International Journal of Advanced Research in Engineering and Applied Sciences
ISSN: 2278-6252

ANALYSIS OF SECURITY THREATS AND PREVENTION IN CLOUD STORAGE: REVIEW REPORT

Prakash Kuppuswamy*

Saeed Q Y Al-Khalidi**

Abstract: *The term "cloud" is used as a representation of the Internet and other communications systems as well as an abstraction of the underlying infrastructures involved. It is a model for enabling global, convenient, on-demand network access to a shared pool of configurable computing resources. Cloud computing is a disruptive technology that has the potential to enhance collaboration, agility, scaling and availability and provides the opportunities for cost reduction through optimized and efficient computing. Data resting in the cloud needs to be accessible only by those authorized to do so, making it critical to both restrict and monitor who will be accessing the company's data through the cloud. In order to ensure the integrity of user authentication, companies need to be able to view data access logs and audit trails to verify that only authorized users are accessing the data. This paper discussed about security threats and prevention methodology of cloud computing storage.*

Key words**:** *Cloud storage, Cloud security, Cloud threats, Malicious attacker etc*.

*Lecturer, Computer Engineering & Networks Department, Jazan University, KSA.

**Dean, Deanship of Libraries Affairs, King Khalid University, KSA

I INTRODUCTION

Cloud Computing is a technology that uses the internet and central remote servers to maintain data and applications. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. This technology allows for much more efficient computing by centralizing data storage, processing and bandwidth [1].

In 1997, Professor Ramnath Chellapa of Emory University and the University of South California defined cloud computing as the new "computing paradigm where the boundaries of computing will be determined by economic rationale rather than technical limits alone". This has become the basis of what we refer to today when we discuss the concept of cloud computing [1].

Amazon was the first major organization to modernize its data centers, which were utilizing only about 10% of their capacity at any given time Amazon realized that the new cloud computing infrastructure model could allow them to use their existing capacity with much greater efficiency.Meanwhile, Google had become a key player in the Internet commerce marketplace. In 2006 the company launched its Google Docs services, which brought the power of cloud computing and document sharing directly to end users [1].

2005 was also a noteworthy year for cloud computing in the hedge fund industry as Eze Castle Integration built and deployed the first hosted cloud platform at a large hedge fund. Over the next year, 18 hedge fund spinouts moved to the hosted platform. In 2008, Eze Castle opened its hedge fund hotel in New York City that combined a cloud computing environment with fully managed office suites. The cloud environment supported 200+ users and was the early foundation for what today is the Eze Private Cloud.In 2009, Eze Castle productized its cloud infrastructure and officially launched the Eze Private Cloud, delivering a fully-hosted IT platform for all hedge funds. By 2010 more than 30 applications were running in the Eze Private Cloud. Today over 60 applications run in the Eze Private Cloud [1]. Present days cloud reaching nearly a petabyte of data, expanding to data centers in London and San Francisco and supporting over 130 hedge funds.In 2013, Cloud user reaches more than 2,500.The benefits of the cloud storage were as follows

- Optimized server utilization
- Cost saving

- Dynamic scalability
- Shortened development life cycle
- Reduced time for implementation[4]

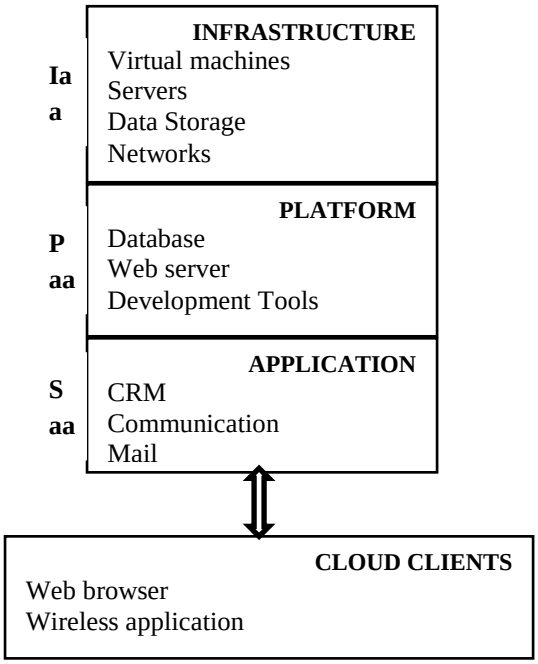

Figure 1. General structure of cloud computing

A) Infrastructure

Infrastructure as a Service is a provision model in which an organization outsources the equipment used to support operations, including storage, hardware, servers and networking components. It differs from a traditional data storage infrastructure in that it accesses files remotely over a network and is usually built on an object-based storage platform. Access to object-based storage is done through a Web services application programming interface based on the Simple Object Access Protocol.

B) Platform

Platform as a Service (PaaS) is a way to rent hardware, operating systems, storage and network capacity over the Internet. The service delivery model allows the customer to rent virtualized servers and associated services for running existing applications or developing and testing new ones.Platform as a Service (PaaS) is an outgrowth of Software as a Service (SaaS), a software distribution model in which hosted software applications are made available to customers over the Internet.

C) Application

A cloud application is an application program that functions in the cloud, with some characteristics of a pure desktop app and some characteristics of a pure Web app. A desktop app resides entirely on a single device at the user's location. A Web app is stored entirely on a remote server and is delivered over the Internet through a browser interface.

D) Cloud Clients

Users access cloud computing using networked client devices, such as desktop computers, laptops, tablets and smartphones. Some of these devices – cloud clients – rely on cloud computing for all or a majority of their applications so as to be essentially useless without it. Many cloud applications do not require specific software on the client and instead use a web browser to interact with the cloud application. Some cloud applications, however, support specific client software dedicated to these applications.

II LITERATURE REVIEW

L. Arockiam, S. Monikandan (2013) discussed reliable and flexible to users to store and retrieve their data at anytime and anywhere. It is an increasingly growing technology. Nowadays, many enterprises have started using cloud storage due to its advantages. Even though the cloud continues to gain popularity in usability and attraction, the problems lie in data security, data privacy and other data protection issues. Security and privacy of data stored in the cloud are major setbacks in the field of Cloud Computing. Security and privacy are the key issues for cloud storage [2].

Sanjoli Singla & Jasmeet Singh (2013) analyzed Cloud computing technology where users can remotely store their data into the cloud to enjoy high quality application and services. Cloud being the most vulnerable next generation architecture consist of two major design elements i.e. the Cloud Service Provider(CSP) and the Client. Even though the cloud computing is promising and efficient, there are many challenges for data privacy and security. This paper explores the security of data at rest as well as security of data while moving [3].

Bhawana (2013) discussed Secure and efficient data transfer is essential in many business sectors. To ensure the security to the applications of business, the business sectors use Public Key Cryptographic Systems. The public key cryptography solves one of the most vexing problems of all prior cryptography: the necessity of establishing a secure channel for

the exchange of the key. This paper has an introduction which includes encryption and decryption using RSA and Cryptographic challenges with issues such as key distribution and speed of RSA [4].

Gurpreet Kaur, Manish Mahajan (2013)This paper analyze the performance of security algorithms, namely, AES, DES, BLOWFISH, RSA and MD5 on single system and cloud network for different inputs. These algorithms are compared based on two parameters, namely, Mean time and Speed-up ratio [5].

III CHALLENGES OF CLOUD COMPUTING

Malicious insiders: The threat of malicious insiders is increased for users of cloud services because of the convergence of IT services and clients under a single management provider. Cloud users often do not have visibility into how a provider grants employees access to physical and virtual resources, how it hires and monitors employees and how it handles policy compliance.

Shared technology issues: At the heart of cloud computing is the premise of sharing underlying infrastructure components. If security requirements and protocols are not integrated into the shared infrastructure at multiple levels (i.e. computing resources, storage, and networking) then vulnerabilities could exist. This is particularly crucial to keep in mind when evaluating public cloud environments, through which there can be limited isolation.

Data loss or leakage: This is a real, yet unacceptable risk for any investment management firm, and the impact is far-reaching. Just as with traditional on-premise environments, threats in the cloud can include accidental deletion of data, unauthorized access or database corruption. It is essential to have strong controls in place, as well as data encryption and data protection processes.

Unknown risk profile: Another threat, which may cause a firm to accept unknown risks, is lack of knowledge of a cloud provider's security protocols and policies. It is important to inquire about a cloud service provider's security software, update and patch procedures, intrusion detection and alerting and overall security design.

IV PREVENTING STRUCTURE OF CLOUD COMPUTING

Proper security in a cloud environment requires specialized practices and processes at both the physical and virtualization levels. Following are some key features to look for when evaluating a cloud servicesprovider.

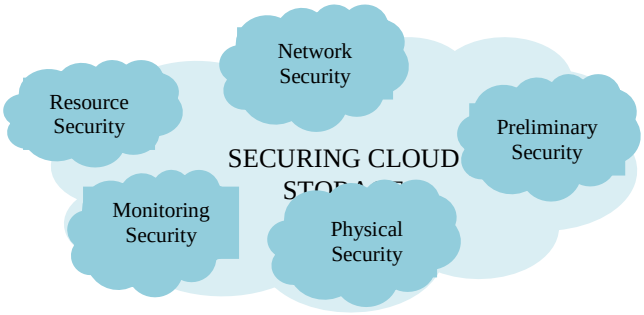

Figure 2. Security infrastructure of cloud Storage

A. Preliminary security

Finally, since we can all use a refresher from time-to-time, here are six fundamental security practices that firms should follow whether using on-premise infrastructure or a cloud service.

- Passwords are essential, but simply having one isn't enough.
- Create strong passwords.
- Remember to lock the doors.
- Laptops are easy prey.
- Add local security measures.
- PDAs need protection too.

B. Physical Security & Infrastructure

In what is sometimes known as a multi-tenant environment, cloud subscribers share the same underlying infrastructure, databases or applications. In public cloud environments, multi-tenancy can pose a security risk if proper isolation measures are not put into place to securely separate data and resources. If you're looking for more security through a private cloud, be sure to look for these requirements

- Availability
- Secure Separation
- Service Assurance
- Management and Monitoring

- Two-phase authentication of visitors (card and biometric)
- Secured access doors and elevator banks
- Monitored security cameras
- Additional door, motion and camera sensors
- Visitor logs for cages
- Key-locked cages and cabinets

C. Monitoring security

- Monitoring
- Security Management, including templates and standardization
- Infrastructure security
- Management security
- Incident response and forensics
- Legal issues, such as compliance, data protection, and SLAs

D. Resource pooling security

With each pooled resource, you must ensure that each tenant's data or applications are kept partitioned from those belonging to other tenants. Any data that is exclusively owned by a consumer should not leak to other sessions nor be accessible by other users or tenants, whether maliciously or not. Partitioning and Role Based Access Control (RBAC) also applies to your administrators, who should not have automatic access to tenant data. In the case where an administrator does require access to tenant data, then that access must be carefully audited.

- Virtualization
- Multi-Tenancy
- Infrastructure security
- Platform security
- Software security
- Data protection
- Service Level Agreements (SLAs)

E. Network infrastructure security

The broad network access cloud characteristic requires IT departments to consider the entirety of the client to service network journey. It is also requires consideration of the

effect of this requirement for universal access on management of the environment. Just as consumers need to access the cloud services from anywhere, so do providers. Coping with broad network access requires consideration of the following factors

- Perimeter network role and location
- Identity and Access Management (IdAM)
- Authentication
- Authorization
- Role-based access control (RBAC)
- Federation
- Auditing
- Public network connectivity
- Service delivery security
- Endpoint protection
- Connectivity to software, platform, and infrastructure layers
- Client security

V CONCLUSION

This paper highlighted how important it is to ensure that information within the Cloud environment is to be secure. We have discussed need of securing Cloud storage systems, basic security requirements of a Cloud computing, some of the possible attacks on the Cloud Storage systems and counter measures to deal with these attacks. The future scope of our work is to both protect the active attacks and passive attacks by designing and implementing new strategy plan of cloud architecture.Proposed paper produce many key findings such as cloud infrastructure equipment failure, backup and retention procedures, type of security and monitoring, Service Level Agreements infrastructure and applications, security breach, preventing data, virtualization application etc.,

REFERENCES

1. John Rhoton, “Cloud Computing Explained: Implementation Handbook for Enterprises”, 2013.
2. L. Arockiam, S. Monikandan, “Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm”, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue 8, August 2013.

3. SanjoliSingla&Jasmeet Singh, "Survey on Enhancing Cloud Data Security using EAP with Rijndael Encryption Algorithm", Global Journal of Computer Science and Technology Software & Data Engineering, Volume 13 Issue 5 Version 1.0 Year 2013.
4. Bhawana ,"An overview and Cryptographic Challenges of RSA", International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-2, Issue-3).
5. GurpreetKaur, Manish Mahajan, "Analyzing Data Security for Cloud Computing Using Cryptographic Algorithms", Int. Journal of Engineering Research and Application, ISSN : 2248-9622, Vol. 3, Issue 5, pp.782-786,Sep-Oct 2013.
6. Ignacio M. Liorente, "An Introduction to Virtualization and Cloud Technologies to Support Grid Computing, New Paradigms", Virtualization and Co. EGEE08, Istanbul, September 25, 2008.
7. M. Li, S. Yu, K. Ren, and W. Lou. "Securing personal health records in cloud computing: Patient-centric and ne-grained data access control in multi-owner settings", In Security and Privacy in Communication Networks. Springer, 2010.
8. N. Liu, Y. Zhou, X. Niu, and Y. Yang,"Querying encrypted character data in DAS model", In Proceedings of the 2nd International Conference on Networking and Digital Society (ICNDS), May 2010.
9. K. Mandl, W. Simons, W. Crawford, and J. Abbett. Indivo, "A personally controlled health record for health information exchange and communication", BMC Medical Informatics and Decision Making, 2007.
10. Mohan, D. Bauer, D. M. Blough, M. Ahamad, R. Krishnan, L. Liu, D. Mashima, and B. Palanisamy, "A patient-centric, attribute-based, source-variable framework for health record sharing. Technical report", Georgia Institute of Technology, 2009.
11. S. Narayan, M. Gagne, and R. Safavi-Naini,"Privacy preserving EHR system using attribute-based infrastructure", In Proceedings of ACM Cloud Computing Security Workshop, 2010.
12. Sahai and B. Waters,"Fuzzy identity-based encryption", In Proceedings of Advances in Cryptology –Eurocrypt, Springer, May 2005.

ABOUT THE AUTHORS

PrakashKuppuswamy, Lecturer, Computer Engineering & Networks Department in Jazan University, KSA He is research Scholar-Doctorate Degree yet to be awarded by 'Dravidian University'. He has published 15 International Research journals/Technical papers and participated in many international conferences in Rep. of Maldives, Libya and Ethiopia. His research area includes Cryptography, Bio-informatics and Network algorithms.

Dr. Saeed Q. Y. Al-Khalidi, Dean, Deanship of Libraries Affairs at King KhalidUniversity, Abha. KSA. He published many National & International papers, Journals. Also, he participated as a Reviewer in many international conferences worldwide. He completed Master Degree and Doctor of Philosophy in University of East Anglia. His research interests include: Information System development, approaches to systems analysis and the early stages of systems development process, IT/IS evaluation practices, E-readiness assessment.