International Journal of Advanced Research and Development
ISSN: 2455-4030; Impact Factor: RJIF 5.24
Received: 21-04-2019; Accepted: 24-05-2019
www.advancedjournal.com
Volume 4; Issue 4; July 2019; Page No. 31-33

Cloud-based Security Solutions

Sourav Mukherjee
PhD Student, Senior Database Administrator & University of the Cumberlands Chicago, United States

Abstract
Cloud computing is an entirely new archetype that overtures a non-traditional computing model for organizations to espouse Information Technology without incurring any upfront investment and with nominal Total Cost of Ownership (TCO). Cloud Computing is the new wave of technology and the favorite buzz word which the corporate world utters every now and then. Cloud computing unlocks the doors to multiple, infinite venues which include upscaling and downscaling the resources in no time and pay as you go model (that says pay to them based upon the usage). Even with the potential advantages attained from cloud computing, the security of the booming technology is under questions which may impact the cloud adoption. Based on several attacks and vulnerabilities took place in recent times and posted by several cloud providers, the more intense observation about Cloud Security Research has started to grow and to find out the probable ways to defend such attacks. There must be appropriate technical enforcement and verifiable accountability with appropriate security policies and measurement with compliance driven audits to generate a sense of urgency to control the Cloud Security.

Keywords: cloud, security, cloud computing, SAAS, CSA, CASB

1. Introduction

We live in the data age. It's a daunting task to measure the total volume of data put away electronically. Cloud computing poses an extra level of jeopardy because of the critical services offered by it to a third party, which makes it hard to uphold the data privacy and security. Security in cloud computing is a serious aspect, which has numerous issues and challenges associated with it. Cloud service providers, brokers, and cloud service users must have better make conscious of cloud safety. It is a conscious effort to prepare the cloud solution to be as safe as possible from all kinds of threats so that the users do not have to face any kind of problem such as; loss of data or data theft. There is a likelihood that a malicious user can go into the cloud by copying an authentic user, thus corrupt the whole cloud. It can significantly affect numerous users who are utilizing these types of clouds. Users' trust in cloud systems is destabilized by the absence of transparency in the standing security policies.

Cloud computing is available for everyone irrespective of any location of the globe, to employ the services and resources based on the demand of an individual. Today, any organization can effortlessly migrate its complete system on the cloud as it offers the pay-as-you-go service. Cloud has a multiplicity of benefits such as multi-tenancy, data storage, resource pooling, and virtualization (hypervisor). Despite many advantages, cloud computing also contributes to security flaws such as loss of subtle data, data seepage, cloning, and added security challenges related to virtualization. Because of the extended security challenges and concerns of the cloud, a substantial amount of study is required to indicate risks in services and deployment models of the cloud. This study characterizes the cloud security complications in numerous cloud-related fields and the intimidations related to the cloud model and cloud network. This paper will also address different security mitigating strategies with regards to virtualization and will be precisely addressed with side effects.

Cloud Security Alliance (CSA) which is a Nonprofit organization every year comes up with the best practice of securing the cloud-based platforms. CSA experts have identified the following nine critical threats to cloud security [2] and those are:

1. Data Breaches
2. Data loss
3. Account traffic hijacking
4. Insecure interfaces and APIs
5. Denial of Services (DOS)
6. Malicious insiders
7. Abuse of Cloud Services
8. Insufficient due diligence
9. Shared technology Vulnerabilities.

Based on my studies through their best practices, I can see that the following ideas to help secure our organization can be very effective and can be easily implemented. Some of them may be:

- Identify the shared responsibilities of security and risk management based on the chosen cloud deployment and service model.
- Develop an appropriate Cloud Governance Framework or model as per the defined industry best practices and the global standards and regulations defined by COBiT, NIST, ISO, CSA, CCM, HIPAA, PCI, GDPR, and so on.
- Develop a clearly defined process for periodically doing the assessment related to Cloud providers. These may include the following action items, such as-
- Documentation and policies
- Change-management policies to monitor the changes trending in the environment due to the use of the Cloud services
- Running periodic Audits and assessments
- Periodic contract review and review the compliance

section.

- If any contract can't be efficiently negotiated and resultant in causing any unacceptable risk, in such conditions need to look for an alternative of handling the risks such as through applying the required encryption or increase the monitoring.
- Ensure that the devices are appropriately patches and upgraded from time to time.
- Stay away from storing data in common locations or storing credentials on devices which could lead to comprise the cloud infrastructure.
- Using federated identify standards to register the devices securely and preserve a secure authentication to the cloud-side application.
- Managing the APIs appropriately. Those may contain malicious code to break into the cloud-based application.
- Encrypt the communication channel, secure the data-collection pipeline. If needed check with Cloud providers if they are using data masking if any service does not offer substantial security, privacy, and compliance needs.
- Sanitize the data appropriately before getting them to the cloud-based application to present any kind of exploitation of the cloud infrastructure through attacks.
- Serverless capabilities do carry a lot of advantages, especially it can dramatically reduce the surface attacks and pathways. It is an excellent method to break links in an attack chain.
- Need to fully comprehend the possible benefits and risks associated to cloud machine-learning or analytics service. Pay heed to privacy and compliance implications.
- Need to ensure that cloud providers do not expose customer privacy data to other employees or administrators by means of sharing any technical or process control methods.
- Cloud users will need to rely more on application-code scanning and logging and less on server and network logs.
- The essential cloud components such as VMs, hypervisors, virtual network devices, should be repeatedly repositioned for the purpose of implementing the load-balancing strategy.
- Exploring cloud-based tools and/or applications which can offer greater a level of protection while mitigating some of the dangers. Some of the well known Cloud based application or tools which offer extended security are as follows:
    - **Bitglass:** It can detect the usage of cloud applications and also can encrypt the data uploaded onto the cloud.
    - Skyhigh Networks: It can discover, analyze and secure your use of cloud applications. It uses logs collected from the existing firewalls, proxies, and gateways to rapidly discover what cloud apps your workforces are using.
    - **Netskope:** Netskope's fine-grained policy implementation allows your employees to use their favorite cloud apps while only blocking unsolicited activity. Your employees can continue to use cloud apps for increased productivity without compromising on your data security.
    - **Cipher Cloud:** It works by encrypting or tokenizing data straight at your business gateway. It also comes with in-built malware detection and data loss prevention techniques.
    - Okta: Okta's goal is to deliver a secure Single Sign-On (SSO) for all the cloud, on-premise and mobile applications used in your business. Okta is pre-integrated with general business applications from Google, Microsoft, Salesforce.com, and others.
    - **Snoop Wall:** It flags and stops access to high-risk data ports such as webcams, microphones, GPS and USB
    - **Silver Sky:** It offers email monitoring and network protection for HIPAA and PCI compliance
    - Logz.io: Here users can form proactive alerts on selected events and applicable dashboards to aggregate and view data trends and monitor security threats as well as password brute force detection, access control, and network access.
    - **Centrify:** It centers on identity management across devices and applications
    - **Metasploit:** It takes a cloud IP address and tests penetration to promise that security is in place.
    - **Qualys:** It scans any and all used web apps for vulnerabilities in SaaS, IaaS, and PaaS tools.
    - Trend Micro Hybrid Cloud Security Solutions: If security issues are noticed, deep Security's dashboard interface offers actionable insights to help rapidly remediate.
    - Symantec Cloud Workload Protection: It can automatically determine what an organization is running across multi-cloud deployments.

There are several types of cloud security solutions to help the organization mitigate risk and improve security. Among them are:

- **Cloud Workload Protection Platforms**: This protection technology works very well with both cloud infrastructure as well as virtual machines, providing monitoring and threat prevention features.
- **Cloud Access Security Brokers (CASB):** This category of a cloud security solution is frequently identified as the Cloud Access Security Broker (CASB) platforms, which monitor activity and applies security policies from an access perspective.
- **SaaS.** There is also a broad spectrum of security tools and technologies that are delivered from the cloud, in a software-as-a-service (SaaS) model to help defend both clouds besides on-premises workloads. It is required to further explore leading SaaS companies to learn more about the overall SaaS market.

It is essential by the cloud providers to perform the required simulation and test dissimilar scenarios to begin to improve adaptability. Most of the time cloud providers never do this as it incurs additional costs for them during the deployment. Penetration testing, Backup & failover tests, and Data transferability tests are required to be performed on a timely basis. Availability must be measured, and drills must be conducted for data availability. Scheduled inaccessibility must be prepared, identifying a time with not as much of client activity. Benchmarking the cloud provider's process of deployment and the security to the standard is not available currently and need to be brought up. It is required

to display the benchmark score and need to be listed for the respective cloud providers by a forum like a cloud security alliance (CSA).

Conclusions and Future Study

Each of these third-party app providers and services attempts to tackle and deliver solutions for the data security issues existing within the cloud computing, yet the appropriateness for the business will greatly depend on your security requirements and problems. The scene of multi-tenancy, subcontracting/outsourcing and the virtualization of data has commanded an environment where cloud security is vital. At the same time, it's important to note that these services are unable to correct a few fundamental key issues that might lead to negotiated data security. If the employees' interest is to use shadow IT cloud applications, possibly it is time to investigate why it is felt the need to avoid the business's IT department. If the employees continue to download business data with the intention to continue working at home, it is now the right time to ask why they feel the need to do so. The rapidly growing sector i.e. cloud security firms and related software such as those listed below are the solid indications that cloud security is inward bound a new era. The businesses which are looking into a public cloud solution is required to discover these options as further ways to defend their data. I strongly stay after my understanding of Information Governance, the techniques and advises to stay protected while providing a solid Cloud Security Solution. The methodology suggests that the above-furnished capacities can significantly improve an organization's overall cloud security practice. Security and prevention are a continuous journey and the organization needs to keep investing heavily in this area to maintain the enterprise to a good standing condition. If the cloud security is not taped, measured and optimized, it might limit the growth of cloud in the coming years.

References

1. Behl A, Behl K. An analysis of cloud computing security issues. In 2012 world congress on information and communication technologies. IEEE, 2012, 109-114
2. Retrieved from https://cloudsecurityalliance.org/working-groups/top-threats/#_overview
3. Retrieved from https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/security-guidance-v4-FINAL.pdf
4. Khaliq Azzief. Top 5 Tools to Secure Your Business Data on The Cloud. Retrieved from https://www.hongkiat.com/blog/cloud-security-tools/
5. YIGAL Asaf. A Guide to Public Cloud Security Tools, 2015. Retrieved from https://devops.com/guide-public-cloud-security-tools/
6. Vera Security. The State of Enterprise Encryption and How to Improve it, 2019. Retrieved from https://www.datamation.com/cloud-computing/top-cloud-security-solutions.html
7. Balamurugan B, Karuppiah Marimuthu, Soundrapandiyan Rajkumar, Alenezi Mamdouh, Niranchana, R. Is Cloud Secure? International journal of computer sciences and engineering. 2016; 4:126-129.
8. Sethi Srinivas, Sruti Sai. Cloud Security Issues and Challenges, 2018. Retrieved from https://www.igi-global.com/chapter/cloud-security-issues-and-challenges/203498
9. Mukherjee S. Benefits of AWS in Modern Cloud. arXiv preprint ar. 2019; 14:1903.03219.
10. Mukherjee S. Popular SQL Server Database Encryption Choices. arXiv preprint ar. 2019; 14:1901.03179.
11. Mukherjee S. How IT allows E-Participation in Policy-Making Process. arXiv preprint ar. 2019; 14:1903.00831.
12. Mukherjee S. How Stakeholder Engagement Affects IT Projects. International Journal of Innovative Research in Science, Engineering and Technology, 2019, 8(3).
13. Chakraborty, Moonmoon, Excellence Operations. Supply Chain & Inventory Management, 2019. 10.6084/m9.figshare.7824107.
14. Mukherjee Sourav. Overview of the Importance of Corporate Security in business, 2019. 10.15680/IJIRSET.2019.0804002.
15. Mukherjee Sourav. How stakeholder engagement affects IT projects, 2019. 10.15680/IJIRSET.2019.0803265.
16. Chakraborty M. Fog Computing Vs. Cloud Computing. arXiv preprint. 2019; 14:1904.04026.
17. Mukherjee Sourav. SQL Server Development Best Practices. International Journal of Innovative Research in Computer and Communication Engineering, 2019. 10.15680/IJIRSET.2019.0803266.
18. Mukherjee S. Indexes in Microsoft SQL Server. arXiv preprint. 2019; 14:1903.08334.
19. Chakraborty Moonmoon, Planning, Control Systems and Lean Operations in Information Technology, 2019. 10.6084/m9.figshare.7886138.
20. Chakraborty Moonmoon. Managing Risk, Recovery & Project Management, 2019. 10.6084/m9.figshare.7886141.
21. Chakraborty Moonmoon. Operation improvements & quality, 2019.
22. Mukherjee Sourav. Information Governance for the Implementation of Cloud Computing, 2019. 10.6084/m9.figshare.8282192.
23. Mukherjee Sourav. Predictive Analytics and Predictive Modeling in Healthcare, 2019. 10.6084/m9.figshare.8247443.
24. Mukherjee Sourav. The battle between NoSQL Databases and RDBMS, 2019. 10.15680/IJIRSET.2019.0805107.