ISSN 2394-739X

International Journal for Research in Science Engineering and Technology

SURVEY On CLOUD COMPUTING AND SERVICE MOBEL BASED SECURITY ANALYSIS IN CLOUD COMPUTING

[1] Kaviyarasu Baluswami, [2] Dr. A. V. Senthil Kumar
[1] Research Scholar, [2] Director of MCA,
[1, 2] Hindusthan College of Arts & Science,
[1, 2] Coimbatore, India.

Abstract:-

This paper displays an administration model based way to deal with cloud computing defenselessness investigation. The technique is adaptable, permitting examination of assaults from both outside and inside the network. In spite of the fact that the term Cloud Computing is broadly utilized, note that all Cloud Models are not the same. Thusly, it is basic that associations don't make a difference an expansive brush one-size fits all way to deal with security over all models. It can dissect dangers to a particular network resource, or look at the universe of conceivable results taking after a fruitful assault. Likewise the objective of this exploration point is to review procedures being proposed to manage vulnerability in security measurements.

Keywods: - Cloud Security Analysis, Security threats in cloud, Service Model

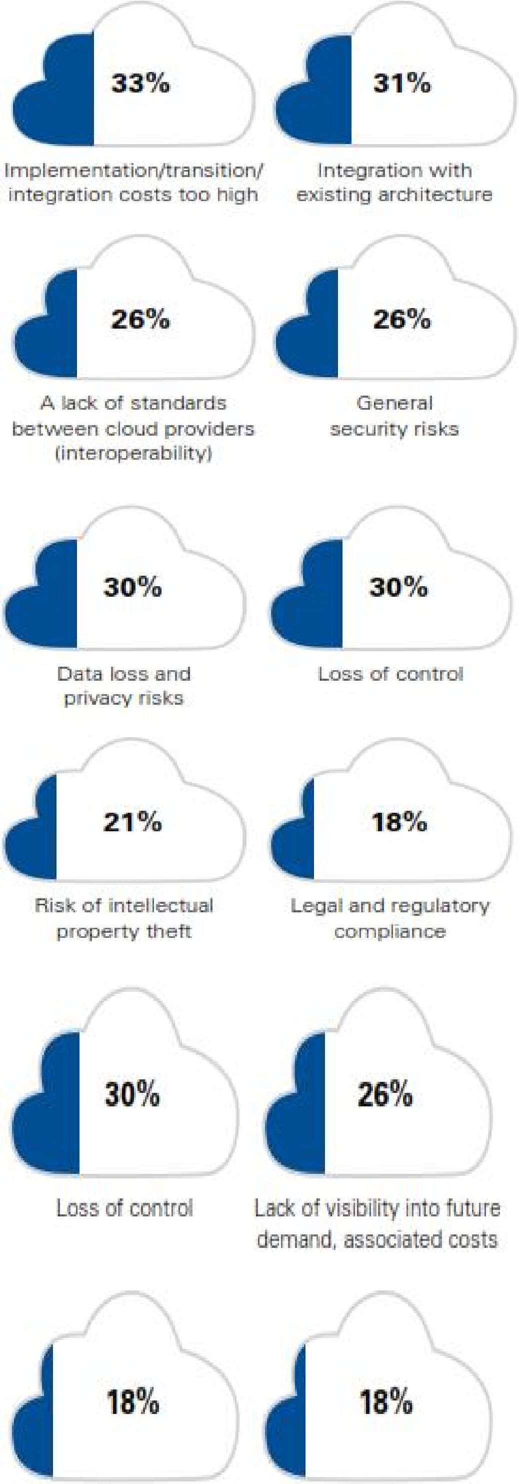
1. INTRODUCTION

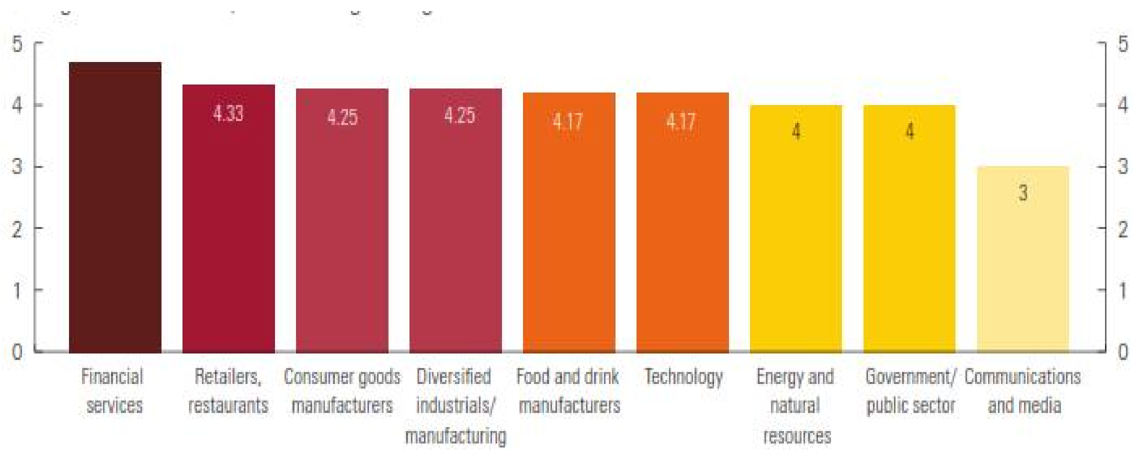
Cloud Computing is an arrangement of diverse sorts of equipment and programming that work all things considered to convey a service over a network. With cloud computing, clients can get to records and utilization applications from any gadget that can get to the Internet. Essentially cloud computing offers: 1. On-demand self-service, which turns out to be quickly accessible for their utilization naturally, without obliging human collaboration. 2. Wide network access, which can be gotten to through the greater part of the register mediums. 3. Fast flexibility - Additional limit stays accessible and open on an 'as required' premise, and is recouped back to the pool when didn't really required for option assignment. 4. Measured service - clients can be naturally charged for their utilization. On the other hand, security concerns keep numerous people and associations from utilizing clouds in spite of its expense adequacy. Determining security issues of clouds may lighten concerns and build cloud use.

2. RELATED WORKS

Users are expecting the three most important protection goals from any system particularly Cloud computing confidentiality, integrity, authenticity. **Confidentiality** - The confidentiality of a system is guaranteed providing it prevents unauthorized gathering of information. **Integrity** - A system guarantees data integrity if it is impossible for subjects to manipulate the protected data unnoticed or in an unauthorized way[1]. **Authenticity** - The authenticity of a subject or object is defined as its genuineness and credibility; these can be verified on the basis of its unique identity and characteristic features [1]. Then again, take note of that Cloud Computing is not on a very basic level frail; it simply should be overseen and got to in a protected manner. Essentially clients need to approach the System in light of the model, which they subscribed. Our overview demonstrates that a portion of the greatest difficulties confronting cloud reception identify with the usage of cloud services. 33% of all respondents said they had discovered expenses identified with usage were higher than anticipated, while 31 percent showed that the procedure of coordinating existing IT construction modeling with new cloud services was making difficulties.

A discriminating test to cloud achievement is that numerous respondents try not to appear to have the privilege aptitudes to coordinate their cloud arranges what's more, aspirations. At the point when asked how gifted their associations were at defeating these difficulties, respondents said that incorporation with existing construction modeling was one of the zones where their associations shown the slightest sum of aptitude. Keeping in mind their aptitudes in overseeing execution costs were positioned to some degree higher, they still fall behind in more mind boggling zones, for example, legitimate and administrative agreeability and assessment. It was fairly astounding, thusly, to observe that a critical larger part of respondents said that they depend essentially on in-house assets as opposed to outer suppliers or experts for their cloud usage, with higher numbers in Asia Pacific and the Europe, Middle East and Africa (EMEA) locales. Study respondents likewise noticed that they are progressively concerned about the loss of control that may originate from moving information and forms into the cloud. This concern is most distinctly felt in the Americas where there has been more prominent cloud experience and uptake to date, outlining that this concern may develop with more prominent cloudexperience and usage elsewhere.

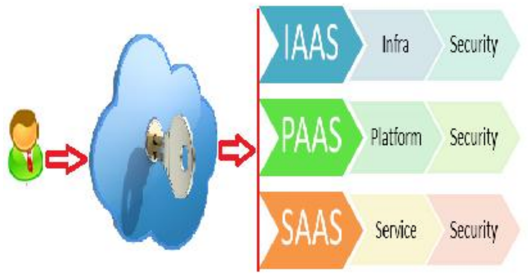




2.1 International's Global cloud survey: the implementation challenge Our survey finds that the majority of organizations around the world have already begun to adopt some form of cloud (or 'as-a-service') technology within their enterprise, and all signs indicate that this is just the beginning; respondents expect to move more business processes to the cloud in the future , gain more budget for cloud implementation and spend less time building and defending the cloud business case to their leadership. Clearly, the business is becoming more comfortable with the benefits and associated risks that cloud brings. With experience comes insight. It is not surprising, therefore, that the top cloud-related challenges facing business and IT leaders has evolved from concerns about security and performance capability to instead focus on some of the 'nuts and bolts' of cloud implementation. Tactical challenges such as higher than expected implementation costs, integration challenges and loss of control now loom large on the cloud business agenda, demonstrating that – as organizations expand their usage and gain more experience in the cloud – focus tends to turn towards implementation, operational and governance challenges.

3 SERVICE MODEL Based Approach

Cloud Models can be segmented into Software as a Service (Saas), Platform as a service (PaaS) and Integration as a Service (IaaS). When the cloud user is considering Cloud security it should consider both the differences and similarities between these three segments of Cloud Models. Also they need to know what are the exact methods available to secure their data. We prepared the Attack templates, which represent generic steps in known attacks, including conditions which must hold for the attack to be possible. Here we are listing the important security threats and solutions for each model.



3.1 IAAS:

Infrastructure As A Service' is the most basic cloud-service model.The services on the infrastructure layer are used to access essential IT resources that are combined under the heading Infrastructure-as-a-Service (IaaS). These essential IT resources include services linked to computing resources, data storage resources, and the communications channel. They enable existing applications to be provisioned on cloud resources and new services implemented on the higher layers. The security issues are a vary depends on the cloud implementation. ie., public cloud or private cloud.

3.1.1 Data protection and usage monitoring: Need to protect the data and monitorhow the data is accessing and who is using/accessing the data. Also Measuring and billing with Multiple levels of providers On-demand billing system availability. We can control the data access by implementing the Rights/Access Management services and Role based access. Also Amazon DevPayor similar billing system can be used for monitoring the usage.

3.1.2 Log and Monitoring Management: In order to keep track of where the information is, who accesses it, which machines are handing it, and which storage arrays are responsible for it, you need robust logging and reporting solutions. A large majority of data breaches are still discovered by third parties because most organizations don't have effective log monitoring Enable logs at all compute, network, memory, storage level. These logs are stored in multiple, secure locations with extremely limited access. Ensure that the principle of least privilege drives your log creation and management activities.

3.1.3 Encryption: Encryption is the most important control for security of sensitive data. Implement the following to achieve the encryption: Full Disk Encryption, Policy-based partial encryption, Database Encryption, Network Encryption, and Encrypting for backup data.

3.1.4Access Control and Identity Management: Identity and Access Controls are even more important in the Cloud as, unlike corporate networks, users may not need physical network connection to access resources in Cloud. To secure this need to implement the following: strong authentication, access control, multifactor, and integration with corporate directories.Multifactor Authentication, Integration with Corporate Directory, RBAC – Use role-based access controls, Verizon Universal Identity Services, etc.,

3.1.5 Infrastructure hardening: Physical attacks against computer hardware. Data security on retired or replaced devices We can implement the following to achieve the Physical security. High secure locked rooms with monitoring appliances, Multi-parties accessibility to encrypted storage, Transparent cryptographic file systems, Self-encrypting enterprise tape drive TS1120.

3.2 PAAS:
Platform As A Service' comprises the environment services where the user can develop and run in-house built applications. Application developers can develop and run their software solutions on a cloud platform without the cost and complexity of buying and managing the underlying hardware and software layers.The services might include an operating system, a programming language execution environment, databases and web servers etc.,

3.2.1 Information processing: Data can be available to the rest of the local network or the web. Sometimes this data is so bulky that the creation process occurs live on the remote server. This increases the document's risk of being intercepted by others who are essential third-parties to its authorship. PaaS can provide applications that reinforce the security of the document even in the process of 'open' processing on a shared server.

3.2.2 Information interactivity:
Information interactivity is the process of sharing data across the board. It goes through various Personal Computers, seeps through networks and migrates through other devices like phones.This interaction sometimes connects local networks that have confidential data with the free web

where everybody gains access to the same. This is where the issues of security come in. PaaS basically enables users to control the data through automated apps from their sources.Also Firewalls authentication and access permissions can be used to secure the interaction.

3.2.3 Data Location and Storing data: Datastorage signifies the hosting aspect of Cloud computing. This has been a prominent issue in the entire Cloud community. PaaSendorse multiple applications to encrypt data in servers, many documents do not leak. The advent of independent clouds even inside dedicated hosting platforms could help to overcome this issue

3.2.4 Vendor Lock In: PaaS does not only provide traditional programming languages, but also does it offer third-party web services components. Thus, PaaS models also inherit security issues related to corresponding web services. Also, PaaS users have to depend on both the security of web-hosted development tools and third-party services. Implement Cloud standards to reduce the dependency.

3.2.5 SDLC: In the application development, developers face the complexity of building secure applications that may be hosted in the cloud. The speed at which applications will change in the cloud will affect both the System Development Life Cycle (SDLC) and security. Follow the secure development techniques and educate the developers about data legal issues as well. Data may be stored on different places with different legal regimes that can compromise its privacy and security.

3.3 SAAS:

'Software As A Service' provides complete applications to a cloud's end user. In this model, the cloud provides the user with access to already developer applications that are running in the cloud. The access is achieved by cloud clients and the cloud users do not manage the infrastructure where the application resides, eliminating with this the way the need to install and run the application on the cloud user's own computers. It is mainly accessed through a web portal and service oriented architectures based on web service technologies.

3.3.1 Virtual Machine: Virtualization is one of the main components of a cloud. But this poses major security risks. Reconfigurable distributed virtual machine and Survey on Virtual machine Security will fix the VM security issues.

3.3.2 Network: All data flow over the network needs to be secured in order to prevent leakage of sensitive information. Implement the network traffic encryption techniques such as Secure Socket Layer (SSL) and the Transport Layer Security (TLS) for securing the data in the network.

3.3.3 Access controland Information Secrecy: Data isstored outside the enterprise boundary, at the SaaS vendor end. Consequently, the SaaS vendormust adopt additional security checks to ensure data security and prevent breaches due to securityvulnerabilities in the application or through malicious employees. Applystrongencryption techniques and appropriate authorization for controlling the data access.

3.3.4 Identity management: Identity management is an area that deals with identifying individualsin a system and controlling the access to the resources in that system by placing restrictions onthe established identities. To avoid the security issues in ID management, need to strictly follow CSA's Identity and Access Management Guidance.

3.3.5 Cloud standards: To achieve interoperability among clouds and to increase their stability and security,

cloudstandards are needed across different standard developing organizations.
Organizations and Groups are developing various guidelines to standardize the Cloud. Example: IEEE Cloud Computing Standard Study Group, ITU Cloud Computing Focus Group, Cloud Security Alliance (CSA) and ISO.

CONCLUSION

Cloud computing offers benefits for organizations and individuals. There are also privacy and security concerns. If you are considering a cloud service, you shouldthink about how your personal information, and that of your customers, can best be protected. Carefully review the terms of service or contracts, and challenge theprovider to meet your needs. Cloud Computing is a rapidly accelerating revolution within IT and will become the default method of IT delivery moving into the future – organizations would be advised to consider their approach towards beginning a move to the clouds sooner, rather than later.We expect this debate to continue and for future versions of “Top Threats to Cloud Computing” to reflect the consensus emerging fromthose debates.

REFERENCES

[1] Eckert, Claudia: IT-Sicherheit. Oldenbourg, 6.edition, 2009.
[2] P. Mell and T. Grance, “Draft nist working definition of cloud computing,” Referenced on Jan. 23rd, 2010 Online at http://csrc.nist.gov/groups/SNS/cloud-computing/index.html, 2010.
[3] Cloud Security Alliance, “Security guidance for critical areas of focus in cloud computing,” 2009, online at http://www.cloudsecurityalliance.org.
[4] C. Gentry, “Computing arbitrary functions of encrypted data,” Commun. ACM, vol. 53, no. 3, pp. 97–105, 2010.
[5] Sun Microsystems, Inc., “Building customer trust in cloud computing with transparent security,” 2009, online at https://www.sun.com/offers/ details/sun transparency.xml.
[6] M. J. Atallah, K. N. Pantazopoulos, J. R. Rice, and E. H. Spafford, “Secure outsourcing of scientific computations,” Advances in Computers, vol. 54, pp. 216–272, 2001.
[6] S. Hohenberger and A. Lysyanskaya, “How to securely outsource cryptographic computations,” in Proc. of TCC, 2005, pp. 264–282.
[7] M. J. Atallah and J. Li, “Secure outsourcing of sequence comparisons,” Int. J. Inf. Sec., vol. 4, no. 4, pp. 277–287, 2005.
[8] D. Benjamin and M. J. Atallah, “Private and cheating-free outsourcing of algebraic computations,” in Proc. of 6th Conf. on Privacy, Security, and Trust (PST), 2008, pp. 240–245.
[9] R. Gennaro, C. Gentry, and B. Parno, “Non-interactive verifiable computing: Outsourcing computation to untrusted workers,” in Proc.OfCRYPTO’10, Aug. 2010.
[10] M. Atallah and K. Frikken, “Securely outsourcing linear algebra computations,” in Proc. of ASIACCS, 2010, pp. 48–59.
[11] A. C.-C. Yao, “Protocols for secure computations (extended abstract),” in Proc. of FOCS’82, 1982, pp. 160–164.