Security threats, risks and open source cloud computing security solutions for libraries

Mayank Yuvaraj

Introduction

In recent years, a large number of organizations have found that cloud computing has many advantages leading to a surge in its adoption. Cloud computing involves the usage of large servers for the access of data, its storage and manipulation as well as provisioning of other services. When infrastructure, applications, data and storage are hosted by cloud providers, there are huge security risks associated with each type of service offered. There are a number of considerations, apart from cost which must be evaluated before choosing any particular provider. Sometimes, the physical location of the servers may also be a factor to consider, if sensitive duty is involved.

Security in the cloud

Security in the cloud implies the security of data and the services offered to the organization by the cloud service provider. The word “security” is an umbrella term used to connote various policies, technologies and controls used for protecting data, applications and the associated infrastructure within the cloud. The data stored in the cloud exist on a set of networked resources remotely which can be accessed through virtual machines. These virtual machines usually run in data centres which could be located anywhere in the world, beyond the control of the users which causes numerous security and privacy challenges. The security concerns can be broadly typified into two categories: one faced by the cloud service provider and another by the end users.

Top threats to cloud security

Data breaches

A data breach is a situation that arises due to the leakage of important and sensitive data. If there is some flaw in the design of the cloud service database, then attackers can access sensitive information from all the client applications posing a serious threat to the data in the cloud. However, data can be encrypted to reduce the impact of the breach so that even if there is a leakage, the hacker cannot decipher the encrypted information. These threats can be overcome through split key management and homo-morphic key encryption. In split key management, the encryption key is split into two parts where the first part of the key is managed by the security application of the cloud, while the other one is looked after by the end user that work jointly for decrypting the data. In this method, if at any point the data are being used illicitly by another, the data remain unaffected.

Data loss

The very presumption of loss of stored data in the cloud permanently is frightening. Even in the cloud, data are a major concern. Loses could be caused by malicious attackers, accidental deletion by cloud service providers or physical catastrophes like fire or earthquakes. Another possibility is if the customer forgets the encryption key of the data; this could also lead to permanent loss of data. Once the data are lost, it is forever irretrievable unless the cloud service provider maintains a backup for the data at all times, although this could indirectly make data breaches easier.

Account or service traffic hijacking

Account or service traffic hijacking could happen through various methods such as phishing, fraud and exploitation of software vulnerabilities. With stolen credentials, attackers can gain access to the cloud computing services and affect the confidentiality and integrity of the cloud services. To meet these challenges, libraries should leverage strong two-factor authentication techniques and prohibit the sharing of account credentials between users and service providers.

Insecure interfaces and Application Programmer Interfaces

There are several Application Programmer Interfaces (APIs) used by cloud service managers to provide services to users. The security and availability of cloud services, in general, is determined through the security of these APIs. Any insecurity in the interfaces or APIs could cause a catastrophe in cloud services.

Denial of service attacks

As the name suggests, it simply means denying users the cloud services, to the extent that they might not even be able to access their own information. Denial of service (DoS) attacks are caused by forcing the victim cloud service to not respond which is mainly caused by making the cloud service consume large amounts of resources like memory, processing power, disk space or network bandwidth. The attackers cause an intolerable system slowdown, thus leaving the users confused and unhappy. Intrusion Detection System can be used for defence against DoS attacks.

Malicious insiders

Malicious insiders within any organization can cause the whole cloud service to become unstable and breach the organization security to access the privileged information. To address this issue, these following measures can be taken: specifying human resource requirements as part of legal contracts, existence of transparency in the overall information security and management practises along with compliance reporting, setting up insider-theft prevention programs and determining security breach notification processes.

Abuse of cloud services

The services and resources rented out by the cloud service provider can be accessed by the attackers for illicit purposes. Through cloud computing services, attackers can easily decrypt the hacked data stored in cloud. Centralized log monitoring, setting alerts for log policy violations as well as encryption key breach alerts assist in early detection of user abuse.

Shared technology vulnerabilities

Sharing technology can create vulnerabilities on the cloud. Various cloud services are delivered to customers through shared infrastructures, platforms and applications. Security best practises like proper installation and configuration, monitoring the environment for unauthorized changes in activities, promoting strong authentication and access procedures should be followed to confront this threat.

Risks in the cloud – policy and organizational risks

Lock-in

The lock-in problem takes place when applications, data and services are dependent on a single cloud provider. Being locked in is one of the biggest problems in the cloud computing environment that occurs due to high level of customization to meet user needs.

Loss of governance

The cloud provider may subcontract or outsource services to third parties who may not offer the same guarantees that are given by the cloud provider. There are chances that control and the operational management of the cloud provider may get changed, so the terms and conditions of their services may also change.

Compliance challenges

Cloud providers make large investments to get external certifications like SAS 70, PCI, HIPPA etc. In the market, these certifications give them the reputation of following the best security practises. In some cases, a particular certification may also be a problem while accessing cloud services.

Cloud service termination or failure

There must be 24 × 7 support and high availability of all cloud based services. It is possible some cloud computing service providers could terminate their services for a short or medium period of time affecting the flow of work. By storing data in the cloud, an organization is completely dependent over the service provider for computing needs.

Supply chain failure

There is the possibility that cloud providers could outsource some services to third parties where lack of coordination may affect the cloud services.

Risks in the cloud – technical risks

Isolation failures

Because cloud computing works on multi-tenancy and shared resources architecture, there is a sharing of computing capacity, storage and network among multiple users. It also leads to some threats like failure of logistics, memory, storage, routing tables, SQL injection attacks and guest hopping attacks.

Resource exhaustion

A cloud service is a fully on-demand, pay-per-use service. There are challenges in the allocation of resources to cloud users. Although there are many resource allocation algorithms used for allocating all the resources of cloud services, insufficient resource provisioning and investments in infrastructure may lead to a problem linked to service unavailability or degradation in performance.

Intercepting data in transit

Cloud services are based on a distributed architecture. Therefore, transmission of data takes place across multiple physical machines from one virtual machine to another and image distribution is between the cloud infrastructure and remote Web, VPN environment, etc. The vulnerability is greater when data are being transferred from on premises to the cloud or vice-versa.

Insecure or ineffective deletion of data

It is impossible to delete any data stored in the cloud without destroying the disk which could also include data of other clients. Data may not be completely wiped out from the cloud for which effective encryption method may be required.

Risks in the cloud – legal risks

Risks arising due to changes in jurisdiction

It is a tedious task to figure out the exact location of the stored data in the cloud. It is possible that data can be stored in countries which lack enforceable rules of law which do not care for international agreements.

Data protection risks

It is impossible for the cloud customer to determine whether their stored data are being handled in a lawful manner. In cloud computing, data confidentiality and leakage is a major issue.

Other risks in the cloud

Unauthorised access to premises

Due to inadequate physical security procedures, unauthorised access in a data centre is possible. Generally, the cloud service providers have large physical control of the data centre which should be stronger to prevent breaches.

Theft of computer equipment

The risk occurs due to inadequate physical security procedures, particularly with relation to data centres. Only authenticated persons must be allowed to enter physical facilities and a dual authentication mechanism should be followed to access those machines.

Natural disasters

Natural disasters are possible at any time, so there must be a perfect disaster recovery plan.

Open-source trusted cloud security solutions

OSSEC – HIDS (open-source security host-based intrusion detection system)

To check the risks and threats, OSSEC (www.ossec.net) is the best cloud computing solution. OSSEC is an open-source host-based intrusion detection system having scalability, and it is compliant on multiple platforms. It works on client-server model. The OSSEC server must be installed on a Linux/UNIX machine and the client can be run on any operating system that works well with cloud instances. OSSEC servers and agents can be installed on AWS instances that can be used to monitor file integrity checking, real time file monitoring and log inspections.

Snort

Snort is a fully open-source network intrusion preventive and detection system. It can perform real time analytics on IP networks. It has three main modes of working – as a sniffer, a packet logger and in network intrusion detection. It can be used with AWS and EC2 instances also. Snort host-based IDS supports tracking of running processes, detection of configuration changes, tracking of file access and detection of any abnormal behaviour. Snort provides in-flight data encryption for cloud instances like in AWS. All incoming traffic passes through the elastic load balancer, which is used as an HTTPS terminator. It works like proxy traffic for back-end IDS instances as HTTP. Snort is used here for packet analysis and to decide whether to reject or accept the packet. After transmission, Snort analyzes the outbound packet and logs the results.

CryptSync

The best way to protect files is to encrypt them before moving them to other services. CryptSync provides an additional layer of security, which makes it difficult for attackers to view files. It uses two folders which work synchronously. One folder contains current working files which are unencrypted and the other folder contains encrypted files.

Crypton

Crypton has been developed by SpiderOAK and licensed under the AGPL. Crypton enables applications to encrypt data in the Web browser itself before moving to cloud storage. It supports the Javascript library for Web applications that offer an object storage API. The data storage backend of Crypton is built with compatibility to PstgresSQL, Redis and Node.JS.

TrueCrypt

It is an open-source disk encryption application that provides real time and transparent encryption support. It has the ability to create a virtual encrypted disk within a file and display it as real disk.

Concluding remarks

The purpose of this short paper was to evaluate risks and security threats that are barriers to the adoption of cloud computing in libraries and to bring to light various open source cloud-based security solutions to overcome these threats. After an exhaustive literature survey and interview of library professionals regarding the adoption of cloud computing in libraries, the core security and risks areas were identified and a search was made to find out existing security solutions to overcome these barriers. This study fills the gap and provides solutions to security concerns that have been the main cause of non adoption of cloud computing in libraries.

Mayank Yuvaraj (*mayank.yuvaraj@gmail.com*) is based at Central University of Bihar, Patna, India.