Security Attacks and Threats, Challenges, Issues in Cloud Computing: A Critical Review

P S V S Sridhar

Department Of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur Dist, AP. psvssridhar@gmail.com

ABSTRACT-

Cloud computing is a development of parallel computing, distributed computing, grid computing and virtualization technologies which define the shape of new era. Cloud computing is an emerging model of business computing. In this paper, we explore the concept of cloud architecture and compare cloud computing with grid computing. We also address the characteristics and applications of several popular cloud computing platforms. In this paper, we aim to pinpoint the challenges and issues of cloud computing. We identified several challenges from the cloud computing adoption perspective and also highlighted the cloud interoperability issue that deserves substantial further research and development. However, security and privacy issues present a strong barrier for users to adapt into cloud computing systems. In this paper, we investigate several cloud computing system providers about their concerns on security and privacy issues.

Key words: challenges, issues, attacks, threats, cloud computing, protocols, services, architecture

Introduction:

Development of parallel computing, distributed computing, grid computing, and is the combination and evolution of Virtualization, Utility computing, Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS). Cloud is a metaphor to describe web as a space where computing has been pre-installed and exist as a service; data, operating systems, applications, storage and processing power exist on the web ready to be shared. To users, cloud computing is a Pay-per-Use-On-Demand mode that can conveniently access shared information technology resources through Internet. Where IT resources include network, server, storage, application, service and so on and they can be deployed with much quick and easy manner and least management and also interaction with service providers. Cloud computing can much improve the availability of IT resources and owns many advantages over other computing techniques. Users can use the IT infrastructure with Pay-per-Use-On-Demand mode; this would benefit and save cost to buy the physical resources that may be vacant.

Architecture of cloud services:

Cloud service models are commonly divided into **SaaS, PaaS, and IaaS** that exhibited by a given cloud infrastructure. It is helpful to add more structure to the service model stacks. Fig: 1 shows a cloud reference architecture [3] that makes the most important security-relevant cloud components explicit and provides an abstract overview of cloud computing for security issue analysis.

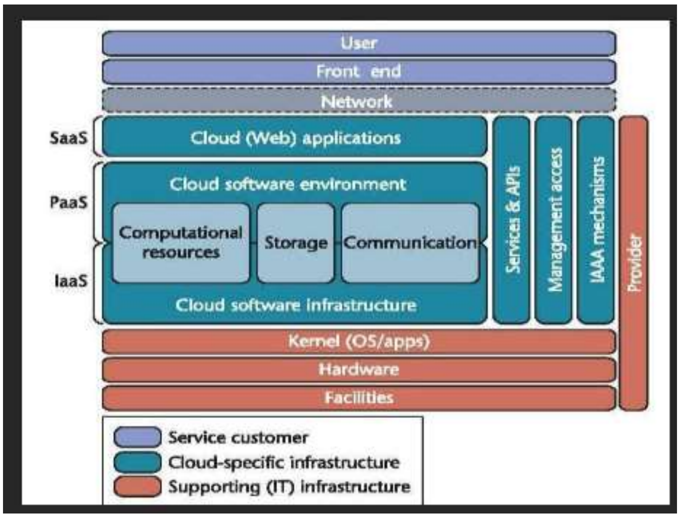

Fig: 1 Cloud reference architecture

Comparison between Cloud and Grid Computing:

A comparison can be summaries as follows:

1. Construction of grid is to complete a specified task, such as biology grid, Geography grid, national educational grid, while Cloud computing is designed to meet general application and there are not grid for a special field.
2. Grid emphasizes on “resource sharing” to form a virtual organization. Cloud is often owned by a single physical organization (except the community Cloud, in this case, it is owned by the community), who allocates resources to different running instances.
3. Grid aims to provide the maximum computing capacity for a huge task through resource sharing. Cloud aims to suffice as many small-to-medium tasks as possible based on users’ real time requirements. Therefore, multi-tenancy is a very important concept for Cloud computing.

Security Issues in the Cloud

Despite the fact that, the virtualization and Cloud Computing conveys extensive variety of dynamic resources, the security concern is most part seen as the tremendous issue in the Cloud which makes the clients to oppose themselves in embracing the innovation of Cloud Computing. A percentage of the security issues in the Cloud are talked about underneath.

Integrity: Integrity ensures that data held in a system is a legitimate representation of the data expected and that has not been altered by an approved individual. At the point when any application is running on a server, reinforcement routine is arranged with the goal that is protected in the case of a data-loss incident. Ordinarily, the data will reinforcement to any compact media all the time which will then be put away in an off-site area [14].

Availability: Availability guarantees that data handling resources are not made distracted by malicious action. It is the basic thought that when a client tries to get something, it is accessible as per their requirement. This is an essential for mission basic systems. Accessibility for these systems is an important that organizations have a Business Continuity Planning (BCP) for their frameworks [4].

Confidentiality: Confidentiality guarantees that data is not accessible to unapproved persons. Privacy hazard happens when data can be seen or read by any people who have an unapproved access on it. Loss of classification can happen physically or electronically. Physical classification misfortune happens through social engineering. Electronic secrecy misfortune happens when the customers are accessing servers aren't encoding their communications.

Security Issues and Risks in Cloud Computing:

In 2008 Gartner recognized seven security issues [5] that need to be tended before organizations switch completely to the cloud computing model.

- Data location: While storing data in cloud some clients might not know where their data is actually located.
- Regulatory compliance: Customers can choose service providers that permit to be examined by third party organizations that check levels of security provided by cloud service providers.
- Data segregation: Since the data in encrypted form from different organizations may be stored in the same place, hence a system is required that separates data from different organizations and it should be provided by the cloud service provider.
- Long-term viability: It alludes to the capability to withdraw an agreement and all information if the current supplier is bought out by another firm.
- Investigative support: In case a customer suspects defective movement from the supplier, client might not have numerous legitimate ways seek after an investigation.
- Recovery: Each supplier ought to have a disaster recovery convention to ensure client data is protected in case of a disaster.
- Privileged user access: Data transmitted from the customer through internet represents a certain level of risk, in view of issues of information.

Possession of ventures ought to invest time getting to know their suppliers and their regulations however much as could be expected before allotting some trivial applications.

The six specific areas of cloud computing where substantial security attention is required are as follows

- Security of data in transit.
- Security of data at rest.
- Cloud legal and regulatory issues.
- Robust separation between data belonging to different customers.
- Authentication of users/applications/processes.

- Incident response.

Threats in cloud computing:

Cloud computing confronts the same amount of security threats that are present and found in the current computing platforms, networks, intranet, internet in enterprises. These threats, risk vulnerabilities come in different structures.

The Cloud Security Alliance (Cloud Computing Alliance, 2010) did a research on the threats facing in cloud computing and it recognized in the following major threats.

- Failures in provider security
- Attacks by other customers
- Availability and reliability issues legal and regulatory issues
- Perimeter security model broken
- Integrating provider and customer security systems
- Abuse and nefarious use of cloud computing
- Insecure application programming interfaces
- Malicious insiders
- Shared technology vulnerabilities
- Data loss/leakage
- Account, service & traffic hijacking
- Unknown risk profile

Authentication Attacks:

Authentication is a powerless point in facilitated and virtual services and is much of the time focused on. There are a wide range of approaches to authenticate users; for instance, taking into account what a man knows, has, or is. The components used to secure the authentication process and the routines utilized are an incessant focus of attackers. Right now, with respect to the architecture of SaaS, IaaS, and PaaS, there is just IaaS offering this sort of data security and data encryption. On the off chance that the transmitted data is sorted to high private for any venture, the distributed computing administration in light of IaaS structural planning will be the most suitable answer for secure data correspondence. Likewise, an approval of data procedure or administration for those data had a place with the undertakings yet put away on the service provider's side must be approved by the client side (enterprises) to rather than the service providers. Most of the clients confronting benefits today still utilize basic username and password kind of knowledge based authentication, except for some money related establishments which have sent different types of secondary authentication (for example, site keys, virtual keyboards, shared mystery questions, and so on) to make it more troublesome for mainstream phishing attacks.

Ensuring security against the various types of Attacks:

Keeping in mind the end goal to secure cloud against different security dangers, for example, SQL injection, Cross Site Scripting (XSS), DoS and DoS assaults, Google Hacking, and Forced Hacking, diverse cloud service suppliers embrace distinctive systems. A couple of standard methods to distinguish the aforementioned attacks include: staying away from the use of powerfully created SQL in the code, finding the meta-structures utilized as a part of the code, approving all user entered parameters, and denying and evacuation of undesirable data and characters, and so on. A non-specific security system should be worked out for an upgraded cost execution proportion. The primary model to be satisfied by the non-specific security system is to interface with a cloud environment, and to have the capacity to handle and recognize predefined and in addition altered security approaches. A comparable methodology is being utilized by Symantec Message Labs Web Security cloud that obstructs the security dangers starting from web and channels the data before they achieve the network web security cloud's security architecture engineering lays on two segments.

With a specific end goal to guarantee data security and piece conceivable malwares, it comprises of multilayer security and henceforth it has a solid security platform. URL filtering is being watched that the attacks are propelled through different pages and internet sites and henceforth shifting of the website pages guarantees that no such destructive or danger conveying pages are open. Additionally, content from undesirable locations can be blocked. With its versatile innovation, it gives security even in exceptionally clashing situations and guarantees insurance against new and meeting malware threats. The security model of Amazon Web Services, one of the greatest cloud service suppliers makes utilization of multi-variable confirmation procedure, guarantee that improved control over AWS account settings, the administration of AWS and assets for which the record is subscribed. On the off chance that the client decides on Multi Factor Authentication (MFA), user needs to give a 6-digit code not withstanding their username and secret key before access is conceded to AWS account or

benefits. This single use code can be got on mobile devices each time the user tries to login into his/her AWS account. Such a system is called multi-factor authentication, since two components are checked before access is conceded.

Conclusion:

Cloud computing conveys an extensive variety of resources such as computational force, computational stages, stockpiling and applications to users via internet. The real cloud suppliers in the present business sector fragment are Amazon, Google, IBM, Microsoft, Sales force, and so forth. With an expanding number of organizations falling back on use of assets in the Cloud, there is a need for securing data of different clients. Some real difficulties that are being stood up by Cloud Computing are to secure, ensure and handle the data which is the property of the client. Beneath, we have depicted the two fundamental expresses that hold your data is out in the Cloud. When the data is in movement (travel) and when the data is very still, where the data is quite anticipated that would be more secure. The underneath showed are the two fundamental situations which we have centered to comprehend the safety of the data in the Cloud.

Cloud computing is an extension of existing techniques for computing system. As such, existing security techniques can be applied within individual components of cloud computing. In this we implement our work on .net platform on the basis of algorithm strength and authentication we conclude that our scheme gives better security. Any application relying upon an emergent science considers the various possible threats. Such an application with an inability to count on or control the threats may frequently result in failure. The classification of various security threats/problems presented on this paper would most likely improvement the cloud users to make out appropriate alternative and cloud provider vendors to manage such threats efficaciously. Authentication is required for providing enhanced security in cloud environment.

References:

[2] D.K. Mishra "Tutorial: Secure Multiparty Computation for Cloud Computing Paradigm", Second International Conference on Computational Intelligence, Modelling and Simulation, xxiv-xxv, Sept, 2010.

[3] Wood K, Pereira E. "An Investigation into Cloud Configuration and Security", 2010 International Conference for Internet Technology and Secured Transactions, 1-6, Nov, 2010.

[4] Qiasi Luoand Yunsi Fei "Algorithmic Collision Analysis for Evaluating Cryptographic System and Side-Channel Attacks", International Symposium on H/W - Oriented Security and Trust, 2011.

[5] Mohamed H. Sqalli, Fahd Al-Haidariand Khaled Salah "EDoS-Shield-A Two-Steps Mitigation Technique against EDoS Attacks in Cloud Computing", 4th IEEE International Conference on Utility and Cloud Computing, 2011.

[6] M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, "On technical security issues in cloud computing," Proceedings of the IEEE International Conference on Cloud Computing (CLOUD-II), 2009.

[7] Ayu Tiwari, SudipSanyal, Ajith Abraham, Svein Johan Knapskog, SugataSanyal, "A Multi-Factor Security Protocol for Wireless Payment – Secure Web Authentication Using Mobile Devices", IADIS, International Conference Applied Computing, pp. 160- 167, 2007.

[8] Tao Peng, Christopher Leckie, Kotagiri RamMohan Rao, "Survey of Network Based Defense Mechanisms Countering the DoS and DDoS Problems", ACM Computing Surveys, vol. 39, No. 1, April, 2007. DOI: 10.1145/1216370.1216373.

[9] Qishi Wu, Sajjan Shiva, Sankardas Roy, Charles Ellis, VivekDatla, "On Modelling and Simulation of game theory based defense mechanisms against DoS and DDoS attacks", Proceedings of 2010 Spring Simulation Multiconference, NY, USA, 0032010. DOI: 10.1145/1878537.1878703.

[10] Richard Chow, Philippe Golle, Markus Jakobsson, Elaine Shi, Jessicca Staddon, Ryusuke Masuoka, Jesus Molina, "Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control", Proceedings of the ACM Workshop on

Cloud Computing Security, pp. 85-90, USA, November, 2009. ISBN: 978-1- 60558-784-4.

[11] H. Shacham and B. Waters, “Compact Proofs of Retrievability,” Proceedings of Asia crypt 08, Dec. 2008.

[12] K. D. Bowers, A. Juels, and A. Oprea, “Proofs of Retrievability: Theory and Implementation,” Cryptology ePrint Archive, Report 2008/175, 2008, http://eprint.iacr.org/.

[13] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable Data Possession at Untrusted Stores,” Proceedigns of CCS ’07, pp. 598–609, 2007.

[14] M. Lillibridge, S. Elnikety, A. Birrell, M. Burrows, and M. Isard, “A Cooperative Internet Backup Scheme,” Proceedings of the 2003 USENIX Annual Technical Conference (General Track), pp. 29–41, 2003.

[15] Cong Wang, Qian Wang, and KuiRen, Wenjing Lou, “Ensuring Data Storage Security in Cloud Computing” IEEE, 2009.

[16] M. A. Shah, M. Baker, J. C. Mogul, and R. Swaminathan, “Auditing to Keep Online Storage Services Honest,” Proceedings of 11th USENIX Workshop on Hot Topics in Operating Systems (HOTOS ’07), pp. 1–6, 2007.

[17] Youngmin Jung, Mokdong Chung; “Adaptive Security Management Model in the Cloud Computing Environment”. The 12th International Conference on Advanced Communication Technology (ICACT), IEEE 2010.

[18] Wenjuan Li, Lingdi Ping, Xuezeng Pan;” Use Trust Management Module to Achieve Effective Security Mechanisms in Cloud Environment”.International Conference on Electronics and Information Engineering, IEEE, 2010.

[19] Mohammed A. AlZain, Ben Soh and Eric Pardede, “MCDB: Using Multi-Clouds to Ensure Security in Cloud Computing”. Ninth IEEE International Conference on Dependable, Autonomic and Secure Computing, 2011.

[20] Prashant Rewagad, YogitaPawar, “Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud

[21]

[22] Computing”. International Conference on Communication Systems and Network Technologies, IEEE, 2013.