International Journal of Latest Trends in Engineering and Technology
Vol.(16)Issue(1), pp.054-059
DOI: http://dx.doi.org/10.21172/1.162.09
e-ISSN:2278-621X

MODERN APPROACHES FOR DATA SECURITY IN CLOUD COMPUTING

Satyam Akunuri[1], A.Chandu Naik[1], S.Chandra Sekhar[1]

Abstract: - Now a days, Data security has consistently been a major issue in information technology. Particularly, when the data is located in different places in the globe. Security as well as protection of data has two major issues in the data is stored using cloud technology. This paper briefs you data protection methods and approaches used in cloud computing to ensure maximum data protection by reducing risks and threats.

Keywords: Data Security, Cloud Computing, Data Protection, Privacy, Risks and threats, Access Controls

I. INTRODUCTION

Cloud computing is a model for enabling global, convenient, on-demand network access, availability of computer system resources, especially data storage and computing power, without direct active management by the user. The term is generally used to describe data centers available to many users over the Internet. Large clouds, predominant today, often have functions distributed over multiple locations from central servers. If the connection to the user is relatively close, it may be designated an edge server.

Main Characteristics of Cloud Computing

NIST (National Institute of Science and Technology) identifies the essential characteristics of Cloud Computing

A. On-Demand Self Service:
Cloud computing resources can be provided on-demand by the requested user, without prerequisite interaction with the service provider. It is an automated process in cloud environment.

B. Resource Pooling:
The sharing of computing capabilities and storage resources provided by service providers are pooled to serve multiple users. Users are assigned virtual resources that run on physical resources.

C. Broad Network Access:
Resources can be accessed over the network by using standard mechanisms which provides platform Independent access.

D. Measured Service
Cloud computing resources are provided to the users on a pay -per-use model. The usage can be measured and charged based on CPU cycles, storage and number of requests.

E. Rapid elasticity

[1]*Assistant Professor, CSE, SNIST, Hyderabad, Telangana, India*

Cloud computing resources can be provisioned rapidly and elastically based on demand by providing additional resources.

II. CLOUD COMPUTING MODELS

Cloud computing services are offered to end users in three different models IaaS, PaaS and SaaS.
Infrastructure-as-a-Service (IaaS) provides the users capability to compute and storage resources as virtually. The users can deploy operating systems and applications on virtual resources on the cloud.

Platform-as-a-Service (PaaS) provides the users the capability to develop and deploy applications in the cloud using development tools, software libraries and services offered by the cloud service provider which manages the underlying cloud infrastructure.

Software-as-a-Service (SaaS) provides the users a complete software application or user interface with access to a vendor's cloud-based software. Users do not install applications on their local devices. Instead, the applications reside on a remote cloud network accessed through the web or an API.

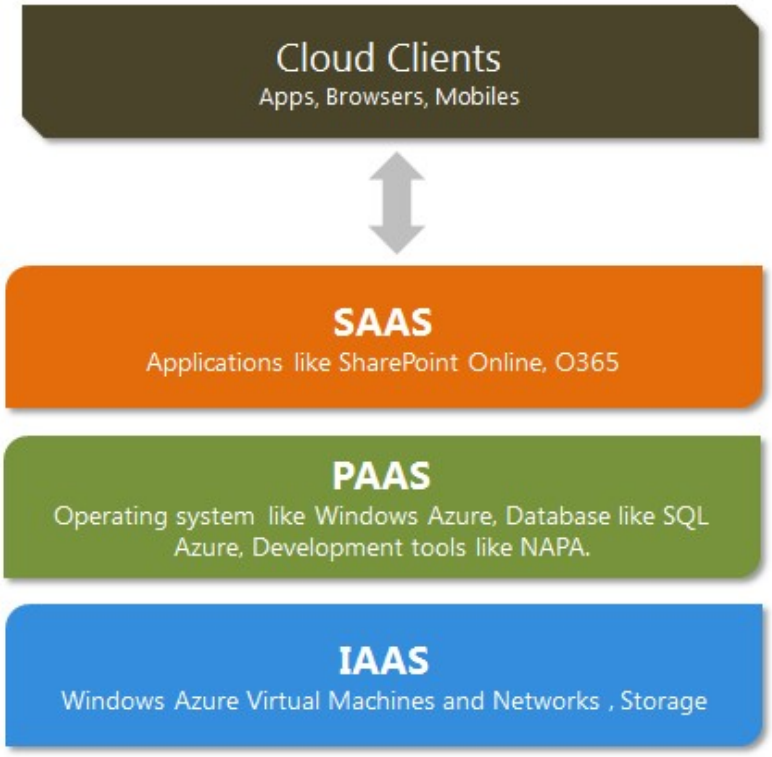

Figure 2.1 Cloud Computing Models

III. DEPLOYEMENT MODELS

NIST defines deployment models of cloud computing are categorized based on their location.

Public Cloud, cloud services are available to the general public or large scale companies. These services are shared among different users and provided by third party vendors. The infrastructure belongs to service providers that manage them and administer pool resources, the need for user to buy and maintain their own hardware is eliminated. Service Provider offers resources as a service on a free of charge or pay-per-use basis via the Internet connection. Users can scale them when required.

Private Cloud, unlike in the public cloud, private cloud operated for exclusive use of one company. Because these data center architectures reside within the firewall, they provide enhanced security. Even though one organization runs its workloads on a private basis, a third party can also manage it, and the server can be hosted externally or on-premises of the user company. Private clouds are best suited for applications where the security is tight control on the data.

Community Cloud, the cloud services are shared by several organizations with similar backgrounds share the infrastructure and related resources. It is best suitable for companies that want to access same applications and data. As the organizations have uniform security, privacy and performance requirements, and this multi-tenant data center architecture helps the companies to achieve their business-specific objectives.

Hybrid Cloud, combines the services of multiple clouds which may be private or public**.** Hybrid clouds are best suitable for companies that want to take advantage of secured applications and data hosting on the private cloud and cost saving by hosting applications and data in public clouds**.**

	Public	**Private**	**Community**	**Hybrid**
Ease of setup and use	Easy	Requires IT proficiency	Requires IT proficiency	Requires IT proficiency
Data security and privacy	Low	High	Comparatively high	High
Data control	Little to none	High	Comparatively high	Comparatively high
Reliability	Vulnerable	High	Comparatively high	High
Scalability and flexibility	High	High	Fixed capacity	High
Demand for in-house hardware	No	Depends	Depends	Depends
Cost-effectiveness	The cheapest one	Cost-intensive, the most expensive one	Cost is shared among community members	Cheaper than a private model but more costly than a public one

Table 3.1 : The comparative analysis of cloud deployment models

IV. KEY SECURITY CHALLENGES FOR CLOUD COMPUTING

Many organizations are migrating their applications and associated data to cloud environment to reduce the cost, operational maintenance and overhead. One of the main considerations is Security of data in the cloud. Most of the Service providers are implementing advanced security features which are very similar to in-house environments. The following are some of key challenges for cloud applications include:

A. Authentication of Requested Entity

Authentication involves confirming the identity of entity requesting access to protected information. Existing authentication policies are under control of individual organization and the process of identity is restricted to some entities. However, in cloud computing environments, where the applications and data accessed over web and complexity of digital authentication increasing more.

B. Authorization on Protected Resources

Authorization refers digitally specifying the access rights to the protected resources by using different access policies. In traditional approach, access policies are controlled by the individual organization and it might be altered with their convenience. But authorization in cloud environment requires the use of service providers specifying the access policies.

C. Security of data in the cloud

Data at rest refers to data in cloud, or any data that can be accessed using Internet. This includes backup data as well as live data. As mentioned earlier, sometimes it is very difficult for organizations to protect data at rest if they are not maintaining a private cloud since they do not have physical control over the data. However, this issue can be resolved by maintaining a private cloud with carefully controlled access.

D. Security of data in the motion

Data in transit normally refers to data which is moving in and out of the cloud. This data can be in the form of a file or database stored on the cloud and can be requested for use at some other location. Whenever, data is uploaded to the cloud, data at time of being uploaded is called data in transit. Data in transit can be very sensitive data like user names and passwords and can be encrypted at times. However, data in unencrypted form is also data in transit.

E. Data Integrity

Data integrity can be defined as protecting data from unauthorized modification or deletion. This is easy in a single database, because there is only one way in or out of the database, which you can control. But in the cloud, especially a multi cloud environment, it gets tricky. Because of the large number of data sources and means to access, authorization becomes crucial in assuring that only authorized entities can interact with data.

F. Auditing of data

Auditing is an important aspect for applications deployed in cloud computing environments. In traditional environment, the organizations have complete monitoring of their applications and accessing of protected data.For cloud environment suitable measures are required to get visibility into the applications, data access and actions performed by the users, including all platforms.

G. Data interception

Unlike with traditional computing, the data in cloud computing is segmented and distributed in transit. This poses more threats due to the vulnerability and fragility of the computing technology and, in particular, sniffing and spoofing, third party attacks and reply attacks .

V. INFRASTRUCTURE BASED PROTECTION

A. Authentication

Authentication refers to confirming the digital identity of entity requesting access to some protected information. This is not limited to authenticate the entity, also uniquely identify such as finger print or smart card the user. In this paper we identify the authentication mechanisms such as SSO,SAML-Token, OTP.

Single Sign-On (SSO) offers the user to access multiple systems after signing in only once. When the user login and access the resources is no need to sign in again. SSO upon receiving initial credential translates to different credentials for different systems and it saves the time spent in authentication.

SAML-Token is an xml based data format for exchanging security information between service provider and requester. It prevents man-in-middle and replay attacks.

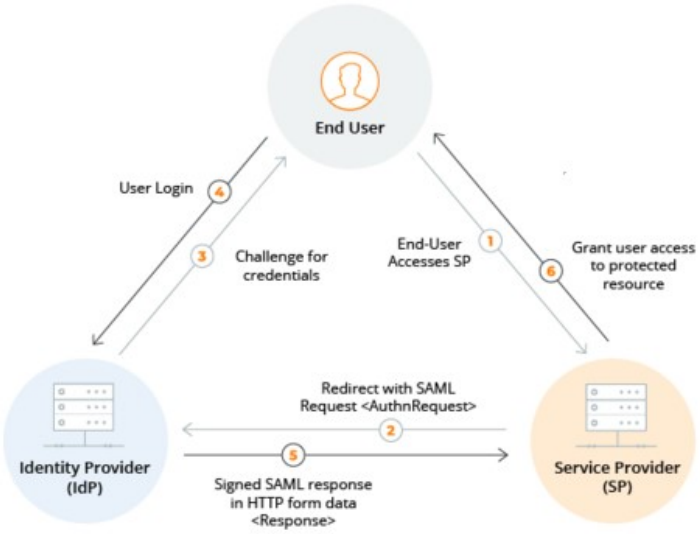

Figure 6.1 SAML-token based SSO authentication

One Time Password (OTP) is another kind of authentication standard that uses passwords which are valid for single time use of a session. It is more secure which avoids replay attacks.

B. Authorization

Authorization specifies the access rights to the protected resources by using access policies. OAuth is standard for authorization which allows to share the resources from one site to another without deal with the credentials. The service provider grants the permission to access the resource in a token form and matching shared secret.

C. Access Controls

Access controls identifies the user and maintain associated identity attributes across multiple organizations. Access controls deals with user privileges like authentication, authorization and access policies. Standardized access controls policies ensure the confidentiality of the data. Role based access controls are used for restricting access to confidential information to the authorized users. These access controls allow defining different roles to the different users.

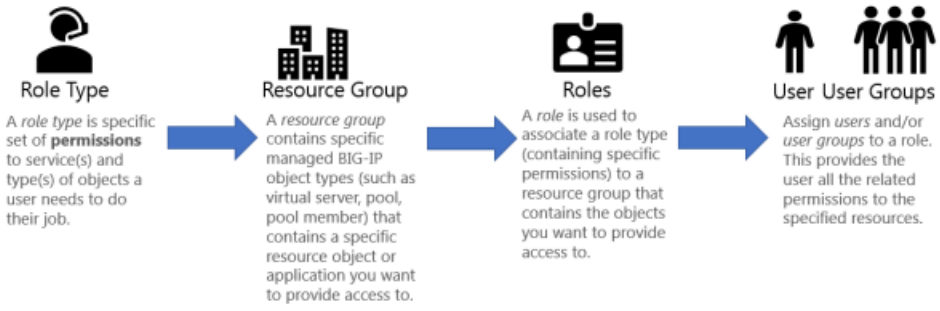

Figure 5.1: Role-based access control in the cloud

VI. DATA BASED SECURITY IN THE CLOUD

Data security in cloud is crucial for cloud applications in which the data flows from applications to storage. Cloud applications deal with data in motion and data at rest. Various types of threats can be raised for data in the cloud such as replay attacks, man-in-middle attacks and unauthorized data access.

Data at Rest

Data at rest is secured by encryption mechanism. Encryption is a process of converting the data from plain to cipher. And decryption performs the reverse process of encryption. Encryption is implemented in two ways. Symmetric Encryption and Asymmetric Encryption.

Symmetric encryption uses the same secret key for encryption and decryption processes. The secret key is shared between service provider and service requester . Symmetric encryption is well suited for securing data at rest.The popular algorithms for symmetric encryption are AES,Twofish,RC6 and MARS.

Asymmetric encryption uses two keys ,one for encryption as public key and another for decryption as private key. Public key can be shared while private key is available with the identified user only.

Data in Motion

Data security in motion, when data flows between one to another over a insecure network, is ensure data confidentiality and integrity. Transport Layer Security and Secure Socket Layer mechanisms are used for securing data in motion TSL and SSL use asymmetric encryption for authentication of key exchange, symmetric encryption fpr confidentiality and message authentication codes for integrity.

Auditing of Data

Auditing is an important aspect for data security which requires all operations with the data to be monitored in a log. The main purpose of auditing is to detect security breaks, hence the required changes can be made in the application and deployment levels. Auditing is even more important in cloud computing for direct control to the service providers.

VII. CONCLUSION

Cloud data security becomes increasingly important as we move our devices, data centers, business processes, and more to the cloud. Ensuring quality cloud data security is achieved through comprehensive security policies, an organizational culture of security, and cloud security solutions. Selecting the right cloud security solution for your business is imperative if you want to get the best from the cloud and ensure your organization is protected from unauthorized access, data breaches and other threats

REFERENCES

[1] Arshdeep Bahga, Vijay Madisetti, “Cloud Computing, A Hands-on Approach ” Cloud Security vol. 1, no.pp. 392-409, 2016.
[2] Peter Mell, Timothy Grance,The NIST definition of Cloud Computing, NIST Special Publication 800-145,Sep 2011
[3] P. S. Wooley, “Identifying Cloud Computing Security Risks,” Contin. Educ., vol. 1277, no. February, 2011.
[4] Ahmed Albugmi,,Madini O Alassaf,Robert Walters “Security in Cloud Computing” fifth International conf. FGCT 2016.
[5] S. Subashini and V. Kavitha, “A survey on security issues in service delivery models of cloud computing,”J. Netw. Comput. Appl., vol. 34, no. 1, pp. 1–11, Jan.2011.
[6] F. Zhang and H. Chen, “Security-Preserving Live Migration of Virtual Machines in the Cloud,” J. Netw. Syst. Manag., pp. 562–587, 2012.
[7] J. Hu and A. Klein, “A benchmark of transparent data encryption for migration of web applications in the cloud,” 8th IEEE Int. Symp. Dependable, Auton.Secur. Comput. DASC 2009, pp. 735–740, 2009.
[8] D. Descher, M., Masser, P., Feilhauer, T., Tjoa, A.M.and Huemer, “Retaining data control to the client in infrastructure clouds,” Int. Conf. Availability, Reliability,Security. (pp. 9-16). IEEE., pp. pp. 9–16, 2009.
[9] E. Mohamed, “Enhanced data security model for cloud computing,” Informatics Syst. (INFOS), 2012 8th Int. Conf., pp. 12–17, 2012.
[10] C. Modi, D. Patel, B. Borisaniya, A. Patel, and M.Rajarajan, “A survey on security issues and solutions at different layers of Cloud computing,” J.Supercomputer., vol. 63, no. 2, pp. 561–592, 2013.
[11] V. J. Winkler, “Securing the Cloud,” Cloud Computing Security. Tech. tactics. Elsevier., 2011.
[12] Google Search engine https://www.forcepoint.com/cyber-edu/cloud-security
[13] Cloud Security Alliance, “The Notorious Nine. Cloud Computing Top Threats in 2013,” Security, no.February, pp. 1–14, 2013.
[14] L. Rodero-Merino, L. M. Vaquero, E. Caron, A. Muresan, and F. Desprez, “Building safe PaaS clouds: A survey on security in multitenant software platforms,” Computer. Security., vol. 31, no. 1, pp. 96–108,2012.
[15] A. U. Khan, M. Oriol, M. Kiran, M. Jiang, and K. Djemame, “Security risks and their management in cloud computing,” 4th IEEE Int. Conf. Cloud Computing Technol. Sci. Proc., pp. 121–128, 2012.