NETWORK COMPUTING AND CLOUD COMPUTING

Dr. DEEPIKA MARWAHA, RIDHIMA DUTTA

PG Department of Computer Science And Applications, Government college for girls, Ludhiana.

E-mail: profdeepikamarwaha@gmail.com, ridhimadutta@gmail.com

I. INTRODUCTION

Cloud Computing‟ has enabled the use of internet related services on any web enabled device such as a phone, a laptop etc. In this, the virtual shared servers provide software, infrastructure, platform hosting to the customers on pay-per-use or on subscription basis in which the users remotely store and access personal files such as music, pictures, videos, play games etc. Though, the increasing adoption of cloud computing has raised several important concerns about security. This paper discusses security issues that are associated with the client and cloud and their effect on the organizations that host their applications in the cloud. It discusses how we can try and reduce the security threats in these platforms and applications to make them as secure as possible.
“Client and Cloud” describes a concept of computing that is currently seeking a great deal of attention in the IT industry. Using cloud computing the clients/companies/organizations can hire the computing resources as a utility on pay-per-use or on subscription basis and can use them to make services available to client applications over the Internet. Though it is being adopted quickly but its adoption has also raised some concerns about its security, both for cloud service providers as well as for the clients using these cloud services. Three main features, which are considered important from security perspective, are as under:

- For managing the computing resources that host the cloud-based applications, a third party is required..
- The client applications‟ data is stored by the cloud services.
- The client application can use any business system that may not necessarily be a web browser.

Any organization wanting to implement “client and cloud” computing must secure the following two elements of cloud environment:

- Third-party Cloud Platform
- “In the cloud” applications

The security of the software that is used to implement the cloud platform and the

operational security applied by the third party that is actually providing the cloud platform, are two areas on which the overall security of the cloud platform depends.This describes some guidelines for the organizations that want to host their applications "in the cloud". The paper begins by explaining how an organization can apply the Security Development Lifecycle (SDL) for developing its "client and cloud" applications, and how the SDL can evolve to meet the demands of this environment. The paper then discusses the operational security policies that can be applied to its cloud platform, and also explain the level of security that clients can expect from the cloud platform.

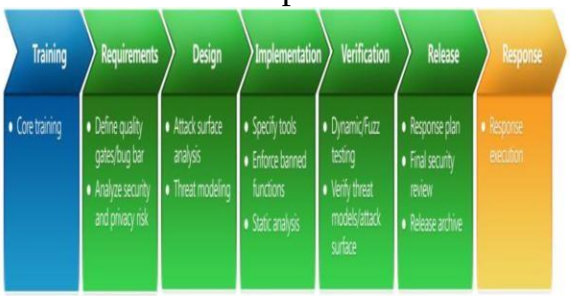
III. NEED FOR SDL

Developing software for "client and cloud" platform and applications is almost similar to developing any other type of software. So software development life cycle must address security issues at all its phases. Like conducting threat modelling in design phase ensures effective security by identifying the potential threats before actually coding of software begins. The software development teams must make sure that coding standards are being followed in the implementation phase as it implies that they are trying to provide security in the best possible manner. In testing phase, along with conducting other tests, tests for security and privacy must also be conducted to make sure that the secure design has been implemented. Realizing this, various development teams/groups have felt the need for security development lifecycle for systematically handling various security threats in the software that is being developed by them for "client and cloud" platform and applications. This security development lifecycle may be used in business environments and must be web or Internet based.

III. THE SECURITY DEVELOPMENT LIFE CYCLE

The Security development Lifecycle (SDL) is a set of processes and tools that are used to reduce the number and severity of problems in the software products. It requires training for developing personnel; secure development processes, and accountability of individuals and product teams for building secure software.

The following diagram outlines the SDL process.



The SDL process requires the above-mentioned activities to be completed by the software development teams during each phase.
Each phase is briefly described below:

- Requirement Phase: In this phase key security objectives are identified which maximizes software security without changing client‟s plans, and schedules.
- Design: In this phase possible attacks are surfaced and threat modelling is conducted.
- Implementation: In this phase the software development team must make sure that the code is in compliance with the standards and is free from any security vulnerability.
- Verification: In this phase, the software development team must ensure that the code is fulfilling all the security and privacy norms that were established in the previous phase.
- Release: In this phase Final Security Review (FSR) is conducted to verify the product‟s security with the security requirements specified in the SDL or the requirements that are specific to that product. The product is shipped only if all the security requirements are met.
- Response: After release, the software development team identifies, monitors, resolves and respond to all kind of security queries.

IV. SHARING SDL

Any organization can share the SDL and related tools publicly, and can also offer consulting assistance in applying the SDL. In this way, any organization can use it for developing more secure software for itself. Using the SDL as a part of its development methodology, any organization having its own “in the cloud” security requirements can make sure that its application meets those security requirements.

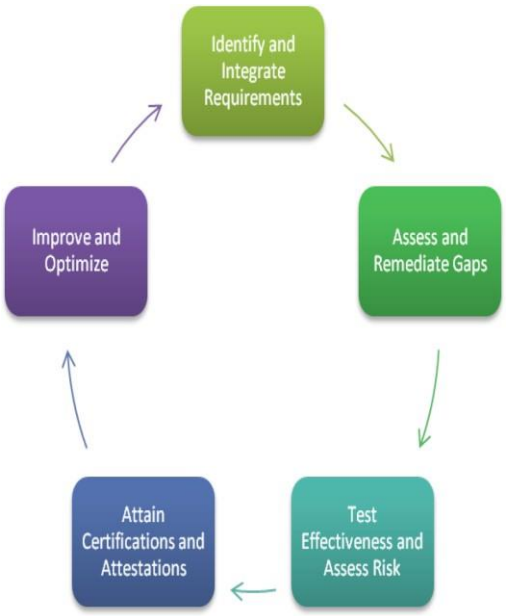
V. OPERATIONAL SECURITY TO CLOUD SERVICES

Client and cloud applications can be developed by using SDL for reducing the number and severity of security threats. After deploying the application to the cloud, a clearly defined set of security policies is applied to it in order to protect the application from various security threats.

The Requirement Phase and the Release Phase of the SDL are involved in the operational security of "in the cloud" applications. During the Requirements phase the security and privacy risks in a cloud-hosted application must consider the target operational environment. An Operational Security Review (OSR) along with the FSR is conducted in the Release Phase. In OSR the application"s network communications, platform requirements, system configuration etc are reviewed against the established security standards. This is done to make sure that security controls are part of the operational plans before giving permission to deploy the software to the cloud environment.

VI. POLICY COMPLIANCE

Almost all online service environments must meet a number of security requirements that are established by the government and industry, in addition to their own business specifications. For this an organization may form a team that may work with the operations, product and service delivery teams, auditors (both internal and external), to ensure that the standards are being complied with and obligations are being met. For this purpose, the team may follow a comprehensive compliance framework. This framework consists of five steps as shown in the following diagram:



Steps in compliance framework

Various activities involved in each step of this Compliance framework are as follows:

Step 1: Identify and integrate requirements: This step includes

- Identification of scope and controls
- Gathering required operating and process documents
- Reviewing the above stated documents and controls.

Step 2: Assess and remediate gaps :

This step includes

- Identifying the gaps/non-compliance to standards in process or control.
- Rectifying these gaps.

Step 3: Test effectiveness and assess risk: This step includes

- Measuring the effectiveness of controls.
- Preparing the report.

Step 4: Attain certifications and attestations: This step includes

- Obtaining the third party certifications from auditors.

Step 5: Improve and optimize:

This step includes

- Analysing the document and identifying the cause of any non-compliance.
- Taking remedial steps to rectify the error.
- Optimising the controls for better security and efficiency in future reviews.

VII. FINAL THOUGHTS: CLOUD SERVICES AND SECURITY

As we have seen, the first phase of the SDL includes the identification of the security requirements that must be met by the product or service to be developed. The security requirements of product or service will differ from one another depending upon the type of system. The systems may be classified as low, moderate, or high business impact for determining security requirements and the strength of security features that they must provide. This classification considers the financial and reputational damage in case the product or service is involved in a security issue. For example, the moderate impact category data is subject to encryption requirements when they are stored on removable media. The high impact category data is subject to encryption requirements for storage and for internal system and network transfers. For all cloud services, the documentation provided to users should always specify what is protected and how it is protected. For example, the users/clients who want to host their applications "in the cloud" may want to have their applications and data protected from the applications and data of other users. The cloud service provider must provide the desired level of protection to all such users. Other security features and protection requirements will vary from user to user, and from application to application, according to type of data and applicable laws and regulations. The "cloud" service client must be clear about the strength and level of the security protections that its cloud services provides so that users willing to use that particular "cloud" will know clearly about the security features available in that cloud, depending on which he will be able to determine how it will protect their applications and data. This information provided to them in clear format by the cloud service providers will help the users/clients to evaluate the suitability of cloud platform for their security requirements and to make decisions about them using a particular cloud services or not.