International Journal of Advanced Research in Engineering and Technology (IJARET)
Volume 11, Issue 7, July 2020, pp. 622-628, Article ID: IJARET_11_07_062
Available online athttp://www.iaeme.com/IJARET/issues.asp?JType=IJARET&VType=11&IType=7
ISSN Print: 0976-6480 and ISSN Online: 0976-6499
DOI: 10.34218/IJARET.11.7.2020.062

© **IAEME** Publication **Scopus** Indexed

"ENCRYPTION AS A SERVICE" FOR MULTI-CLOUD ENVIRONMENT

Karamath Ateeq
School of Information Technology,
Skyline University College, Sharjah, United Arab Emirates

Manas Ranjan Pradhan
School of Information Technology,
Skyline University College, Sharjah, United Arab Emirates

Beenu Mago
School of Information Technology,
Skyline University College, Sharjah, United Arab Emirates

Taher Ghazal
School of Information Technology,
Skyline University College, Sharjah, United Arab Emirates

ABSTRACT

Challenges and security concerns are preventing businesses from consolidating a data center or joining a cloud service. They contribute to the slow progress in shifting workloads from physical servers to virtual machines. There is a big shift in infrastructure which is a challenge for IT professionals. New encryption technologies are needed to support service providers and dynamic data centers. Today data is stored on premises, in the cloud on mobile devices and across a hybrid IT landscape which has compelled a move from traditional approach to adopting and managing encrypted data [1].

In this paper, an "Encryption as Service" for Multi- Cloud Environment is suggested that requires an encrypting agent to take care of encryption and manage the encryption keys and auditing process.

Key words: Data centers, Encryption, Cloud, key-management, Encryption as a Service.

Cite this Article: Karamath Ateeq, Manas Ranjan Pradhan, Beenu Mago and Taher Ghazal, Encryption as a Service for Multi-Cloud Environment, *International Journal of Advanced Research in Engineering and Technology*, 11(7), 2020, pp. 622-628.
http://www.iaeme.com/IJARET/issues.asp?JType=IJARET&VType=11&IType=7

1. INTRODUCTION

Instead of viewing encryption as a liability, it can be deployed correctly to achieve compliance, data privacy and flexibility in business environments. In the world of cloud computing and virtualization, there is a need to have control over data.

If the encryption key and data are accessible by the service provider, it is still unsafe and insecure. Encrypting the data before sending it to the cloud and having a hold over the keys makes sense. Many organizations feel multi cloud is a secure option but managing the keys is a challenging task [2].

The Cryptography and key management requires a third party that takes care of issues like backup, disaster recovery and availability of encryption keys. The service provider has no access to the keys and handles the data alone. The encryption or security service provider does not access to the data. The owner of the data can fragment the data and use multi cloud for deployment after the security provider encrypts the data.

It is necessary to encrypt the data at the data center level before adopting a multi cloud environment. There is a need to differentiate between data center and cloud. This paper deals with the challenges faced by organizations to develop and maintain their own data center. An encryption model is proposed [Figure-1] that can possibly be a solution to the issues and challenges discussed in this paper.

2. LITERATURE REVIEW

Richa H. Ranalkar Richa H. Ranalkar [3] has proposed a DNA based Cryptography in Multi-Cloud. Critical data is fragmented into parts using biological DNA sequences. Pieces of data encrypted using DNA model is proposed for privacy and security concerns.

According to S. Jaya Prakash [4] multi-cloud and multi-cloud service providers provide service availability and reduced risk of loss of data.

Reema Gupta et al [5] present a file security model to meet security needs. This model uses modified version of RSA and Blowfish.

Maha Tebaa et al [6] proposed a Homomorphic Encryption system. The client still holds the secret key. Cloud service provider is allowed to perform operations on encrypted data without decrypting using Homomorphic Cryptosystem. Various Homomorphic Encryption Cryptosystems are compared in the paper, based on encryption type and keys used etc.

3. DATA CENTER VS CLOUD

The terms data centers and cloud sound like inter-changeable buzz words. Both these systems have common factor “Data storage” but otherwise they are different.

Cloud is a form of off-premises computing that uses internet to store data. Data center is a form of on-premises us computing using hardware, servers and other equipment to store data. Cloud can store data from different clients whereas data center stores data related to a local network.

A third party is used for updating and maintenance operation for a cloud whereas the IT maintenance department shoulders the responsibility of maintenance and security of data center. Cloud services such as IaaS, PaaS, SaaS are provided by service providers using one or more data centers and cloud based resources.

Data center can undergo a failure or outage. Thus more than one data centers (can be located in different locations) can be used to host a cloud [7].

4. WHAT DOES A BUSINESS NEED-CLOUD OR DATA CENTER

Decisions on choosing between cloud (private or public) or private owned data center depends on business needs, security needs and cost factor.

When a business has a complex workload and uses different applications, constructing a data center gives full control on data and enhances security management. But managing the equipment is a challenge. Constructing a data center that matches the business requirements along with adding new equipment, servers, cables and installing the new equipment is a challenging task.

A cloud has virtually unlimited capacity there is no need to purchase new equipment but loss of control is a prominent feature in public cloud.

If security is a concern for the business, forming a private cloud with data centers located in different locations within a territory is a possible solution. Security measures are required for each location. Information and applications are accessed after verifying the credentials [8]. A cloud also tests for proper credentials before allowing the connection but it opens a large number of entry and exit points that are difficult to control. It is not possible for the organization to secure all points where data is transmitted to and from.

Cloud is the ideal choice for a small business as there is no need to invest on capital, servers or infrastructure. Administration and maintenance cost can be avoided as there is no need to compromise on security. Moreover, services can begin instantaneously once the organization is registered on the cloud. There is no time wasted in getting approvals to build infrastructure or make plans to meet the budget for maintenance.

When services are provided at national level, private cloud is a better choice [9]. The cost involved is not less than 10-20 million dollars to get started and operate. Where security overrules the cost factor, data centers located in different locations should form a part of the national budget.

5. CHALLENGES FOR A DATA CENTER

- Automation and digitization of devices creates security problems. With the excessive use of smart devices, large amounts of data are collected. Preserving the privacy of consumers with increased volumes of data creates pressure for the storage makers. The server technology has to be improved to match with the sky rocketing usage of bandwidth [10].
- Data centers are expected to protect expanding volumes of mission critical applications and large volumes of customer data. In addition, they are also expected to manage challenging environments and service level agreements.
- Around 38% of data centers are understaffed. In 43% finding qualified employees is an issue. When multiple data centers are involved, staff trained cryptographic key management are hard to find where as the number of business applications that require encryption are growing at a fast pace. The solution suggested here is to outsource or to go for increased automation of task. This strategy reduces cost and frees the staff for considering strategic initiatives.
- Management of storage task like RAID reconfiguration, resizing file system and defragmentation are a challenge. Solutions like online administration and configuration, creating dynamic multi-path, dynamic storage tier, centralized storage management and remote replication reduce operation and capital cost of storage management.

- Data centers have to monitor the application status and automatically move them to another server in the event of failure or fault. Clustering tools can be used to detect faults in components and applications. These tools shut down the application and restart it on another server and connect it to a storage device to continue with normal operations. Clustering tools combined with replication technology can deal with disaster recovery and ensure efficiency of virtual and physical environments.
- Data centers have to comply with SLA (Service Level Agreement) that are internal and governance requirements that are external. Automated tools are used for service level management.
- In addition to increased efficiency, storage management and virtualization data centers are expected to practice “Green IT”.
- Virtualization improves utilization of resources but it also introduces complexity. A frame work is needed that supports virtualization platforms and architectural flexibility.
- One of the challenges of a data center is the storage resource management (SRM). It is required to view the storage environment, the application contained in each storage, space and storage area of these applications. It is necessary to predict and be prepared for future storage requirements as well as to reclaim under-utilized storage. Storage arrays and thin provisioning are used for just in time and just enough basis.
- The cost of security and power is a concern while managing the data center. The power utilized is called “black hole”. Many managers of data centers are neglecting this issue.

6. TOOLS FOR DATA CENTER SECURITY

6.1. Webguard

A major challenge for data centers is Web integrity. When web pages are altered, it causes not only business loss but embarrassment too. A software security application can be disabled and proves ineffective as if the server is visible from outside. The WebGuard is placed between the web server and the firewall. It is a hardware solution. The dynamic (java servlets, images, CGI’s) and static content of every transmitted web page is verified based on the network policy to ensure security and recovery of contents [11].

6.2. i-Security

It consists of the “black network” and “the trusted network”. Attacks like DoS (Denial of Service), password cracking and intrusion degrade the services. This network compromises the services. Trusted network administrators are employed to administer the network services and counter any security threats. Thus the central control unit controls, administers and runs network services.

6.3. Smart E-Ticket Dynamic Password Authentication

In this method, password is cryptographically stored. Once the password is entered from any global location, after verification a soft token (a smart e-ticket) is generated which can be verified offline using a handheld scanner [12].

6.4. Adopting Multi Cloud

When more than one data centers are connected, they form a multi cloud environment.

- It reduces the risk of downtime that happens due to component failure.

- Various infrastructures can be used thus avoiding vendor lock in and improving the performance for customers.
- Traffic from different partners or customer bases is steered through the network, offering software, hardware and infrastructure fault tolerance [13].

7. PROPOSED FRAMEWORK

The suggested cryptosystem model focuses on providing an encryption infrastructure. Public key infrastructure is provided on commercial terms. It is a good idea to have an internal version through an encrypting agent which encrypts the company data before sending it to the cloud. The encrypting agent fragments the data and encrypts it with different keys for each fragment. A multi cloud used to transmit data can provide a secure solution. The keys are maintained and updated by the agent. This relieves the client or organization of maintaining updated keys. The organization can change the key when the need arises. Decryption of synthesized data is also handled by the agent. Such an encryption must have standards, capabilities and technical compliance. It must possess audit, authorization service.

Generally, encryption can degrade the performance if the ideal procedure is not adopted. The encrypting agent is an individual entity and is separated from the data center authority. The agent is subjected to auditing and quality compliance and thus takes up the responsibility of reducing the load on the datacenter and providing security for the organization as well. The cloud customer need not take time to learn about the procedures and policies for encryption at the providers end.

The data from client 1 is fragmented as d1 with key1. (d1k1) for cloud 1 and d2 with key k2 (d2k2) for cloud 2. Similarly, another client 2 sends data d2 to the encrypting agent which is fragment as d2with key k3 (d2k3) for cloud 2 and d2 with key k4 (d2k4) for cloud 3 and so on.

The keys k1, k2, k3, k4 etc. are stored and managed by the encrypting agent.

At the receiving end the encrypting agent will receive all sent encrypted data and decrypt it before the client as normal data.

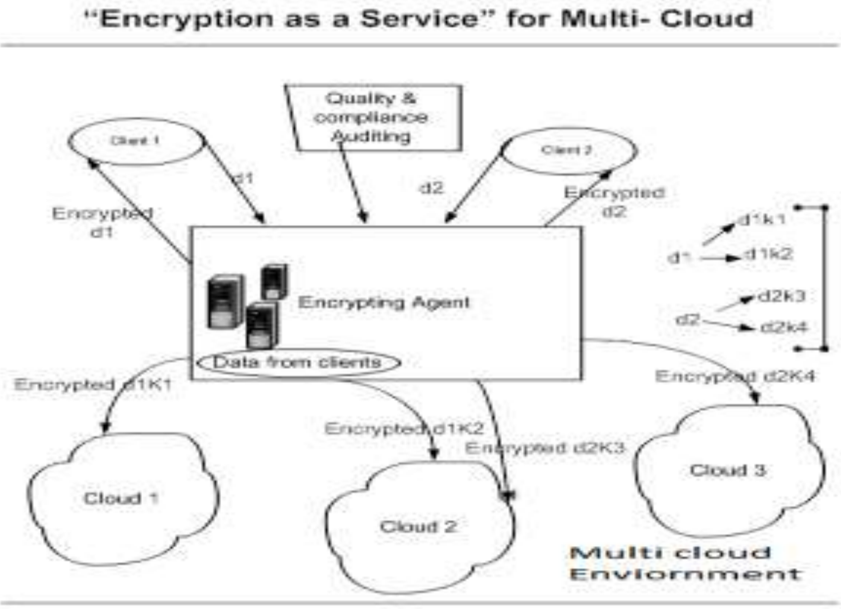

Figure 1 Proposed Framework-Encryption as a Model

8. ADVANTAGES OF THE ENCRYPTION MODEL

Data is as unsafe in the cloud as it is in the data center. Strangers cannot only see data but it could also be in the same storage as the competitor. Encryption protects the data from unauthorized access. Even if the data is copied, many times by virtual machines it is in encrypted form. It is possible to revoke the keys when desired.

When an organization wants to leave a service provider, even the service provider is unable to account the number of copies of the data made by virtual machines. It is also not possible to assure if all copies are retrieved and deleted.

Encryption enables multi-tenancy by serving the workload of many enterprises on the same physical server. Multi-tenancy increases flexibility and cuts down costs [14]. Even if servers become targets in public cloud, encryption creates firewall of security.

There is some information like health care or credit cards that adopt security standards but not all types of data comply with security standards. Considering the cost of breach of data, encryption is a recommended option and could save millions of dollars in the event of a breach.

The service providers can have a competitive advantage and expand revenue. They can satisfy privacy requirements and reduce hardware cost. Backup tapes if lost will make it difficult to retrieve its data if encrypted.

Organizations like tax accountants and financial planners who have sensitive data on remote offices and unprotected servers are afraid of adopting the cloud. Having a third party to encrypt the data, manage the keys for as long as desired by the organization and deliver it to the cloud ensures that data is safe even if there is scarcity of well-trained IT staff.

9. RISK ASSOCIATED WITH THE ENCRYPTION MODEL

Generally, encryption is applied in layers. If strategic approach is not used, it will result in business risk, increased complexity and costs.

Attackers generally attack the encrypted keys. If the issue of key management is overlooked, it will create vulnerability.

Organizations should be supportive to auditors to manage issues related to key management.

Encryption can be an intensive process that may degrade the performance of platforms, gateways and servers if not implemented in an ideal manner [15].

When key management depends on manual process, poor trained staff and poor documentation along with human errors, it poses a risk [16].

10. CONCLUSION

Challenges regarding key management and encryption contribute to the progress in consolidating a data center. Loosing encryption keys is a major concern. Securities in management of keys along with strong encryption model are critical issues related to data centers. The suggested model takes care of this issue. There is a need for centralized encryption management across virtual physical and public clouds. Compliance reports and detailed logs have to be generated for external and internal auditors.

Data encryption is a service that is offered by cloud service providers. They transform data using algorithms and then place it on the cloud. Encrypted data is called cipher text.

The capabilities of the encrypting agent need to match the sensitivity level of the data hosted. Many cloud service providers offer encryption at a basic level such as for account numbers or passwords [17]. For the entire database to be fragment and encrypted it becomes expensive and consumes more power. The” Encryption as a service model “would reduce the hassles of power consumption and data security management. The proprietary encrypting algorithms which are created by the encrypting agent take care of key management.

REFERENCES

[1] Sashank Bajpai and Padmija Srivastava (2014),” A Fully Homomorphic Encryption implementation on Cloud Computing”. International Journal of Information and Computation Technology. ISSN 0974-2239, volume 4, pp 811-816.

[2] Abdul Rahman bin Ahlan, Murni bt Mahmud, Yusri bin Arshad (2010),” Configuring thin client solution for Orang Asli community in Malaysia”. Proceedings of the 9th WSEAS International Conference on Applications of Computer Engineering. ISBN: 978-960-474-166-3, pp331-336.

[3] Richa H. Ranalkar and Prof. B.D. Phulpagar (2014),” DNA based Cryptography in Multi-Cloud: Security Strategy and Analysis”. International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 3, Issue 2, pp189-192.

[4] S. Prakash, K. Subramanyam, and S. Prasad (2013), Multi Clouds Model for Service Availability and Security, IJCSET, vol. 4, issue 2, pp. 158-161.

[5] Reema Gupta, Tanisha Priyanka (2013), “Enhanced Security for Cloud Storage using Hybrid Encryption”. International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 7, July.

[6] Maha Tebaa, Said El Haji (2013),” Secure Cloud Computing through Homomorphic Encryption”. International Journal of Advancements in Computing Technology(IJACT), Volume5, Number16, pp-29-38.

[7] Derick Leony, Abelardo Pardo, Hugo A. Parada G., Carlos Delgado Kloos (2012),” A cloud-based architecture for an affective recommender system of learning resources”. 1st International Workshop on Cloud Education Environments (WCLOUD 2012), pp 41-46.

[8] Kashif Bilal, Saif Ur Rehman Malik, Samee U. Khan and Albert Y. Zomaya (2014), “Trends and Challenges in Cloud Datacenters”. IEEE Cloud Computing published by the IEEE computer society, May 2014.PP-10-20.

[9] Sara Angeles (2013),” Cloud vs. Data Center: What's the difference?” Business News Daily, 26th August.

[10] M. Sethurama (2013),” Cryptography and Network Security Group” AU-KBC research Centre

[11] Xiang-Yang Li (2013),” Cryptography and Network Security”. Teaching note: CS549-Cryptography and Network Security.

[12] William Stallings (2010),” Cryptography and network security”. Book, Fourth Edition

[13] Wierman, A.,” Opportunities and challenges for data center demand-response” Green Computing Conference (IGCC), Dallas, TXNov.2014.

[14] A. Wierman, Z. Liu, I. Liu and H. Mohsenian-Rad (2014), "Opportunities and challenges for data center demand response," *International Green Computing Conference*, Dallas, TX, pp. 1-10, doi: 10.1109/IGCC.2014.7039172.

[15] D. Aikema, R. Simmonds, and H. Zareipour (2012). Data centres in the ancillary services market. In Green Computing Conference (IGCC), 2012 International, pages 1–10. IEEE.

[16] Baltimore,” Global Survey Reveals Security Concerns Migration”. Holding Back Data Center Consolidation and Cloud. February 11, 2014

[17] Feng Zhao (2014),” A cloud computing security solution based on fully homomorphic encryption”, Advanced Communication Technology (ICACT), Pyeong Chang, ISBN 978-89-968650-2-5, pp485-488.