Resolving Cloud Vulnerability From Hijacking Using Illegal Security Access And Secure Conformity

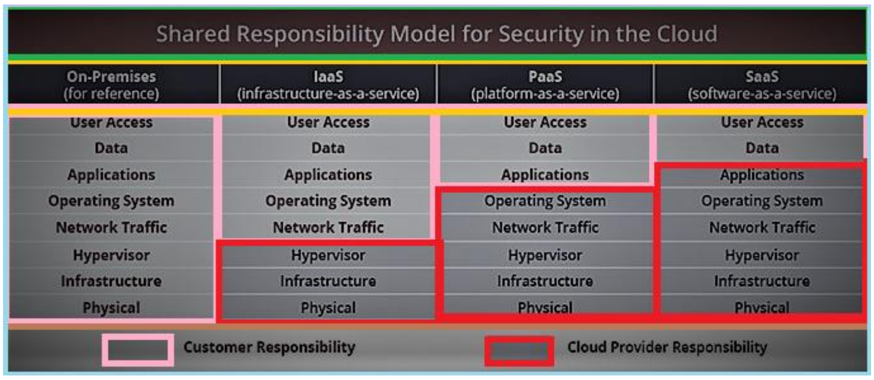
S.Shobana[1], P. Jeyamedona [2], D.Shankar [3], N. Keerthana [4], S.Radha Rammohan [5]
[1] *Assistant Professor, Department of Information Technology*
[2] *Assistant Professor, Department of Computer Science and Engineering,*
[3] *Assistant Professor, Department of Information Technology*
[4] *Research scholar, Department of Computer Applications,*
[5] *Professor, Department of Computer Applications,*
[1, 2, 3, 4, 5] *Dr.M.G.R. Educational and Research Institute University, Chennai, India*

Abstract

Cloud computing is a technology used nowadays in larger scale which uses accumulating and access of large amount of data in a single external cloud. The main use of cloud is that it will reduce the cost and maintenance of the resources and infrastructure. This technology gives the applications resilience, protection and redundancy and hence has been used by various organizations. The major concern in cloud computing is that since it involves an external person the security of the cloud is a major problem. Lots of security attacks are happening in the cloud which makes the applications more vulnerable. The proposed system deals with some of the security challenges the cloud is facing and also the solutions to overcome this. The following are some of the security issues, Hijacking and illegal access control, Risk inside organization, cloud Vulnerabilities in app and system and Secure conformity. Various solutions to overcome these issues are discussed below.

1. Introduction

Cloud computing is a technology which offers technological resources in the internet in an apparent and simple process. Most of the telecommunication companies use cloud for deploying their applications. The main use of cloud is that the infrastructure cost is very less and also the flexibility is increased and the user is required to pay only for the required resources. This also helps the user to increase their subscriber's thereby increasing scalability. There are three service models in cloud namely SaaS, PaaS and Iaas [1-4]. Software as a service SaaS is a process in which the application will be in the cloud location, Platform as a service PaaS is a process in which the application will be deployed in the cloud provider infrastructure and Infrastructure as a Service Iaas is a service wherein the user will be able to access the resources through virtual environment.



Shared Responsibility Model for Security in the Cloud

On-Premises (for reference)	IaaS (infrastructure-as-a-service)	PaaS (platform-as-a-service)	SaaS (software-as-a-service)
User Access	User Access	User Access	User Access
Data	Data	Data	Data
Applications	Applications	Applications	Applications
Operating System	Operating System	Operating System	Operating System
Network Traffic	Network Traffic	Network Traffic	Network Traffic
Hypervisor	Hypervisor	Hypervisor	Hypervisor
Infrastructure	Infrastructure	Infrastructure	Infrastructure
Physical	Physical	Physical	Physical

Customer Responsibility
Cloud Provider Responsibility

Figure 1 sharing responsibility between providers and customers

There are also three deployment models in the cloud namely public cloud, private cloud and hybrid cloud [5-7]. In public cloud the resources will be owned by the organization which will be used by all the public. The private cloud is a cloud in which the resources will be both used and owned by the organization. Hybrid cloud is a combination of both public and private cloud.

One of the main concern for cloud computing is the security [8]. This is due to the reason that the resources of the organizations are deployed in a third party system rather than the complete control of the organization. So one of the main challenges is that giving access to growing number of the customers as well as providing them the necessary securities [9]. This leads to a lot of security vulnerabilities [10] like Cross Site Scripting ,SQL Injection ,LDAP Injection ,Cross Site Request Forgery ,Insecure Cryptographic Storage .

Generally cloud security is considered as a shared responsibility both by the service provider as well as by the customer. The figure 1 indicates model which denotes the process of sharing between customers and providers. There are two responsibility namely customer responsibility and cloud provider responsibility. Some processes as indicated in the figure is the sole responsibility of customer and the rest of the processes are the responsibility of the providers. Most of the security threats are associated with cloud data only[12-21]

2. Literature Review

P. Mell and T. Grance propose cloud computing as a paradigm in which various deployment processes and comparisons of various clouds are provided. It also explains about the types of three service models namely SaaS, PaaS and IaaS. K. Ren, C. Wang, and Q. Wang investigate the importance of various security issues, their solutions to provide a reliable environment and framework and also explain about the future investigation in this issue [10]. R. B. Uriarte and C. B. Westphall propose architecture for monitoring private cloud as well as analyze the requirements of autonomous frameworks. The frame work is combined as a self isolation framework for private clouds. It also explains about the fundamentals of system and its process on decision making [11].

F. Shaikh and S. Haider aims at identifying the vulnerabilities and security issues off cloud computing which helps the cloud provider and the customer to identify the areas of security and to overcome those issues by analyzing various tools and security models. It explains about the cloud security metrics which is a numerical process to security in terms of meaning and performance. Some of the security measures followed in employment payroll and possibility plans. These process are auto generated and examined using various security tools.

3. Proposed Methodology

3.1 Hijacking and illegal access control

Hijacking of accounts in cloud computing is one of the simpler threats which occur by accessing the account of valid user by unauthorized person. This is done thefting the password of the user, phishing, and also by illegal control of access by the hacker. This may assume simpler threat but the result is that the secure data of user will be hacked. The solution to this problem is that the password has to be made complex like using difficult passwords such that the hacker will be unable to find it. The Figure 2 indicates various process of hijacking and illegal access control.

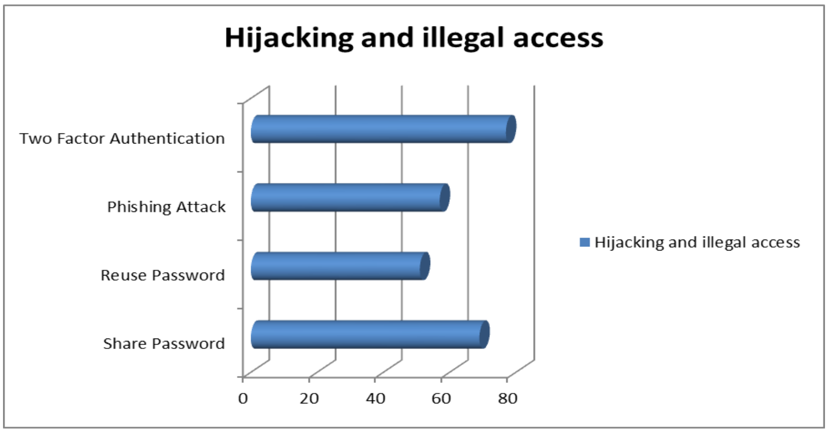


Figure 2 Hijacking and Illegal access

This may sound simpler but most of the hacking occurs in the users who have very much simpler passwords and also those who have not authenticated even after one phishing attack. So by following a complex password illegal access of application will be reduced too much extent.

3.2 Risk inside organization

One of the most important risk to find in cloud computing is that the theft which occur inside the organization itself. This is done by an authorized user who will access the secure information of the organization through valid access. This is very difficult to find since the user will be the member of the organization. This type of security threat will take longer time to detect since the person will be an authorized user. But to prevent these log details of applications has to be checked periodically. This is done by using cloud based logging tools which will help in minimizing the attack.

3.3 Cloud Vulnerabilities in app and system

One of the major vulnerabilities in cloud environment is that the attack caused in applications and systems. There are lots of security vulnerabilities like Cross Site Scripting, SQL Injection ,LDAP Injection ,Cross Site Request Forgery ,Insecure Cryptographic Storage as indicated in the Figure 3 . Sometimes attack may cause in the application due to the code present inside. These kinds of codes are not detected by security firewalls and port screening systems. To overcome this each and every new code has to be tested before they are implemented in the cloud.

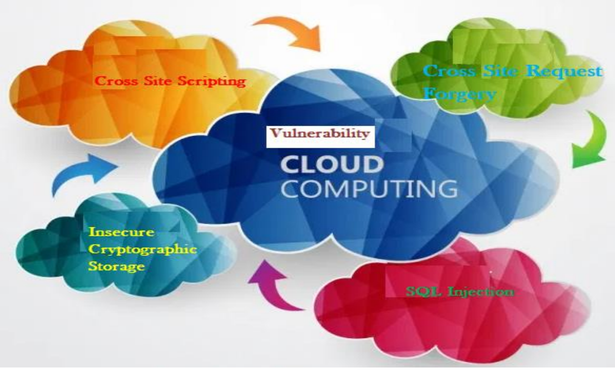


Figure 3. Vulnerability attacks

Also these kinds of attacks occur in the operating system of the cloud environment. It is this is achieved by using software vulnerability services and scanning software which will reduce the code attack

3.4 Secure conformity

One of the major challenge in cloud computing is securing conformity. Security conformity is an integrated and automatic solution which is used to secure the details in the data level itself. All the organizations have to comply the security process provided by the industry management. This will help in mitigating the risk of threat to a greater extent. One of the main solutions to this is to implement an identity and access manager which will help in authentication of user, checking of policies and systems in compliance with the management and validation of access.

4. Result analysis

The proposed system gives solutions to overcome some of the major security threats in cloud computing like Hijacking and illegal access control, Risk inside organization, cloud Vulnerabilities in app and system and Secure conformity. This can be done by adopting various security measures like using a complex and strong password, using cloud logging tools to check the attack which occur from inside the organization, using software vulnerability services and scanning software to identify the attack of code inside the cloud and also by using identity and access management tools to authenticate the access policies and users.

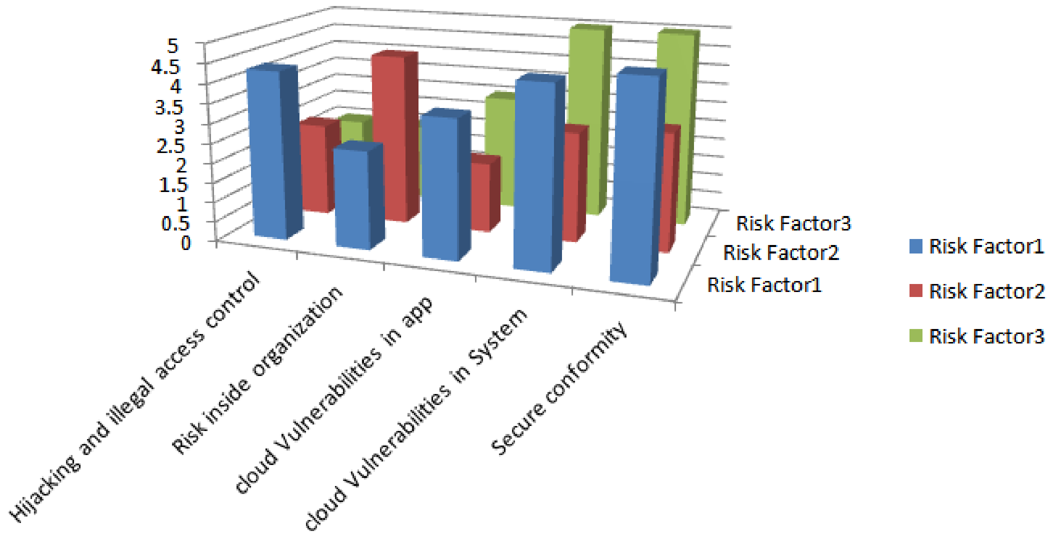


Figure 4 Performance analysis

The Figure 4 indicates the overall performance analysis of cloud computing security issues. The result thus obtained has showed greater performance and reduces the attack on cloud thereby reducing cloud security issues.

5. Conclusion

This paper gives solution to some of the security issues occurring in cloud computing. This deals how security threats like Hijacking and illegal access control, Risk inside organization, cloud Vulnerabilities in app and system and Secure conformity affects the cloud. The solutions to overcome this includes usage of complex passwords to reduce illegal access control as well as by using logging tools for clouds to identify the inside attack from the organization. Some of the solutions include usage of vulnerability software and also by using identity and access manager to rectify the code attack and also to overcome the breach in access policies and systems.

References

1. D. Sam et.al, Progressed iot based remote health monitoring system, International Journal of Control and Automation, Vol. 13, No. 2s, (2020), pp. 268-273.
2. L. Natrayan et al., Effect of graphene reinforcement on mechanical and microstructure behavior of AA8030/graphene composites fabricated by stir casting technique, AIP Conference Proceedings, 2166, (2019), pp. 020012.
3. V.R. Niveditha et.al, Detect and classify zero day Malware efficiently in big data platform, International Journal of Advanced Science and Technology, Vol. 29, No. 4s, (2020), pp. 1947-1954.
4. Natrayan, L., and M. Senthil Kumar. Optimization of squeeze casting process parameters on AA2024/Al2O3/SiC/Gr hybrid composite using taguchi and Jaya algorithm, International Journal of Control and Automation, Vol.13, No.2s, (2020), pp.95-104.
5. V. R. Niveditha and Ananthan TV, Detection of Malware attacks in smart phones using Machine Learning, International Journal of Innovative Technology and Exploring Engineering, 9(1), 2019, 4396-4400.
6. L Natrayan, MS Santhosh, R Mohanraj, R Hariharan, Mechanical and Tribological Behaviour of Al_2O_3 &SiC Reinforced Aluminium Composites Fabricated via Powder Metallurgy, IOP Conference Series: Materials Science and Engineering 561 (1), (2019), 012038.
7. Nirmala Sugirtha Rajini et.al, Reliability of Cloud Services Provided To Non-Banking Financial Institutions, International Journal of Control and Automation, Vol. 13, No. 2s, (2020), pp. 165-172165.
8. Natrayan, L and M. Senthil Kumar. Influence of silicon carbide on tribological behaviour of AA2024/Al2O3/SiC/Gr hybrid metal matrix squeeze cast composite using Taguchi technique." Mater. Res. Express, 6, (2019), pp.1265f9.
9. V. R. Niveditha and Ananthan TV, “Improving Acknowledgement in Android Application”, Journal of Computational and Theoretical Nano science. 16, (2019), pp. 2104–2107
10. K. Amandeep Singh and T. V. Ananthan, Research Challenges on Big Internet of Things Data Analytics, Journal of Computational and Theoretical Nano science, Vol. 16, (2019), 2113–2116,
11. Natrayan, L., and M. Senthil Kumar. "A potential review on influence of process parameter and effect of reinforcement on mechanical and tribological behaviour of HMMC using squeeze casting method". Journal of Critical Reviews, Vol 7, Issue 2, (2020), pp.1-5.
12. S. Velliangiri, P. Karthikeyan & V. Vinoth Kumar (2020) Detection of distributed denial of service attack in cloud computing using the optimization-based deep networks, Journal of Experimental & Theoretical Artificial Intelligence, DOI: 10.1080/0952813X.2020.1744196
13. Praveen Sundar, P.V., Ranjith, D., Vinoth Kumar, V. et al. Low power area efficient adaptive FIR filter for hearing aids using distributed arithmetic architecture. Int J Speech Technol (2020). https://doi.org/10.1007/s10772-020-09686-y,
14. Vinoth Kumar V, Karthikeyan T, Praveen Sundar P V, Magesh G, Balajee J.M. (2020). A Quantum Approach in LiFi Security using Quantum Key Distribution. International Journal of Advanced Science and Technology, 29(6s), 2345-2354.
15. Umamaheswaran, S., Lakshmanan, R., Vinothkumar, V. et al. New and robust composite micro structure descriptor (CMSD) for CBIR. International Journal of Speech Technology (2019), doi:10.1007/s10772-019-09663-0
16. Karthikeyan, T., Sekaran, K., Ranjith, D., Vinoth kumar, V., Balajee, J.M. (2019) “Personalized Content Extraction and Text Classification Using Effective Web Scraping Techniques”, International Journal of Web Portals (IJWP), 11(2), pp.41-52
17. Vinoth Kumar, V., Arvind, K.S., Umamaheswaran, S., Suganya, K.S (2019), “Hierarchal Trust Certificate Distribution using Distributed CA in MANET”, International Journal of Innovative Technology and Exploring Engineering, 8(10), pp. 2521-2524
18. Maithili, K , Vinothkumar, V, Latha, P (2018). “Analyzing the security mechanisms to prevent unauthorized access in cloud and network security” Journal of Computational and Theoretical Nanoscience, Vol.15, pp.2059-2063.

19. Dhilip Kumar V, Vinoth Kumar V, Kandar D (2018), “Data Transmission Between Dedicated Short-Range Communication and WiMAX for Efficient Vehicular Communication” Journal of Computational and Theoretical Nanoscience, Vol.15, No.8, pp.2649-2654

20. Kouser, R.R., Manikandan, T., Kumar, V.V (2018), “Heart disease prediction system using artificial neural network, radial basis function and case based reasoning” Journal of Computational and Theoretical Nanoscience, 15, pp. 2810-2817

21. Shalini A, Jayasuruthi L, Vinoth Kumar V, “Voice Recognition Robot Control using Android Device” Journal of Computational and Theoretical Nanoscience, 15(6-7), pp. 2197-2201