2020 IEEE International Conference for Innovation in Technology (INOCON)
Bengaluru, India. Nov 6-8, 2020

Cloud Storage Security Risks, Practices and Measures: A Review

Aamir Syed
Department of CSE
Ramaiah Institute of Technology
Bengaluru, India
iapetus333@gmail.com

Keerthana Purushotham
Department of CSE
Ramaiah Institute of Technology
Bengaluru, India
keerthupuru@gmail.com

Ganeshayya Shidaganti
Department of CSE
Ramaiah Institute of Technology
Bengaluru, India
ganeshayyashidaganti@msrit.edu

***Abstract*— The world has seen a quick transition from hard devices for local storage to massive virtual data centers, all possible because of cloud storage technology. This has brought about the advent of transfer and sharing of data between multiple individuals and organizations, making it one of the most commonly used services on the cloud platform. Businesses have grown to be scalable, meeting consumer demands on every turn. However, with massive developments in this field, security and privacy are at the forefront of concerns and needs. Poor data visibility, storage sinks without secured pointers, instances with massive data overflows, etc. are concerns that can cause monetary and information damage to people on a large scale. With this in mind, current data security and advisory methods to monitor data sinks is one of the biggest challenges we face today. This paper aims to look at some of the security concerns and current state of the art implementations to refurbish the same.**

Keywords—Cloud Storage, Cloud Security.

I. INTRODUCTION

Cloud-based internet security is an outsourced solution for storing data. Instead of saving data onto local hard drives, users store data on Internet-connected servers. Data Centers manage these servers to keep the data safe and secure to access. Anytime you access any file that was stored remotely, you are accessing the cloud. How is cloud storage any different from local storage? The primary contrast is that the cloud vendor uses internet for data transfer, from secure data centers to individual devices that the cloud is accessed on. Hence, this makes cloud centralized [1], i.e., can be accessed from anywhere. As is obvious, there are multiple types of clouds. Network Security encompasses three types of clouds – public, private, and hybrid. To understand better, we conservatively define these below.

Cloud computing denotes a computing platform that is outside of an organizations' firewall on shared systems. In this scenario, your cloud service provider is in control of the infrastructure. In contrast, a private cloud is the same platform; however, it is implemented within the corporate firewall, under the control of the organization's IT department.

A private cloud is designed to offer the same features and benefits of public cloud systems, but removes a number of objections to the cloud computing model including control over corporate and customer data, worries about security and issues connected to regulatory compliance [2].

A hybrid cloud platform is a combination of the above two, where high volume data files are kept on the public cloud and the sensitive data is on the private one. This time of platform is a crowd favorite for larger corporations. This approach also gives extensibility in terms of customization.

Cloud Computing Security refers to a plethora of policies, technologies, and controls that are used to protect our data on a cloud. It is a subcategory of cloud security, network security and information security as seen in "Fig. 1". We will be looking at cloud Security Risks in detail in this paper. All the files stored on a cloud platform benefit from state-of-the-art security measures. Advanced Firewalls, Event Logging, Intrusion Detection, Internal Firewalls, and Security are some of the standard cloud security practices.

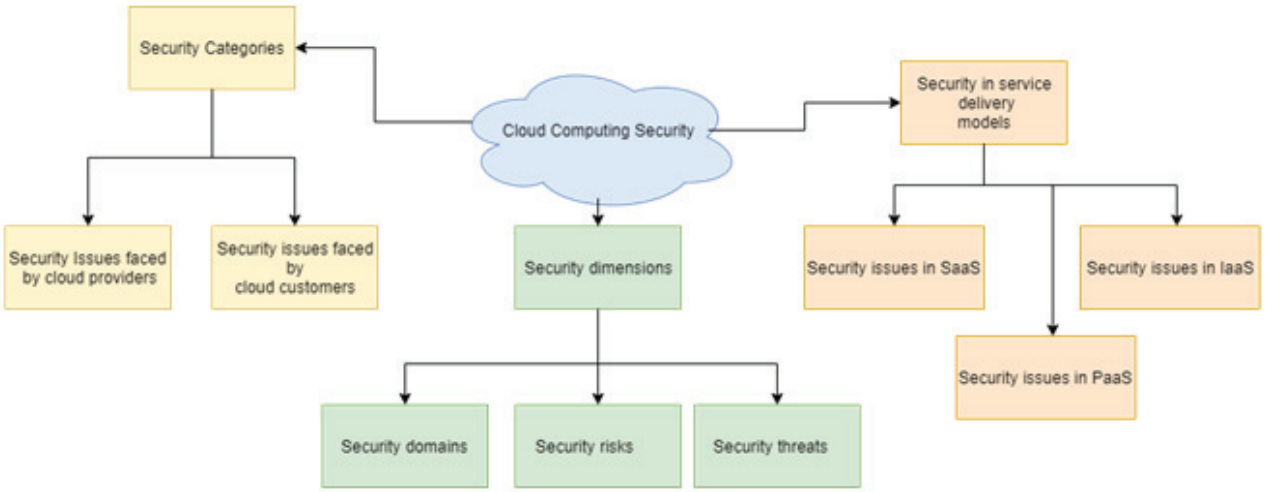

Fig. 1. Cloud Computing Security: A flow diagram of the abstracted hierarchy and types of cloud computing security

978-1-7281-9744-9/20/$31.00 ©2020 IEEE

II. Literature Survey

With the improvement in cloud infrastructure, security issues and standards have been on the rise. To this end, multiple research projects have been conducted to exploit and understand the severity of said threats, if any. Some of the examples can be seen as demonstrated by Zissis et. al. [3].

They focus on user-specific security requirements, on the basis of Trust, Availability, Integrity, etc. among other Security Identification of Threats. They categorize threats under 5 classes/issues, as can be seen from "Fig. 2".

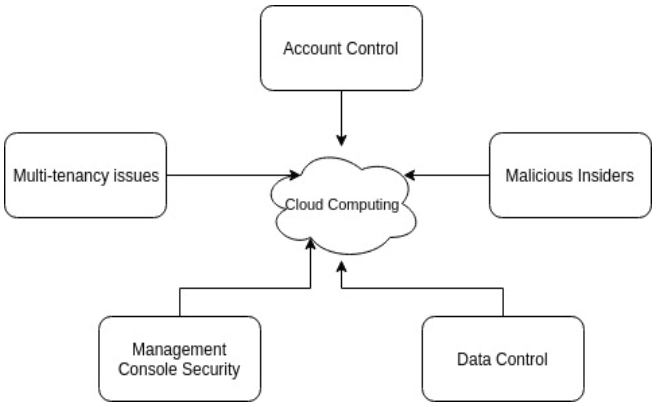

Fig. 2. Five main classes of security identification threats.

There are mainly 5 types of threats:

A. Account Control

Through hijacking, attackers can gain access to sensitive/private information. In cloud environments, the accounts at the highest risk are subscription accounts or cloud service accounts.

B. Malicious Insiders

Since insiders do not have to break through firewalls, VPNs, and other security defences; they operate on a trusted level where they can access networks, data, and systems. A malicious insider would be able to sell/use this information for personal gain or collective loss of the target user(s).

C. Data Control

A data breach can be any attack or incident in which sensitive information is stolen/viewed/used by an unauthorized party. Unsecured data storage containers, excessive permissions, unpatched systems, etc. show lack of data control.

D. Management Console Security

UIs and APIs form the most exposed part of a system. From authentication to access control, these need to be designed to prevent circumventing security.

E. Multi-tenancy Issues

Ensuring data isolation, traffic bandwidth, etc. need to be the primary concern for a cloud service provider. Logical security, trust, access control and encryption of both keys and data is paramount to alleviating this.

The paper also goes in length on Third party trust, establishing authentication, authorization, certificate categories, sharing private keys for portable environments, etc. among other reliability factors of the third party. It concludes that security in cloud computing requires a systemic point of view, with security being built on trust parameters. Data integrity, confidentiality, and trust are the key points of this paper.

Chen et. al. [4] summarizes threat models in cloud computing with 'novel elements'. The paper notably states that along with data and software, activity patterns and business reputation also merit protection. It outlines security issues involving building of covert side channels that are possible due to visibility of shared resources, leading to critical business information, computation, etc. It also puts into view the end user statistic, where a service used may or may not depend on a single third party.

For example, an end user may employ an application built a SaaS provider, which uses a platform by another party, which in turn is run on an infrastructure by an IaaS provider. Hence, longer trust chains need to be accommodated. "Fig. 3" shows the dependency for such a case.

Other interesting point of note raised is the Multics security design principles for building protected subsystems. It also divulges into security defaults on the part of providers, since often times they would be better connected with the security aspect. Isolation, side channels, longer trust chains, mutual auditability, and multics security design were the key elements of this paper.

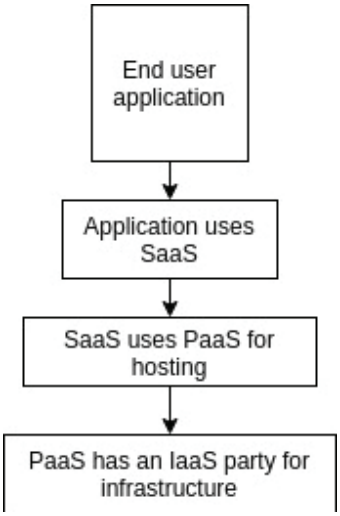

Fig. 3. Hierarchical representation of third party dependence

Rao et. al [5] focus on Data Security Challenges, going over a 9 factor design for the same. Data leak prevention is considered the most important factor under critical and very important challenges, topping at an 88%. Data Segregation and Protection also raise a 92% impact concern for challenges in data security. Security on the basis of authentication, intimation of server locality, data integrity w.r.t. ACID properties, encryption based access, and awareness about data storage for confidentiality form five of the nine factors. The other four factors comprise of Breaches, Segregation, Storage, and Data Center Operation; with accidental transmission issues / insider attacks, data segregation detection via SQL injections, physical infrastructure for virtual machines, and data loss due to bottlenecks are outlined respectively as issues for the above four factors. Information security via Encryption and using RSA based data integrity checks are proposed as solutions to the challenges in data security.

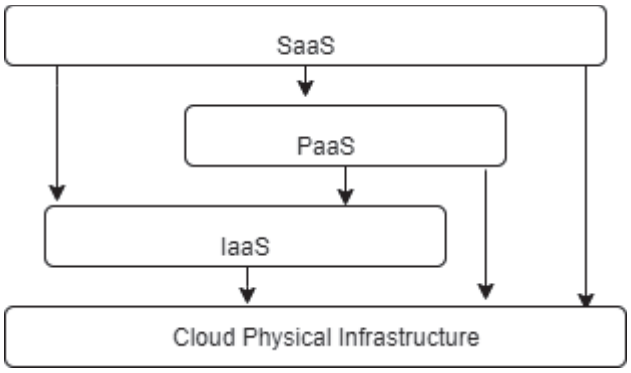

Fig. 4. Fig shows how multiple service delivery models could be connected and contingent on a particular cloud infrastructure.

Security Management in different delivery models is complicated due to multiple implementations [6]. Developing a standard, standalone security model hence becomes convoluted, and inefficient. Moreover, security management becomes complicated since multiple service delivery models may coexist in the same cloud platform as seen in "Fig. 4". Two key characteristics of the cloud computing model are stated to be elasticity and multi-tenancy. The paper discusses elasticity at length, where elasticity implies scaling of resources assigned to services based on current demand. Placement engines for resource management under elasticity for efficient utilization of resources are employed for security constraints. The idea of secure multi-tenancy is delivered through isolation and location transparency to avoid attacks focused on locating victim assets. Dependency stack is lightly touched upon to give an idea about model layers in cloud computing, and the paper divulges into security issues in IaaS, PaaS, and SaaS. It concludes with key points in the area of Security, Multi-Tenancy, and Security Management. Solutions on the various above points are proposed, including holistic security wrappers, integration support, adaptive environment changes, etc.

Over a trend of issues in the papers stated above, we can summarize risks and practices to avoid them. These are discussed under the respective subtopics.

III. SECURITY RISKS

Storage in particular seems like the most attractive use of the cloud platform, since it eliminates the cost of the physical hardware required. Also, extensible memory and on-demand remote access makes it a very useful feature for individuals and organizations alike. But depending on the cloud framework, the security measures that protect your data come in various designs.

A. Lack of Control

On one hand, you won't have to manage your data, on the other, your data on the cloud is managed by someone else. This lack of control over your data storage means that anything impacting your vendor's storage capabilities inhibits your access to data as well. This is one of the biggest risks in cloud storage - being locked out of your own storage platform. Choosing a safe and secure vendor is hence, very important.

B. Shared Servers

Cloud based storage systems make use of on-site servers to hold data, and servers hold data from multiple users. While users cannot directly access these servers, the type of data shared on the server might cause potential risks. Anomalous data uploads can also be a security threat, if your data is shared on the same server [7].

C. Data Leakage

Making sure no unauthorized user can access your organization's data is one part of security, making sure your data is not sent to anyone outside your organization (without due diligence in checks, etc.) is another. Data Leakage could expose sensitive and private data to external sources. Even if data security practices are in place inside the organisation, the cloud counterpart largely depends on the storage providers security measures.

D. API and Storage Sinks

Cloud migration is a tedious process, and is often eased by using the cloud's storage APIs and storage gateways. However, these tools are a middleware service from the user to the platform, making this a potential security breach point. An unsecured API or gateway can cause data leaks, so choose only services that have strong encompassing security during data transit as well.

As is common practice, educating the users on share-ability of data, use and access rules, device configurations and security mapping is a given. However, mitigating cloud security issues is virtually impossible. Staying vigilant and setting in place some security practices is a better transition towards safe storage. We now take a look at some standard practices to ensure safe and secure cloud storage.

IV. SECURITY PRACTICES

It is vital to establish a cloud storage framework with these practices –

A. Assessing cloud framework

All organizations are required to monitor connected devices, update current accessible devices, and remove old / unused devices to protect against unauthorized access. Mapping data flows across systems, applications, and devices will allow greater scrutiny of the cloud usage. Many cloud services allow for services to ease this.

B. Security Encryption

A fundamental requirement of any cloud storage platform is to understand how data is protected (especially in a transit between data centers, servers, etc.). Robust user management and machine intelligent algorithms to check geo-locations and IP addresses of accesses make for additional security. Learned filters about regular areas of access and showing the same in event logging adds a layer of abstraction for the cloud engineer monitoring services as well.

C. Data Classification

All data stored on the cloud is not the same in terms of importance and sensitivity. Keeping classification methods to segregate data [8] can help keep data more secure, notifying users to store something on-device rather than cloud/drive storage. This is especially important when corporations use voluminous hybrid clouds, and have unstructured data lying around.

D. Multi Factor authentication

Cloud security, more often than not, is jeopardized by irresponsible usage of devices. This includes keeping older

and unnecessary devices connected to the cloud, which can be accessed by someone who is unauthorized to. Adding security in terms of multifactor authentication across all systems and applications allows for safer data storage.

V. Advanced Security Measures

What we have seen so far are standard security practices. However, while dealing with sensitive data and business-centric information, no amount of security is enough. Tweaking security measures and adding more check mechanisms at every turn makes for a more dedicated safe storage platform. Here are some of the advanced security measures such a platform would employ-

A. Private Encryption

Also known as Zero Knowledge, it prevents anyone but yourself from reading your data. The encryption key is unique and is available only to you, not even your cloud vendor. As such, in the event of data leak / breach [9], no harm can come from any sensitive data. However, there is a downside to using such an encryption - if you lose the password key for the data, it is lost forever. A zero-knowledge service does not manage or reset passwords [10].

B. In-Transit Encryption

The latest encryption available is AES, which is also the most secure encryption algorithm to date. It has varying levels of security depending on the key length. The 256-bit encryption is the most secure version known, and has zero cracked instances. However, this is used for at-rest data, not in transit [11]. Cloud data in transit uses the TLS protocol to protect from eavesdropping, via a handshake between machines using ciphers, authentication, and key exchanges [12].

C. Ransomware Protection

While encryption is desired, it is only so when you have the cipher to it. Ransomware finds sensitive data files and encrypts them, locking you out of your own data. A decryption key is required to gain access to data, and is a gamble even if the culprit is compensated monetarily. A scanning service that employs machine intelligence to learn flow and data accesses can potentially help become an AI solution for ransomware detection. Current standard practice is to use 'versioning', a roll-back that allows for cloud's variant of version control.

Naturally, the question arises - what services adhere to such strict security norms? Proper content control, permission and access scrutiny, etc. are afforded by some of the relatively new services. Modern services like Sync.com allow zero-knowledge encryption for no added cost, and have gained popularity for exceptional security measures. pCloud is yet another such cloud platform for storage, while some confirm to Dropbox as an established mainstream solution.

VI. Conclusion

Cloud services are used widely by large corporations, but even independent organizations and small scale businesses have migrated to cloud platforms in recent times. This makes security an utmost concern, and is a forefront in digital data protection. As such, cloud computing is still not mature and needs a boost in research based applications for security. Security is the responsibility of both - vendors, and users. It is a threat that needs to be handled by both the service providers and clients, both maintaining security protocols on their end. Data visibility should be monitored by the vendor services, while data abstraction and uses should be an intra-organizational security measure. Clouds should comply with industry standards for accepted GRC (governance, risk, and compliance) practices. Achieving end-to-end security is almost impossible due to the complex structure of the cloud, but securing data and encryption standards at every possible turn mitigates many risks pertaining to shared data.

Acknowledgment

The authors wish to thank the Department of Computer Science and Engineering, the Principal and the Management of Ramaiah Institute of Technology, Bengaluru for providing us the required facilities and support to carry out our research work.

References

[1] Mladen A. Vouch, ―Cloud Computing Issues, Research and Implementations‖, Journal of Computing and Information Technology - CIT 16, 2008, 4, 235–246

[2] Rongxing et al, ―Secure Provenance: The Essential Bread and Butter of Data Forensics in Cloud Computing‖, ASIACCS‘10, Beijing, China.

[3] D. Zissis et al, - Addressing Cloud Computing Security Issues, Future Generation Systems 2012, Pages 583-592.

[4] Chen et. al, - What’s New About Cloud Computing?, Technical Report no. UCB/EECS-2010-5, University of California at Berkeley, 2010.

[5] Rao et. al, - Data Security Challenges and Its Solutions in Cloud Computing, ICCC 2015, Procedia Computer Science 48 (2015), Pages 204-209.

[6] Mohammad et. al., - An Analysis of the Cloud Computing Security Problem, 2016, Swinburne University of Technology, Hawthorn, Victoria - Australia.

[7] R. La‘Quata Sumter, ―Cloud Computing: Security Risk Classification‖, ACMSE 2010, Oxford, USA.

[8] Wenchaoet al, ―Towards a Data-centric View of Cloud Security‖, CloudDB 2010, Toronto, Canada

[9] Soren Bleikertz et al, ―Security Audits of Multi-tier Virtual Infrastructures in Public Infrastructure Clouds‖, CCSW 2010, Chicago, USA.

[10] Miranda & Siani, ―A Client-Based Privacy Manager for Cloud Computing‖, COMSWARE‘09, 2009, Dublin, Ireland

[11] Dan Lin & Anna Squicciarini, ―Data Protection Models for Service Provisioning in the Cloud‖, SACMAT‘10, 2010, Pittsburgh, Pennsylvania, USA

[12] Rabi et. al, ―Cloud Computing: Security Issues and Research Challenges, IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS) Vol. 1, No. 2, December 2011