International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 2 | ISSN : 2456-3307

Survey on Security Issues and Challenges in Cloud Computing

M. Savithiri[1], A. Mercy[2]

[1]Assistant Professor, Department of Computer Science, Dr N.G.P Arts and Science College, Coimbatore, Tamilnadu, India

[2]M Phil Research scholar, Department of Computer Science, Dr N.G.P Arts and Science College, Coimbatore, Tamilnadu, India

ABSTRACT

Cloud computing is a promising technology in the creation of the mixture of traditional computing technology. The network technology includes grid computing, distributed computing parallel computing and so on. It has transformed the software support for large systems from the server to a service-oriented paradigm. It aims to build a perfect system with powerful computing capability throughout a large number of relatively low-cost computing entity, and using the advanced Service models like SaaS (Software as a Service), PaaS (Platform as a Service), IaaS (Infrastructure as a Service) to distribute the powerful computing capacity to end users hands. This paper tackles the security risks and challenges and certain solutions also followed since security is one of the most critical aspects in cloud computing due to the sensitivity of user's data.

Keywords: Cloud computing, security issues, privacy issues, thread issue, security challenges.

I. INTRODUCTION

Cloud Computing means we can access all Software and Hardware without downloading and installation through the web service with the help of Service providers[1]. The explanation of "Cloud Computing" from the NIST definition, "cloud computing is a model for enabling ubiquitous, 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."

The National Institute of Standards and Technology's definition of cloud computing identifies "five essential characteristics":

On-Demand Self-Service

A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad Network Access

Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource Pooling

The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

Rapid Elasticity

Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear unlimited and can be appropriated in any quantity at any time.

Measured Service

Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

Cloud Computing Deployment Models

There are primarily the following deployment models generally seen.

(i) Public Cloud - A public cloud is best suite for user who want to use cloud infrastructure for development and testing of applications and host aplications. Examples: Amazon Elastic-Compute-Cloud, IBM's BlueCloud, Sun Cloud, Google AppEngine.

(ii) Private Cloud - A private cloud is one in which the computing environment is operated exclusively for an organization. It is best suite for where security is very important an organisations that want have very tight control over their data.

(iii) Community Cloud - A community cloud is somewhat similar to a private cloud, but the infrastructure and computational resources are shared by several organizations that have common privacy, security, and regulatory considerations, rather than for the exclusive use of a single organization. Examples of community cloud include Google's "Gov Cloud".

(iv) Hybrid cloud - A hybrid cloud 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 interoperability.

Cloud Computing Service Models

The three well-known and commonly used service models in the cloud paradigm are Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

(i) Software as a Service (SaaS) – Software with related data is deployed by a cloud service provider, and users can use it through the web browsers.

(ii) Platform as a Service (PaaS) – A service provider facilitates services to the users with a set of software programs that can solve the specific tasks.

(iii) Infrastructure as a Service (IaaS) – The cloud service provider facilitates services to the users with virtual machines and storage to improve their business capabilities.

Cloud Computing Benefits

Enterprises would need to align their applications, so as to exploit the architecture models that Cloud Computing offers. Some of the typical benefits are listed below[13]:

- ✓ Reduced Cost
- ✓ Increased Storage
- ✓ Flexibility

II. CLOUD COMPUTING CHALLENGES

Despite its growing influence, concerns regarding cloud computing still remain. In our opinion, the benefits outweigh the drawbacks and the model is worth exploring[3]. Some common challenges are:

1. Data Protection Data Security is a crucial element that warrants scrutiny. Enterprises are reluctant to buy an assurance of business data security from vendors. They fear losing data to competition and the data confidentiality of consumers. In many instances, the actual storage location is not disclosed, adding to the security concerns of enterprises. In the existing models, firewalls across data centers (owned by enterprises) protect this sensitive information. In the cloud model, Service providers are responsible for maintaining data security and enterprises would have to rely on them.

2. Data Recovery and Availability All business applications have Service level agreements that are stringently followed. Operational teams play a key role in the management of service level agreements and runtime governance of applications. In production environments, operational teams support

- ✓ Appropriate clustering and Failover
- ✓ Data Replication
- ✓ System monitoring (Transactions monitoring, logs monitoring, and others)
- ✓ Maintenance (Runtime Governance)
- ✓ Disaster recovery
- ✓ Capacity and performance management

If any of the above-mentioned services are under-served by a cloud provider, the damage & impact could be severe.

3. Management Capabilities Despite there being multiple cloud providers, the management of platform and infrastructure is still in its infancy. Features like "Auto-scaling" for example, are a crucial requirement for many enterprises. There is huge potential to improve the scalability and load balancing features provided today.

4. Regulatory and Compliance Restrictions In some of the European countries, Government regulations do not allow customer's personal information and other sensitive information to be physically located outside the state or country. In order to meet such requirements, cloud providers need to set up a data center or a storage site exclusively within the country to comply with regulations. Having such an infrastructure may not always be feasible and is a big challenge for cloud providers.

III. ISSUES IN CLOUD COMPUTING

Security issues, Privacy issue, Application issue, and Thread issues are there, Data loss is one of the major problems in Security issue, because of user can access our data in anywhere. The privacy issue occur users have no the knowledge about who is actually accessing the data and where data stored in the cloud and only the authorized person can maintain the cloud service model. In application issue the cloud provider frequently monitor and maintaining the cloud security. There are top twelve threat that pose severe danger to the cloud computing in year 2018 according to "The dirty dozen: Cloud Computing Top Threat" by the Cloud Security Alliance (CSA) [2]. The top twelve threats that have been mentioned in the white paper are:

1. Data breaches

Information that put away to the cloud by the clients may be vital and delicate. The information store in cloud may be stole by the unapproved clients and that may represents some level of threat to the clients under assault. It is the best danger to risk to the distributed computing since programmers or assailants can without much of a stretch access to the information of the clients which store in the cloud. The cloud put away a pool of private data of numerous clients. The cloud benefit clients ought to likewise guarantee the quality, unwavering quality and execution of the cloud specialist organizations through Administration Level Understandings (SLAs) consulted amongst suppliers and clients [4]. Therefore, data breaches are the worst problem that the cloud computing service faces.

2. Insufficient identity, credential, and access management

Awful on-screen characters taking on the appearance of honest to goodness clients, administrators, or designers can read, alter, and erase information; issue control plane and administration capacities; snoop on information in travel or discharge noxious programming that seems to start from a true blue source, CSA says[4,5]. Subsequently, inadequate personality, certification, or key administration can empower unapproved access to information and possibly disastrous harm to associations or end clients.

3. Insecure interfaces and application programming interfaces (APIs)

Cloud suppliers uncover an arrangement of programming (UIs) or APIs that clients use to oversee and associate with cloud administrations. Provisioning, administration, and checking are altogether performed with these interfaces, and the security and accessibility of general cloud administrations relies upon the security of APIs, CSA says. They should be intended to secure against inadvertent and vindictive endeavors to bypass arrangement[6].

4. System vulnerabilities

Framework vulnerabilities are exploitable bugs in programs that aggressors can use to invade a framework to take information, taking control of the framework or disturbing administration activities[6,2]. Vulnerabilities inside the parts of the working framework put the security of all administrations and information at noteworthy hazard, CSA says. With the coming of multi-occupancy in the cloud, frameworks from different associations are set near each other and offered access to shared memory and assets, making another assault surface.

5. Account hijacking

The user's account is stolen or hijacked and the hackers might impersonate he user to perform malicious and unauthorized activities which might also harm the user [11]. For example, the hackers might manipulate the data; provide false information and eavesdropping on transactions using the stolen account. In addition, no native APIs are used for login and anyone can register as a cloud service user hence the chances of the account being hijacked is high [6].

6. Malicious insiders

While the level of danger is available to face off regarding, the way that insider risk is a genuine enemy isn't, CSA says. A malignant insider, for example, a framework overseer can get to possibly delicate data, and can have expanding levels of access to more basic frameworks and in the end to information[7]. Frameworks that depend exclusively on cloud specialist co-ops for security are at more serious hazard.

7. Advanced persistent threats (APTs)

APTs are a parasitical type of digital assault that penetrates frameworks to set up a toehold in the IT foundation of target organizations, from which they take information. APTs seek after their objectives stealthily finished broadened timeframes, frequently adjusting to the safety efforts proposed to shield against them[11,3]. Once set up, APTs can move horizontally through server farm systems and mix in with ordinary system activity to accomplish their goals, CSA says.

8. Data loss

Information put away in the cloud can be lost for reasons other than noxious assaults, CSA says[4]. A unintentional erasure by the cloud specialist co-op, or a physical calamity, for example, a fire or tremor, can prompt the lasting loss of client information unless the supplier or cloud shopper takes satisfactory measures to go down information, following prescribed procedures in business congruity and fiasco recuperation.

9. Insufficient due diligence

At the point when officials make business techniques, cloud advances and specialist organizations must be viewed as, CSA says. Building up a decent guide and agenda for due perseverance while assessing advancements and suppliers is fundamental for the best possibility of achievement[4]. Associations that hurry to receive cloud innovations and pick suppliers without performing due industriousness open themselves to various dangers.

10. Abuse and nefarious use of cloud services

Most of the cloud computing systems have weak registration system. For example, anyone with a valid credit card may register and start using the cloud service immediately[12]. Thus, attackers often conduct the malicious activities by abusing the relative anonymity of the registration of the cloud computing services. Future areas of concern include password and key cracking, DDOS attack, launching dynamic attack points and hosting malicious data.

11. Denial of service (DoS)

Hacker use this type of attack to flood the machine or network resources of the cloud service provider which interrupt the users and prevent the users from connecting to the network access [11,7]. This is also a security issues that might harm the user because cloud service becomes unavailable to users and they might not get what they need in time.

12. Shared technology vulnerabilities

IaaS vendors deliver their services in a scalable way by sharing infrastructure. It is not designed to offer strong isolation properties for a multi-tenant architecture.

13. Bonus cloud threat for 2018: Spectre and Meltdown

An outline highlight regular in most present day microchips that could permit content, including scrambled information, to be perused from memory utilize pernicious JavaScript code[7]. The two varieties of this issue, called Meltdown and Spectre, influence all gadgets from Cell phones to servers. This is a direct result of the last that we are adding them to the most critical cloud dangers for 2018, making it a messy dough puncher's dozen. Both Specter and Meltdown permit side-channel attacks because they break down the isolation between applications[8]. An attacker that is able to access a system through unprivileged log in can read information from the kernel, or attackers can read the host kernel if they are a root user on a guest virtual machine (VM).

IV. SOLUTION AND PRACTICES FOR CLOUD SECURITY ISSUES

The cloud computing have become more popular because many users start to realize its benefits. It allows the user to easily shrink the operation and also help to save cost. However, with the increased adoption rate of the cloud service, the security issues and risk have been increased as well [11]. In order to make cloud computing a better option to increase the user storage capacity and save their confidential information securely, there are few solutions and practice that helps.

Vulnerability shielding

The cloud service provider should improve the patch management. They should check the vulnerability of their cloud service frequently and always update and maintain the cloud to limit the possible access point and reduce the risk of attack of the cloud by the hackers. The cloud service provider might also use the Intrusion Detection System (IDS) to make sure the cloud service provided is secure and safe.

Trusted cloud service provider

The user should make sure that they find the right cloud service provider. Each cloud service provider has different approaches on data management in the cloud. Well established and experienced cloud service provider is more trust worthy and better choice. Besides, the standards and regulations of the cloud service provider are also very important. Examples of trusted clouds service providers are Amazon Web Services (AWS), IBM, Google and Microsoft. [2] Shares the comparison of cloud database so that user can have better understanding of each database and choose the appropriate database accordingly. In order to guide users in choosing the best cloud service provider, CloudCmp have been developed in studies by [11]. They claimed that the application compares the cost and performance of cloud service providers and ensure fairness, representativeness and compliance while limiting measurement cost structure.

Use cloud service wisely

The data stored in the cloud should be confidential and even the cloud service provider should not have access to those information [4]. The data stored in the cloud should be well encrypted to ensure the security of the users' information. Anyone who needs access to the data in the cloud should ask for the permission of the users before doing so.

Security check events

The users should have clear contract with the cloud service provider so that the users can claim if any accidents or breaches of the sensitive data stored in the cloud. The users must have clear agreement with the cloud service provider before using the cloud services provided by that particular cloud service provider. The users should ensure that the cloud service provider give enough details about fulfillments of promises, break remediation and reporting contingency.

Data storage regulations

The architecture of the cloud environment is an important aspect to ensure the security of the data stored in the cloud. The users must understand the concept of the data storage regulations which the cloud service provider follows. Cloud service provider that provide security solution compliant with regulations such as HIPAA, PCI DSS, and EU data protection laws are some of the best choice.

Facilities for recovery

Cloud service provider should take the responsibility to recover the data of the users if there is any data loss due to certain issues [5]. Cloud service provider should make sure that they have proper backup and can retrieve and recover the confidential data of the users that might be costly. Moreover, the cloud service providers can also implement the following solutions to ensure data recovery [9]:

i. Using fastest disk technology in event of disaster for replication of data in danger.
ii. Changing dirty page threshold.
iii. Prediction and replacement of risky devices.

Enterprise infrastructure

The user must secure the data that they want to keep in the cloud infrastructure. The cloud service provider should provide an infrastructure that gives facilitates for the users to install and configure hardware components like firewalls, routers, server and proxy server.

Access control

The cloud service provider should set up the data access control with rights and the users who access the data should be verified by the cloud service provider every time. The cloud service provider must ensure that only the authorized users may have access to the data stored in cloud. The method can help to reduce the risk of the data access by the unauthorized users and thus provide a much secure environment to store sensitive data. In addition, third party auditing can also be one of the alternatives to ensure data integrity of the storage in the cloud [11]. However, the auditing procedure should have the following properties:

i. Confidentiality: Auditing protocols should keep user's data confidential against auditor.
ii. Dynamic auditing: Auditing protocol should support updates of data in the cloud.
iii. Batch auditing: Auditing protocol should support batch auditing for multiple users and clouds.

Identification management and authentication

When the user wants to access the data stored in the cloud, they must be authenticated not only by using the username and password but also the digital data. Multi-level authentication technique introduced by [5] can also be implemented in cloud computing. The technique generates password in several levels before the user can access the cloud services. Anonymous authentication (i.e. identity of user is protected from the cloud) can also be implemented where only valid users are able to decrypt the information [8]. Other than that, proposed scheme by [11] can also be applied in cloud computing where they claimed that their new password authentication scheme are secured from impersonation , off-line guessing and man in the middle attack. Furthermore, leakage-resilient authentication can also be utilized in order to improve the security of the cloud services [12].

Kernal Protection

The cloud provider might also use the KAISER a kernal modification to not have the kernal mapping in the user space. This modification was intened to prevent side-channel attack breaking KASLR(kernel address space layout randomization)[8].

V. CONCLUSION

Distributed computing is a model that velocities up and increment the adaptability of information administration with diminished cost. It is certain that distributed computing has brings us bunches of advantages and ending up more prevalent these days. Numerous extensive organizations begin utilizing cloud benefit in their business. While the distributed computing is broadly utilized, the security turns into a worry to everybody who utilizes cloud administrations. There is a considerable measure of security emerges constantly while there are change too on the security model of the cloud benefit gave. In spite of the expanding utilization of the cloud benefit, the client should utilize the cloud benefit gave carefully in a way that dependably guarantee great security hones with the goal that this innovation can possibly convey the data innovation to the following level. Distributed computing may help us to isolate the programming from the equipment as more innovations are utilized as administration utilizing cloud and programming may have a profoundly dynamic space with the PC equipment. It is normal that this paper gives some premise or establishment with respect to issues and difficulties in distributed computing.

VI. REFERENCES

[1]. Mell P and Grance T 2011 The NIST definition of cloud computing Retrieved from http://dx.doi.org/10.6028/NIST.SP.800-145

[2]. Cloud Security Alliance 2018 The The dirty dozen: Cloud Computing Top Threat in 2018 Retrieved from https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf

[3]. Qi. Zhang Lu. Cheng, Raouf Boutaba, "Cloud computing: state-of-the-art and research challenges", "The Brazilian Computer Society", April 2010.

[4]. T. T. W. Group et al., "The notorious nine: cloud computing top threats in 2013," Cloud Security Alliance, 2013.

[5]. W. A. Jansen, "Cloud Hooks: Security and Privacy Issues in Cloud Computing," Proceedings of the 44th Hawaii International Conference on System Sciences, 2011.

[6]. Ashktorab, V., & Taghizadeh, S. R. (2012). Security Threats and Countermeasures in Cloud Computing. International Journal of Application or Innovation in Engineering & Management (IJAIEM) , Vol. 1(2), pp. 234-245.

[7]. Khorshed, M.T., A.S. Ali, and S.A. Wasimi, A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. Future Generation computer systems, 2012. 28(6): p. 833-851.

[8]. LIU, F., YAROM, Y., GE, Q., HEISER, G., AND LEE, R. B. Last-Level Cache Side-Channel Attacks are Practical. In IEEE Symposium on Security and Privacy - SP (2015), IEEE Computer Society, pp. 605-622.

[9]. McDowell M 2009 Understanding denial-of-service attack Retrieved from https://www.us-cert.gov/ncas/tips/ST04-015

[10]. Ashktorab, V., & Taghizadeh, S. R. (2012). Security Threats and Countermeasures in Cloud Computing. International Journal of Application or Innovation in Engineering & Management (IJAIEM) , Vol. 1(2), pp. 234-245.

[11]. Kandias M, Virvilis N and Gritzalis D 2011 The insider threat in cloud computing Proc. of 6th International Conf. on Critical Infrastructure Security 95-106

[12]. Shin S H and Kobara K 2010 Towards secure cloud storage Demo for CloudCom2010

[13]. https://www.questsys.com/files/Challenges-Benefits-Cloud-Computing.pdf