IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 19, Issue 5, Ver. III (Sep.- Oct. 2017), PP 54-60
www.iosrjournals.org

Cloud Computing: Enterprise Applicationand Data Security Challenges And Solutions

Gautam Deb
Lead Engineer, Software AG, Hyderabad, TS 500032, India.
Corresponding Author:Gautam Deb

***Abstract**: The purpose of this paper was to identify and establish the capabilities of cloud computing as a secured solution for an enterprise, where both the data and application can be stored and accessed in a secure way. Cloud computing claims to help enterprises achieve more by eliminating the common enterprise IT concerns. At the same time, certain concerns have emerged as potential barriers to rapid adoption of cloud services such as security, privacy and reliability. Givingconfidential data and services to the cloud provider to maintain, implies giving access to your valuables to a third party, hence it is crucial that we ensure that the cloud services are capable enough to provide state of the art security and leaves no scope for vulnerabilities. Security is the degree of resistance to harm and the options explored here are various tools and techniques that cloud computing provides for making the deployed application and data secure. In the light of all the security related advantages provided by cloud, we were able to establish how a cloud based solution can prove to be a valuable investment for an enterprise, which ensures security of data among other benefits andhence allowsthe enterprise to focus on its core business competencies and delegating non-functional IT requirements implementation to the cloud.*
***Keywords**: Cloud computing, Data Security, Security Concerns.*

I. Introduction

An enterprise is an organizational entity involved in the provision of goods and services to consumers, in a particular business domain [1].These enterprises deal with massive volume of highly confidential data, mostly related to the clients, and their business domain.Needless to say, any failure in protecting the data can create a threat to the customer and definitely will be a cause of reputation and credibility loss for the organization. Traditionally where the whole infrastructure is owned and managed by the enterprise, security is also the responsibility of the enterprise which is implemented by following enterprise architecture security modelslaid out with multiple layers of protection, some of the reference models are SABSA, Zachman Framework etc. [2].Protecting confidential data is a top priority for any enterprise and for that many layers of security is employed, that includes delivering, monitoring and managing security across all data objects and repositories within an organization. Application and data should be secure regardless of where it is stored or consumed within the organizationand whether it is in rest or motion.With cloud based approach, the cloud provider needs to ensure and comply to various risk and security standards which are auditable. In the following sections, we will see what cloud computing is, what are security related concerns around it, and what are the various offerings it provides in terms of securitysolutions which can be used by an enterprise to operate seamlessly and efficiently without bothering about the non-functional system requirements like security. The following figure highlights the important aspects of enterprise IT security:

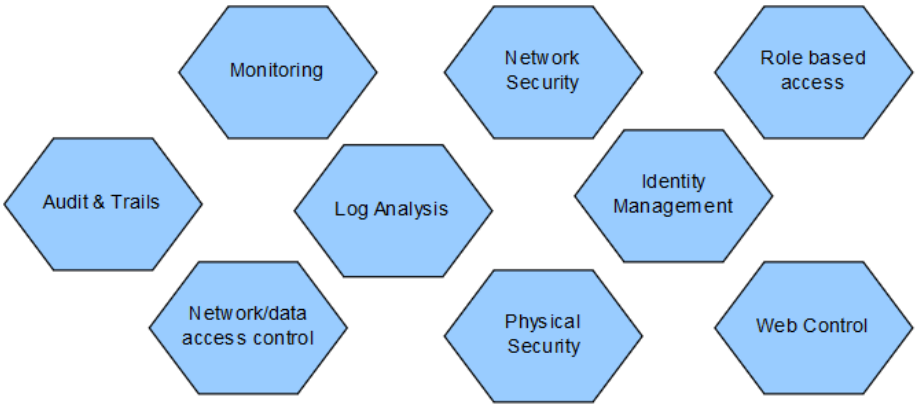

Figure 1. Various aspects of Enterprise IT security

II. Cloud Computing

The term Cloud Computing refers to the delivery of computing services – servers, storage, databases, networking, software, analytics and more – over the internet. Companies offering these computing services are called cloud providers and typically charge for cloud computing services based on usage, similar to how you are billed for water or electricity at home [3]. The abstraction created around network, storage and computing is fundamental to cloud computing. Cloud computing removes the traditional approach to application management and hosting and introduces a new level of scalability and flexibility to the enterprise.

With cloud computing, cloud providers manage and maintains the technology infrastructure in a secure environment and enterprise access these resources via the Internet to develop and run their applications. Capacity can grow and shrink as needed and enterprise need to pay only for what they actually use.

These Are The Cloud Computing Service Models:

- Software as a Service (SaaS): here a service provider delivers software and applications through the Internet.
- Platform as a Service (PaaS): here a service provider offers access to a cloud-based environment in which users can build and deliver applications
- Infrastructure as a Service (IaaS): here a service provider offers the clients pay-as-you-go access to storage, networking, servers, and other computing resources in the cloud.

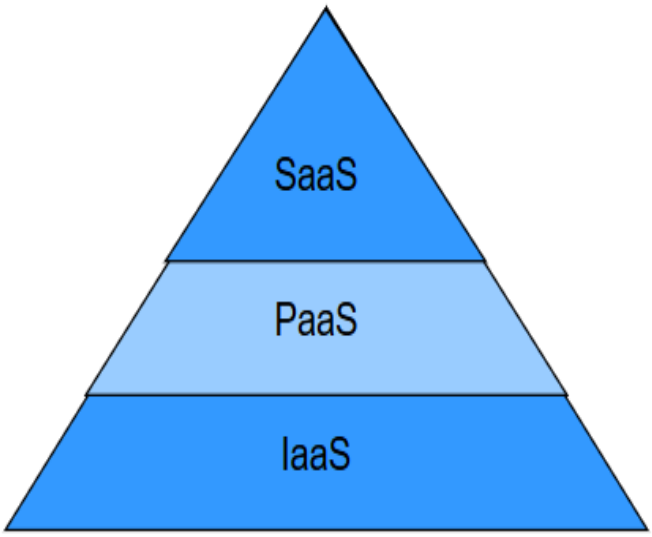

Figure 2. Various cloud computing service models

These Are The Cloud Computing Deployment Models [4]:

- Public Clouds: the cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
- Private Clouds: the cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
- Community Clouds: The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
- Hybrid Clouds: the cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

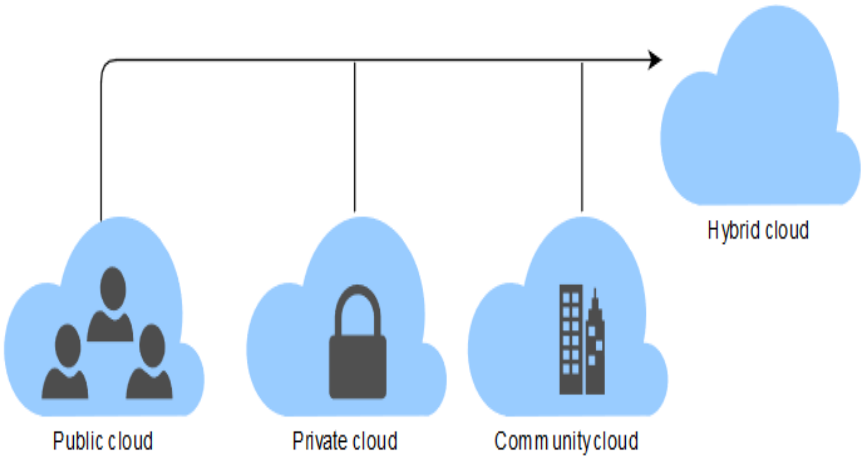

Figure 3. Various cloud computing deployment models

III. Compliance And Security Concerns With Cloud Computing

Cloud computing does not solve all of today's security problems, however; in fact, it creates new security problems that must be dealt with in addition to the existing problems. In fact, many of the cloud computing associated threats can be found in the traditional computing environment as well. Cloud computing does not magically protect application data from abuse or prevent attacks against the application level. Uploading the most hardened virtual machine will not prevent attacks against the web-based management consoles that are used to administer the virtual machines. High availability comes at a cost; this cost can be high if an attacker chooses to launch a sustained, data-intensive attack against the cloud provider. Fortunately, newly emerging attacks against cloud systems keeps security engineers on their toes as they fight to defend the data and application logic in the cloud [9].

In 2010, the Cloud Security Alliance (CSA) published apublication, namely, Top Threats to Cloud Computing (Cloud Security Alliance, 2010). In this article, seven threats were listed as the top threats to cloud computing which are as follows:

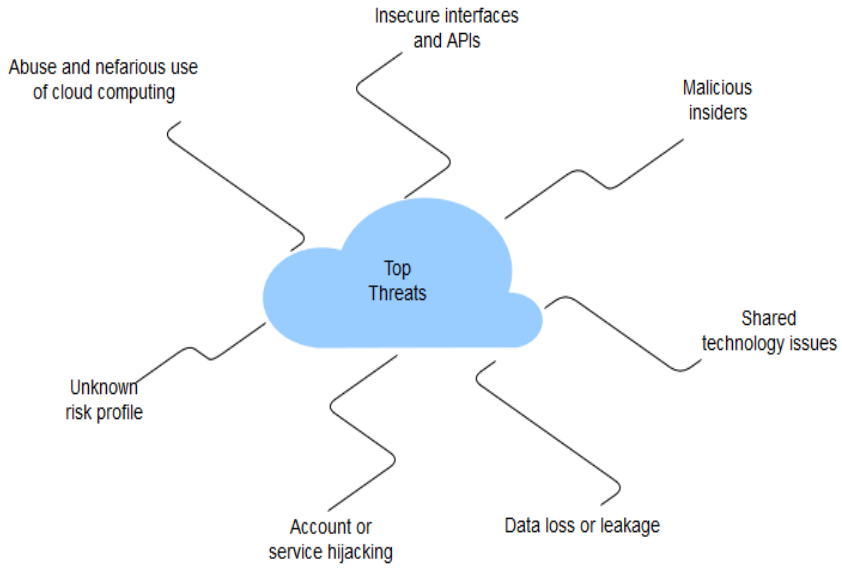

Figure 4. CSA Top Threats to Cloud Computing v1.0

The four basic security challenges that organizations face in cloud setup are as follows [10]:

3.1 Governance

When enterprises outsource parts of their IT infrastructure to the cloud provider, they give up some control of their information profile. While enterprises still get to define how their information is handled, who gets access to that information, and under what conditions in their private or hybrid clouds, they must largely take cloud providers at their word that their SLA trusting security policies and conditions are being met. Also, in

order to prove compliance and audit requirements, enterprises have to rely on cloud providers to supply logs, reports etc.

3.2 Co-tenancy and Noisy Neighbours

Cloud computing introduces new risks resulting from multi-tenancy, an environment in which different users within a cloud share physical resources to run their virtual machines. Many cloud providers find it challenging to create secure partitions between co-residentialsystems. Results range from the unintentional, noisy-neighbour syndrome whereby workloads that consume more than their fair share of compute, storage, or I/O resources starve the other virtual tenants on that host; to the deliberately malicious efforts, such as when malware is injected into the virtualization layer, enabling hostile parties to monitor and control any of the VMs residing on the system.

3.3 Architecture and Applications

Cloud services are virtualized with an added layer of hypervisor on a traditional IT application stack. This new layer introduces opportunities for improvements in security and compliance, but it also creates new attack surfaces and different risk exposure which enterprises needs to evaluate and mitigate.

3.4 Data

Cloud services raise access and protection issues for user data and applications and its source code. There are many aspects that needs to be define, like who has access to data, encryption of data, at rest, in transit and eventually in use. These kinds of security requirement will be defined and mandated by the enterprise but eventually the cloud provider need to provision such facility.

IV. Cloud As A Secured Solution For Enterprise

After defining what are the general enterprise security requirements, what cloud computing is and what are the general risks and security concerns around cloud, in this section we will try to explore the various security aspects provided by cloud which tries to address the concerns. Note that Amazon web services (AWS) is cited here as the cloud provider to demonstrate cloud security capability. Other cloud providers are equally capable, efficient and secure, and provides similar quality of service.

4.1 Shared Responsibility Security Model

When an enterprise runs and manages its own IT infrastructure on premises, within its own data centre, it is responsible for the security of that infrastructure, as well as the applications and data that run on it. When an organization moves to a public cloud computing model, it hands off some, but not all, of these IT security responsibilities to its cloud provider. Each party, the cloud provider and cloud user, is accountable for different aspects of security and must work together to ensure full coverage [5].

For example, Amazon Web Services (AWS), which is one of the major cloud provider, uses a shared responsibility model where AWS is responsible for the security “of” the cloud and the customer (enterprise) is responsible for the security “in” the cloud [6].

4.2 Compliance

Compliance means conforming to a rule, such as apolicy, standard or law. Regulatory compliance describes the goal that organizations try to achieve in their endeavours to ensure that they are aware of and take steps to comply with relevant laws, polices, and regulations of the region. Due to the increasing number of regulations and need for operational transparency, organizations are increasingly adopting the use of consolidated and harmonized sets of compliance controls. This approach is used to ensure that all necessary governance requirements can be met without the unnecessary duplication of effort and activity from resources [7].

For example, Amazon Web Services (AWS) provides a robust control in place to maintain security and data protection in the cloud. AWS compliance is built on traditional programs, by tying together governance-focused, audit-friendly services features with applicable compliance or audit standards. The IT infrastructure that AWS provides is designed and managed in alignment with security best practices and a variety of IT security standards [8], a few of those are:

- SOC 2/3
- DoD Cloud Computing Security Requirements Guide (SRG) Levels 2 and 4.
- Payment Card Industry Data Security Standards (PCI DSS) Level 1
- International Traffic in Arms Regulations (ITAR)

4.3 Infrastructure Security

Infrastructure security covers the threats, challenges, and guidance associated with securing an enterprise's core IT infrastructure at the network, host, and application levels. The foundational infrastructure for a cloud must be inherently secure whetherit is a private or public cloud or whether the service is SaaS, PaaS or IaaS.It will require [11]:

4.3.1 Infrastructure Security at Network Level

For network level of infrastructure security, it is important to distinguish between public clouds and private clouds. With private clouds, there are no new attacks, vulnerabilities, or changes in risk specific to this topology that information security personnel need to consider. Although an enterprise's IT architecture may change with the implementation of a private cloud, but the existing network topology will probably not change significantly.

However, if public cloud services are chosen, changing security requirements will require changes to the network topology and also how it interacts with the cloud provider's network topology. There are four significant risk factors in this use case:

- Ensuring the confidentiality and integrity of your organization's data-in-transit to and from your public cloud provider.
- Ensuring proper access control (authentication, authorization, and auditing) to whatever resources you are using at your public cloud provider.
- Ensuring the availability of the Internet-facing resources in a public cloud that are being used by your organization, or have been assigned to your organization by your public cloud providers.
- Replacing the established model of network zones and tiers with domains.

4.3.2 Infrastructure Security at Host Level

When reviewing host security and assessing risks, the context of cloud services delivery models (SaaS, PaaS, and IaaS) and deployment models (public, private, and hybrid) should be taken into account. The host security responsibilities in SaaS and PaaS services are transferred to the provider of cloud services. IaaS customers are primarily responsible for securing the hosts provisioned in the cloud.

4.3.3 Infrastructure Security at Application Level

Application or software security should be a critical element of your security program. Most enterprises with information security programs are yet to formalize application security programs to address this realm. Designing and implementing applications for cloud platform will require existing application security programs to be re-evaluate existing practices and standards. The application security spectrum ranges from standalone single-user applications to sophisticated multiuser e-commerce applications used by millions of users.

4.4 Data Security and Storage

Data security becomes more important when using cloud computing at all levels: IaaS, PaaS and SaaS. These are the different aspects of data security that the cloud provide needs to ensure:

- Data-in-transit
- Data-at-rest
- Processing of data, including multitenancy
- Data lineage
- Data provenance

For example, Amazon Web Services (AWS) Simple Storage Service (Amazon S3) allows to store and retrieve data anytime from anywhere on the web. Data is stored as objects in S3 buckets with an option to set permissions to control access to the data. For each bucket, you can control access like who can create, delete and query objects in that bucket [12].

4.5 Identity and Access Management

In a typical organization where applications are deployed within the organization's perimeter the trust boundary is mostly static and is monitored and controlled by the IT department and access to the network, systems, and applications is secured via network security controls including virtual private networks (VPNs), intrusion detection systems (IDSs), intrusion prevention systems (IPSs), and multifactor authentication.

With the adoption of cloud services, the organization's trust boundary becomes dynamic and moves beyond the control of IT and extends into the service provider domain. This loss of control continues to challenge the established trusted governance and control model and if not managed properly, will impede cloud service adoption within an organization.

To compensate for the loss of network control and to strengthen risk assurance, enterprises are forced to rely on other higher-level software controls, such as application security and user access controls. These

controls manifest as strong authentication, authorization based on role or claims, trusted sources with accurate attributes, identity federation, single sign-on (SSO), user activity monitoring, and auditing. In particular, enterprises need to pay attention to the identity federation architecture and processes, as they can strengthen the controls and trust between enterprises and cloud service providers.

For example, Amazon Web Services (AWS) provides IAM service that allows to control how people and programs are allowed to manipulate the AWS infrastructure. It uses traditional identity concepts such as users, groups, and access control polices to control who ca use AWS account, what services and resources they can use, and how they can use them [12].

4.6 Monitoring

Monitoring is an important aspect of any enterprise setup which enables usage of application and access to data traceable and auditable. For example, Amazon Web Services (AWS) provides Amazon CloudWatch which is s monitoring service for AWS cloud resources and applications. It allows enterprises to collect and track metrics, collect and monitor log files, and se alarms. By leveraging Amazon CloudWatch, enterprises can gain system wide visibility into resource utilization, application performance, and operational health. By using these insights, enterprises can react as necessary, to keep application running smoothly and securely [12].

V. Conclusion

Cloud computing erupted as a path-breaking way on how technology, infrastructure and services can be used and has impacted everyone in some or the other way, big enterprises are no exception to that. For an enterprise to consider cloud as an IT infrastructure, there are few initial apprehensions which they need to overcome. For enterprises, data security is one of the top most priority and major concern before considering cloud based solution.

In this paper, we saw how cloud effectively and positively addresses various enterprise security related concerns and comes as a winner solution for various real-world enterprise data storage challenges.

Cloud computing is already getting wide consumer acceptance, Amazon e-commerce is fully operated from cloud, even start-ups are using cloud based IT infrastructure because of its flexibility in capacity usage and pricing. Big financial institutions like Goldman Sachs [13] and JP Morgan Chase [14] are exploring and investing in cloud computing as part of their long-term strategy. Cloud solutions are still evolving and with coming time cloud providers will make their products and platform more secure with superior control mechanism in place for the client to configure security. With major retail and financial instructions showing trust in cloud solutions, there is no doubt that it will turn out as a good option for enterprises and businesses looking for security, flexibility, cost savings and ultimately better solutions. The prominence of cloud computing and its security is beautifully encapsulated in this quote by VivekKundra, Executive Vice President, Salesforce.com:

"Cloud computing is often far more secure than traditional computing, because companies like Google and Amazon can attract and retain cyber-security personnel of a higher quality than many governmental agencies"

References

[1]. O'Sullivan, Arthur; Sheffrin, Steven M. (2003). Economics: Principles in Action. Upper Saddle River, New Jersey: Pearson Prentice Hall. p. 29. ISBN 0-13-063085-3.
[2]. Nicholas A Sherwood . (2015). Enterprise Security Architecture: A Business-Driven Approach. CRC Press. ISBN978-1578203185.
[3]. Microsoft. What is cloud computing. https://azure.microsoft.com/en-in/overview/what-is-cloud-computing/ (accessed 22 Sep 2017).
[4]. IEEE. Cloud Service and Deployment Models. https://cloudcomputing.ieee.org/images/files/education/studygroup/Cloud_Service_and_Deployment_Models.pdf (accessed 22 Sep 2017).
[5]. Tech Target. Shared responsibility model. http://searchcloudcomputing.techtarget.com/definition/shared-responsibility-model (accessed on 23 Sep 2017).
[6]. Paul, Allen, Bambara, Joseph. Enterprise Architect Guide. p. 35. ISBN 978-93-392-2222-2.
[7]. Tom C. W. Lin. Compliance, Technology, and Modern Finance. 2016.
[8]. Amazon Web Services. AWS Cloud Compliance. https://aws.amazon.com/compliance/. (accessed on 23 Jul 2017).
[9]. Dhanjani Nitesh. Hacking: The Next Generation. ISBN: 8184048149.
[10]. Raghuram Yeluri, Enrique Castro-Leon. Building the Infrastructure for Cloud Security: A Solutions View. ISBN: 1430261455.
[11]. Mather Tim. Cloud Security and Privacy. ISBN: 8184048157
[12]. Baron, Joe, Baz, Hisham et al. AWS CSA official study guide. ISBN 978-81-265-6578-8.
[13]. McKinsy. Banking on the cloud. http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/banking-on-the-cloud. (accessed on 23 Jul 2017).
[14]. NetworkWorld. JP Morgan: "Monumental" shift of enterprise workloads to the cloud. http://www.networkworld.com/article/3059282/cloud-computing/jp-morgan-monumental-shift-of-enterprise-workloads-to-the-cloud.html. (accessed on 23 Jul 2017).

Author

Gautam Deb is currently working as a Lead Engineer with Software AG in Hyderabad (TS), India. He has overall 12 years of industry experience in designing and developing large scale, highly available, fault tolerant and scalable enterprise software systems. He holds a MCA degree from JNV University Jodhpur, India and also an AWS Certified Solutions Architect – Associate certification for cloud computing.

IOSR Journal of Computer Engineering (IOSR-JCE) is UGC approved Journal with Sl. No. 5019, Journal no. 49102.

Gautam Deb. "Cloud Computing: Enterprise Applicationand Data Security Challenges And Solutions." IOSR Journal of Computer Engineering (IOSR-JCE), vol. 19, no. 5, 2017, pp. 54–60.