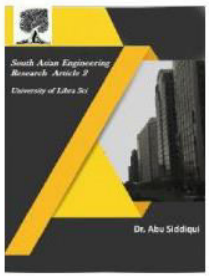
2581-4575

International Journal For Recent Developments in Science & Technology

Crossref

A Peer Reviewed Research Journal



ANALYSIS OF SECURITY FOR CLOUD COMPUTING

DR. T. PREM CHANDER

Associate Professor, ISL Engineering College, Hyderabad, India

Email: tudiprem@gmail.com

Abstract: cloud computing is cost reasonable for services. Various risks are present because of outsources data leading to security and privacy. Security issues are discussed here, identifying the systems and important threats in cloud computing and its environment as well as to identify the threats.

Index Terms: **cloud computing, security threats.**

I. INTRODUCTION

The important of cloud computing is more and growing in industries and communities. Cloud computing as the first among important technologies and with successive years by companies.

Cloud computing provides convenient, on-demand access to a scattered configuration computing resources. Some sources released with less effort and provide data change.

Cloud computing computes computational parameters to provide secure and convenient data collaboration to adapt development potential for cost reduction through optimized computing.

Cloud computing combines a number of computing and technologies such as SOA and other technologies with reliance on the internet providing business applications online to satisfy the computing needs of customers.

Security concerns relates to risk areas such as data storage, dependency and sources on public to lack control. Cloud computing is different in an IT environment. However, cloud service operational model employed to enable cloud services.

Moving data to cloud environment is of great concern for moving data centers under their control. It ensures customers to have the same security controls over applications and their service agreements prove more legal.

We give detailed security issues for cloud computing and solutions.

e journal is published in colour. Colours used for headings, subheadings and other captions must be strictly as per the template given in colour.

II. SECURITY ISSUES

With Saas, the security lies with the cloud services. High degree of abstraction is based on high degree of integrated functionality with less customer control. Largely lower degree of hidden data, Iaaas provides greater cutomer control over security than Paas or SaaS.

Saas Issues:

It provides application services on demand such as email, business applications as ERP,CRM and SCM. Less control over security among the three fundamental models in the clouds.

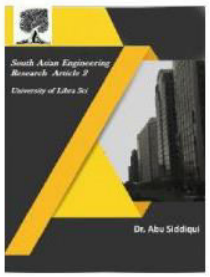
Application security issues:

Saas applications are not different from any web applications technology protect it from attacks, so new approaches are necessary. The open web security has identified the critical web applications security threats.

Saas applications grouped in models that determined as :

1. Scalability
2. Configurability
3. Multi-tenacy

In scalability the security is very bad. In configurabilitythe vendors provide various ways of applications for each one.

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal


In multitenacy a single instance serves to all customers.

Data security is a concern for technology users havind rely on proper security. In SaaS the provider is responsible for security concerns. The subcontract with third party service providers.

Accessing applications on web browsers makes access for devices on net even computers and wireless devices. The cloud security state of mobile computing is at top threat for information stealing insecure data places.

PaaS with usage of applications without maintaining and using hardware. Paas provides software layers responsible for securing the platform for software to run.

Third party relation during web security is related to data and network security. The inherit data and network security change with single integrated unit.

Application developers face the complexity of secure applications that may be hosted in the cloud. Data may be stored in different areas with different rules to solve security and privacy issues.

IaaS has a pool of resources as server, storage and networks in the form of virtual systems and accessed through internet.

The Various virtualization users may copy, create and roll back data for various applications. Machine security is important in infrastructure and security challenges as virtual. Virtual machines physical and virtual identity and security issues.VMM is responsible for virtual machine isolation, low-level software that controls and monitors its virtual machines. So need security flaws for easier monitoring facilities. Shared resources and communicate bypassing the rules defined by the security modules monitored by shared devices. Public VM is prepackaged template with configurations and images are fundamental for the overall security of the cloud. Some confidential information such as passwords keys can be recorded while image is created. VM rollback re-enable the re-expose the previously disabled accounts or passwords. The roll-back make a copy of the VM and propagates the errors in the configurations.

Network components are shared by different customers due to resource pooling. The most secure way is to book each virtual machine by using physical channels.

II. ANALYSIS OF SECURITY ISSUES WITH CUSTOMER RELATED

Security issues are analyze with existing threats as follows:

1. Vulnerabilities
2. Negative impact due to security underlying platforms

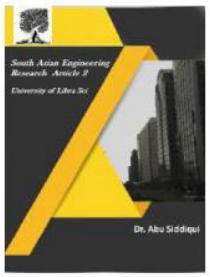
Cloud computing has many technologies such as web services, web browsers and virtualization which contributes to the evaluation of cloud even significantly.

Data storage plays a major role in virtualization and critical attack to them can be most harm. The environment of cloud service models are exposed to threats and emphasis the associated. VMM Protected systems is present and active, threat is another cloud type of virus can create a VM image and publish it in providers repository.

Cloud security is a non-profitable organization that promotes the cloud environments in secure way usage. The control, access management is managed by duties and identities access reporting.

The three basic operations in cloud data are transferred stored and encrypted. The process

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal



order may change in applications and response time and power of consumptions.

The following are the security solutions in every layer of data exchange:

1. Hyper control integrity between data flow from each cloud during transactions.
2. Customer data manipulation measure at very level of access.
3. Trusted cloud computing platforms.
4. VM migration strategies defined at each level of access and creation.
5. Trusted data centres.

IV. CONCLUSIONS

Cloud computing is a relatively new concept that presents a benefits for users. The usage of cloud has various issuesof data security. In this paper we have listed various security issues in the cloud management. Next we will discuss the security solutions and its models.

REFERENCES

[1] P. Mell, T. Grance, The NIST Definition of Cloud Computing, NIST Special Publication 800-145, 2011

[2] M. Hogan, F. Liu, A. Sokol, J. Tong, NIST Cloud Computing Standards Roadmap, NIST Cloud Computing Standards Roadmap – Version 1.0, Special Publication 500-291, 2011.

[3] L. Wu, S. K. Garg, R. Buyya, SLA-Based Admission Control for A Software-as-a-Service Provider in Cloud Computing Environments, Journal of Computer and System Sciences 78, 1280-1299, 2012

[4] K. Buck, D. Hanf, D. Harper, Cloud SLA Considerations for the Government Consumer, 2015 The MITRE Corporation.

[5] W. Chenkang, Z. Yonghua, P. Shunhong, The SLA Evaluation Model for Cloud Computing, Intl Conf. on Computer, Networks and Communication Engineering (ICCNCE 2013).

[6] F. Faniyi, R. Bahsoon, G. Theodoropoulos, A Dynamic Data-Driven Simulation Approach for Preventing Service Level Agreement Violations in Cloud Federation", Intl Conf. on Computational Science, ICCS 2012

[7] P. Patel, A. Ranabahu, A. Sheth, Service Level Agreement in Cloud Computing, https://www.researchgate.net/publication/228343067. 2009

[8] R. El-Awadi, A Framework for Negotiating Service Level Agreement of Cloud-based Services, Intl Conf. on Communication, Management and Information Technology (ICCMIT 2015)

[9] N. Ranaldo, E. Zimeo, Capacity –Driven Utility Model for Service Level Agreement Negotiation of Cloud Services, Future Generation Computer Systems 55 (2016) 186–199

[10] M. Cochran, P. Witman, Governance and Service Level Agreement Issues in A Cloud Computing Environment, Journal of Info. Technology Management Volume XXII, Number 2, 2011.

[11] J. Huang, R. Kauffman, D. Ma, Pricing strategy for cloud computing: A damaged services perspective", Decision Support Systems 78 (2015) 80–92

[12] Z. Mahmood (ed.), Cloud Computing, Computer Communications and Networks, DOI 10.1007/978-3-319-10530-7_3 Springer International Publishing Switzerland 2014.

[13] Ajayi, O., Oladeji, F., Uwadia, C., Multi-Class Load Balancing Scheme for QoS and Energy Conservation in Cloud Computing, West African Journal of Industrial and Academic Research, 17(1), pp. 28-36. 2016

[14] F. Jrad, J. Tao, A. Streit, SLA Based Service Brokering in Inter cloud Environments, 2nd International Conference on Cloud Computing and Services Science, 2012.

[15] Mahmood, Z. (Ed.). Cloud Computing: Challenges, Limitations and R&D Solutions. Springer. 2014.

[16] L. Badger, T. Grance, R. Patt-Corner, J. Voas, Draft cloud computing synopsis and recommendations. NIST special publication, 800, 146, 2011.

[17] Baig R., Khan W., Haq I. and Khan I. Agent-based SLA negotiation protocol for cloud computing. Intl. Conf. of Cloud Computing Research and Innovation, CloudAsia2017, p.5.

[18] Amazon Web Services Inc., Products and Services, 2015. Available online at http://aws.amazon.com/products/?nc2=h_ql_sf_keynote/

Zikos M., Microsoft Azure Load Balancing Services, 2014, Available Online at http://azure.microsoft.com/blog/2014/04/08/microsoft-azure-load-balancing-services/