A REVIEW WORK ON INFORMATION SECURITY OF DATA IN CLOUD PLATFORM FOR AN ORGANIZATION

Abstract

In today's world Organizations are rapidly moving towards cloudification of their infrastructure and applications. Cloudification is the process of conversion and/or migration of data and application programs in order to make use of cloud computing. This trend involves both utilization of public cloud providers like Amazon, Azure, Google, IBM and using private cloud providers like IBM Bluemix, Azure Private Cloud, etc.

One of the most important challenges organization face in successful cloudification is w.r.t ensuring stringent Information Security and compliance requirements are effectively implemented in Cloud environment. The organizations information consists of a treasure trove of customer data, employee records, organizations confidential data, etc. The potential impact of any data leak is enormous. This can cost an organization, both monetarily and in loss of reputation. This book chapter is intended to showcase how an Organization can safeguard themselves in ensuring no data leak during cloudification process. Furthermore, this paper will also discuss how an organization needs to implement right Information Security Practices. The survey paper will discuss the best procedures and processes to be implemented. The paper will also discuss necessary tools and implementation methodology to be adopted in cloud systems both as part of application security and cloud security to safeguard data.

Keywords: ISMS, Cloud, MFA, WAF, Azure.

Authors

Dr. Madhura K
Assistant Professor-Senior Scale
MIT, MAHE Bengaluru
Karnataka, India.
maddyksd87@gmail.com

Dr. H M Manjula
Assistant Professor
CSE Department
Presidency University
Bangalore, India.
hmmanjula@presidencyuniversity.in

I. INTRODUCTION

Moving to Cloud is not a choice anymore that enterprises can decide upon. It is a necessity now to stay relevant, reduce cost and compete with other enterprises. Cloudification is the process of conversion and or/migration of data and application in order to make use of cloud computing. This trend involves both utilization of public cloud providers like Amazon, Azure, Google, IBM and using private cloud providers like IBM Bluemix, Azure Private Cloud, etc.

One of the most important challenges organization face in successful cloudification is w.r.t ensuring stringent Information Security and compliance requirements are effectively implemented in Cloud environment. The organizations information consists of a treasure trove of customer data, employee records, organizations confidential data, etc. The potential impact of any data leak is enormous. This can cost an organization, both monetarily and in loss of reputation.

The organizations must ensure correct information security practices are implemented during Cloudification process. The public cloud systems are especially vulnerable to cyber threats and external attacks like DDOS, malware, information stealing, etc.

The security of data must be ensured during both transit and at rest. The data should never be left unencrypted during transit or during rest. Organizations must ensure that data during transit is not modified/altered. Once data is available in cloud, steps needs to be taken that data can be accessed only by its intended recipient. Once the organization data is in Cloud, steps needs to be applied to apply correct classification of data (this classification should be same as their original classification). Example of data classification include- internal, private, public, confidential.

One important aspect of security involves how the cloud system is connected to Organization and how users access data. The Organization should be connected to Cloud system using dedicated Virtual Private Networks. Many Cloud Providers like Amazon/Azure provide a LAN/WAN like connectivity using Direct Connect/ExpressRoute respectively. Direct access using public internet is usually not a safe way to access data which has confidential/internal/private classifications. In addition to above measure to prevent common security attacks like DDOS Firewalls like Web Application Firewalls and network firewalls within cloud should be implemented. Users themselves should be allowed access data using MFA or multi factor authentication. Cloud Information Security of Data is multi-disciplinary. It encompasses:

- **Philosophy:** How do we adopt the mindset that Data will be stored outside the enterprise data center and enterprise doesn't have any direct control over its storage? However, all the information security and compliance that are associated with Data store on premise will still be applied on cloud. How do we evangelize this philosophy to the entire organization?

- **Theories:** What are the core paradigms of working with Data and security? What is Data, itself? What is a repository? Where is it located? What is a channel? What is Data classification? What is information security for data?

- **Practices:** How do we design Data storage policies and practices on cloud? How do we manage it in such a way that all information security and compliance guidelines are managed effectively?

- **Tools:** What types of tools are required to implement information security for data on cloud?

II. LITERATURE SURVEY

Cloud information security is not a new thing. From the day when enterprises are moving to cloud there are works done in area to ensure information security is strictly followed.

There are several organizations like Center for Internet Security that have given/published articles in this area. In-fact Center for Internet Security has come up with security practices for cloud as well. What this paper however is trying to establish, or focus is information security of Data for cloud.

The Cloud service providers themselves are treasure trove of information. Though they don't specify exactly how information security and compliance on data should be applied, what they do provide is a list of enablers. Selecting the right set of Enablers can help organizations to effectively implement data protection and classification policies and help achieve information security requirements. Companies like Microsoft Azure, Amazon AWS has detailed information on various enables like network security, Storage security, VM security, Identity management, end point protection, PaaS security, etc.

1. **Architecture of IAAS Cloud:** Let us look at how are a IAAS Cloud architecture can be setup with applicable Information Security applied for Data in Cloud environment.

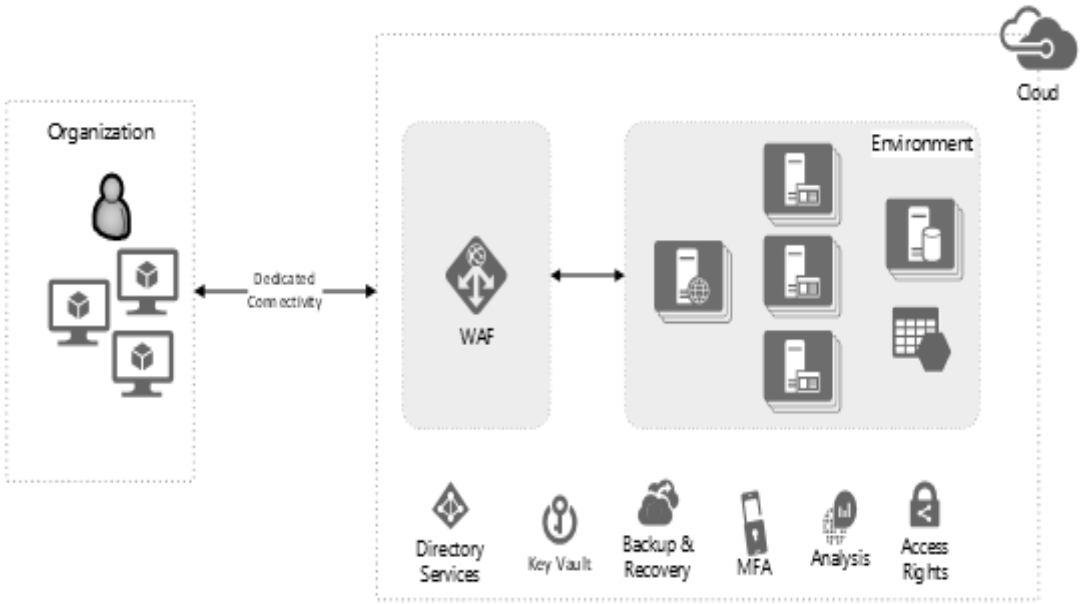

Figure 1: Reference IaaS Cloud Architecture

The above figure represents a reference IaaS architecture for any solution in Cloud. To enforce strict Information Security for data, the architecture must have the following features:

- **Data Repositories:** Data Repository can be a database or new storage mechanism like File, queue, table, blob storage. Companies like Microsoft, Amazon, and Google ensure that they provide several enables for Data repository security. This include providing encryption at rest capabilities. In addition to this, the implementer should ensure that Data is encrypted at transit. This is by making using of HTTPS based communication all the time.

- **Multi Factor Authentication:** All cloud providers now a day provides multi factor authentication support. This is especially important to ensure that even if password of a user is compromised, there is still additional security implemented to block access to the restricted Data.

- **Web Application Firewall:** Any new implementation which uses https communication must ensure implementing WAF as perimeter security. WAF's are first line of defense for any cloud solution. The WAF provides centralized protection to the solution from common exploits and vulnerabilities like SQL Injection, DDoS, Cross Site scripting, etc.

- **Cloud Directory Services:** Directory Service is a backbone of any authentication and authorization. All Cloud service provider provide directory services that can be used to configure users and groups. Combined with right group policies this becomes be an effective way to manage authentication and authorization need of a user. In addition to this all machines or compute resources used in Cloud should be domain joined with the directory service provider. This ensures centralized group policies can be applied on the computing resources itself.

- **Connectivity:** The cloud environment should be connected to the organization network using a dedicated connectivity option. All major cloud provides like Amazon and Azure provide such an option. All connection to cloud should ideally originate from within the organization network. Such an architecture allows no unauthorized connections can be made to cloud services.

- **Networking:** The cloud itself is a shared environment and proper design must be taken for networking within an organization's subscription. The best practice is to have isolate different application in its own virtual network. Within virtual network further segregation should be done between front end layers, application layer, data layer, management layer. Communication between these layers should be implemented using firewall rules provided by the cloud provider.

- **Data Classification:** All Data stored within cloud should follow the standard data classification rules.

The classification of the data stored on the cloud are listed below:

- **Public:** Data should be classified as Public when the unauthorized disclosure, alteration or destruction of that Data would result in little or no risk to the Organization and its affiliates. Examples of Public data include press releases, course information and research publications. While little or no controls are required to protect the confidentiality of Public data, some level of control is required to prevent unauthorized modification or destruction of Public data.

- **Internal Use:** Data should be classified as Internal Use when the unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk to the Organization or its affiliates. By default, all Organizational Data that is not explicitly classified as Restricted or Public Data should be treated as Internal Use Data. A reasonable level of security controls should be applied to Internal Use Data.

- **Confidential:** Data should be classified as Confidential when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to the Organization or its affiliates. Examples of Confidential Data include Data protected by state or federal privacy regulations and Data protected by confidentiality agreements. The highest level of security controls should be applied to Confidential Data.

- **Access Control List:** An ACL should be applied to each Data to ensure only authorized users can access the Data. The ACL must be designed to ensure the Data classification rules adopted by the organization are fully met. Password management, including the use of strong passwords, periodic password changes, and restriction of sharing access and/or passwords should also be implemented. System access is authorized according to business need and password files are not stored in clear text or are otherwise adequately protected.

- **Data Retention Policy:** With the implementation of GDPR in Europe and Privacy laws in US, Data Protection Laws in India, it is important that data must be retained only for the requirement amount of time and right retention and destruction policy must be adopted by the cloud solution.

- **Monitoring:** There must be good monitoring tool implemented within Cloud solution to ensure at any given time audit logs and monitoring logs can be provided to Information Security office to validate and prove the security restrictions applied in the solution.

- **Backup and Disaster Recovery:** The architecture must ensure data is backed up on a regular basis to comply with recovery point objective set by an organization. In addition, a disaster recovery plan should be built and implemented to ensure data protection in case of disaster. For cloud provider this may be moving between one geographical locations to another in case of disaster.

2. **Advantages:** A proper Information Security implementation for data in cloud can have many advantages to an organization

- The first and foremost advantage is that it helps protects information and data of an organization in cloud.
- It significantly increases an organization's resilience to cyber-attacks and external threats in cloud.
- Provides a standard framework for keeping an organizations information safe in cloud and managing it in compliance with on premise information security policy.
- It offers a set of policies, procedures, technical and physical controls to protect the confidentiality, availability and integrity of data.
- With Data privacy laws becoming more and more rigid and personal data (PII) is a need of hour it's more of a necessity for organizations to ensure no data leakage as costs and loss of brand value associated with it are too high.

3. **Existing Status:**

- **Products and Services:** This section describes how major Cloud providers are providing various tools and utilities to implement the architecture pattern described above. The paper takes the example of Microsoft Azure cloud provider and demonstrates the tools/products the can be used.

  - **Azure Storage:** Microsoft Azure Storage is a Microsoft-managed cloud service that provides storage that is highly available, secure, durable, scalable, and redundant. Azure Storage consists of Blob storage, File Storage, and Queue storage. The storage can be encrypted at rest using encryption keys provided by Microsoft or customers. The keys can be 128 bit or 256 bit keys stored in Azure Key Vault for safe keeping. The storages are highly available and massively scalable. This helps in protecting data from any type of loss. The storages should themselves be configured with Virtual network service endpoint to ensure the traffic between VNET to Storage always remain in Azure backbone network. In addition, Azure Storages can be set as GRS or LRS allowing storage to be geographically or locally redundant, meaning multiple copies of data exist to achieve high availability.

  - **Azure Active Directory:** Azure AD is a directory service solution provided by Microsoft. It provides Multi Factor authentication using SMS or email or RSA token. Furthermore, the AAD can be used to join computing resources to a domain to ensure secure access to the resources.

  - **Azure Application Gateway:** Application Gateway is a WAF service provided by Microsoft Azure. This can be configured as preventive mode or detection mode depending on the solution. It provides security of websites against common attacks like SQL injection, DDoS, Cross Scripting, etc.

- **Express Route:** Microsoft Azure Express Route gives an organization fast and reliable connection to Azure. With high throughput and latencies, Organizations will feel azure as a natural extension to their existing data center. This way organization can enjoy the scale and economics of public cloud without having to compromise with network security and performance.

- **VNET and NSG:** A virtual network (VNET) isolates your resources from others' resources in the Azure cloud. You can connect virtual networks to other virtual networks, or to your on-premises network. We can limit network traffic to resources in a virtual network using a network security group. A network security group contains a list of security rules that allow or deny inbound or outbound network traffic based on source or destination IP address, port, and protocol. NSG's can be applied at VNET level, subnet work level or individual resources like VM level.

- **Network Watcher:** Azure Network Watcher Monitor and diagnose networking issues. When and issue is observed Organizations can investigate in detail for better diagnoses. In addition, this helps in building a deeper understanding of network traffic pattern using Network Security Group flow logs. Information provided by flow logs helps you gather data for compliance, auditing and monitoring Organizations network security profile.

- **Content Management System:** Implementing a strong Content Management Product like File Net, SharePoint, Open Text, etc. and Organization can implement effective data classification rules, Access control list within the content itself and proper data retention policies.

- **Azure Backup Services and Site Recovery:** Azure backup services ensure that any resources like VM can be backed up in a recovery vault that can be used if a VM is crashed. In addition, Microsoft Azure provides a feature called Azure Site Recovery that allows the entire site to be recovered to another geographical location in case of Disaster. The combination of backup, geo redundant storages and Azure Site recovery can be an effective DR strategy for an organization.

- **Information Security Checklist:** Organization should work towards preparing a checklist that helps them to ensure all information security of data is complied with in a cloud solution. This checklist should include sections for Infrastructure, Application, Physical Security, Procedural compliance. Each section should have multiple audit questions or checks. A supplier or a solution implementer should ensure that they collect evidences for all the security checks and questions. Information Security officer needs to validate this checklist and certify an implementation. Only after this the implementation should be allowed to Go Live in production. This checklist can be used to regularly audit an project for its compliance. The audit frequency should be once every quarter. Any section or checks that are found non-compliant should be remediated immediately on an emergency basis. Repeat offenders should be penalized heavily by applying high fines.

Table1: A sample Checklist Format.

ID	Control Req.	Evidence Req.	Pass/ Fail/ N/A	Response /Evidence

III. CONCLUSION

Modern organizations are rapidly moving towards adaption of new technologies. Cloud is a key enabler for an organization to stay relevant and compete with other organizations in market. However, without any checks and balances security of data can drastically go out of control, and organizations can suffer data loss, huge fines from lawsuits. It is essential that Organization adopt a strict information security policy of data in cloud, build their architecture to comply with security standards and perform periodical security assessment of their infrastructure in cloud. This paper showcased all the major trick Organization can use to safeguard themselves in ensuring no data leak during cloudification process. Furthermore, the paper discussed the best procedures and processes to be implemented and all necessary tools and implementation methodology to be adopted in cloud systems (using Azure as a reference) both as part of application security and cloud security to safeguard data.

REFERENCES

[1] Zhong Hua, Xin Wang, "Cloud Computing and the Essentials of Security Management",Scientific Research Publication, published 30 may 2016.
[2] https://www.cisecurity.org/
[3] https://azure.microsoft.com/en-in/
[4] https://aws.amazon.com/security/
[5] https://cloud.google.com/security/
[6] https://docs.microsoft.com/en-us/azure/security/azure-security
[7] https://cloudcomputing.ieee.org/publications
[8] https://download.microsoft.com/download/0/A/3/0A3BE969-85C5-4DD2-83B6-366AA71D1FE3/Data-Classification-for-Cloud-Readiness.pdf
[9] https://www.ibm.com/cloud/security
[10] https://docs.microsoft.com/en-in/azure/expressroute/
[11] https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-overview
[12] https://docs.microsoft.com/en-in/azure/network-watcher/
[13] https://www.ibm.com/support/knowledgecenter/en/SSNW2F_5.2.1/com.ibm.p8.sysoverview.doc/p8sov146.htm
[14] https://www.ibm.com/in-en/marketplace/cloud-enterprise-records
[15] https://docs.microsoft.com/en-us/azure/multi-factor-authentication/multi-factor-authentication
[16] https://docs.microsoft.com/en-us/azure/key-vault/key-vault-whatis
[17] https://docs.microsoft.com/en-us/azure/application-gateway/application-gateway-introduction
[18] https://docs.microsoft.com/en-in/azure/active-directory/
[19] https://docs.microsoft.com/en-us/azure/storage/
[20] https://docs.microsoft.com/en-us/azure/backup/backup-azure-vms-introduction
[21] https://docs.microsoft.com/en-us/azure/virtual-network/

