International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 6 | ISSN : 2456-3307

Threats of Cloud Computing Techniques

Sivakumar Nadarajan*, P. Shanmugasundaram
Department of Computer Science, J.J.College of Arts and Science, Bharathidasan University, Tiruchirappalli, Tamil Nadu, India

ABSTRACT

The term cloud computing is that the foremost well likable keyword in IT-industry currently. Cloud computing is model that uses combine thought of "software-as-a-service" and "utility computing", offer convenient and on-demand services to requested end users. Security in Cloud computing may be a crucial and important aspect, and has various issues and problem associated with it. though cloud computing provides cost-efficient storage services, it is a third party service so, a client cannot trust the cloud service provider to store its data firmly among the cloud. Hence, many organizations and users may not be willing to use the cloud services to store their data within the cloud until sure security guarantees are created. This paper discus regarding cloud computing applications and so the Threats for Cloud Service Users additionally because the Threats for Cloud Service suppliers.

Keywords : Cloud Computing, SAAS, Utility Computing

I. INTRODUCTION

Cloud computing is nothing but a computing that depends on sharing computing resources instead of having native servers or personal devices to handle applications. In cloud computing, the word cloud is used as a metaphor for "the net," therefore the phrase cloud computing means that "a kind of Internet-based computing," wherever different services — like servers, storage and applications —are delivered to an organization's computers and devices through the web. Cloud Computing is depends on net & it's storage for files, applications, and infrastructure. today company buys the area or takes for rent for his or her activity.

II. HOW CLOUD COMPUTING WILL SAVE YOUR MONEY

A. You no longer have to pay for to do things like install & update computer code package, install and manage email servers and/or file servers, run backups – the sweetness of cloud computing is that each one of the business of maintaining the service or application is that the responsibility of the cloud businessperson, not yours.

B. You no longer have to purchase computer code package. Besides the convenience of not having to buy for software package programs and install them on your own servers/computers, using cloud applications instead may be cheaper.

C. You'll be ready to consolidate your separate application needs into one multi-application cloud computing service. as an example, Google Apps for Business includes email, a calendar programming application, Google Docs for creating documents, displays and forms and using on-line file storage and Google Sites for creating websites, Even Microsoft's ancient workplace application suite, that used to be solely accessible in desktop versions costing several dollars, is presently accessible during a cloud-based version referred to as office 365. it's sold by annual subscription and additionally includes on-line video conferencing, Skype and instant electronic communication property, and much of different choices. dearer plans embody the desktop applications. other cloud computing vendors like Infostreet give a set of cloud applications likewise as CRM, calendar programing, email, conference business, file sharing Associate in Nursingd an worker directory for as little as $10 per person per month.

D. you'll be ready to reduce on system hardware. File storage, data backup and software package programs all

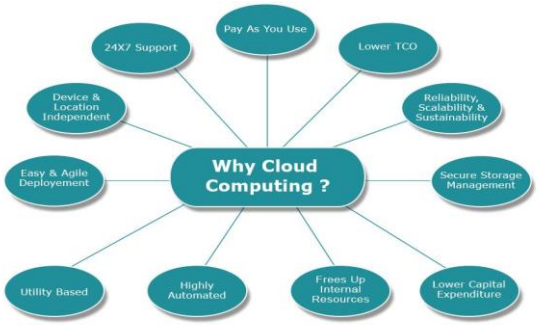
take up lots of house on servers/computers. With cloud computing, you use someone else's servers to store all this data instead, liberating up your in-house laptop instrumentation for various functions or even rental you get obviate a number of it.

E. A cloud computing application might produce integration easier. as a results of many cloud computing applications embody an Application Programming Interface (API) you'll be ready to notice "compatible" applications rather than having to pay to have the applications you want to be integrated customized for you.

F. Cloud computing applications are oftentimes updated, thus you do not need to pay time Associate in Nursingd money doing it – and providing you with the advantage of continuously having access to an application's latest choices and functions.
Other Cloud Computing advantages

G. Cloud computing permits you and your workers easy accessibility to applications and data from totally different computers&devices. therefore cloud applications are based on browser they are accessible from mobile devices like tablets and smartphones.
Note that accessing workplace applications via a browser on a mobile device is also a however ideal user experience, thus (for example) Microsoft offers mobile versions of workplace applications, like workplace for iPad.

H. Cloud computing permits you to line out or grow your very little business quickly. it's plenty easier and faster to check in for a cloud computing application than to buy for a server, latch on up and running and install software system package on it. and since you do not ought to purchase hardware and software system package, your set out or enlargement is cheaper, too.



III. THREATS FOR CLOUD SERVICE USERS

A. Answerability Ambiguity

Cloud service customers consume delivered resources through service models. The customer-built IT system thus depends on the services. the shortage of a transparent definition of responsibility among cloud service users and suppliers may evoke conceptual conflicts. Moreover, any written agreement inconsistency of provided services would possibly induce anomaly, or incidents. however the matter of that entity is that the data controller that on is that the information processor stays open at a world scale (even if the international side is reduced to a stripped third party outside of the actual region like EU).

B. Loss of Control

In associate enterprise, migrating a section of its own IT system to a cloud infrastructure implies to partially offer management to the cloud service suppliers. The loss of governance basedon the cloud service models. for instance, IaaS solely delegates hardware&network management to the provider, whereas SaaS additionally delegates OS, application, and service integration thus on provide a turnkey service to the cloud service user.

C. Loss of Hope

It is sometime tough for a cloud service user to acknowledge his provider's trust level due to the black-box feature of the cloud service. there is no measure the way to get and share the provider's security level in formalized manner. moreover, the cloud service users have no abilities to judge security implementation level achieved by the provider. Such a lack of sharing security level ocular of cloud service provider will become a significant security threat in use of cloud services for cloud service users.

D. Service Provider Lock-In

A consequence of the loss of governance can be a lack of freedom relating to the way to replace a cloud provider by another. this can be the case if a cloud provider depends on non-standard hypervisors or virtual machine image format and does not provide tools to convert virtual machines to a regular format.

E. Secure Less Cloud Service User Access

As most of the resource deliveries are through remote connection, non -protected apis, (mostly management apis and PaaS services is one of the simplest attack vector). Attack methods like phishing, fraud, and exploitation of computer code package vulnerabilities still achieve results. Credentials and passwords are generally reused, that amplifies the impact of such attacks. Cloud results add a brand new threat to the landscape. If fraudster gains access to your credentials, they will snoop on your activities and transactions, manipulate information, return falsified data, and direct your shoppers to illegitimate sites. Your account or service instances may become a innovative base for the assailant. From here, they will leverage the ability of your name to launch ulterior attacks.

F. Lack of Knowledge/Asset Management

When applying to use Cloud Computing Services, the cloud service user will have serious considerations on lack of information/asset management by cloud service suppliers like location of sensitive asset/information, lack of physical management for information storage, dependableness of information backup, countermeasures for BCP and Disaster Recovery then on. moreover, the cloud service users even have important considerations on exposure of knowledge to foreign government and on compliance with privacy law like EU knowledge protection directive.

G. Information Loss And Leak

The loss of secret writing key or privileged access code will bring serious problems to the cloud service users. consequently, lack of cryptologic management data like encryption-keys, authentication-codes & amp;access privilege will heavily lead sensitive damages on data loss and fast escape to outside. for an example, insufficient authentication, authorization, and audit (AAA) controls; inconsistent use of secret writing and/or authentication keys; operational failures; disposal problems; jurisdiction and political issues; information center reliability; and disaster recovery are usually recognized as major behaviors throughout this threat class.

IV. THREATS FOR CLOUD SERVICE SUPPLIERS

A. Responsibility Ambiguity

Different user roles, like cloud service provider, cloud service user, client IT admin, data owner, is additionally outlined and used in a cloud system . Ambiguity of such user roles and responsibilities definition associated with data ownership, access management, infrastructure maintenance, etc, could induce business or legal dissention (Especially once addressing third parties. The cloud service provider is so mehow a cloud service user).

B. Protection Inconsistency

Due to the decentralized style of a cloud infrastructure, its protection mechanisms are attainable to be inconsistency among distributed security modules. as an example, an access denied by one IAM module is additionally granted by another. This threat is additionally profited by a attainable offender that compromises every the confidentiality and integrity.

C. Evolutional Risks

One abstract improvement of cloud computing is to delay some decisions from the design section to the execution section. This means, some dependent software parts of a system is additionally designated and enforced once the system executes. However, normal risk assessment methodology won't match such an evolution. A system that's assessed as secure throughout the look section may exploit vulnerabilities throughout its execution due to the new enforced code elements.

D. Business Discontinuity

The “as a service” feature of cloud computing allocates resources and delivers them as a service. the entire cloud infrastructure together with its business workflows thus depends on an outsized set of services, ranging from hardware to application. However, the separation of service delivery, like black out or delay, may bring out a severe impact associated with the provision.

E. Providers Lock-In

The service provider is created by some software code and hardware parts by suppliers. few supplier dependent modules are implemented for integration/practicality extension. However, due to the dearth of traditional apis, the portability to migrate to a different supplier is not obvious. The consequence of provider locked in may be an absence of freedom regarding the way to replace a supplier.

F. License Risks

Software licenses are sometimes supported the number of installations/the nos. of users. Since created virtual machines are going to be used only some times, the provider might have to be compelled to acquire from extra licenses than very required at a given time. the dearth of a "clouded" license management theme that allows to pay only for used licenses might cause code use conflicts.

G. Bylaw Conflict

Depending on the instruction of hosting country, info is also protected by fully different applicable jurisdiction. as an example, the USA subject Act might authorize such seizures. EU protects cloud service user's personal info, that mustn't be processed in countries that do not provide a decent level of protection guarantees. a world cloud service provider might commit bylaws of its native datacenters that might be a legal threat to be taken under consideration.

H. Unhealthy Integration

Migrating to the cloud implies moving big amounts of knowledge and major configuration changes (e.g., network addressing). Migration of a vicinity of AN IT infrastructure to AN external cloud service provider desires profound changes inside the infrastructure style (e.g. network and security policies). a foul integration caused by incompatible interfaces or inconsistent policy group action might evoke every helpful and non - helpful impacts.

I. Unsecure Administration API

The administration middleware standing between the cloud infrastructure and additionally the cloud service user is additionally undecided with deficient attention dedicated to sanitation of cloud service user inputs and authentication. Non-protected Apis, mainly administration Apis becomes a target of different for attackers. this could be not specific to cloud atmosphere. However, the service-oriented approach makes apis a basic building-block for a cloud-infrastructure. Their protection can become a main concern of the cloudsecurity.

J. Shared Atmosphere

Cloud resources ar virtualized, completely different cloud service users (possibly competitors) share constant infrastructure. One key concern is said to design compartmentalization, resource isolation, and information segregation. Any unauthorized and violent access to cloud service user's sensitive information could compromise each the integrity and confidentiality.

K. Hypervisor Isolation Failure

The hypervisor technology is taken into account because the basis of cloudinfrastructure and Multiple virtualmachines cohosted on one physical server share each hardware&memory resources are virtualized by hypervisor. This threat covers failure of mechanisms analytic attack" can well be launched on a hypervisor to achieve extralegal-access to alternative virtual machines' memory.

L. Service Inaccessibility

Availability isn't specific to cloud atmosphere. However, attributable to the service - minded style principle, service delivery is also wedged whereas the cloud infrastructure in not offered. Moreover, the dynamic dependency of cloud computing offers way more potentialities for an offender. A typical Denial of Service attack on one service could clog the complete cloud system.

M. Information Unreliableness

Data protection includes access to information for the confidentiality additionally as its integrity. Cloud service users have considerations regarding however suppliers handle with their information, and whether or not their information is disclosed or illicitly altered.

even though the cloud service user trust isn't within the central of cloud security, it's a serious selling soul for a cloud service supplier to advance the migration of IT system to cloud atmosphere.

N. Abuse Right of Cloud Service Supplier

For a cloud service user, migrating a district of its own IT to a cloud infrastructure implies to partly offer management to the supplier. This becomes a heavy threat to cloud service user's information, notably concerning role and privileges assignment to suppliers. in addition to lack of transparency concerning cloud supplier practices could lead mis-configuration or malicious business executive attack. Such security breaches can lower the provider's name, leading to lower cloud service user confidence.

V. CONCLUSION

To summarize, the cloud provides have several choices for the everyday computer user as well as massive and tiny businesses. It parades the world of computing to a broader range of uses and will increase the benefit of use by giving access through any net connection. However, with this inflated ease additionally come back drawbacks. you've got less management over who has access to your data and small to no knowledge of wherever it's keep. you also should bear in mind of the safety risks of getting information keep on the cloud. The cloud may be a massive target for malicious people and will have disadvantages as a result of it may be accessed through an unsecured net association.

VI. REFERENCES

[1] S. Zhang, S. F. Zhang, X. B. Chen, and X. Z. Huo, "The Comparison between Cloud Computing and Grid Computing," 2010 International Conference on Computer Application and System Modeling (ICCASM), pp. V11-72 - V11-75, DOI= 22-24 Oct. 2010.

[2] T. Dillon, C. Wu, and E. Chang, "Cloud Computing: Issues and Challenges," 2010 24th IEEE International Conference on Advanced Information Networking and Applications(AINA), pp. 27-33, DOI= 20-23 April 2010.

[3] B. R. Kandukuri, R. V. Paturi and A. Rakshit, "Cloud Security Issues," 2009 IEEE International Conference on Services Computing, Bangalore, India, September 21-25, 2009. In Proceedings of IEEE SCC'2009. pp. 517-520, 2009. ISBN: 978-0-7695-3811-2.

[4] Ohlman, B., Eriksson, A., Rembarz, R. (2009) What Networking of Information Can Do for Cloud Computing. The 18th IEEE International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises, Groningen, The Netherlands, June 29 - July 1, 2009.

[5] Marios D. Dikaiakos, Dimitrios Katsaros, Pankaj Mehra, George Pallis, Athena Vakali, "Cloud Computing: Distributed Internet Computing for IT and Scientific Research," IEEE Internet Computing Journal, vol. 13, issue. 5, pp. 10-13, September 2009. DOI: 10.1109/MIC.2009.103.

[6] Hanqian Wu, Yi Ding, Winer, C., Li Yao, "Network Security for Virtual Machines in Cloud Computing," 5th Int'l Conference on Computer Sciences and Convergence Information Technology, pp. 18-21, Seoul, Nov. 30- Dec. 2, 2010. ISBN: 978-1-4244-8567-3.

[7] Bisong, A. and Rahman, S.S.M. (2011). An Overview of the Security Concerns in Enterprise Cloud Computing. International Journal of Network Security & Its Applications, 3(1), 30-45. doi:10.5121/ijnsa.2011.3103

[8] Suresh, K.S. and Prasad, K.V. (2012). Security Issues and Security Algorithms in Cloud Computing. International Journal of Advanced Research in Computer Science and Software Engineering, 2(10), 110-114.

[9] Yassin, A.A., Jin, H., Ibrahim, A., Qiang, W. and Zou, D. (2012). Efficient Password-based Two Factors Authentication in Cloud Computing. International Journal of Security and Its Applications, 6(2), 143-148.

[10] Xia Z., Zhu Y., Sun X. and Chen L. (2014), "Secure semantic expansion based search over encrypted cloud data supporting similarity ranking "Journal of Cloud Computing",Springer 3.1, pp. 1-11.

[11] Yunqi Ye, Liangliang Xiao, I-Ling Yen, Farokh Bastani, "Secure, Dependable, and High Performance Cloud Storage", 2010 29th IEEE International Symposium on Reliable.

[12] Chandrahasan, R. Kalaichelvi, S. Shanmuga Priya, and L. Arockiam. "Research Challenges and Security Issues in Cloud Computing." International Journal of Computational Intelligence and Information Security 3.3 (2012): 42-48.

[13] Chun-Ting Huang, Zhongyuan Qin, C.-C. Jay Kuo., "Multimedia Storage Security in Cloud Computing: an Overview" 978-1-457701434-4/11/$26.00,IEEE,2011.

[14] Cloud Security Alliance, "Top Threats to Cloud Computing v1.0," Prepared by the Cloud Security Alliance, March 2010, pp. 1-14.