Security Issues with Cloud Computing

Trimuke Digambar[1]

[1]*Senior Scale Lecturer, Department of Computer science and Engineering, Government Women's Polytechnic Kalaburagi, India.*

ABSTRACT

The term "cloud computing" refers to an approach to IT that allows users to access shared resources including networks, storage, servers, applications, and services over the internet on an as-needed basis and pay for what they use. Therefore, it helps firms save time and money on controlling costs. Banking, healthcare, and education are just a few of the many industries making the switch to cloud computing. This is mostly due to the cost-effectiveness of the services offered by the cloud, which are based on a pay-per-use model that takes into account resources and transactions. In cloud computing, clients' data is kept and maintained in the data center of a cloud provider, such as Google, Amazon, Salesforce.com, Microsoft, etc., and the technology relies entirely on the internet. A number of security risks and challenges, including as data leakage, insecure interfaces, resource sharing, data availability, and insider assaults, may arise from a lack of control over the data. A number of research obstacles exist when it comes to cloud computing adoption, including privacy, interoperability, and reliability, as well as well-managed service level agreements (SLAs). Cloud computing, its architecture, the many cloud models, and the primary security threats and challenges in the cloud computing industry are all defined and discussed in this research study. Included in this study is a discussion of best practices for service providers and businesses looking to use cloud computing to boost their bottom line amid the current economic downturn.

Keywords: Security Issues, Cloud Security, Cloud Architecture, Data Protection, Cloud Platform, Data Security, virtual memory.

I. INTRODUCTION

One of the most recent technological developments is cloud computing. On the basis of utility and use of computational resources, it is a metaphor or lexicon that has been developed in the field of computing. The term "cloud computing" refers to a method of storing and retrieving data and other resources via the interconnection of many distant servers and computer programs. This computing architecture involves connecting a large number of devices across private or public networks. The goal is to provide a cheap, highly scalable infrastructure for applications, data, and file storage.

The major milestones of Cloud computing

Quickness: It gets back up and running when users are able to re-provision resources in the technical infrastructure.

Capital: Claimed savings from cloud service providers. Operating expenses are transformed into capital expenditures in a public-cloud approach. This is designed to make it easier to get in, as third-party infrastructure is usually already in place, so there's no need to buy it for occasional or one-off demanding computing jobs.

This feature allows users to access systems via web browsers regardless of their location or the device they are using, such as a PC or mobile phone. Because the infrastructure is often hosted by a third party and accessible over the Internet, users have the freedom to join from any location.

Because they don't need to be installed on every user's computer and may be accessed from different locations, cloud computing apps are simpler to maintain.

By allowing many users to share the same resources and costs, multitenancy improves efficiency, increases peak-load capacity, and allows for the centralization of infrastructure in cheaper locations (e.g., real estate, electricity, etc.).

Productivity: Instead of waiting for data to be stored and sent by email, it might be enhanced when several users can access the same data simultaneously. Users may save time and avoid installing application software updates by not having to re-enter information when fields are matched.

Credibility: It becomes even more suitable for business continuity and disaster recovery when numerous redundant locations are used, which is achieved with well-designed cloud computing.

Centralization of data, improved security-based resources, etc., may all contribute to greater security, but worries about losing control of sensitive data and stored kernels remain.

1. **Service Models or cloud architecture:** Services offered by cloud providers can be grouped into three categories.

- Software as a service(SaaS)
- Platform as a service (PaaS)
- Infrastructure as a service (IaaS).

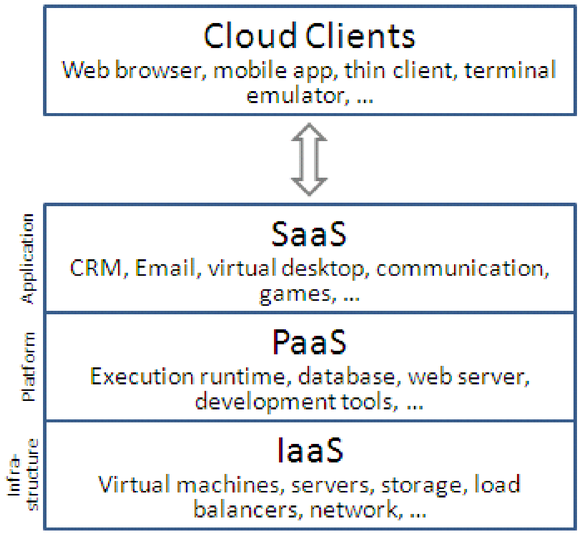
Cloud Clients
Web browser, mobile app, thin client, terminal emulator, ...
Application
SaaS
CRM, Email, virtual desktop, communication, games, ...
Platform
PaaS
Execution runtime, database, web server, development tools, ...
Infra-structure
IaaS
Virtual machines, servers, storage, load balancers, network, ...

Fig.1 Cloud Architecture

2. **Deployment model:** Deployment models offered by cloud providers can be grouped into four categories:

- Public Cloud
- Private Cloud
- Community Cloud
- Hybrid Cloud

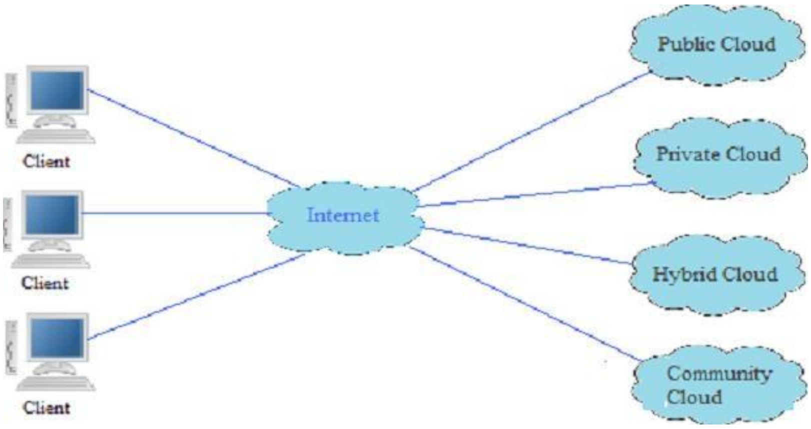

Fig.2 Cloud Deployment model

The private cloud, according to IBM's JitheshMoothoor and Vasvi Bhat, is best suited for organizations like governments and associations who want more oversight of their data and applications than what is provided by publicly available cloud services. The services, data, and applications in a private cloud are managed by the client, and the cloud is specifically designed for their usage. Typically, these clouds are set up behind the association's firewall, so that only authorized personnel inside the organization may access them. The advantage of a private cloud is the increased elasticity and adaptability of the cloud computing platform. Customers who choose for private cloud services are able to better manage and protect their data while still meeting all applicable regulations and standards.

Hosting for public clouds is often done by other parties other than the actual customers' facilities. In most cases, the customer has no idea where exactly the public cloud they are using is located. When it comes to public clouds, anybody may join up and utilize them. A "public cloud" is a cloud that filters its services via a publicly accessible network. You may either get its services for free or pay for them as you go. Customers may buy or rent a private connection to a peering point given by the cloud provider for direct connect services like "AWS Direct Connect" from AWS and "Azure ExpressRoute" from Microsoft.

Similar to a private cloud, a community cloud allows several companies with comparable security, privacy, and regulatory concerns to share resources. Many businesses or government organizations with shared interests, such as shared security requirements or long-term objectives, work together to run and utilize a community cloud. The community cloud restricts access to its resources, data, and applications to its members alone.

A hybrid cloud combines the best features of several deployment models by combining two or more separate clouds, which might be public, community, or private. The capacity to integrate cloud resources with association, managed, or dedicated services is another definition of hybrid cloud. The multitenant nature, reduced development time, and cheap cost of the hybrid cloud computing paradigm make it attractive to numerous governments and corporations. Public clouds pose a significant security risk due to their public nature; under this model, the vendor, not the client, retains control of the cloud, which is a major concern for governments and other organizations considering public cloud adoption.

3. Security of data on Cloud

Client data is kept and maintained in the data centers of a cloud provider, such as Google, Amazon, Salesforce.com, Microsoft, etc. Limited, in cloud computing, an internet-dependent technology. Since the machines used to provide services are unrelated to the consumers, cloud computing security becomes an extremely problematic issue. Users are unaware of the potential consequences for their data and lack control over the situation. If consumers have sensitive or important data saved in a cloud service, this should be a major red flag. Cloud computing service providers have a responsibility to guarantee the security of their customers' data since users value their privacy and do not want it compromised. Data security is becoming more of a challenge as time goes on. It seems like someone will always find a method to circumvent security measures and exploit user information. [18] in The security risks with cloud computing are now known to certain companies. The mission of the non-profit organization known as the Cloud Security Alliance is to educate the public about the benefits of cloud computing for data security and to advocate for industry standards for cloud computing security. [18] Another group concerned with security is the Open Security Architecture (OSA). They suggest the OSA pattern as a way to try to show the fundamental activities of the cloud, the important parts played by different internal organizations in terms of supervision and risk mitigation, the controls that need more attention, and so on.

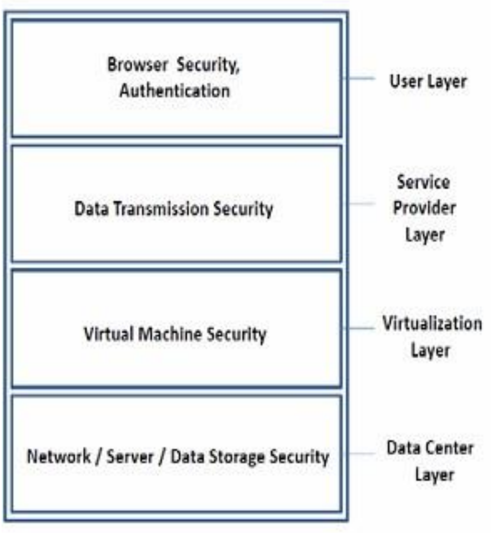
Browser Security, Authentication
User Layer
Data Transmission Security
Service Provider Layer
Virtual Machine Security
Virtualization Layer
Network / Server / Data Storage Security
Data Center Layer

Fig. 3. High Level Security Architecture

- Access to Servers & Applications
- Data Transmission
- Virtual Machine Security
- Network Security
- Data Security
- Data Privacy
- Data Integrity
- Data Location
- Data Availability

Access to Servers & Applications

Access control mechanisms ensure that only authorized users can access servers and applications. Multi-factor authentication (MFA), role-based access control (RBAC), and encryption help protect sensitive data and prevent unauthorized intrusions.

Data Transmission

Data transmission security ensures data is protected while being transferred between systems. Encryption protocols such as TLS/SSL, VPNs, and secure file transfer methods like SFTP help prevent data interception and unauthorized access.

Virtual Machine Security

Virtual machines (VMs) require security measures such as hypervisor protection, regular patching, and isolation from other VMs. Using hardened VM images, monitoring for vulnerabilities, and restricting access helps mitigate threats like VM escape attacks.

Network Security

Network security safeguards infrastructure from cyber threats using firewalls, intrusion detection and prevention systems (IDS/IPS), and network segmentation. Secure access is maintained through VPNs, zero-trust architecture, and encrypted communications.

Data Security

Data security involves protecting stored and processed data from breaches, unauthorized access, and corruption. Techniques such as encryption, access control, data masking, and regular security audits help maintain confidentiality and integrity.

Data Privacy

Data privacy ensures compliance with regulations like GDPR and HIPAA by controlling how personal and sensitive information is collected, stored, and shared. Implementing privacy policies, user consent management, and anonymization techniques helps protect user data.

Data Integrity

Data integrity ensures that information remains accurate, consistent, and unaltered throughout its lifecycle. Hashing, checksums, digital signatures, and regular backups help detect and prevent unauthorized modifications or corruption.

Data Location

Data location refers to where data is stored, which impacts compliance with legal and regulatory requirements. Organizations must ensure data residency laws are met by using geo-fencing, cloud region selection, and secure data storage policies.

Data Availability

Data availability ensures that data is accessible whenever needed, minimizing downtime and disruptions. High-availability architectures, redundant storage, disaster recovery plans, and load balancing help maintain continuous access to critical data.

CONCLUSION

Sharing resources is a major cause for worry when it comes to cloud computing security. Cloud service providers have an obligation to inform their clients about the security measures they take on their cloud. We began by going over the different cloud computing models, then moved on to cloud computing architecture, and then covered cloud computing security challenges. Cloud computing has a big problem with data security. Data stored in the cloud is often append-only with infrequent updates, and it might be extremely big, unstructured, or partially organized. An important aspect of cloud computing is the administration and security of data stored in the cloud. The onus for complete data security is on the infrastructure provider, since service providers seldom have access to data centers' physical security systems. Network and virtualization security are two of many more issues. With an emphasis on how data security on the cloud may improve, this study has brought attention to all of these problems with cloud computing.

Future Scope

Obtaining end-to-end security is very challenging due of the cloud's complexity. Improved security will need the creation of new security measures and the drastic simplification of existing ones to conform to the architecture of the cloud. Cloud computing is still in its infancy as a technology, therefore many questions remain unanswered and new problems arise from its use in many fields. Cloud data encryption, service level agreements (SLAs), interoperability, energy management, multitenancy, common cloud standards, reliability and availability of service, and migration of virtual machines are among the difficult research issues in cloud computing. Since the development of cloud computing is in its infancy, we hope that our study will shed light on the difficulties inherent in cloud computing's architecture and pave the way for future studies in this field.

REFERENCES

1. Vecchiola, X. Chu, and R. Buyya(2009) Aneka: A Software Platform for .NET-based Cloud Computing. High Speed and Large Scale Scientific Computing, pp267-295, W. Gentzsch, L. Grandinetti, G. Joubert (Eds.), ISBN: 978-1-60750-073-5, IOS Press, Amsterdam, Netherlands, 2009.
2. David C. Wyld, (2010), The cloudy future of the Government IT: Cloud Computing and the
   Public Sector around the World. Available:
   http://airccse.org/journal/ijwest/papers/0101w1.pdf
3. Garg, S.K., Venugopal, S., and Buyya, R.(2008): A Meta-scheduler with Auction Based Resource Allocation for Global Grids, *Proceedings of the 14th IEEE International Conference on Parallel and Distributed Systems*, IEEE CS Press, Los Alamitos, USA, 2008.
4. IBM Sales and Distribution, Thought Leadership White Paper, (2013), Cloud computing for banking Driving business model transformation.
5. Munich, Gerald Kaefer G., (2010), Cloud Computing Architecture, Siemens, *Corporate Research and Technologies*, SATURN 2010
6. Pollan, Michael et al., The Omnivore„s Dilemma: A Natural History of Four Meals. New York: Penguin, 2006.
7. Yigitbasi N., Iosup A., Epema D. &Ostermann S.,(2009), C-Meter: A Framework for Performance Analysis of Computing Clouds, *9th IEEE/ACM International Symposium on Cluster Computing and the Grid*, DOI 10.1109/CCGRID.2009.40