A Survey on the factors affecting security of the cloud

Ruksar Ahmadi, Student(M.Tech), The National Institute of Engineering, Mysuru, India, ruksarahmedi7@gmail.com

Abstract- Cloud has recently emerged as a technology which provides effective storage and computational mechanism to its users. Almost all the IT infrastructures these days rely on the various services offered by the cloud to carry out their day to day business tasks. One of the main benefits of the cloud is that the services are made available at a lower cost than the other conventional mechanisms. The cloud is also reliable because even if one of the servers providing the service goes down, the functionality can still be supported by other servers so that the customer always gets what he asks for. Though the cloud and the advantages associated with the usage of the cloud are really high, there are certain security factors which cannot be overlooked. Some of the factors that affect the security parameter of the cloud have been discussed in this paper.

Keywords —availability, cloud computing, EDoS attack, reliability, scalability, security

I. INTRODUCTION

The first major company that adopted the cloud infrastructure model was the Amazon in the year 2002. The company believed that this approach would help them achieve better efficiency. Many other companies later followed up. 2007 was the year that saw two IT giants IBM and Google collaborate to establish a server farm that could help in research activities. The University of Washington was the first to tie up with this project. Carnegie Mellon University, MIT, Stanford University, the University of Maryland, and the University of California at Berkeley soon joined in giving the project a big boost [4].

There are three different service models of the cloud: SaaS(Software as a Service), PaaS(Platform as a Service), IaaS(Infrastructure as a Service). An organization can rent any type of service based on the nature and requirement of the service. The IaaS model provides your business with hardware and network, and you can install your own operating system, software, and apps. You get the hardware, network and an operating system for corporations that choose the PaaS model. Then you have the liberty to install or build your own software and apps. Finally, you get the hardware, network, operating system and any software and apps your company wants in the SaaS model [4].

Cloud services are popular because they can decrease owning and running pcs and networks ' costs and complexity. Since cloud consumers do not need to invest in IT infrastructure, purchase equipment, or purchase software licenses, the advantages are low upfront expenses, fast investment return, fast implementation, customization, flexible use, and solutions that can make use of fresh technologies. Furthermore, cloud suppliers specializing in a specific region (such as e-mail) can provide sophisticated services that a single business may not be able to afford or create [5].

Cloud computing brings small and medium-sized enterprises a whole host of opportunities. There's no need to invest in expensive hardware that you typically can't use fully, and your service provider will also take care of license fees, maintenance of equipment and IT support so you don't have to worry about updates and get IT experts that can guide your customers with their concerns. Plus study demonstrates that small and medium-sized enterprises can save up to 70% of their IT expenses if they migrate their IT facilities to the cloud as you're only charged for what you're using, and if the worst thing happens with cloud-based company continuity facilities you can back up and run in the shortest moment possible [5].

There are several unique security issues and challenges in cloud computing. With a third-party supplier, records are stored in the cloud and accessed via the internet. This indicates that there is restricted visibility and control over that information. It also raises the issue of how one can secure it properly. It is essential that everyone knows their corresponding roles and cloud computing security problems [2].

Providers of cloud services treat the hazards of cloud security as a shared liability. The cloud service supplier is covering cloud security itself in this model, and the client is covering the safety of what they placed in it. Cloud computing customers are always accountable for shielding their details from safety threats and controlling access in any cloud service — from software-as - a-service (SaaS)

 DOI : 10.35291/2454-9150.2019.0251 © 2019, IJREAM All Rights Reserved.

such as Microsoft Office 365 to infrastructure-as - a-service (IaaS) such as Amazon Web Services (AWS) [2].

II. PRELIMINARIES

A. *Architectural model of cloud computing*

The cloud is broadly divided into two categories: Front-end and Back-end. It is the back-end's duty to provide cloud users with data security along with the traffic control program. The server also offers the middleware for connecting equipment and communicating with each other. Cloud infrastructures are used by businesses to work with these apps. Unlike subscription-based pricing systems, the cloud's payment system allows users to subscribe to supplier services and pay on a ' pay-per-use ' basis for cloud infrastructure.

The architecture of cloud technology also consists of front-end systems named the cloud clients that include servers, thin & fat clients, tablets and mobile equipment. The middleware or web browser is used to establish communication. Cloud-oriented architecture can mainly be the IoT's (Internet of Things) building block where anything can be linked to the internet. The architecture of the cloud is a mixture of service driven architecture and event-driven architecture.

B. *Deployment models of cloud computing*

There are four major cloud deployment models that vary substantially and are opted for by most businesses: a public, private, hybrid and a community one.

Public clouds are publicly accessible and information is generated and stored on third-party servers. The need for customer businesses to purchase and retain their own hardware is eliminated as server infrastructure belongs to service suppliers that manage them and administer pool resources. Provider businesses give free or pay-per-use services through the Internet connection. When needed, users can scale them [3].

Private From the technical point of view, there is little or no difference between public and private clouds, as their designs are very similar. Unlike the public one, however, only one particular business owns a private cloud, which is why it is also called an internal or corporate cloud. Because these architectures of the data center live within the firewall, they offer increased security. Although the organization operates its workloads privately, it can also be managed by a third party and the server can be hosted internally or at the customer company's premises [3].

Community A community cloud deployment model to a big extent resembles a personal one; the only distinction is the user set. While a private form indicates that the server is owned by only one business, several organizations with comparable backgrounds share the infrastructure and associated assets in the event of a community one [3].

Hybrid As is generally the case with any hybrid occurrence, the finest characteristics of the above-mentioned cloud computing deployment models are included in a hybrid cloud – public, private, and community. It enables businesses to blend and match all three kinds of facets that best suit their needs [3].

C. *Characteristics of cloud computing*

- Users access data, apps or other services in cloud computing with the help of a browser, regardless of the device used and the place of the user.
- With the help of the internet, the infrastructure mostly supplied by a third party is accessed.
- Price is decreased to a substantial point because a third party provides the infrastructure.
- Implementation requires less IT skills.
- Reliable services are often acquired through the use of various locations that are suitable for continuity of company and recovery from disasters.
- Sharing of resources and prices among a vast array of customers allows the infrastructure to be used economically.
- Maintenance is easier for cloud computing apps as they have not been placed on the pc of each user.
- Pay per usage unit allows activity on periodic bases to use application per shopper.
- Performance is frequently tracked and is therefore ascendable.
- Security is often fairly much as good or greater than old schemes as vendors can devote resources to solving safety issues that several clients are unable to afford.
- However, safety stays a key issue once the data is confidential. Cloud might be a huge resource pool that you should just purchase according to your needs [6].

III. RELATED WORKS

A. *Security issues associated with Software as a Service*

Issues encountered with SaaS apps are evidently focused on information and access, as most models of shared safety responsibilities leave these two as SaaS customers ' primary liability. It is the responsibility of each organization to understand what data they have put into the cloud, who can access it, and what level of protection they have applied [6].

It is also essential to consider the SaaS provider's position as a potential point of access to the information and procedures of the organization. Developments such as the increase of ransomware XcodeGhost and GoldenEye

 DOI : 10.35291/2454-9150.2019.0251 © 2019, IJREAM All Rights Reserved.

emphasize that attackers acknowledge the importance of software and cloud suppliers as a vector for attacking bigger assets. As a consequence, the focus of attackers on this prospective vulnerability has increased. Make sure that you scrutinize the safety programs of your cloud provider to safeguard your organization and its information. Set the expectation of predictable third-party auditing with shared accounts and insist on terms for reporting breaches to complement alternatives to technology [6].

B. Security issues associated with Infrastructure as a Service

In IaaS, information protection is critical. Additional threats are implemented as client liability extends to apps, network traffic and operating systems. The latest evolution of assaults that extend beyond information should be considered by organizations as the core of IaaS danger. Malicious actors conduct hostile takeovers of calculated assets to mine cryptocurrency and reuse those funds as a vector of assault against other components of company infrastructure and third parties [6].

It is essential to evaluate your capacity to avoid theft and control access when constructing infrastructure in the cloud. Determining who can enter information into the cloud, monitoring resource changes to recognize unusual behaviors, securing and hardening orchestration instruments, and adding North-South and East-West traffic network assessment as a future compromise signal are all rapidly becoming normal steps to protect cloud infrastructure deployments on a scale [6].

C. Security issues in private cloud

The fine-tuned control available in private cloud settings is a significant factor in the decision-making process for allocating resources to a public versus private cloud. Additional levels of control and extra security in private clouds can compensate for other constraints of private cloud deployments and can lead to a practical shift from monolithic data centers based on servers.

Simultaneously, organizations should consider that keeping fine-tuned control generates complexity, at least beyond what has evolved into the public cloud. Cloud suppliers are currently making a great deal of effort to preserve their own infrastructure [6].

IV. CONCLUSION

Although the cloud and the advantages associated with the usage of the cloud are really high, there are certain security factors which cannot be overlooked. The clients of the cloud computing must be well aware of the security concerns and drawbacks that run parallel with the cloud computing. The confidentiality of data will always be at a risk because the providers are semi trustable entities and can hence not be fully trusted. The current model is also such that it is prone to many types of attacks like the DoS(Denial of Service) attacks and EDoS(Economic Denial of Sustainability) attacks. New models must be proposed which can eliminate the risks associated with the cloud computing such that the quality of service is maintained and the overheads are minimum.

REFERENCES

[1] McAfee, “Navigating a Cloudy Sky: Practical Guidance and the State of Cloud Security.” Retrieved on June 27, 2019 from the site https://www.mcafee.com/enterprise/en-us/solutions/lp/cloud-security-report.html.

[2] McAfee, “Cloud Computing Security Issues and Solutions.” Retrieved on June 27, 2019 from the site https://www.mcafee.com/enterprise/en-in/security-awareness/cloud/security-issues-in-cloud-computing.html

[3] Yuliya Shaptunova, Sam Solutions, “Top 4 Cloud Deployment Models You Need to Know.” Retrieved on June 27,2019 from the site https://www.sam-solutions.com/blog/four-best-cloud-deployment-models-you-need-to-know/

[4] Keith D. Foote , June 22, 2017, Dataversity. “ A Brief History of Cloud Computing” Retrieved on June 27, 2019 from the site https://www.dataversity.net/brief-history-cloud-computing/#

[5] Bluecube, “Why are cloud computing services so popular ?” Retrieved on June 27, 2019 from the site https://www.bluecube.uk.com/blog/why-are-cloud-computing-services-so-popular.html

[6] Palvinder Singh, “Survey Paper on Cloud Computing”, International Journal of Innovations in Engineering and Technology, Vol 3, issue no 4, 2014.

[7] Q. Zhang, L. Cheng, and R. Boutaba, “Cloud computing: state-of-the-art and research challenges,” Journal of Internet Services and Applications, vol. 1, no. 1, 2010, pp. 7–18.

[8] K. Ren, C. Wang, and Q. Wang, “Security challenges for the public cloud,” IEEE Internet Computing, no. 1,2012, pp. 69–73.

[9] J. Idziorek, M. F. Tannian, and D. Jacobson, “The insecurity of cloud utility models,” IT Professional, no. 2, 2013, pp. 22–27.

[10] N. Vlajic and A. Slopek, “Web bugs in the cloud: Feasibility study of a new form of edos attack,” in Proceedings of 2014 Globecom Workshops (GC Wkshps). IEEE, 2014, pp. 64–69.

[11] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, “Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption,” IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 1, 2013, pp. 131–143.

[12] S. Yu, K. Ren, and W. Lou, “Attribute-based content distribution with hidden policy,” in Proceedings of 4th Workshop on Secure Network Protocols (NPSec2008). IEEE, 2008, pp. 39–44.

[13] S. Hohenberger and B. Waters, “Online/offline attribute-based encryption,” in Public-Key Cryptography–PKC 2014. Springer, 2014, pp. 293–310.

 DOI : 10.35291/2454-9150.2019.0251 © 2019, IJREAM All Rights Reserved.