Volume 5, Issue 10, October-2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Storage Threat Avoidance Using Data Encryption on Cloud

Archana G. Said

AISSM IOIT, Assistant Professor, Computer Engineering

India

Abstract— Cloud computing is current buzzword in the market and IT industry. It is paradigm in which the resources can be leveraged/shared on per usage criteria thus reducing the cost and complexity of service providers and thus increases availability. Cloud computing promises to cut operational and capital costs and more importantly let IT sectors focus on strategic projects instead of keeping huge datacenters running. It is much more than only internet. It is a construct that allows user to access services that actually reside at location other than user's personal computer or other Internet-connected devices. There are numerous benefits of this factor. For instance other company hosts user application. This implies that they handle variable cost of servers, they manage software updates/validations and depending on the contract user pays less i.e. for the service only. Confidentiality, Integrity, Availability, Authenticity, and Privacy are essential factors for both Cloud providers and consumers as well. Security is considered a key requirement for cloud computing consolidation as a robust and feasible multipurpose solution [1]. This perspective is shared by many distinct groups, including academic researchers [2,3], business decision makers [4] and government/semigovernment organizations [5,6]. Infrastructure as a Service (IaaS) serves as the foundation layer for the other release models, and a lack of security in this layer is going to affect the other delivery models, i.e., PaaS, and SaaS that are built on top of IaaS layer. This paper presents an exhaustive study of Cloud threats and its corresponding security aspects of data on cloud.

Keywords—Cloud Computing, Cloud Computing Security, Security Characteristics

I. INTRODUCTION

Cloud is large pool of easily available, usable, accessible and sharable virtualized resources. These resources can be on demand reconfigured to adjust to a variable load (scale), allowing optimum and efficient resource utilization. It is a pay-per-usage model in which the Infrastructure Provider by means of customized Service Level Agreements (SLAs) offers guaranteed pool of resources. Organizations and individuals can benefit from mass computing and storage centers, provided by large companies with stable and strong cloud architectures in terms of highly available resources. Cloud computing incorporates virtualization, on-demand deployment and request provider, Internet delivery of services, and open source software. Cloud computing uses approaches, concepts, and best practices that have already been established. Cloud computing is a technology that uses the internet as a backbone and central remote servers to maintain huge amount of data, applications and numerous sharable resources. Cloud computing allows consumers and businesses to use applications without installation of software on their personal computers and access their personal files at any remote computer with internet access.

II. CLOUD COMPUTNG SERVICES

Corporate and government entities utilize cloud computing services to address a variety of application and infrastructure needs such as CRM, database, compute, and data storage. **Cloud Computing Services** provide information technology (IT) as a service over the Internet or dedicated network, with delivery on demand, and payment based on usage. **Cloud computing services** range from full applications and development platforms, to servers, storage, and virtual desktops.

A. Infrastructure-as-a-Service

The Infrastructure as a Service is a provision model in which an organization outsourcers the equipment used to different support operations, includes various resources like storage, hardware, servers and networking components. The service provider owns the resource and is responsible for handling, running and maintaining it. The client typically pays on a per-use basis.

Characteristics and components of IaaS include:

1. Utility computing service and billing model.
2. Automation of administrative tasks.
3. Dynamic scaling.
4. Desktop virtualization.

5. Policy-based services.
6. Internet connective

Infrastructure-as-a-Service like Amazon Web Services provides virtual server instances with unique IP addresses and blocks of storage on demand. Customers use the provider's application program interface (API) to start, stop, access and configure their virtual servers and storage. In the enterprise, cloud computing allows a company to pay for only as much capacity as is needed, and bring more online as soon as required. Because this pay-for-what-you-use model resembles the way electricity, fuel and water are consumed it's sometimes referred to as utility computing. Infrastructure as a Service is sometimes referred to as Hardware as a Service (HaaS).

B. Plateform-As-A-Service

Platform as a Service (PaaS) is a way to rent out hardware, operating systems, storage and network capacity over the Internet. The service delivery model allows the customer/consumer to rent virtual servers and associated services/resources for running existing/predefined applications or developing and testing new ones. Platform as a Service (PaaS) is an outcome of Software as a Service (SaaS), a software distribution model in which hosted software applications are made available to customers over the distributed network. PaaS has several advantages for developers. With PaaS, operating system features can be changed and upgraded frequently. Geographically separated development teams can work together on software development projects in an efficient way. Services can be obtained from different sources that cross international boundaries. Initial and ongoing costs can be reduced by the use of available infrastructure services from a single vendor rather than maintaining multiple hardware facilities that often perform duplicate functions or suffer from incompatibility problems. Overall expenses can also be reduced down by unification of programming development efforts. On the downside, PaaS involves some risk of "lock-in" if offerings require proprietary service interfaces or development languages. Another potential shortcoming is that the flexibility of offerings may not meet the needs of some users whose requirements rapidly evolve.

C. Software-As-A-Service

No Software as a service referred to as "software on demand or software on request" is software that is deployed over the internet and/or is deployed to run behind a protected firewall on a local area network or user’s personal computer. With SaaS, a provider licenses an application to customers either as a service on demand, through a subscription on timely basis, in a "pay-as-per-usage" model, or at no charge at all. This approach of application delivery is part of the utility computing model where all of the technology is in the "cloud" accessed over the Internet as a service on demand. SaaS was initially widely deployed for sales force automation and Customer Relationship Management (CRM). Now it has become commonplace for many business tasks, including computerized billing, invoicing, human resource management, financials, content management, collaboration, document management, and service desk management.

III. CLOUD COMPUTNG SECURITY ISSUES

In the recent years, cloud computing has grown from being a adhering business concept to one of the fastest growing segments of the IT and commercial industries. Now, recession-hit companies are increasingly realizing that simply by tapping into the cloud they can gain fast access to best-of-effort business applications or drastically fasten their infrastructure resources, all at almost negligible cost. But as more and more information on individuals and companies is placed in the cloud, concerns are beginning to grow about just how safe an environment it is.

A. Security

Consumers are using cloud infrastructure such as a file, memory and sharable resources on demand as per need for their project development. Data processing is done and again processed data in uploaded back to the cloud storage. One question arises that whether data is secured on cloud or not ?

B. Privacy

Different from the traditional computing model, cloud computing utilizes the virtual computing technology, users’ personal data may be dispersed in distributed virtual data center rather than stay in the same physical location, even across the national borders, at this time, data privacy protection will face the controversy of different legal systems. On the other hand, users may leak hidden information when they accessing cloud computing services. Attackers can analyze the critical task depend on the computing task submitted by the users .

C. Reliability

Servers in the cloud have the same problems as your own resident servers. The cloud servers also experience downtimes and slowdowns, what the difference is that users have a higher dependent on cloud service provider (CSP) in the model of cloud computing. There is a big difference in the CSP’s service model, once you select a particular CSP, you may be locked-in, thus bring a potential business secure risk.

D. Legal Issues

Regardless of efforts to bring into line the lawful situation, as of 2009, supplier such as Amazon Web Services provide to major markets by developing restricted road and rail network and letting users to choose “availability zones”. On the other hand, worries stick with safety measures and confidentiality from individual all the way through legislative levels.

IV. CLOUD COMPUTNG MODELS

A. Public Cloud

A public cloud is one based on the standard cloud computing model, in which a service provider makes resources, such as applications and storage, available to the general public over the Internet. Public cloud services may be free or offered on a pay-per-usage model.

The main benefits of using a public cloud service are:

1. Easy and inexpensive set-up because hardware, application and bandwidth costs are covered by the provider. Scalability to meet needs.
2. No wasted resources because you pay for what you use.
3. The term "public cloud" arise to differentiate between the standard model and the private cloud, which is a proprietary network or data center that uses cloud computing technologies, such as virtualization. A private cloud is managed by the organization it serves. A third model, the hybrid cloud, is maintained by both internal and external providers. Examples of public clouds include Amazon Elastic Compute Cloud (EC2), IBM's Blue Cloud, Sun Cloud, Google AppEngine and Windows Azure Services Platform

B. Community Cloud

Private cloud (also called internal cloud or corporate cloud) is a marketing term for a proprietary computing architecture that provides hosted services to a limited number of people behind a firewall. Advances in virtualization and distributed computing have allowed corporate network and datacenter administrators to effectively become service providers that meet the needs of their "customers" within the corporation. Marketing media that uses the words "private cloud" is designed to appeal to an organization that needs or wants more control over their data than they can get by using a third-party hosted service such as Amazon's Elastic Compute Cloud (EC2) or Simple Storage Service (S3).

C. Hybrid Cloud

A hybrid cloud is a Cloud Computing environment in which an organization provides and manages some resources in-house and has others provided externally. For example, an organization might use a public cloud service, such as Amazon Simple Storage Service (Amazon S3) for archived data but continue to maintain in-house storage for operational customer data. Ideally, the hybrid approach allows a business to take advantage of the scalability and cost-effectiveness that a public cloud computing environment offers without exposing mission-critical applications and data to third-party vulnerabilities.

D. Private Cloud

A community cloud may be established where several organizations have similar requirements and seek to share infrastructure so as to realize some of the benefits of cloud computing. With the costs spread over fewer users than a public cloud (but more than a single tenant) this option is more expensive but may offer a higher level of privacy, security and/or policy compliance. Examples of community cloud include Google's "Gov Cloud".

V. CLOUD COMPUTING THREATS

Before deciding to migrate to the cloud, we have to look at the cloud security vulnerabilities and threats to determine whether the cloud service is worth the risk due to the many advantages it provides. The following are some of the security threats in a cloud environment:

Ease of Use: Data on cloud is scattered and shared between no. of user by cloud providers. As cloud allows ease of user characteristic it may be harmful as it can be attacked by attackers as data is sharable.

Secure Data Transmission: When transferring the data from clients to the cloud, the data needs to be transferred by using an encrypted secure communication channel like SSL/TLS. This prevents different attacks like MITM attacks, where the data could be stolen by an attacker intercepting our communication.

Insecure APIs: Various cloud services on the Internet are showing no. of interfaces to the application programming interfaces. Since the APIs are accessible from anywhere on the Internet, malicious attackers can use them to compromise the confidentiality and integrity of the enterprise customers. An attacker gaining a token used by a customer to access the service through service API can use the same token to manipulate the customer's data. Therefore it's imperative that cloud services provide a secure API, rendering such attacks worthless.

Malicious Insiders: Employees working at cloud service provider could have complete access to the company resources. Therefore cloud service providers must have proper security measures in place to track employee actions like viewing a customer's data. Since cloud service provides often don't follow the best security guidelines and don't implement a security policy, employees can gather confidential information from arbitrary customers without being detected.

Shared Technology Issues: The cloud service SaaS/PasS/IaaS providers use scalable infrastructure to support multiple tenants which share the underlying infrastructure. Directly on the hardware layer, there are hypervisors running multiple virtual machines, themselves running multiple applications.

Data Loss: The data stored in the cloud could be lost due to the hard drive failure. A CSP could accidentally delete the data, an attacker might modify the data, etc. Therefore, the best way to protect against data loss is by having a proper data backup, which solves the data loss problems. Data loss can have catastrophic consequences to the business, which may result in a business bankruptcy, which is why keeping the data backed-up is always the best option.

VI. DATA STORAGE & SECURITY IN CLOUD COMPUTING

In cloud network data is stored in distributed environment where data owner also not knowing where his/her data is hosted. Cloud storage is a model of networked enterprise storage where data is stored not only in the user's computer, but in virtualized pools of storage which are generally hosted by third parties, also. Hosting companies operate large data centers, and people who require their data to be hosted buy or lease storage capacity from them. The data center operators, in the background, virtualized the resources according to the requirements of the customer and expose them as storage pools, which the customers can themselves use to store files or data objects. Physically, the resource may span across multiple servers which are physically separated among different areas. The safety of the files depends upon the hosting websites [3].

Cloud storage services may be accessed through a web service application programming interface (API), a cloud storage gateway or through a Web-based user interface.

Cloud storage characteristics are:

1. It is made up of many distributed resources, but still acts as centric data storage
2. It is highly fault tolerant through redundancy and distribution of data across number of storage servers
3. It is highly durable through the creation of randomized copies scattered over the entire network
4. Data replication provides consistent data availability in case of system downtime

Data storage security refers to the security of data on the storage media which are hosted on distributed data servers, which means non-volatile or fast recovery after data loss due to unavoidable interrupts. This security should be taken into account by software engineers/risk analyses in design stage of cloud storage services. It includes not only data redundancy (replication of data over different machine like RAID system) storage and dynamic, but also isolation (Full data transfer or not at all). Redundancy is the most basic measures to protect data storage security, and dynamic means user data may often change, so effective measures are needed to ensure data consistency. Isolation is that since different user's data is stored in the same platform, to guarantee the independence between the data, which means user can only access their own data, and data changes of other users will not affect the current user so that data loss will not occur while transaction is going on.

VII. CENTRALIZED DATA-ENCRYPTION AND DATA STORAGE ON DISTRIBUTED ENVIRONMENT

Data-centric protection through encryption renders the data unusable to anyone that does not have the key to decrypt it. No matter whether the data is in motion or at stable state, it remains protected. The owner of the decryption keys maintains the security of that data and can decide who and what to allow access to the data. Encryption procedures can be inte-grated into the existing workflow for cloud services. For example, an admin could encrypt all backup data before send-ing into the storage cloud. An executive can protect corporate IP before putting it into the private cloud. And a sales representative could encrypt a private customer contract before sending it to a collaborative worksite, like Sharepoint, in the public cloud. For data encryption process following algorithms can be used

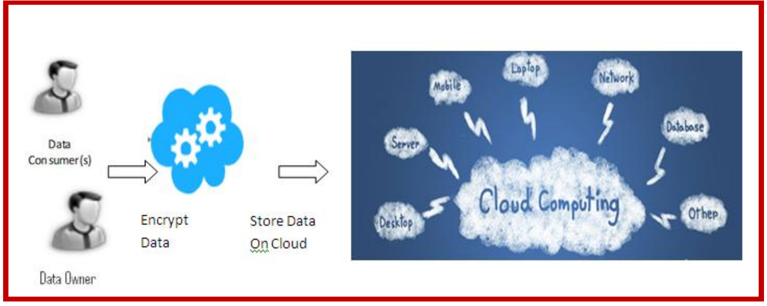

Fig 1. Secure Cloud Storage

`

1. **RSA**- It is an asymmetric encryption algorithm in which two keys are used private key for data encryption and public key for decryption at other end.
2. **DES** – It is symmetric data encryption algorithm in which large key size is used which is hard to be affected by Brute-Force attack. Variation of DES like 2DES, 3DES can increased data encryption complexity which is good so that attacker can cannot decrypt the data.
3. **AES** – Multiple rounds can be used to increase complexity level.

VIII. CONCLUSION

When an enterprise company wants to move their current operations and data to the cloud, they should be aware of the cloud threats in order for the move to be successful and profitable. We shouldn't rely on the cloud service provider to take care of security for us; rather than that, we should understand the security threats and communicate with our CSP to determine how they are addressing the security threats and continue from there. We should also create remote backups of our data regardless of whether the CSP is already providing backup service for us – it's better to have multiple data backups than figure out the data was not backed up at all when the need for data restoration arises. We should store data in encrypted format before it is uploaded on cloud so that it cannot be hacked even if any of the data center on the cloud in compromised

REFERENCES

[1] Oleshchuk VA, Køien GM (2011) Security and Privacy in the Cloud – A Long-Term View. In: 2nd International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology (Wireless VITAE), WIRELESS VITAE '11. pp 1–5

[2] Cong Wang, Qian Wang, Kui Ren and Wenjing Lou "Ensuring Data Storage Security in Cloud Computing." IEEE 2009.

[3] Genovese S (2009) Akamai Introduces Cloud-Based Firewall. http://cloudcomputing.sys-con.com/node/1219023

[4] Hulme GV (2011) CloudPassage aims to ease cloud server security management. http://www.csoonline.com/article/658121/cloudpassageaims- to-ease-cloud-server-security-management