ISSN 2349-4506
Impact Factor: 2.785

Global Journal of Engineering Science and Research Management

CLOUD COMPUTING OVERVIEW AND CHALLENGES: A REVIEW PAPER

Satish Kumar*, Vishal Thakur, Payal Thakur, Ashok Kumar Kashyap
* University Institute of Information Technology, Himachal Pradesh University, Shimla-171005

DOI: 10.5281/zenodo.343686

KEYWORDS: Cloud Security, Challenges, IaaS, PaaS, SaaS.

ABSTRACT

Cloud computing era is the most resourceful, elastic, utilized and scalable period for internet technology to use the computing resources over the internet successfully. Cloud computing did not provide only the speed, accuracy, storage capacity and efficiency for computing but it also lead to propagate the green computing and resource utilization. In this research paper, a brief description of cloud computing, cloud services and cloud security challenges is given. Also the literature review of some researchers in the field of cloud computing is discussed. It has been finally concluded in this research paper to provide remedies to the cloud threats in the cloud environment.

INTRODUCTION

Cloud computing model is introduced by National Institute of Standards and Technology (NIST) [1] as “a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.” Multi-tenancy and elasticity are two key characteristics of the cloud model. Multi-tenancy enables sharing the same service instance among different tenants. Elasticity enables scaling up and down resources allocated to a service based on the current service demands. Both characteristics focus on improving resource utilization, cost and service availability [2].

In a Cloud computing environment, internal threats have steadily increased over the past few years [3]. Internal threat refers to those threats which occur within the organisation. Internal users within an organisation generally have more knowledge of the data stored therein and hence more informed about how to access that data and applications than do external users. Although internal threats cannot be entirely eliminated, some effective barriers can be developed to mitigate them.

According to NIST [4], Deployment models refer to those models which are based upon the deployment of different computing resources. A cloud computing system may be deployed privately or hosted on the premises of a cloud customer, may be shared among a limited number of trusted partners, may be hosted by a third party, or may be a publically accessible service, i.e. a public cloud. Depending on the kind of cloud deployment, the cloud may have limited private computing resources, or may have access to large quantities of remotely accessed resources. The different deployment models have different characteristics and requirements in terms of scalability, cost, and availability of resources.

CLOUD COMPUTNIG MODELS

Cloud computing models are classified into two categories which are based upon the services being provided by a cloud service provider (CSP) and how to deploy these services. Former is known as cloud service models and latter are cloud deployment models. These both are discussed as follows:

Cloud Deployment Models

Cloud deployment models refers to those models which consider the type of cloud user organizations. These models specify the deployment technique of various cloud services over the internet. There are following type of deployment models defined by NIST [4]:

Private cloud

The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise. A private cloud is one in which the services and infrastructure are maintained on a private network. These clouds offer the greatest level of security and control, but they require the company to still purchase and maintain all the software and infrastructure, which reduces the cost savings [5].

Community cloud

The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns e.g. mission, security requirements, policy and compliance considerations. It may be managed by the organizations or a third party and may exist on premise or off premise [4]. It is a multi-tenant model which provides resources to the different clients which are shared among several organizations from a specific group with common computing concerns and objectives.

Public cloud

The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services. In apublic cloud model resources such as applications and storage, can be accessed by the general public over the Internet. Public cloud services may be free or offered on a pay-per-usage model. The main advantage of the public model will be that we have to pay only for what we need, hence no resource wastage. Also the clients need not to be worried about the set-up requirements and implementation because all of these services will be made available to them by their service providers [5].

Hybrid cloud

The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability. A hybrid cloud includes a variety of public and private options with multiple providers. By spreading things out over a hybrid cloud, users keep each aspect at their business in the most efficient environment possible. The downside is that user has to keep track of multiple different security platforms and ensure that all aspects of their business can communicate with each other [5].

Cloud Service Models

A cloud can provide access to software applications such as email or office productivity tools (the Software as a Service, or SaaS, service model), or can provide a toolkit for customers to use to build and operate their own software (the Platform as a Service, or PaaS, service model), or can provide network access to traditional computing resources such as processing power and storage (the Infrastructure as a Service, or IaaS, service model) [4]. The different service models have different strengths and are suitable for different customers and business objectives. Generally, interoperability and portability of customer workloads is more achievable in the IaaS service model because the building blocks of IaaS offerings are relatively well-defined e.g. network protocols, CPU instruction sets, legacy device interfaces. There are following type of cloud service models

Cloud Software as a Service (SaaS)

The capability provided to the consumer is to use the provider’s applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser e.g. web-based email. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings[6].

Cloud Platform as a Service (PaaS)

The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or -acquired applications created using programming languages and tools supported by the provider [7]. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations [8].

Cloud Infrastructure as a Service (IaaS)

The capability provided to the consumer is to provide processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. In IaaS most of the services are provided virtually on virtual machines (VMs) e.g. data storage, firewalls and networks etc.[9].

LITERATURE REVIEW

In this section, the views and conclusions of various researchers related to cloud computing and cloud security issues are discussed as follows:

Christodorescu et al. has taken a more sober view of virtualization as a security mechanism[10]. They described a threat model which is much more challenging than those provided by the previous authors. Specifically, they assumed that customers can run any Virtual machine (VM) on a cloud Virtual Machine manager (VMM) and that the cloud provider has no prior knowledge about the software (Operating System (OS), applications, malware, etc.) running on the guest VM. To cope with this model the authors offered a novel technique for virtual machine introspection. By examining the location of a VM's interrupt descriptor table (IDT), they can identify the version of operating system being used. Then, using a body of known secure code (white-list) for the operating system, they work outwards from the interrupt descriptor table (IDT) and validate linked code (system calls, kernel modules, etc.) against the white-list. Code that is validated becomes trusted and provides a new starting point from which to expand the search for malicious code[10].

Meiko et al. addressed the technical security issues arising from computing model such as extensible markup language (XML) attacks, browsers attacks, and flooding attacks [11]. In their paper, they initiated the discussion by contributing a concept which achieves security merits by making use of multiple distinct clouds at the same time. They also presented the results of their security analysis of Amazon and Eucalypts cloud systems and revealed several highly critical vulnerabilities in web interfaces. They concluded that interfaces are very likely to become one of the most attractive targets for organized crime in the nearby future ahead. Additionally, they also mentioned that cross site scripting attacks against web based cloud control surfaces have severe effects on the overall security of the cloud computing system. Cross site scripting refers to a type of computer insecurity vulnerability typically found in the web applications that enables attackers to inject client side script into web pages viewed by other users [12].

Aviram et al. offered a technique for potentially combating side-channel information leaks. Because central processing unit (CPU) timers provide a reference clock, it can tell a malicious virtual machine (VM) owner when their VM has been pre-empted (possibly by the target VM), thus indicating to the attacker that they should attempt to read a side-channel such as the disk-cache discussed earlier. The authors concluded that a cloud computing environment devoid of high-resolution clocks and other timing indicators which would aid in such side-channel attacks. This is done by essentially providing customers with a deterministic compute-cloud gateway. In this way, the users could only supply deterministic inputs to the gateway and all timing information is inaccessible to client VMs [13].

Kresimir et al. [14] discussed high level security cloud computing model such as data integrity, payment and privacy of sensitive information. They derived the conclusion that there are many new technologies are emerging at a rapid rate with the potential of making human's lives easier, however, one must be very careful to understand the security risks and challenges posed in utilizing these technologies. They concluded from the discussion that cloud computing has the potential to become a frontrunner in promoting a secure, virtual and economically viable IT solution in the future.

Subashini et al. [15] discussed the security challenges of the service delivery model, focusing on the SaaS and discuss critical areas of cloud computing. They deliver a set of best practices for the cloud provider, consumers and security vendors to follow in each domain. Cloud security alliance (CSA) published a detailed reports discussing for some of these domains. In their research they did a deep investigation in the cloud model to identify the root causes and key participating dimensions in such security issues/problems. It helped users in better understanding of the problem and to find solutions to them [16].

APT(Advanced persistent threat) research team found that 91% of targeted attacks involve spear-phishing emails, reinforcing the belief that spear phishing is a primary means by which APT attackers infiltrate target networks.

Spear phishing remains the most favoured vector for instigating targeted attacks because users continue to fall prey to spear-phishing emails, causing substantial damage to their respective organizations. Spear-phishing email attachments are difficult to spot from normal document attachments passed on from user to user each day in a corporate environment, increasing the likelihood of successful computer infection. The availability of organizational information on the Internet allow attackers to gain relevant data on their chosen targets, making their APT campaigns more effective. Our findings highlight how spear phishing aids APT attacks because of the vast amount of information available at the touch of our fingertips. Organizations should strive to improve their existing defenses and take into careful consideration what types of and how much information they make available online [17].

Ashwini Rao et al. emphasised that long password is a promising user authentication mechanism. However, to achieve the level of security and usability envisioned with long passwords, users have to understand the effect of structures present in them. Further, we have to make policies and enforcement tools cognizant of the effect of structures. As a first step, they developed some techniques to achieve these goals. They studied grammatical structures, but other types of structures such as postal addresses, email addresses and URLs present within long passwords may have similar impact on security. They said that more research is necessary to fully understand the effect of structures on long passwords [18].

Jyoti Chhikara et al. described briefly information about phishing, its attacks, steps that users can take to safeguard their confidential information. They also showed a survey conducted by netcraft on phishing [19]. They concluded that phishing differs from traditional scams primarily in the scale of the fraud that can be committed. In order to combat phishing, business and consumers need to adopt best practices and practice awareness, educate themselves about phishing and anti-phishing techniques, use current security protection and protocols, and report suspicious activities. By doing so, they can reduce their exposure to fraud and identity theft, safeguard their confidential information, and help fight one of today's most serious and ongoing threats of phishing. The most effective solution to phishing is training users not to blindly follow links to web sites where they have to enter sensitive information such as passwords. The final technical solution to phishing involves significant infrastructure changes in the Internet that are beyond the ability of any one institution to deploy.

J. Alex Halderman et. Al. concluded that many users (including those who should know better) fail to take adequate steps to protect their passwords. Often the cause is not a failure to understand that strong passwords are important, but rather frustration with the difficulty of doing the right thing. In our study we attempted to make strong password management more convenient. Whereas previous schemes were lacking in either transportability for mobile users or security against brute force attacks, our design achieves a balance of the two by using password strengthening techniques. Our implementation, Password Multiplier, is available on the web. We encourage novices and experts alike to try it [20].

Stephen G. Batsell et al. developed an integrated cyber security framework for identifying and containing attacks within an organizational network domain. The framework is distributed, autonomous, and capable of detecting new attacks. It integrated existing cyber security systems and provides a single picture of the entire network, which allowed real-time situational awareness of large scale network systems. It consisted of individual components for host-level anomaly detection, attack source localization, and attack containment [21].

CONCLUSION

It has been concluded that the cloud computing model is one of the promising computing models for service providers, cloud providers and cloud consumers. But to best utilize the cloud computing model thereis a need to solve the existing security problems.

Some of the security problems are inherited from the used technologies such as virtualization. Multi-tenancy and isolation is a major dimension in the cloud security problem that requires a robust solution. Physical location of data and its movement between server and client is the more prone to unauthorized access and destruction of data, so strong security mechanisms must be developed to secure data storage and its transfer among clients. Secure access mechanisms are also needed to avoid unauthorized and unauthenticated access to data. The study concluded following ten most vulnerable security issues related to the cloud computing are as follows [22]:

1. Abuse and nefarious use of cloud computing
2. Insecure interfaces and APIs (Application Programming interfaces).
3. Malicious insiders.
4. Shared technology vulnerabilities.
5. Data loss or leakage.
6. Account or service hijacking.
7. Unknown risk profile.
8. Data Breaches.
9. Denial of Service.
10. Browsers.

These all are discussed briefly as follows:

Abuse and nefarious use of cloud computing

One of cloud computing's greatest benefits is that it allows even small organizations access to vast amounts of computing power. It would be difficult for most organizations to purchase and maintain tens of thousands of servers, but renting time on tens of thousands of servers from a cloud computing provider is much more affordable. However, not everyone wants to use this power for good. It might take an attacker years to crack an encryption key using his own limited hardware, but using an array of cloud servers, he might be able to crack it in minutes. Alternately, he might use that array of cloud servers to stage a DDoS attack, serve malware or distribute pirated software.

Initial registration with a cloud computing service is a pretty simple process. In many cases the service provider even offers a free trial period. Organisation should consider their risks due to anonymous sign up, lack of validation, service fraud and ad-hoc services.

Remediation

- Stricter initial registration and validation processes
- Enhanced credit card fraud monitoring and coordination
- Comprehensive introspection of customer network traffic

Insecure interfaces and APIs (Application Programming interfaces)

Cloud computing providers expose a set of software interfaces or APIs that customers use to manage and interact with cloud services. Provisioning, management, orchestration, and monitoring are all performed using these interfaces. The security and availability of general cloud services is dependent upon the security of these basic APIs. From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy.

Furthermore, organizations and third parties often build upon these interfaces to offer value-added services to their customers. This introduces the complexity of the new layered API; it also increases risk, as organizations may be required to relinquish their credentials to third-parties in order to enable their agency.

Remediation

- Analyze the security model of cloud provider interfaces
- Ensure strong authentication and access controls are implemented in concert with encrypted transmission
- Understand the dependency chain associated with the API

Malicious insiders

A malicious insider threat to an organization is a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems.

The threat of a malicious insider is well-known to most organizations.

This threat is amplified for consumers of cloud services by the convergence of IT services and customers under a single managementdomain, combined with a general lack of transparency into providerprocess and procedure. For example, a provider may not reveal how itgrants employees access to physical and virtual assets, how it monitorsthese employees, or how it analyzes and reports on policy compliance.

Remediation

- Enforce strict supply chain management and conduct a comprehensive supplier assessment
- Specify human resource requirements as part of legal contracts
- Require transparency into overall information security and management practices, as well as compliance reporting
- Determine security breach notification processes

Shared technology vulnerabilities

Cloud computing allows multiple organisations to share and store data on the servers. However, the original server hardware and operating system were most likely designed for use by a single tenant (one organisation). Organisations should ensure the appropriate controls are in place to keep cloud data secure. A defense in depth strategy is recommended, and should include compute, storage, and network security enforcement and monitoring. Strong compartmentalization should be employed to ensure that individual customers do not impact the operations of other tenants running on the same cloud provider. Customers should not have access to any other tenant's actual or residual data, network traffic, etc.

Remediation

- Implement security best practices for installation/configuration
- Monitor environment for unauthorized changes/activity
- Promote strong authentication and access control for administrative access and operations
- Enforce service level agreements for patching and vulnerability remediation
- Conduct vulnerability scanning and configuration audits

Data loss or leakage

With shared infrastructure resources, organisation should be concerned about the service provider's authentication systems that grant access to data. Organisations should also ask about encryption, data disposal procedures and business continuity. Any accidental deletion by the cloud service provider, or worse, a physical catastrophe such as a fire or earthquake, could lead to the permanent loss of customers' data unless the provider takes adequate measures to backup data. Furthermore, the burden of avoiding data loss does not fall solely on the provider's shoulders. If a customer encrypts his or her data before uploading it to the cloud, but loses the encryption key, the data will be lost as well.

Remediation

- Implement strong API access control
- Encrypt and protect integrity of data in transit
- Analyses data protection at both design and run time, Implement strong key generation, storage and management and destruction practices
- Contractually demand providers wipe persistent media before itis released into the pool
- Contractually specify provider backup and retention strategies

Account or service hijacking

Account or service hijacking is not new. Attack methods such as phishing, fraud, and exploitation of software vulnerabilities still achieve results. Credentials and passwords are often reused, which amplifies the impact of such attacks. Cloud solutions add a new threat to the landscape. If an attacker gains access to user credentials, they can eavesdrop on user activities and transactions, manipulate data, return falsified information, and redirect user clients to illegitimate sites. User account or service instances may become a new base for the attacker. From here, they may leverage the power of user reputation to launch subsequent attacks.

Remediation

- Prohibit the sharing of account credentials between users andservices
- Leverage strong two-factor authentication techniques wherepossible
- Employ proactive monitoring to detect unauthorized activity
- Understand cloud provider security policies and SLAs

Unknown risk profile

For many service providers, the focus is on functionality and benefits, not security. Without appropriate software updates, the intrusion prevention and firewalls, user organisations may be at risk.

Remediation

- Disclosure of applicable logs and data
- Partial/full disclosure of infrastructure details (e.g.patchlevels, firewalls, etc.)
- Monitoring and alerting on necessary information

Data Breaches

In a multitenant cloud service model, if cloud database is not properly designed, a flaw in one client's application could allow an attacker access not only to that client's data, but every other client's data as well. Unfortunately, while data loss and data leakage are both serious threats to cloud computing, the measures a user put in place to mitigate one of these threats can exacerbate the other. User may be able to encrypt user data to reduce the impact of a data breach, but if he lose user encryption key, he will lose his data as well. Conversely, the user may decide to keep offline backups of user data to reduce the impact of a catastrophic data loss, but this increases user exposure to data breaches.

Remediation

- Data security and integrity
- Strong encryption management
- Remote user multi-factor authentication

Denial of Service

Denial-of-service attacks are attacks meant to prevent users of a cloud service from being able to access their data or their applications. By forcing the victim cloud service to consume inordinate amounts of finite system resources such as processor power, memory, disk space or network bandwidth, the attacker (or attackers, as is the case in distributed denial-of-service (DDoS) attacks) causes an intolerable system slowdown and leaves all of the legitimate service users confused and angry as to why the service isn't responding.

Remediation

- Optimal capacity/resource planning
- Equipment power failures prevention
- Application Security

Browser Security

Browser security is also the major concern in case of cloud technology as most of the cloud services are accessed through browser. Several years ago, hackers use to attack software operating systems. More recently, hackers have shifted their attacks to target user browsers. By exploiting browser vulnerabilities, hackers have access to same applications and data that cloud user access.

Remediation

- Browser strong authentication capabilities
- Detection and Prevention of loading fake and harmful website pages
- Automation of secure browser configuration

REFERENCES

1. Peter Mell and Tim Grance, "The NIST definition of cloud computing", at National Institute of Standards and Technology, Gaithersburg, MD 20899-28930, September 2011.
2. Jensen, Schwenk, J. Gruschka, and Iacono, “On technical security issues in cloud computing”, In IEEE, International conference on cloud computing, pp. 109, 21-25, September 2009.
3. Kenneth Kofi Fletcher, “Cloud security requirements analysis and security policies development using a high-order object-oriented modelling technique”, Presented to the faculty of the Graduate School of the Missouri at University of Science and technology, Missouri, 2010.
4. Frank Gens, Robert, P Mahowald and Richard L Villars, "Cloud computing: benefits, risks and recommendations for information security", November 2009.
5. Judith Hurwitz, Robin Bloor,Marcia Kaufman andDr. Fern Halper, "Service oriented architecture (SOA for dummies)", 2nd IBM limited addition,Published by Wiley Publishing, Inc., Indianapolis, Indiana, March 2009.
6. Ristenpart, T. Tromer, E. Shacham and H. Savage, “Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds”, In Proceedings of the 10thassociation of computer machinery(ACM) conference on Computer and communications security (CCS), November 2009.
7. European Network and Information Security Agency (ENISA), "Cloud computing: benefits, risks and recommendations forinformation security," November 2009.
8. Bernd Grobauer, A. Antony, Tobias Walloschek and Elmar Stocker, "Understandingcloud-computing vulnerabilities", In IEEE Security and Privacy, vol. 99, 2010.
9. Mohamed Al Morsy, John Grundy and Ingo Müller, "An analysis of cloud computing security problem", In Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 30th November 2010.
10. Christodorescu, M. Sailer, R. Schales, D.L., Sgandurra and D. Zamboni, "Cloud security is not (just) virtualization security", In Proceedings of the 2009 association of computer machinery (ACM) workshop on Cloud computing security (CCSW), 2009.
11. Meiko Jensen, JorgSchwenk, Nils Gruschka and Luigi Lo Iacono, "On technical security issues in cloud computing", In IEEE ICCC, pp. 109-110, at Bangalore, August 2009.
12. Wikipedia Contributors, The free encyclopaedia, Wikimedia foundation, inc.22 July 2004. Web.10 Aug. 2004, <en.wikipedia.org./wiki/cross-site_scripting#citecite_note-symantec-2007-2nd-exec-0>, Last accessed on December 2016.
13. Aviram, S. Ford and Gummadi, “Determining timing channels in compute clouds”, In Proceedings of the 2010, association of computer machinery (ACM) workshop on Cloud computing security workshop (CCSW), 2010.
14. Kresimir, Popovic and ZeljkoHocenski, "Cloud computing security issues and challenges", In the third international conference on advances in human-oriented and personalized mechanisms, technologies, and services, pp. 344-349, 2010.
15. S. Subashini and Kavitha, "A metadata based storage model for securing data in cloud environment", Journal of Network and ComputerApplications, vol. 298, In Press, Corrected Proof.
16. Cloud security Alliance (CSA), "Top threats to cloud computing" Available: http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf
17. APT Research Team, “Spear-Phishing Email: Most Favored APT Attack Bait”’ by TrendLabsSM, http://www.trendmicro.co.uk/media/wp/apt-primer-whitepaper.pdf.
18. https://www.cs.cmu.edu/~agrao/paper/CMU-ISR-12-113_Effect_Grammar_Long_Passwords.pdf
“Effect of Grammar on Security of Long Passwords”, by Ashwini Rao, Birendra Jha and Gananandkini
19. Jyoti Chhikara,Ritu Dahiya,Neha Garg and Monika Rani, “Phishing & Anti-Phishing Techniques: Case Study”, International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE) by
20. J. Alex Halderman, Brent Waters and Edward W. Felten, “A Convenient Method for Securely Managing Passwords” by International World Wide Web Conference Committee(IW3C2), *WWW 2005*, May 1014, 2005, Chiba, Japan.ACM 1595930469/05/0005
21. Stephen G. Batsell, Nageswara S. Rao and Mallikarjun Shankar, “Distributed Intrusion Detection and Attack Containment for Organizational Cyber Security”, Computational Sciences and Engineering Division, Computer Science & Mathematics Division.

22. Yasir Ahmed Hamza1, Marwan Dahar Omar "Cloud Computing Security: Abuse and Nefarious Use of Cloud Computing", Department of Computer Science, Computer and IT Faculty, Nawroz University, Duhok, Iraq, International Journal of Computational Engineering Research, Vol, 03, Issue 6, June 2013.