IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-7, Special Issue-12, May 2019 E-ISSN: 2347-2693

A Study on Data Storage Security Issues in Cloud Computing

Nayana Bnasod[1*], Pranjal Dhore[2], Nisha Balani[3]

M.Tech., Department of Computer Science & Engineering, Jhulelal Institute of Technology, Nagpur, India

Corresponding Author: nainabansod4495@gmail.com

Available online at: www.ijcseonline.org

Abstract :- Cloud computing , a remote service platform used to store information and execute applications. It lets you run services and data online by request via a simple internet connection. Cloud computing is a relatively new technology that will become more widespread. The adoption of this technology is not without its challenges and risks.
With the cloud model, you lose control over physical security. In a public cloud, you are sharing computing resources with other companies. In a shared pool outside the enterprise, you don't have any knowledge or control of where the resources run. Exposing your data in an environment shared with other companies could give the government "reasonable cause" to seize your assets because another company has violated the law. Simply because you share the environment in the cloud, may put your data at risk of seizure.
Storage services provided by one cloud vendor may be incompatible with another vendor's services should you decide to move from one to the other. Vendors are known for creating what the hosting world calls "sticky services"—services that an end user may have difficulty transporting from one cloud vendor to another (e.g., Amazon's "Simple Storage Service" [S3]
is incompatible with IBM's Blue Cloud, or Google, or Dell). This study aims to review and classify the issues that surround the implementation of cloud computing which a hot area that needs to be addressed by future research.

***Keywords*:** Cloud Computing, security issues in cloud computing

I. INTRODUCTION

Cloud Computing , in turn, refers to sharing resources, software, and information via a network, in this case the Internet. The information is stored on physical servers maintained and controlled by a cloud computing provider, such as Apple in regards to iCloud. As a user you access your information on the cloud via the Internet. Cloud computing is a fast- growing, lucrative industry. The seven largest enterprise cloud venders- Microsoft, Amazon, IBM, Salesforce, Oracle, SAP, and Google – posted combines 2017 cloud revenue of $76.3 billion.

These earnings, combined with the sheer volume of data stored in the cloud naturally make cloud computing a target for cybercriminals. Sensitive data stored in the cloud naturally make cloud computing a target for cybercriminals. Sensitive data stored in the cloud is at risk if it isn't secured properly. Cloud security involves a broad set of regulations, technologies, and policies to protect data, applications, and the ever-expanding infrastructure of cloud computing.

II. OVERVIEW :

The US National Institute of Standards and Technology (NIST) has developed a working definition that covers the commonly agreed aspects of cloud computing. The NIST working definition summarises cloud computing 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"

The NIST definition is one of the clearest and most comprehensive definitions of cloud computing and is widely referenced in US government documents and projects. This definition describes cloud computing as having five essential characteristics, three service models, and four deployment models. The essential characteristics are:

- On-demand self-service: computing resources can be acquired and used at anytime without the need for human interaction with cloud service providers. Computing resources include processing power, storage, virtual machines etc.
- Broad network access: the previously mentioned resources can be accessed over a network using heterogeneous devices such as laptops or mobiles phones.
- Resource pooling: cloud service providers pool their resources that are then shared by multiple users. This is referred to as *multi-tenancy* where for example a physical server may host several virtual machines belonging to different users.

- Rapid elasticity: a user can quickly acquire more resources from the cloud by scaling out. They can scale back in by releasing those resources once they are no longer required. Measured service: resource usage is metered using appropriate metrics such monitoring storage usage, CPU hours, bandwidth usage etc. The above characteristics apply to all clouds but each cloud provides users with services at a different level of abstraction, which is referred to as a service model in the NIST definition. The three most common service models are:

- Software as a Service (SaaS): this is where users simply make use of a web-browser to access software that others have developed and offer as a service over the web. At the SaaS level, users do not have control or access to the underlying infrastructure being used to host the software. Salesforce's Customer Relationship Management software3 and Google Docs4 are popular examples that use the SaaS model of cloud computing.
- Platform as a Service (PaaS): this is where applications are developed using a set of programming languages and tools that are supported by the PaaS provider. PaaS provides users with a high level of abstraction that allows them to focus on developing their applications and not worry about the underlying infrastructure. Just like the SaaS model, users do not have control or access to the underlying infrastructure being used to host their applications at the PaaS level. Google App Engine5 and Microsoft Azure6 are popular PaaS examples.
- Infrastructure as a Service (IaaS): this is where users acquire computing resources such as processing power, memory and storage from an IaaS provider and use the resources to deploy and run their applications. In contrast to the PaaS model, the IaaS model is a low level of abstraction that allows users to access the underlying infrastructure through the use of virtual machines. IaaS gives users more flexibility than PaaS as it allows the user to deploy any software stack on top of the operating system. However, flexibility comes with a cost and users are responsible for updating and patching the operating system at the IaaS level. Amazon Web Services' EC2 and S37 are popular IaaS examples.

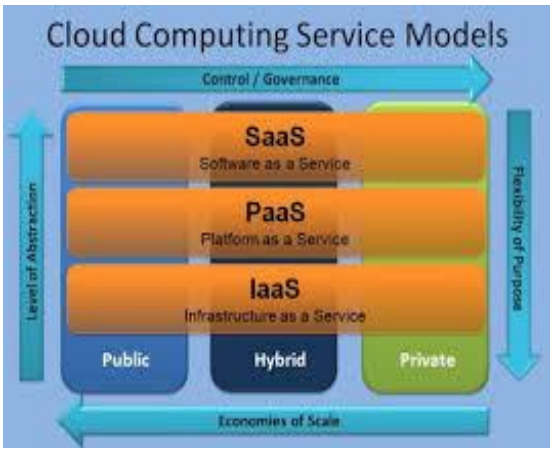

Figure 2: Cloud computing deployment and service models

The service models described in the NIST definition are deployed in clouds, but there are different types of clouds depending on who owns and uses them. This is referred to as a cloud deployment model in the NIST definition and the four common models are:

- Private cloud: a cloud that is used exclusively by one organisation. The cloud may be operated by the organisation itself or a third party. The St Andrews Cloud Computing Co-laboratory8 and Concur Technologies are example organisations that have private clouds.
- Public cloud: a cloud that can be used (for a fee) by the general public. Public clouds require significant investment and are usually owned by large corporations such as Microsoft, Google or Amazon.
- Community cloud: a cloud that is shared by several organisations and is usually setup for their specific requirements. The Open Cirrus cloud testbed could be regarded as a community cloud that aims to support research in cloud computing.
- Hybrid cloud: a cloud that is setup using a mixture of the above three deployment models. Each cloud in a hybrid cloud could be independently managed but applications and data would be allowed to move across the hybrid cloud. Hybrid clouds allow cloud bursting to take place, which is where a private cloud can burst-out to a public cloud when it requires more resources.

III. CHALLENGES TO CLOUD SECURITY

The Cloud Security Alliance (CSA) compiled comprehensive reporting on the threats to cloud security. These critical challenges we feel must address right away. The following offers a roadmap to protecting your organization from the most common cloud security risks.

1. Data Breaches :

Small businesses and nonprofits often assume they are immune to data breaches. Large organizations tend to be overly confident that they are protected against this risk. Unfortunately, the number and scope of data breaches is growing every year, and no company or industry is safe.
In the first six months of 2017, there were 791 data breaches reported – a 29 percent increase compared with the same period in 2016. The data loss has impacted organizations in every industry:

- 55 percent occurred in the general business sector
- 23 percent occurred in the healthcare industry
- 10 percent occurred in the education sector
- 6 percent occurred in the financial services industry
- 6 percent occurred in the government/military

These are just a few of the incidents that were reported in 2017:

- An Equifax breach exposed the sensitive personal data of more than 145 million people.
- Hacking tools believed to originate with the National Security Agency (NSA) and the Central Intelligence Agency (CIA) were leaked to the public.
- In her Congressional testimony, former Yahoo CEO Marissa Mayer stated that a 2013 data breach compromised three billion Yahoo user accounts – not the one billion figure originally reported.

While data breaches are not unique to cloud computing, these incidents have a devastating effect on cloud users. Billions of records were lost to data breaches in 2017, many of which involved cloud servers.

2. Inadequate Access Management :

Even the most advanced cloud security can't protect against theft when data thieves have system access. Unfortunately, unauthorized access is a significant issue. Organizations of every size demonstrate "a lack of scalable identity access management systems, failure to use multi-factor authentication, weak password use, and a lack of ongoing automated rotation of cryptographic keys, passwords and certificates," making this one of the top five issues to address in 2018.

3. Spectre and Meltdown :

One of the most alarming cloud security-related issues of 2018 was uncovered at the end of 2017. A flawed set of design features in most modern microprocessors has the potential to permit content to be read from memory through the use of malicious JavaScript code. These two design features have since been (ominously) named Spectre and Meltdown.

Spectre affects almost every system, including desktops, laptops, cloud servers, and smartphones. According to the CSA report, Meltdown affects cloud providers "which use Intel CPUs and Xen PV as virtualization without having patches applied. Furthermore, cloud providers without real hardware virtualization, relying on containers that share one kernel, such as Docker, LXC, or OpenVZ are affected."

4. Data Loss

Accidents happen, and human error is inevitable. Even when actions are not malicious, data can be permanently lost if it is not backed up properly. CSA offers the following guidance to mitigate this risk:

"Cloud consumers should review the contracted data loss provisions, ask about the redundancy of a provider's solution, and understand which entity is responsible for data loss and under what conditions. Some providers offer solutions for geographic redundancy, data backup within the cloud, and premise-to-cloud backups. The risk of relying on the provider to store, backup and protect the data must be considered against handling that function in-house. The choice to do both may be made if data is highly critical."

5. Denial of Service (DoS) attacks :

DoS attacks are attacks meant to disable a machine or network, making it inaccessible to its intended users. The rise of cryptocurrency like Bitcoin and Ripple makes it possible for DoS attacks to happen more frequently. Through the use of cryptocurrency, cybercriminals no longer have to learn the necessary skills or have control over a botnet. They can simply pay another hacker through these funding methods to do the job for them.

IV. CLOUD ENCRYPTION SOLUTIONS:

The necessity of protecting yourself against threats to the cloud is a critical issue in 2018. Fortunately, there are effective, well-tested solutions available. For example, Data encryption has been shown to dramatically reduce the likelihood of a data breach.

Since 2013, only 4% of data breaches have occurred where encryption was used. In the few cases where data was compromised, the stolen records were rendered useless by encryption tools . as a result, unauthorized parties were unable to use or sell the information.

Deploying encryption software in the cloud can reduce the likelihood of a data breach in the event of an attack.

Finally, cloud encryption can also mitigate the impact to an organization's public image and reputation when a breach does occur. Per the General Data Protection Regulation (GDPR), companies using encryption aren't required to file a report according to the 72-hour breach notification rule, and can avoid related penalties.

V. CONCLUSION

Cloud computing is a new emerging technology, which every organization these days adapt it to facilitate the flexibility of their businesses in terms data storage, exchange, transform which enable them to upgrade their profitability, interoperability, capability, and scalability. This study deals with various security issues. The ultimate purpose of those issues is to store the data in secure manner.

REFERENCES

[1] V.S. Varnika, " Cloud Computing Advantages and Challenges for Developing Nations", International Journal of Scientific Research in Computer Science and Engineering Vol.6, Issue.3, pp.51-55 , June (2018)

[2] Ramona Carr, "Top Challenges in Cloud Security", 2018

[3] Naresh vurukonda, B.Thirumala Rao, "A Study on Data Storage Security Issues in Cloud Computing",2nd International Conference on Intelligent Computing, Communication & Convergence (ICCC-2016).

[4] Ilango Sriram, Ali Khajeh-Hosseini, "Research Agenda in Cloud Technologies".

[5] John W. Rittinghouse and James F. Ransome, "Cloud Computing, Implementation, Management, and Security", © 2010 by Taylor and Francis Group, LLC.

[6] Dr. Ramalingam Sugumar, K.Raja, "A Study on Enhancing Data Security in Cloud Computing Environment", Dr. Ramalingam Sugumar *et al*, International Journal of Computer Science and Mobile Applications, Vol.6 Issue. 3, March- 2018, pg. 44-49.

[7] Prof. Syed Neha Samreen, Prof. Neha Khatri-Valmik, Prof. Supriya Madhukar Salve, Mr. Pathan Nouman Khan,"Introduction to Cloud Computing", International Research Journal of Engineering and Technology (IRJET), Volume: 05 Issue: 02 | Feb-2018.

[8] Qusay Kanaan Kadhim , Robiah Yusof , Hamid Sadeq Mahdi, Sayed Samer Ali Al-shami , Siti Rahayu Selamat, "A Review Study on Cloud Computing Issues", 1st International Conference on Big Data and Cloud Computing (ICoBiC) 2017 .

[9] Everaldo Aguiar, Yihua Zhang, and Marina Blanton," An Overview of Issues and Recent Developments in Cloud Computing and Storage Security".

[10] M.B. Jayalekshmi and S.H. Krishnaveni, "A Study of Data Storage Security Issues in Cloud Computing", Indian Journal of Science and Techonology, Vol 8(24), DOI:10.17485/ijst/2015/v8i24/84229, September 2015.

