individual user contents. [2]

Author Paul Watson stated that, "multi-level security model for partitioning workflows over federated clouds" there need to be considering the aspect of multilevel security method for improving the cloud service access over the public cloud network. The various level of user application, documents is partitioned as different segments then; it will process identity federated cloud management. [3]

From this survey reports it will determine the level of security solution through the general approaches of cloud security platform. It is not concentrated on the fully guaranteed (or) fully secured platform development for end-users.

3. Proposed Work

The proposed system mainly focuses on providing security in the public infrastructure of cloud environment. An advanced security system makes the security solution more and more accurate use of cloud service provider security system. Data loss is also another major cloud security concern in the cloud client focal point.

Security for the data can be attained by the means of powerful security tools and authentication techniques. The process of accessing information contains the multiple levels of authentication and authorization verification operation will be initiated.

The following system architecture will depicts the functional units of the client level guaranteed security system by using the suitable security tools, algorithms and techniques. These parameters are used to increase the more security rate in the public cloud service access which is illustrated in figure 3.1.

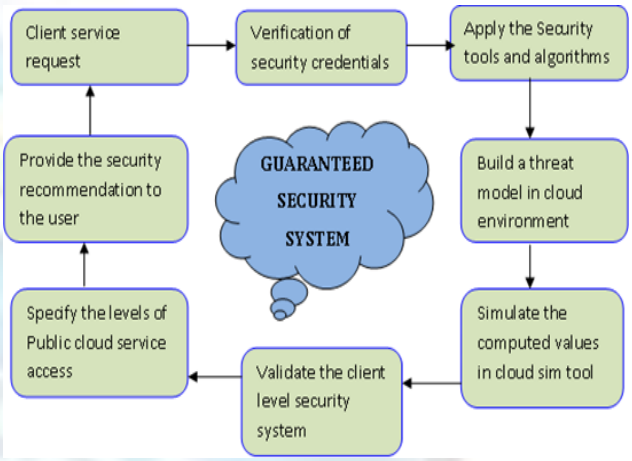


Fig: 3.1 proposed system architecture

To provide the guaranteed security system, it is important to analyze the scope of identity and access management (IAM). It will emphasize the various security factors which is listed below:

- OpenAuth
- Open API
- Information cards
- Open ID

So, with the help of strong security tools it can eliminate and reduce the possible occurrences of intruder's entry.

4. Implementation Work

In order to protect the cloud user from the various vulnerable, it is very important aspect of creating and developing the effective security system which relies on the customer end potential risks. There will be different types of security risks in the cloud computing which is given below:

- Technical risk
- Business risk
- Service usage risk
- Service damage risk

 DOI:10.22362/ijcert/2017/v4/i2/xxxx

By considering the various security parameters, it is noted that the piece every single application has been posted on the cloud server location and it is needed to take the certain security based considerations for easy use of client level access. The threat model will also emphasize the scope of this new approach, by knowing the user behavior, service usage scenario's, security policies, authentication mechanism.

4.1 Build a threat model

The major approach has been focused on the development of cloud security credentials by the form of designing some standard security layer or security system. In this proposed work it will majorly concentrates on improving and giving the guaranteed security system through the developing a threat model.

Threat model will performs of the following functionalities:

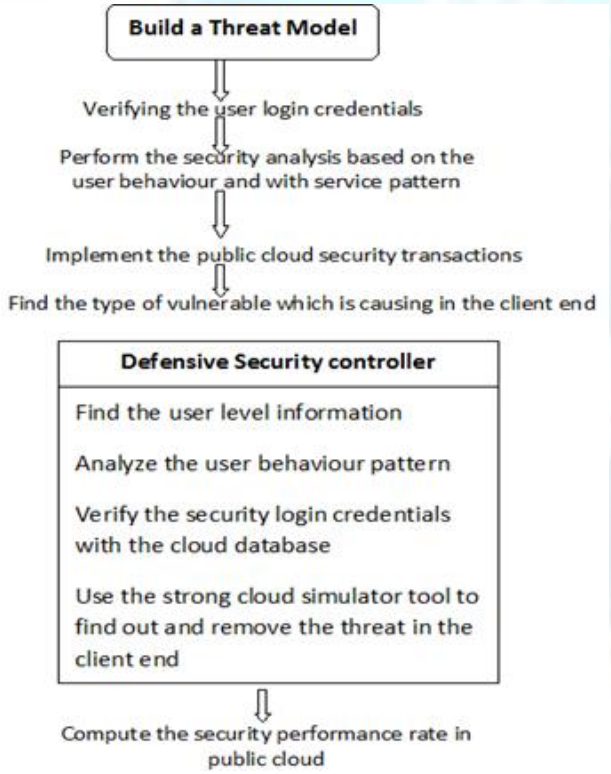


Fig: 4.1.a) Illustrating the Development of threat model

From an above figure 4.1.a it shows that the various level security assertions can be taken to improve the security system for any user application. It also considering the additional secondary level attributes of security parameters to enhance the security system effectively.

The following formula has been used to compute the values of user level service protection mechanism which is given below:

Defensive Security system = User service pattern+ user behavior analysis value + Security credentials best matching value / 100

4.2 Operational Procedures

In a cloud environment, for each and every application its need to be identifies the security based potential risks. It can allow the users to set the various kinds of security and access privileges to create the strong security protocol.

The additional set of parameters is given below:

- User service level Access history
- IAM segmented values
- Security assertion factors
- Type of service request
- Guarantee for avoiding data loss
- Ensure the quality of system protection
- Access type

It also defines the usage scenarios of particular process to be iterated and implemented on the cloud service access platform. After the development of security system users can make use of the cloud service in an attack free surface. It will consider the other aspects of improving and strengthening the additional components to ensure the security level requirements.

5. Simulation Work and Results Discussion

In the above techniques, it was mentioned and proved that the security mechanism has been obtained in the various domains particularly it will focus on the security environment of public cloud network. It is a kind of proving the security process in effective way that has to be processed in the client location.

Various implications and results are following the standard mechanism by the improving the level of

 DOI:10.22362/ijcert/2017/v4/i2/xxxx

security in VM and also preventing the operational values of and controlling component of hypervisor. This guaranteed level security system will explicitly operates on the user application. After the simulation process in cloud sim cloud vendor has obtained the following results which is tabulated in table 5.1

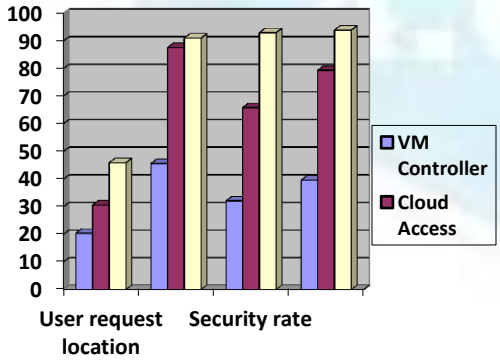
Table: 5.1 Result set

User request location	Service type	Security rate (%10)	Performance efficiency (% 100)
192.168.10.26	SAAS	8.043	67%
194.156.95.40	IAAS	9.84	92%
194.153.10.75	CAAS	9.01	78.3%
187.093.85.98	SECAAS	9.89	97.1%
190.13.98.43	PAAS	8.81	9.84%

The result set values are specified and showed in the public cloud user access to improve the solution for cloud security operation.

6. Experimental Results

Cloud user transactions are safeguarded and protected with the proposed approach of defensive model. The various components are incorporated and executed on the cloud access platform. The result set value shows that, SECAAS (security-as-a-service) has been strengthened in the cloud vendor location. The following graphical outcomes will depict the security performance during the service execution time.



So, from the result graph it shows that security rate has been increased for the user application. This mechanism will also help to avoid the problem of data loss.

7. Conclusion

From the experimental analysis, the work has been proved that there is an enforcement kind of security mechanism exists in the proposed model. This proposed work is contributed the major role in the public cloud service access. Hence, cloud user can use the cloud services in an attack-free manner.

8. Future Enhancement

Security factor is playing as a major strategy for decision making process. Service providers can apply this kind security mechanism in the other domains of data analytics, IOT, Social mining. This might be helpful to the service broker and service provider to ensure the QOS.

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

3) Velciu, M.-A. ; Comput. Sci. Dept, Mil. Tech. Acad., Bucharest, Romania; Patrascu, A. ; Patriciu, V.-V, "Bio-cryptographic authentication in cloud storage sharing", Applied Computational Intelligence and Informatics (SACI), 2014 IEEE 9th International Symposium on – 2014.

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

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

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

 DOI:10.22362/ijcert/2017/v4/i2/xxxx

7) Hussain, M. ; Dept. of Interdiscipl. Studies, Zayed Univ. Dubai, "Effective Third Party Auditing in Cloud Computing", Advanced Information Networking and Applications Workshops (WAINA), 28th International Conference on 13-16 May 2014.

8) Vikas Saxena, et al "Implementation of a secure genome sequence search platform on public cloud-leveraging open source solutions", Journal of Cloud Computing: Advances, Systems and Applications 2014.

 DOI:10.22362/ijcert/2017/v4/i2/xxxx