SECURITY REQUIREMENTS SPECIFICATION FRAMEWORK FOR GOVERNMENT SECTOR CLOUD USERS FOR CLOUD COMPUTING PROJECTS

by

Rida Naveed

A thesis submitted to the faculty of Information Security Department Military College of Signals, National University of Sciences and Technology, Rawalpindi in partial fulfillment of the requirements for the degree of MS in Information Security

MAY 2014

SUPERVISOR CERTICATE

IT IS CERTIFIED THAT THE FINAL COPY OF THESIS HAS BEEN EVALUATED BY ME, FOUND AS PER SPECIFIED FORMAT AND ERROR FREE.

_____

ASST. PROF. DR. HAIDER ABBAS

ABSTRACT

SECURITY REQUIREMENTS SPECIFICATION FRAMEWORK OF GOVERNEMENT SECTOR CLOUD USERS FOR CLOUD COMPUPTING PROJECTS

BY

Rida Naveed

Cloud computing is a novel way of using a collection of easily accessible virtualized computing resources from hardware, to development platforms or services. It gives an enterprise opportunity to scale up itself and deploy new applications and resources in no time in order to meet increasing demand of its customers; hence reducing their expenses for hardware, maintenance and IT staff. Many organizations are embracing cloud computing in their businesses around the world. These organizations contain systems consisting of a huge volume of critical processes and information whose security must certainly be ensured. Security is one major concern for the individuals or organization. These security issues arise because of exploiting vulnerabilities within cloud infrastructure. An attacker can exploit these vulnerabilities and can easily compromise a system if security requirements are not considered at the time system functional requirements are being identified. Therefore, a system engineering methodology for security requirements identification and elicitation centered on vulnerabilities and threats is needed.

In this research work, we aim to fill this gap of incorporating security requirements at the early stage of cloud system deployment process for government sector cloud users for cloud computing projects. This thesis focuses on the state of the

art concerning security requirements for governmental organization having classified data by highlighting critical security challenges introduced in cloud environment, analyzing and engineering these specific security requirements to form a system having security enforcement mechanisms incorporated at the time system's functional requirements are been met thus eliminating security challenges within it.

A security requirements specification framework is proposed that provides a methodology to Gcloud users to move step by step for achieving secure cloud services for their organizations.

DEDICATION

“In the name of Allah, most Gracious, most Compassionate".

I dedicate my thesis work to my parents, my husband, my daughter and my teachers who have always been there for me for constant encouragement and guidance and without their presence this work might not have been possible.

ACKNOWLEDGEMENT

To begin with my thesis, I would like to thanks Almighty Allah Who has bestowed upon me with His countless blessings and mercy, gave me strength and intellect, increased my knowledge and made me capable of what I am today.

First of all, I would like to present gratitude to my supervisor Dr. Haider Abbas, who was always there for me for his kind help throughout my work. He continuously inspired and encouraged me with his novel ideas and suggestions which kept me in right path till the end of my work. He was the one who believed in me and provide me confidence in myself to write an international paper which was later published in Future Information Technology, Lecture Notes in Electrical Engineering by Springer. Without his devotion, constant support, guidance, encouragement and patience my research work would not have been possible.

I would like to acknowledge my guidance committee members Dr. SeemabLatif, Mr. Ahmed Raza Cheema, Mr. MianWaseem Iqbal and Phd Scholar Ms. Rabia Latif for their persistent support and motivation.

I would also like to thank Mr. Ali Raza and Mr. Tanveer Mujtaba who provided me an opportunity to discuss and interview different personals in their organization which provided me great understanding of their security requirements issues and their concerns for moving to cloud service providers.

I would also like to pay gratitute to my Head of Department Dr. BaberAslam and his team for administrative help and support.

I am immensely thankful to my mother and husband who constantly encouraged and supported me throughout my MS studies.

Table of Contents

LIST OF FIGURES

LIST OF TABLES

KEY TO ACRONYMS

OS	Operating Ssystem
NIST	National Institute of Science and Technology
HaaS	Hardware as a Service
IaaS	Infrastructure as a Service
DaaS	Data as a Service
CaaS	Communication as a Service
API	Application Program Interface
AES	Advanced Encryption Standard
SSL	Secure Socket Layer
ACW	Anti Corruption Wing
PaaS	Platform as a Service
SaaS	Software as a Service
CSP	Cloud Service Provider
SRE	Security Requirements Engineering
SR	Security Requirements
RE	Requirements Engineering
Gcloud	Government sector cloud
SRSFGCU	Security Requirements Specification Framework for Government sector Cloud Users

Chapter 1

Introduction

1.1 Overview

Cloud computing has emerged as outsourced resource sharing computing technology that provides on-demand storage, software, computational power, infrastructure and network access to its users over the internet [6]. The implementation of virtualization, service orientation and grid computing technologies, has increased the trend of organizations and business entities towards its adaption. Because of various benefits like rapid resource sharing, location independence and elasticity, it has overcome a long awaited vision of separating users from their physical hardware needs thus; providing them more flexible and scalable IT services [2][4][5].

Cloud computing, despite of its tremendous benefits,doesn't come without its drawbacks. The combination of different computing technologies in cloud computing gives rise to various security and privacy concerns. These concerns, if not taken into consideration can become security threats for the organizations adapting cloud model.

1.2 Need for Research

The wide spread emergence of cloud technology signifies that more in depth study must be done to explore its prospective from deployment point of view. Cloud is in a process of adoption by many businesses from private to government sector cloud users, having classified data. When these Gcloud users have to move their confidential systems and processes to cloud, they must know in depth about the technology i.e.; cloud architecture, its security concerns and security requirements onto which their data will reside. Thus, a need arises to analyze system specific

security requirements and form a methodology for secure cloud adoption. This work will fill in the gap of secure cloud adaption and deployment; for government organizations having classified data by taking into consideration their user's specific security requirements. Analyzing the Gcloud user's security requirements and engineering them into appropriate solutions to be realized will be my area of focus.

1.3 Problem Statement

Cloud computing is a new field to explore. A number of researches have been carried out relating to cloud security but analyzing system specific security requirements and realizing them in a methodology for secure cloud adaption by government organizations; is still an open field for research. Therefore, there is a need to research Gcloud users' specific security requirements and propose them with a framework that can provide safe asylum to their classified data in cloud computing environment.

1.4 Objectives

The objectives of this research is to analyze security requirements of government organization cloud users and device a methodology in a form of framework; which they can use in achieving secure cloud services for their cloud computing based systems. The analysis will be carried out through a study of literature on cloud computing architecture, its security concerns and requirements. It also aim to develop an efficient security requirements benchmark checklist to be used by Gcloud users before they borrow services from CSP.

1.5 Research Methodology and Achieved Goals

The research work comprised of two phases. The first phase of this thesis provides literature review about cloud computing technology and security issues for

this system, followed by security requirements for its service models. In second phase, engineering security requirements concept is thoroughly investigated and a methodology in a form of framework is proposed for classified cloud users.

1.6 Thesis Organization

The thesis constitutes of seven chapters. Chapter 2 contains background and literature review about cloud conputing architecture, cloud computing security issues, cloud computing security requirements and SRE in adopting cloud computing models. Cloud computing security requirements and Security Requirements of Government sector Cloud Users are given in chapter 3 and 4 respectively. Security Requirements Specification Framework for Government Sector Cloud Users is explored in chapter 5. Chapters 6 evaluate and comparison of proposed framework on a case study project. Chapter 7 concludes this thesis report and suggests future work.

Chapter 2

Background and Literature Review

2.1 Introduction

Cloud Computing is promising technology that is under rapid adoption by enterprise as well as individuals. In this chapter an overview of cloud computing technology and security concerns faced by it is given. Security requirements engineering; an emerging concept which emphasize on the importance of considering security and privacy requirements of any system at the very beginning of its deployment. A brief overview of work related to security requirements engineering, its integration in cloud computing technologies and its adoption by government sector cloud users is also given in this chapter.

2.2 Cloud Computing Technology Literature Review

Cloud Computing refers to a collection of IT resources accessible over the network. With the use of virtualization, service orientation and grid computing technologies, has increased trend of organizations and business entities towards its adaption. National Institute of Standards and Technology (NIST) has defined Cloud Computing as: "*a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models [11].*"

2.2.1 Cloud Architecture

There are three service models that describe in what ways a cloud can render services to its users. Different layers in the cloud architecture serve different purposes. There is low coupling between the layers hence the cloud architecture is readily adaptable to the changes.

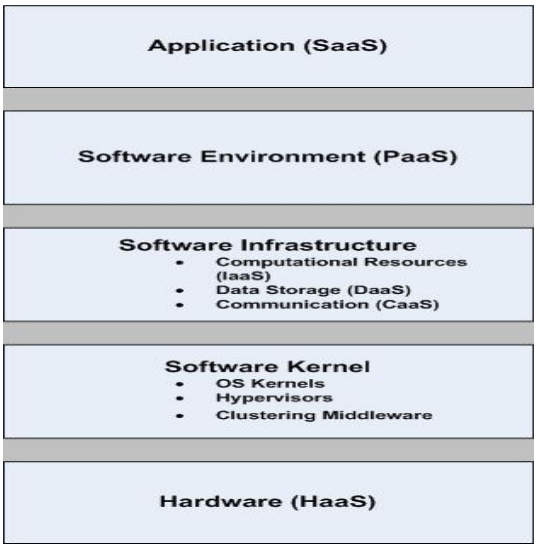

Figure 2.1: Cloud Architecture

2.2.1.1 Hardware as a Service - Hardware is the lowest layer in cloud architecture that is available in the form of servers like high ended computing machines or database servers and the network infrastructure contains network devices e.g. switches and routers. Since the cloud is a collection of more than one servers and machines, so they all need to connect in order to form a cloud. For this connection the communication devices are an essential.

This is one major edge of the cloud computing that the resource sharing and reusing is made possible. Cloud computing is attracting many users because it is cheaper as compared to each user buying its own hardware. So this layer is called Hardware as a Service (**HaaS**).

2.2.1.2 Software Kernel - The layer above the hardware layer is the software kernel of the cloud. This layer is a connection between the software part of the cloud and the

cloud hardware. Its job is to manage the hardware resources. As this layer has to perform different but relevant responsibilities this layer is composed of an operating system kernel, hypervisors and clustering middleware. Just like the normal operating system kernel's responsibilities, the job of this ***software kernel*** is to handle system calls, memory management and device management. ***Hypervisors*** support virtualization i.e. more than one operating system can run on the same machine (server in this case). Virtualization improves the utilization of under lying hardware. Hypervisors can run directly on the underlying hardware or on the operating system kernel. Another part of this layer is ***clustering middleware***. Different processes or applications running on the cloud do not seem distributed to the user though they might be running on different servers at a time. The application running process is seamless to the users but still if one application is running on more than one server at a time, the inter process communication is inevitable. The clustering middleware serves this purpose.

2.2.1.3 Software Infrastructure- Layer that lies exactly above the software kernel is the software infrastructure layer. The responsibility of this layer is to provide network resources to the other two abstract layers. This layer works as a software infrastructure for the users. The services this layer provides broadly fall into these categories:

- Computing Service
- Storage Service
- Communication Service

The **computing services** are available to the cloud users in the form of virtualization. With virtualization one physical server appears to be more than one logical servers. Hence the cloud resources are utilized in a better way.

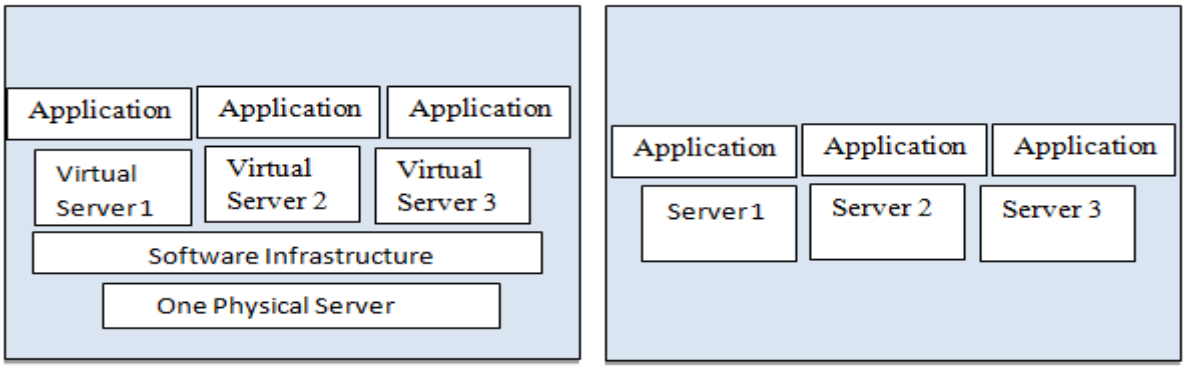

Figure 2.2: Virtualization

The **storage service** allows the cloud users to store their data on cloud servers and access from anywhere using the internet connection. Storage service is also called Data-Storage as a service (**DaaS**). The usage of these servers has some related performance measures e.g. Speed of access, scalability and reliability etc. Cloud providers choose among these measures that which measure they want to focus in their cloud design.

The communication cloud makes with its users should also be reliable, secure and if required it should also be encrypted. This layer also provides this service and is termed as Communication as a Service (**CaaS**). The provision of network bandwidth, management of traffic flows and network monitoring are done by this layer.

2.2.1.4 Software Environment - This layer is also called platform as a service. This layer serves as a platform for the cloud applications. The main interaction of this layer is via the predefined set of APIs. The cloud developers use these APIs to develop application for cloud. The cloud is hence used as a means to distribute applications. Two examples of existing software environments to cloud software developers are the Google App Engine and Salesforce.com's Apex code. These two cloud software environments are available to the clouds software developers to develop application that can be deployed on the cloud. Another platform available for cloud hosting is Microsoft's Windows Azure.

The applications developed using the software environments are able to benefit from the existing cloud services e.g. load balancing, dynamic scaling and authentication.

2.2.1.5 Application Layer- The top layer in the cloud architecture is application layer. This layer is also called Software as a Service (SaaS). It serves as a bridge between the cloud applications and the cloud application consumers. It lets the cloud application consumers access the cloud software applications free or on payment based on the usage permissions of that application.

The applications installed on the cloud use cloud hardware and computing power and the consumers access these applications via the web browsers on thick or thin clients using the internet. The computing costs at the user's end are hence dramatically reduced.

The software applications that exist on the cloud are managed and maintained by the cloud service hosts. The update or modification in the deployed applications is easy in a way that the change is seamless to the users as the whole application resides on the servers of the cloud service provider. Google apps are an example of software as a service (SaaS).

2.2.2 Cloud Service Models

The NIST has suggested three service models for cloud computing from a cloud service provider's point of view i.e. SaaS, PaaS and IaaS.

Infrastructure as a Service or Hardware as a Service is used to provide cloud users with the expensive and fast cloud hardware e.g. high processing power, huge storage, servers and network bandwidth. The hardware is an important resource that all the individual users or small organizations cannot afford to own. Cloud computing offers this hardware as a service to the users hence this huge cost at the users' end is

eliminated. Platform as a Service is popular among the cloud application developers. The cloud software application developers use the cloud software platform as a service to render their application to the cloud users.

2.2.3 Cloud Deployment Models

These deployment models are suggested by the NIST and each has certain specialties. Each type offers a different security level and caters different business requirements from service host point of view.

2.2.3.1 Private Clouds - This deployment model is an isolated cloud that can be accessed only by a specific group of people via a virtual private network or an intranet within that organization's firewall. It can be set up off site and managed by a third party as well.

This model is also suitable for mission specific computing needs. There can be some private and confidential data that only needs to be accessed for the target. These clouds are common when a service provider lets the clients to manage their own private clouds and interact with the service provider as needed, for example AMAZON.

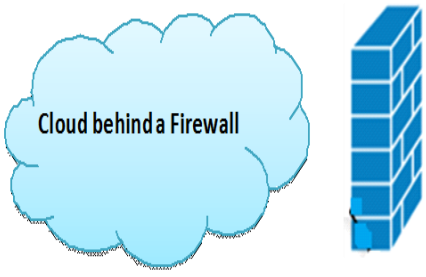

Figure 2.3: Private Cloud

2.2.3.2 Public Clouds- These clouds are set up for general public and host the services targeted by them. These cloud infrastructures are large and may be managed by more than one cloud service vendors. The logical data and concerns separation

within the hosts is always present and data access and modification is possible only by authorized access.

Webmail services offered by HOTMAIL and YAHOO are an example of public clouds.

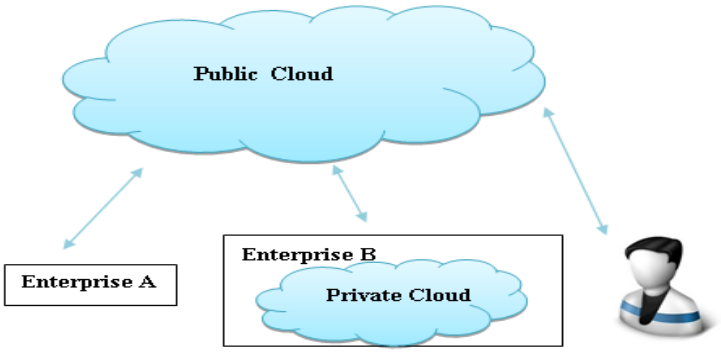

Figure 2.4: Public Clouds

2.2.3.3 Community Clouds - This cloud infrastructure is a shared structure with multiple organizations based on alike benefits. When more than one organization may have similar cloud set up requirements, they may agree and set up a community cloud. In this manner the set up costs are divided in the sharing organizations.

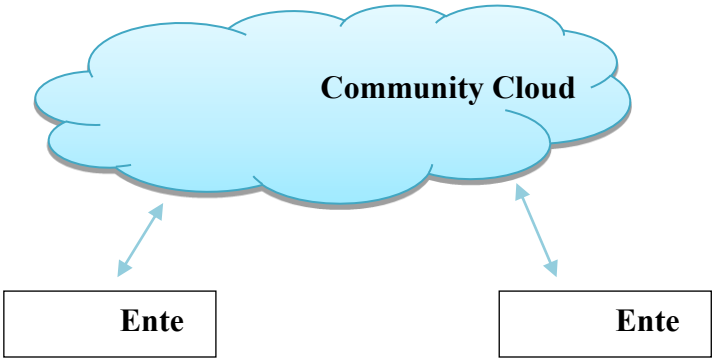

Figure 2.5: Community Clouds

2.2.3.4 Hybrid Clouds - This cloud infrastructure is a blend of different cloud infrastructures i.e. public, private and community clouds. In this infrastructure different clouds interact via predefined APIs. Via these APIs applications and data can travel between the clouds.

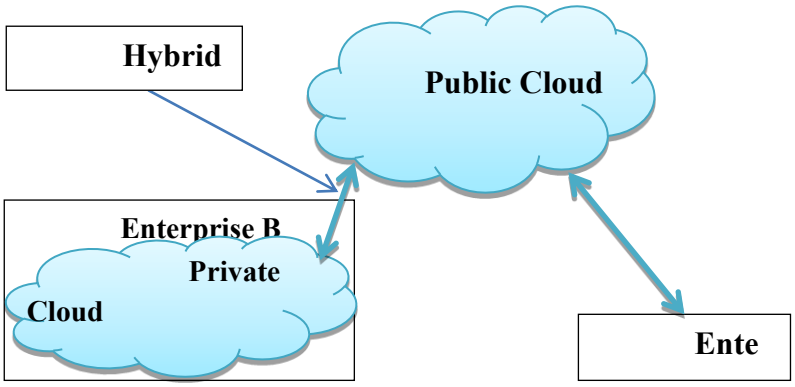

Figure 2.6: Hybrid Clouds

2.2.4 Cloud Computing Security Concerns

Cloud computing, despite of its tremendous benefits, does not comes without its pitfalls [15]. The amalgamation of different computing technologies in cloud computing gives rises to various security and privacy concerns. These concerns, if not taken into consideration can become security threats for the organizations adopting cloud model [21].

Gcloud users must understand this fact that CSPs are independent entities and moving towards cloud infrastructure will take away direct control over their systems that manages their data and applications. Although CSPs have more reliable and powerful infrastructure and managing capabilities than individual computing systems, yet they are faced by various security issues. CSPs can also intentionally examine users' data, multi-tenancy and virtualization allows multiple users to simultaneously share distinct applications on same physical hardware. These features despite of increasing resource sharing also presents new security and privacy concerns for cloud users. Here we present several critical security challenges that are faced by users when introduced in cloud environment.

2.3.1 Data Confidentiality and Integrity - Due to clouds greater flexibility and cost-efficiency, users tend to store more and more data onto it. Here its confidentiality and integrity are at risk, as users no longer physically possess their data.

2.3.2 Lack of transparency - Cloud lack transparency of its operations from its users especially if their outsourced computational workloads contain sensitive information.

2.3.3 Service Metering and Usage Charges - It is of critical importance for CSPs to have a trustworthy relationship with its customers on its service metering and usage charges. As cloud is a shared resourced network so its memory, network bandwidth, I/O and CPU cycles consumed per user cannot be isolated, nor can its charges per resource consumption is fairly computed.

2.3.4 Multi-tenancy and virtualization - It increases risk of side channel attacks and privacy leaks, making reliable security difficult to achieve.

2.3.5 In House Security Risks - As the data of client is residing on host servers there are chances of intentional or unintentional data modification or falsification of clients' data from within the host organization. The in house employees have easy access to this data. For example Amazon's EC2 is a service provider that can read and alter clients' data [18].

2.3.6 Risks for Cloud Host - Cloud services are offered to different user accounts. If any of these accounts is compromised then the compromised account has access to cloud services and data, if this data is misused or tempered then the clients will lose faith in the cloud host which can result in great business loss. The cloud service users are not going to tolerate the security breaches or corruption of their data so the cloud host needs to focus much on implementing high cloud security[18] [19].

2.3.7 Security and Speed Tradeoff - Low or no security implementation will result in higher data rates and higher computation rates on user's data. If some encryption is

implemented, it will result in security but the usage of that data will be relatively slow due to the fact that encrypted information cannot be used as such in computations or by user directly, it needs to be decrypted before use [18] [19] [20].

2.3.8 Increasing Cloud Users - As cloud computing is delivering quite reliable and high performance, there are high chances of having more users shifting to cloud in near future. Hence more information security risks are expected [22].

2.3.9 Data Security over the Network - There is a lot of data transfer between the client and the cloud when the client uses the cloud services. The network over which the data travels needs to be secure in order for successful cloud service utilization.

2.3.10 Privacy - The users should be given the guarantee of confidentiality, integrity and availability of their data. Confidentiality means the users' data that is residing on the host servers will only be accessed by the authorized personnel. Integrity means that the data will not be corrupted or modified rather it will stay in its original form and data will be available to the user when needed [23].

2.3.11 Inherent Security Challenges - Cloud is a collection of servers, storage servers and network devices which are connected to each other via network, cloud computing therefore, suffers from its traditional network and computer security challenges. For example, back doors, denial of service, traffic flow analysis, session hijacking, impersonation, man in middle, distributed denial of service, network attacks, hardware theft, misuse or modification, IP spoofing and packet sniffing etc are quite known attacks [22]. Sometimes the users by unfair means can seize more network bandwidth than allowed. It results in business loss for the host as less band with is available hence less users will be entertained [23].

2.3.12 Other Security Concerns - Security of cloud data becomes even more complex when there will be applications that will let data travel between different

service providers. Data interception, impersonation, infrastructure misuse, latency, natural disaster, returning of incorrect results, software bugs, hardware failure, cross user data de-duplication, data deletion and attack on cloud servers can cause the cloud to behave deceitfully [18].

2.2.5 Cloud Computing Security Requirements Literature Review

The critical security challenges discussed above have become commonplace and they need to be addressed keenly. These security concerns arise by not considering the security requirements at the beginning of the system development process.

When cloud user decide to take cloud services, the security requirements for their systems and processes that will reside on CSP infrastructure are not taken into consideration. This reults into a cloud based system with vulnerabilities and loopholes. Therefore, a need of considering security requirements of a cloud based system, at an early stage of system development process rises. Many researches have been carried out that highlight the need of considering security requirements of a system at the stage its functional requirements are been defined [1], yet considering security requirements of Gcloud users; having classified data; in adopting cloud computing has not been taken care of.

This work fills gap towards this field of research, we have used security requirement engineering methodology for this purpose, which has not been proposed in current research work to date. By the use of SRE we intend to analyze Gcloud user's security requirements and will propose them a methodology in a form of a framework for secure cloud adoption.

SRE is being used by several authors in their research work to propose framework for systems to identify their security requirements alongside their

functional requirements. Below is a brief overview of work done previously by several authors:

2.2.5.1 Security Requirements Engineering: A Framework for Representation and Analysis – In this paper Haley's and his colleagues provides representation and analysis of security requirements of a system and engineering them in the form of a framework [1]. In their work, they have explained *adequate security requirement* that must satisfy definition, assumptions and satisfaction criteria. According to them, security requirements vary depending on a system's context. These are non-functional requirements of any system and are not considered as an essential component of systems deployment processes; rather they are usually ignored in creation of a system.

Analysis: A framework for security requirements engineering is presented that must satisfies four main activities in every iteration one, *identify functional requirements* - In this step they suggest to provide a system's context and to achieve system's context is left open to the user, two, *identify security goals* - these are achieved by identification of system's assets and applying managing principles to them, three, *identify security requirements* defines security requirements as constraints on functional requirements of a system and they must satisfy applicable security goals identified in step two and four *construct satisfaction argument* involves verification of security requirements as per system's context[1].

2.2.5.2 A Model Based Security Requirements Engineering Framework Applied for Online Trading System – In their paper, authors have described the importance of security requirements engineering for a system at the time its requirements engineering is done [5]. The framework they provide take few steps from Haleys' model and built their own model which overcomes the complex nature of framework proposed by Haley in [1].

Analysis: It includes followiing steps, *Inception* includes *identifying objectives of software system, identify stakeholders, identify assets. Elicitation* that involves stakeholders and requirement engineers work together to identify problem in a system, propose its solution and then determine set of security requirements. *Elaboration, negotiation and validation, specification* leads to design of security requirement.

2.2.5.3 Evaluating Cloud Deployment Scenarios Based on Security and Privacy Requirements – This paper depicts a need of security and privacy requirements for cloud, selection of suitable deployment models according to organizations' needs, modeling languages techniques and RE framework generalized for cloud users and CSP's [7].

Analysis: The modeling language and processes involved in this framework doesnot clearly mention which steps to follow in order to adopt cloud services by cloud users or vice versa. Security requirements need is highlighted but generalized overview of necessary possible security requirements checklist is not given. Move over, a complex structure is proposed to meet security and privacy in cloud deployment.

2.2.5.4 NIST, Challenging Security Requirements for US Government Cloud Computing Adoption – In this paper authors provide challenging security requirements to US government for cloud adoption in order to reduce setup cost and avail necessary services. The risks and concerns faced by US government in migration of their services to cloud are highlighted.

Analysis: The paper not only describes important security requirements but also identify improvements in each, if applicable. If mitigations are not identified, it provides a set of activities and makes recommendations that help to improve security threats and risks identified by each SR.

2.2.5.5 Other Related Work - Literature provides efforts that take cloud computing security and privacy concerns, identifying threats, vulnerabilities and attacks on cloud infrastructure [8] [9] [12]. Cloud security concerns and security issues with its deployment models, provide points to consider before mitigating to cloud and highlight various approaches for migrating to cloud are discussed [13]. Cloud adoption by several governments including US,UK and Australia and provide guidelines for government agencies in cloud adoption [11] [14].

2.3 Summary

In this chapter, we have provided literature review of cloud computing technology, its architecture, service and deployment models. Important security issues faced by cloud computing are also discussed. Security requirements and its need in cloud computing technology is provided along with existing work on the topic by different authors. Haley provides a four step artifact based framework for SRE of a system in [1], Salini and Kanmani, provides inception, elicitation and elaboration based framework for SRE [5]. Cloud migration based framework for both cloud users and CSPs is provided [7]. Where as challenging security requirements checklist for cloud adoption are provided to US government are explained in [11].

Chapter 3

Cloud Computing Security Requirements

3.1 Introduction

Cloud computing being an amalgamation of complex networked system is inherently affected by a great number of computer and network security issues. These security concerns arise by not considering the security requirements at the beginning of the system development process. Security requirements being constraint on systems' functional requirements must satisfy security goals [1] [25]. As cloud is available to users in three service models, therefore, understanding and clearly documenting user specific security requirements is very crucial in designing of vulnerability free computer systems [33] [39].

In this chapter security requirements for cloud service models are analyzed. The SR explained must be essential part of a CSP and these must be satisfied for providing a secure cloud services.

3.2 Security Requirements of Cloud Service Models

A detailed list of security requirements for cloud users in analyzed in Table 1 [6].

Table 3.1 Security Requirements of Cloud Service Models

Service Model	**Users**	**Security Requirements**	**Security Goals**
SaaS	End Users/Organizations who needs to access its application resources on rent	- True server authentication - Application software testing - Scalability - Maintenance of infrastructure - Service uptime and security - Security of sensitive data - Abstract interaction dynamics issues - Browser-based Risks - Network Dependence issues - Efficiency vs. Cost Tradeoffs - Privacy in multitenant environment - Access control - Communication protection - Service availability	- Confidentiality - Integrity - Availability - Accountability
PaaS	Developers/Moderators who needs to construct high quality dynamic applications and requires more application level logic to perform	- Browser-based Risks - Network Dependence issues - Efficiency vs. Cost Tradeoffs - Compatibility issues between PaaS Clouds - Processor Scheduling concerns - Application Reuse security issues - Access control - Application security - Data security - Cloud management control security - Secure images - Virtual cloud protection - Communication security	- Confidentiality - Integrity - Availability - Accountability
IaaS	System administrators who needs to access computational infrastructure available over the internet such as virtual computers, network, storage, infrastructure components such as firewalls, and configuration services.	- Abstract interaction dynamics issues - Browser-based Risks - Network Dependence issues - Efficiency vs. Cost Tradeoffs - Compatibility with legacy software vulnerabilities - Virtual Machine updating, checking and maintenance - Verifying Legitimacy of Web sites - VM-level Isolation - Data Erase Practices - Network protection - Network resources protection	- Confidentiality - Integrity - Availability - Accountability

3.2.1 Software as a Service

SaaS known as “Web Services” provide application services to its user to execute on the service provider’s servers via web browsers over the internet. The service providers rent these applications to subscribers. The subscribers get their full right to use any particular application including data management applications like data sharing and data backup[33].

Critical security requirement that must be considered in SaaS are [6]:

3.2.2.1 True server authentication- At the time of connection establishment between a server and a client, authentication should be two ways i.e. the server should also be authenticated so that any fake server or machine may not trick the user into being the original one [18] [19].

3.2.2.2 Application software testing- The applications deployed in the cloud should be tested for security. Any vulnerable or malicious application installed will damage cloud, its subscribers and host.

3.2.2.3 Scalability-The applications provided by the cloud should be able to handle the increasing cloud users i.e. at burst time.

3.2.2.4 Maintenance of infrastructure- The maintenance and uptime of cloud application services must be ensured.

3.2.2.5 Service uptime and security- Cloud services should be up and running most of the time and the security of these services must be ensured.

3.2.2.6 Security of sensitive data- The cloud subscribers may keep sensitive personal or business data on the cloud. So the service provider must ensure the security of this data.

3.2.2.7 Abstract interaction dynamics issues- One cloud application may be rented to more than one cloud subscribers via application execution resources. These execution resources must be risk free [18].

3.2.2.8 Browser-based Risks- Subscribers use web browsers to establish a link with the server. Weak or faulty cryptography in browsers can lead to information loss. Moreover, data from multiple applications may get mixed up in browsers. The separation of this data is important.

3.2.2.9 Network dependence issues- For reliable SaaS delivery, reliable network is required. Reliable service delivery is possible with reliable network.

3.2.2.10 Efficiency vs. cost tradeoffs- Multiple applications can co-exist in one client's computer without getting mixed up. This segregation is provided at huge cost by the operating system.

3.2.2.11 Privacy in multitenant environment- Maintaining privacy in a multitenant environment is important because users will never compromise on the privacy of their data stored on cloud or in their communication with cloud.

3.2.2.12 Access control- The users should be given more control while using cloud data storage service. It will give them more confidence that their data is not used by the host without their consent.

3.2.2.13 Communication protection- The communication subscribers do with the cloud should be strongly encrypted. Any intruder or malicious user must not be able to violate its security and hence protection [19].

3.2.2 Platform as a Service

A PaaS cloud service allows developers to develop feature rich vigorous cloud applications by publicizing a set of software building blocks, development tools and APIs. The software building blocks may include run-time environment and

programming languages. This layer contains more application development logic than application usage in comparison with SaaS [6]. There are few security concerns specific to PaaS clouds which are highlighted below:

3.2.2.1 Service availability- The cloud services should be available when subscribers request them.

3.2.2.2 Browser-based Risks- Subscribers use web browsers to establish a link with the server. Weak or faulty cryptography in browsers can lead to information loss. Moreover, data from multiple applications may get mixed up in browsers. The separation of this data is important.

3.2.2.3 Network dependence issues- For reliable service delivery, reliable network is required. Reliable service delivery is possible with reliable network.

3.2.2.4 Efficiency vs. cost tradeoffs- Multiple applications can co-exist in one client's computer without getting mixed up. This segregation is provided at huge cost by the operating system.

3.2.2.5 Compatibility issues between PaaS clouds- Portability is a concern when new applications for clouds are developed because the way platform services are implemented differs from one CSP to another.

3.2.2.6 Processor scheduling concerns- Application resources load increases with the increasing subscribers' request. The processor has a specified time in which it has to answer each service otherwise it gets queued for later services [18] [19].

3.2.2.7 Application reuse security issues- Cloud provides a set of services and tools for system development to its users, the security of these services and tools must be ensured.

3.2.2.8 Access control- The PaaS access must be controlled and balanced. No user would take more than the allowed access to any service.

3.2.2.9 Application security- The developed applications using PaaS must be tested for security. They need to be security ensured.

3.2.2.10 Data security- Data stored on the host platform must be made secure. No users with malicious intent or from within the host organization should be able to violate its security.

3.2.2.11 Cloud management control security- Cloud management and security mainly lies on the shoulders of the host. Services must be well managed and secure.

3.2.3 Infrastructure as a Service

IaaS, is used by system administrators. The IaaS service provide subscribers access to computational infrastructure available in the form of virtual computers, network, storage, infrastructure components such as firewalls, and configuration services over the network. IaaS also depends on a protected and steadfast network for service delivery and browser for account maintenance [6]. There are a number of issues specific to IaaS clouds as:

3.2.3.1 Abstract interaction dynamics issues- One cloud application may be rented to more than one cloud subscribers via application execution resources. These execution resources must be risk free.

3.2.3.2 Browser-based Risks- Subscribers use web browsers to establish a link with the server. Weak or faulty cryptography in browsers can lead to information loss. Moreover, data from multiple applications may get mixed up in browsers. The separation of this data is important.

3.2.3.3 Network dependence issues- For reliable service delivery, reliable network is required. Reliable service delivery is possible with reliable network.

3.2.3.4 Efficiency vs. cost tradeoffs- Multiple applications can co-exist in one client's computer without getting mixed up. This segregation is provided at huge cost by the operating system.

3.2.3.5 Compatibility with legacy software vulnerabilities- If a user runs legacy software with security vulnerabilities, these will be inadvertently inherited to the user [18].

3.2.3.6 Data erase practices- Multiple users access disk resource at different times, so data of previous user must not be accessible to the next. It must be made practice to erase data before lending disk resource to new user.

3.2.3.7 Virtual machine updating- When VM are accessed after a long time, they may become security out-o-date. It is users' responsibility to keep them security updated.

3.2.3.8 Checking and maintenance-VMs must be checked for security and security patches from host must be used.

3.2.3.9 VM-level isolation- VMs from different users must be kept separate because there might be malicious users in the users' pool. To avoid bugging each other, they must be kept separate [6].

3.2.3.10 Verifying legitimacy of websites- Third part credential services must be used to verify identify of the cloud service provider's website etc. Doing so is cloud users' responsibility and they can use public key cryptography for it.

3.2.4 Summary

These security requirements identified play an important role in system design. In this chapter we have discussed SR specific to each of cloud security model. Security of sensitive data, abstract interaction dynamics issues, browser-based risks, network dependence issues, efficiency vs. cost tradeoffs, access control and

communication protection are SR common to all service models. SR specific to SaaS explained are true server authentication, application software testing, scalability, maintenance of infrastructure, service uptime and security, privacy in multitenant environment, service availability. Compatibility issues between PaaS Clouds, processor scheduling concerns, application reuse security issues, cloud management control security, secure images and virtual cloud protection are SR specific to PaaS. Where as, **c**ompatibility with legacy software vulnerabilities, virtual machine updating, checking and maintenance, verifying legitimacy of web sites, VM level isolation, data erase practices, network protection and network resources protection are important SR needed for IaaS.

Chapter 4

Security Requirements of Government sector Cloud Users

4.1 Introduction

Security Requirements are defined as constraints on functional requirements of a system which provide a way to achieve system's security goals according to Haley and his colleagues [1].These SR plays an important role in formation of a vulnerability free system. This security requirements analysis must be done at the start of the cloud system development process so that the essential security enforcement mechanisms must be fitted in a system design process. This overcomes the common approach of including security within a system after the definition of a system [17].

In this chapter, the need of engineering security requirement of Gcloud users has been discussed.

4.2 Security Requirements Engineering

In this modern era of science and technology, information and systems are becoming critically important in day to day life. These systems are being used not only by individuals, small-to-large corporations but also by governments in their businesses, resulting in these systems containing a huge volume of critical data and processes, which must be taken care in order to keep it secure. When a system is designed it must satisfy functional requirements of its users, at the same time it must also be made secure. However, an idea to add security into a system comes after defining a system's needs, this result in fitting security mechanisms into already

designed system which can create various design challenges. When such systems come into being, they are highly affected with security vulnerabilities and threats.

As studies from various security models [1] [2] [3] propose solution to this problem through an amalgamation of security and requirement engineering [4]. Requirement engineering being a subfield of software engineering begins with the very first development phase and continues throughout lifecycle of a system. Security engineering, being a new field includes design, plan and processes required to maintain security of a system. Similarly, engineering a system that fulfills specific system's requirements, its business and security goals, provide security solutions, illustrates security specifications and policies, protect its assets, type of security level required and built a trustworthy system with adequate security needs and requirements is referred to as ***Security Requirement Engineering***.

According to Stefan Wind and Holger Schrödl, eliminating errors and vulnerabilities, at the deployment stage is one hundred times difficult than at development stage [3]. The same goes true for security requirement engineering, which enforce the identification of systems' security requirements at the stage where its functional requirements are defined; at system's development stage. Doing so will not only minimize security and functional requirements conflicts but will also isolate them at the beginning of systems development process.

4.3 Security Requirement Engineering and Cloud Computing

Cloud computing has emerged as a very promising technology that relies on the currently available IT infrastructure to function properly. Using the already laid network structure to deliver huge collection of IT resources is indeed a benchmark.

With great benefits that come with cloud computing, there come few risks as well. By shifting the data and commutation from local machines to cloud has greatly

helped many companies lower their IT expense. The cloud host has to take care of the maintenance and provision of services. The user does not have to worry about any such issue. One main concern that is almost equally important for both the user and the cloud host is cloud security.

Requirement Engineering for cloud computing has been addressed which emphasize on understanding of cloud user's requirements and implementing them into a realizable solution [3]. The analysis, understanding, elaboration and documentation of security requirements engineering for cloud computing is an area to explore.

4.4 Security Requirements Engineering for Government Sector Cloud Users

Computer literacy among common users and enterprises has enabled them to make use of online available resources, instead of creating their own infrastructure, through a developing utility model called cloud computing. In order to move towards cloud, governments need to understand how it differs from their existing traditional network architectures. Despite of its cost saving, flexibility and productivity benefits, it is a shared and large virtual environment. Enterprises need to understand the consequences of their data residing on cloud service provider's data center and under its protection. It is also important for them to understand the controls its cloud provider's has in place. In the cloud, federal managers need to recognize that while they still retain accountability for their data, the responsibility of its protection has passed to the vendor. They must fulfil the security requirements analyzed in chapter 3 inorder to provide secure cloud services and building a trust relationship with its customers.

This decision of moving towards cloud by a government organizations can be simply choosing the system they want to be on cloud and hire services from a CSP who fulfills their functional requirements and make it available to their users. But as the system comes in use many vulnerabilities may arise, although the system was developed according to organization's users' need. The reason being the system in use contains *a large amount of critical information and processes, which inevitably need to remain secure* [2]. Usually these security requirements are taken into consideration after system's development which results into fitting in security ensuring mechanisms into already designed system. Thus, an urge of considering security requirements along with functional requirements arises for the systems/services that government organizations wish to migrate to cloud.

4.4.1 Case Study

Security requirements must be documented along with functional requirements of any development process. A case study is taken from anti-corruption department of a government organization, whose main task is to deal with organized crimes such as anti-corruption, spurious drugs, counterfeit currencies, PPC and other laws, is assigned a project to develop an online cloud based system that must ensure free and fair recruitment of employees for a government agency. The functional requirements for the system to be designed may include a fair press release announcing vacancies in all electronic forums, creating an online thin client web based application form which everyone can access and apply, maintaining record of applicants, scrutinizing applicants, taking online tests, marking, informing qualified applicants and eventually forwarding them to the concerned department. Without considering security requirements at this early stage of system development process results in a system full of vulnerabilities and loop holes e.g.; the database where applicants' curriculum vita

is stored might come under hackers attack or what if a back up of this database is not maintained? Thus security requirements consideration at the beginning of system plays a crucial role in its smooth running.

4.5 Need of Security Requirements Engineering for Government Sector Cloud Users

There is a paramount shift in the way computing is now being performed in the computer Industry. Moving towards cloud computing symbolizes a major cultural transformation and is an important decision that organizations have to make. In order to make a right decision for Gcloud users in adopting cloud infrastructure, security requirement engineering must be done. Specific security requirements with respect to Gcloud users needs must be investigated and engineering these security requirements in a form of realizable framework needs to be done.

The thesis proposes a security requirements engineering framework, which helps Gcloud users from security burden [6], by providing them a methodology of identifying security requirements of their assets from the early stages of the cloud deployment process along side system's deployment requirements [2].

The next chapter introduces a theoretical framework for security requirements engineering. This framework is based on extensive study related to this field and from various discussions and interviews from Gcloud users and managing personals. The framework presented does not suggest a universal methodology it makes up already existing security requirements engineering frameworks.

4.6 Summary

In this chapter concept of security requirements engineering is discussed. SRE and its use in cloud computing technology by considering its security requirements

from early stage of systems' development process is explained. Its need and usefullness for Gcloud users is also presented.

Chapter 5

Security Requirements Specification Framework for Government Sector Cloud Users

5.1 Introduction

In this chapter, we have engineered the security requirements of classified Gcloud users in the form of a framework. This framework model provides a methodology to cloud users in general and government sector cloud users in specific, to identify security requirements of their assets at the time they decide to move their data towards cloud. It will help them to specify the level of security and privacy they require for their system that they would run on cloud infrastructure [2] [3].

5.2 Development Methodology

This framework is constructed by extensive study carried out about cloud computing, security requirements engineering, security requirements frameworks and models for systems, cloud security requirements, and is based on wide range of inputs and discussions about the cloud computing adoption by different law enforcement departments of Pakistan government. For details Appendix-A may be referred.

As a case study, a law enforcement department has been taken (as a governmental organization) who has to make decision of moving their processes to cloud service provider. A framework described shows how to move step by step for achieving secure cloud services for their organization. This cloud security assurance framework could be a road map for the governments and enterprises for moving their data to cloud.

5.3 Security Requirements Specification Framework

The framework is depicted as follows:

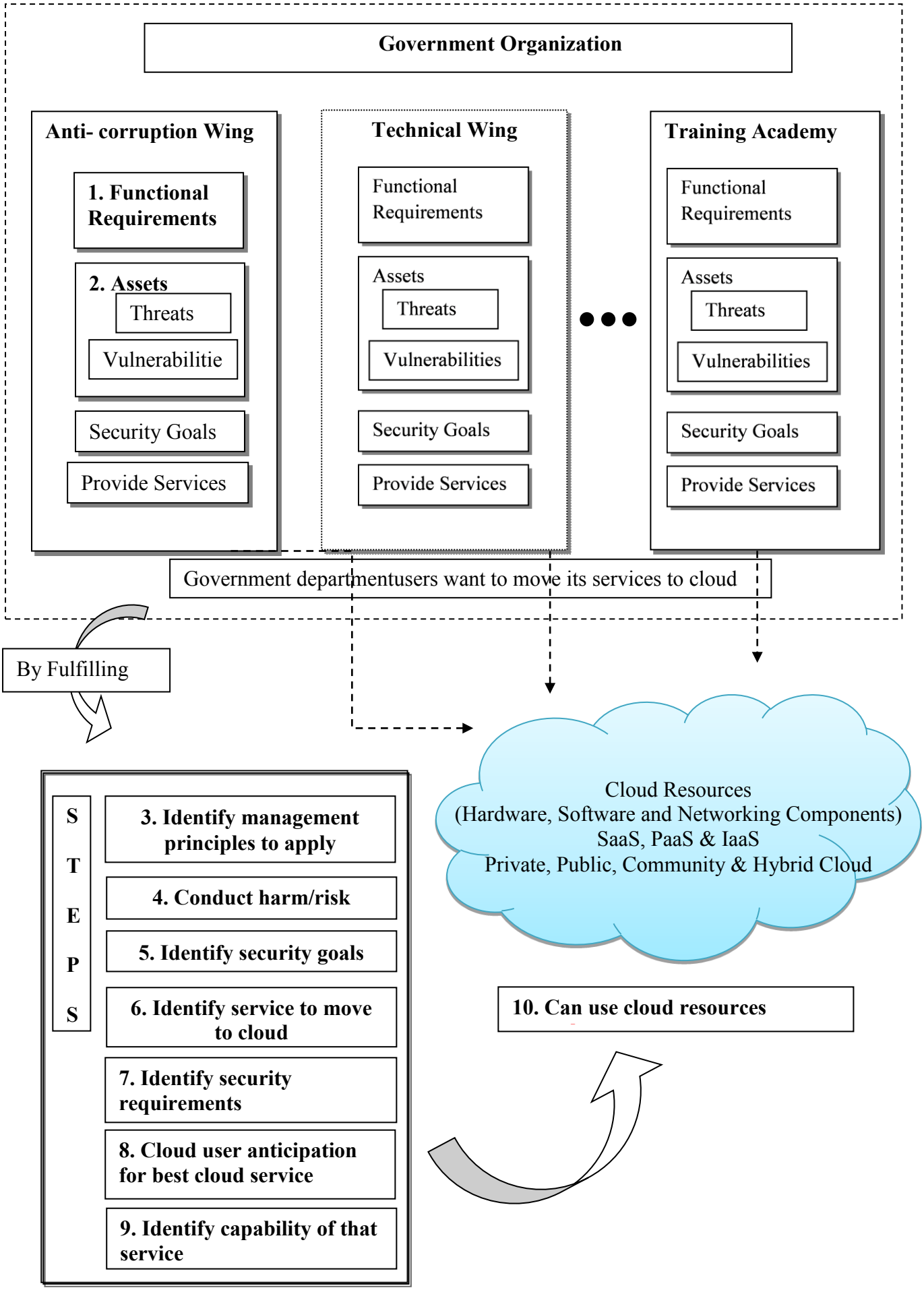

Figure 5.1 Security Requirements Specific Framework for Classified Cloud Users

Our cloud security assurance framework consists of following steps:

5.3.1 Identify Functional Requirements of Government Department

By identifying functional requirements means to draw all systems context for the law enforcement department under consideration [1]. It is done by identifying the necessary task, action or activity that must be accomplished by each of its department. A brief overview of tasks or actions each wing has to perform is shown in Table 6.1 [21].

Table 5.1Functional requirements identification table

Law Enforcement Departments	Functional Requirements
Anti-Corruption Wing	Deals with organized crimes such as anti-corruption, spurious drugs, counterfeit currencies, PPC and other laws.
Economic Crime Wing	Responsible for investigation of cases related to government revenue thefts.
Technical Wing	Provides scientific assistance to various units of federal government departments.
Immigration Wing	Regulates flow of incoming and outgoing international passengers and prevents human smuggling via airports, land routes, sea ports and railway stations.
Anti-Trafficking Unit	Deals with the prevention and control of human trafficking.
Legal Branch	Provide legal guidance in all administrative and operational matters.
Intellectual Property Rights Branch	Ensures that every system provides different types of warranty to ensure peaceful possession of property, tangible and intangible.
Interpol	Coordinate efforts relating to international police corporation.
Counter Terrorism Wing	Responsible to identify, arrest and put to trial most wanted terrorists and to provide qualitative investigations for counter terrorism
Academy	Responsible to prepare and train the newly hired officers of federal government

5.3.2 Identify Assets

The goal of this step is to find all resources in the system context that might have value. Assets may include information/data asset, technology asset, human

resource asset and service asset. In general, assets consist of the information resources stored in or accessed by the system-to-be and any tangible resources such as the computers themselves [1] [2] [21].

Taking Interpol as example, its assets include criminal record, finger print record, data base record, exit control list, police force working under it, hardware and software it uses etc.

5.3.3 Conducting Harm/Risk Analysis

After identification of assets one needs to classify them according to their threat severity and vulnerability. A harm/risk analysis must be done to identify the impact level that loss of confidentiality, integrity and availability may have on the assets. A value to the risks is then assigned to these assets in order to know its value, frequency of occurrence of threat or vulnerability and damage that the risk might inflict in the company [8].

Harm/risk analysis of each asset of Interpol must be done e.g; check threats and vulnerabilities for finger print record. What impact level it has if it gets available to unauthorized person (confidentiality breach), if the record is changed (integrity breach) and if the record is no more available to the organization (availability breach). A risk value is assigned on the basis of frequency of occurrence of these threats and vulnerabilities.

5.3.4 Identify Management Principles to Apply

After identifying system assets and doing their harm/risk analysis, the functions that each department is to provide must be compared to the management principles that it wishes to apply [1] [2] [21].

For Interpol as our government department has a duty to coordinate efforts relating to international police corporation. The management principles it wishes to apply include separation of duties of its employees, separation of functions they perform, required inspect trails and applicable global policies within the system under consideration must be identified and fed into the next step.

5.3.5 Identify Security Goals

A set of security goals is identified with respect to each asset after their harm/risk analysis and application of management principles to them [1] [2] [21].

One of security goals for Interpol includes, finger print record must be kept confidential. Other being, integrity of the data must be maintained for smooth running of system, the record must be available anytime to authorize users.

5.3.6 Describe Service that should be Migrated to Cloud

After defining security goals, organization must decide which parts of its services must be moved to cloud and which must not. This decision made must be based on security level of its assets and services. Mission critical services must not at all be moved to cloud in order to remain secure.

Interpol's ECL, must be available at all exits countrywide cloud users but adding/editing its contents must not at all be available to all users. So a decision of moving towards cloud must be made on security level impact for each asset and services.

5.3.7 Cloud User Anticipation for Best Cloud Service

An analysis of selecting appropriate cloud service provider must be done that best fit an organization's cloud needs. Identify the cloud composite architecture

needed from the cloud deployment and service models e.g. *Public IaaS, Public PaaS, Public SaaS or Private IaaS, Private PaaS, Private SaaSor Hybrid IaaS, Hybrid PaaS, Hybrid SaaSor Community IaaS, Community PaaS, and Community SaaS* [40].

5.3.8 Identify Necessary Capabilities of the Service

Next step is the identification of the necessary capabilities of the service that is selected in the previous step and check if the capability satisfies our system requirements.

Interpol can handle its service of fingerprint record system by the use of public SaaS with its roles and controls in place for remote users.

5.3.9 Identify Security Requirements

In this framework we have focused on identifying security requirements that are constraints on functional requirements of a system [1] [2] [21].These security requirements play a crucial role in achieving security goals and thus must be kept under consideration by cloud users before moving towards cloud. Generalized security requirement checklists for our government departments to consider are given below, these requirements can dynamically change and identifying new security requirements can be done from an updateable knowledgebase [11] [21] [42] [43] [44] [45] [46] [47]. For details, Appendix-A may be referred.

Pricing – The initial setup fee for cloud deployment, the ongoing charges for its services, if the fee is charged according to bandwidth usage or the number of users and by how much the cloud provider can increase their rates must be taken into consideration by the cloud users. Infrastructure setup cost and cloud service usage cost comparison should also be done.

Service Provider's Size - The actual size of the cloud service provider CSP, type of office it is housed in, size of its security team and if security a full-time job at the vender must be made sure by the cloud users.

Secure Area/ Physical entry control – The location where cloud service provider hosts its facilities must be in secure area. The level of security at entrance for the physical security, entry mechanisms, possible threats for computer rooms and data center and separate key access to each equipment rack in place where server hardware is stored must be ensured.

Power Supplies– protection of electronic equipment from power failures and other electrical anomalies must be ensured.

Cabling Security – All power and telecommunications cabling must be protected from interception or damage.

Equipment Maintenance – procedures must be established to correctly maintain IT equipment to ensure its continued availability and integrity.

Separation of Development and Operational Facilities – Operational and development facilities must be separated to minimize the risk of unauthorized access or accidental changes to data or production software.

Environmental Monitoring – Monitoring of host computer environments must be- done, including temperature, humidity, and power-supply quality, to identify conditions that might adversely affect the operation of computer equipment and to facilitate corrective action.

System Planning and Acceptance – Resource availability must be ensured by doing capacity planning and preparations in advance so that customers growing demand must be met.

Capacity Planning - Are capacity requirements monitored, and future requirements projected, to reduce the risk of system overload?

Availability of provider – Availability of provider must be ensured to by knowing the uptime guaranteed by the provider, how it is calculated, compensation for not satisfying the guaranteed uptime, cost per minute of your service downtime and is there a disaster recovery/business continuity plan available?

Sensitivity of Information Stored – The cloud users must be aware of the sensitivity of their data that they want to move towards cloud and risk profile must be made.

Data Storage – users must know the location of their data, data servers and who can access this data inside data centers. Whether the data is hosted on dedicated, or shared, hardware, the formats in which data is stored and are those formats easily convertible to the data storage formats used in house. Is the provider allowed to use data and/or metadata?

Data Accessibility – Cloud users must ensure that who has access to their data and applications and systems hosting them in cloud. What are the access controls in place according to roles and responsibilities of cloud users i.e. which user has to access which part of information; administrator has access to all information etc.

Authentication of Users – It is cloud provider's responsibility to authenticate each cloud user, it must check that users are who they say they are to avoid unauthorized user sign in and uses cloud services.

Data Encryption – Cloud users must make sure that their data is properly encrypted when on cloud servers. How and what methods are being used to secure this data e.g. 256 bit AES encryption and SSL encryption for secure data transfer.

Controls– User must look for the controls in place to ensure confidentiality of data in networks and protection of cloud resources from unauthorized access. Controls like roles, permissions to file access, viruses detection and prevention and user awareness procedures must be implemented.

Protection from Malicious Software – It is cloud provider's responsibility to take precautions to prevent and detect spread of malicious software in order to retain availability and integrity of data and other software.

Data Security Responsibility – Cloud users must know who is responsible for storing, processing and using their personal and sensitive information. Who will be responsible in case of any security breach, how will a cloud provider respond to it and the time frame to inform a customer about the breach must be known to the user.

Network Monitoring – Network monitoring must be done 24hrs a day through a year to make sure that the cloud infrastructure, networks and resources are safe and protected.

Asset Maintenance – It is important that the cloud provider must manage routine maintenance of windows, its timings for customer support hours, and provision of meaningful problem response and resolution commitments to its users.

Firewalls – Cloud users should be concerned about the control of the influx and outflow of the traffic of their organization.

Patches - To be safe, latest version of operating system and desktop applications should be used in conjunction with the cloud applications.

Data Backup – User's data should be backed up, preferably off-site. Established documented procedures must be there for taking regular backup copies of essential business data and software to ensure recovery, after any media failure or computer disaster.

Policies and Procedures - Procedures and policies must exist for handling sensitive data to protect data e.g. a *clear desk policy* to cater for unauthorized access, loss or damage beyond office timings, *documented management authorization* for the removal of property like equipment, data or software, *management of all computer and networks* should be done according to established procedures and responsibilities, *cloud provider's security policies and standards*, *operating procedures documentation*, *incident management responsibilities and procedures*, taking *backup* copies of data to be logged in operator logs, *logging events and faults*, *removable computer media management*, *fault logs* for recording reported faults by the users and for reporting and taking corrective action.

Vulnerability Testing – Users must make sure that the test for all categories of vulnerability must be done on an ongoing basis.

Security Audits – Users must ensure that the security audits are conducted on timely basis. Systems that stores data, how it is stored and encrypted and the path by which it can be read and written must be observed.

Termination clauses – It must be known to the users that under what grounds cloud providers can dismiss their contract and how sooner will they get their data back from cloud after termination.

5.3.10 Cloud User Satisfaction

The steps explained above provide a model framework for classified government sector cloud users in specific and all cloud users in general. Government organizations can follow these steps in order to move its businesses on cloud securely and classifiably. Each step provides a guideline to its users, by proper analysis, understanding and implementation, this framework can help them built a trust

relationship with cloud provider and for the development of real time secure cloud systems.

5.4 Summary

In this chapter we have engineered the security requirements of classified Gcloud users in the form of a framework. This SRSFGCU framework consists of ten steps, identification of functional requirements, identification of assets, identify management principles to apply, conduct harm/risk, identify security goals, identify service to move to cloud, identify security requirements, cloud user anticipation for best cloud service, identify capability of that service and secure use of cloud resources by cloud users. These steps if followed leads to secure adaption of cloud services by Gcloud users.

Chapter 6

Evaluation and Comparison of Proposed Framework

6.1 Introduction

The framework described in the previous chapter is implemented for cloud computing case study given to ACW explained in 4.4.1. How ACW can use our framework to fulfill its task assigned is explained below.

6.2 Evaluation of Proposed Framework on a Case Study

A case study explained in 4.4.1 is evaluated on our proposed security requirements specific framework for Gcloud users.

6.2.1 Identify Functional Requirements - As already explained in chapter 4 functional requirements of ACW deals with organized crimes such as anti-corruption, spurious drugs, counterfeit currencies, PPC and other laws. The functional requirements for the system to be designed may include a fair press release announcing vacancies in all electronic forums, creating an online thin client web based application form which everyone can access and apply with no difficulty, maintaining the record of applicants, scrutinizing applicants, taking online tests, marking, informing qualified applicants and eventually forwarding them to the concerned department.

6.2.2 Identify Assets - Asset is any piece of information which is valuable to an organization. It includes data, physical hardware supporting data storage, routers, switches, entire network and its components , software's, resources and database services like authentication and authorization service, system log in service, application storage and accessibility service on-line test and evaluation software.

6.2.3 Conducting Harm/Risk Analysis - After identification of assets, we prioritize them according to criticality levels. This categorization is done on the basis of discussions from ACW personals. Harm/risk analysis is done following steps from [29]. Risk values assigned will determine the level of security required for each asset. For example: Resources and database services are *critical* services as there loss may result in ceasing of systems functioning. Network components are *essential* assets while workforce database are categorized as normal assets.

6.2.4 Identify Management Principles to Apply - Management principles the ACW wishes to apply are derived from its security policy. A brief overview of which is given as:

6.2.4.1 The processes involved in this project must ensure equal and fair opportunity for everyone to apply.

6.2.4.2 Application forms must be user friendly with its confidentiality, integrity and availability maintained.

6.2.4.3 Selection and evaluation process must be error free.

6.2.4.4 Online test and marking must be fair and secured.

6.2.4.5 Information must be available to concerned people only.

6.2.4.6 Natural disasters must be catered for.

6.2.4.7 Physical security must be maintained.

6.2.4.8 Authentication, authorization and availability must be ensured.

6.2.5 Identify Security Goals - Security goals is generated by applying above mentioned management principles to each asset.

6.2.6 Describe Service that should be Migrated to Cloud - Top secret and mission critical data must not be moved to cloud. In this case project, all services need to be moved to cloud for its smooth running with proper controls and security in place.

6.2.7 Cloud User Anticipation for Best Cloud Service - The cloud service that fulfills this requirement is private SaaS. Chapter 2, 3, 4 can be seen for detail.

6.2.8 Identify Necessary Capabilities of the Service - A variety of CSP exists; therefore, identifying a CSP that fulfills required capabilities is very crucial. CSP must ensure all above mentioned functional requirements as well as its security goals. ACW must check for following security requirements in a CSP in order to establish a trust worthy customer-provider relationship.

6.2.9 Identify Security Requirements - ACW must put the security requirements explained in chapter 6 in mind and determine their necessary security requirements required for smooth running of their system that also fulfills their business and security goals. These security requirement checklists must be provided to CSP.

6.2.10 Cloud user satisfaction - Last but not the least by following all these step we have achieved our goal of providing a government sector cloud user i.e; ACW to move its data to cloud securely. Thus our aim of achieving services with necessary security is achieved.

6.3 Comparison

Framework proposed in this thesis is compared with similar frameworks as elaborated in chapter 2 is shown in table below:

Table 6.1 Comparison of proposed SRSFGCU with other similar work

Silent Features	SRSFGCU	Framework for SRE [1]	SRE Framework [5]	Security & privacy framework [7]	NIST SR guidelines [11]
A comprehensive framework for Gcloud users to adopt cloud model	✓	✗	✗	✗	✗
Step by step approach for achieving secure cloud services	✓	✗	✗	✗	✗
Security Requirements specific model with SR checklist for Gcloud users	✓	✗	✗	✗	✗
An approach to fill gap between security requirements engineering in cloud computing architecture for Gcloud users services	✓	✗	✗	✗	✗
5.3.1, 5.3.2, 5.3.4, 5.3.5 & 5.3.9 are basic steps for SRE framework	✓	✓	✓	✗	✗

Conducting Harm/Risk Analysis, prioritizing assets, identifying CSP capabilities, identifying services to migrate to cloud, SR checklist w.r.t cloud computing	✓	✗	✗	✗	✗
Framework specific to Gcloud users having classified data/assets	✓	✗	✗	✗	✗

Analysis of Comparison: The SRSFGCU framework proposed in chapter 5 is unique to all frameworks available in literature [1] [5] [7] [11]. As it provide step by step approach for achieving secure cloud services. Security requirements specific model, with security requirements checklist for Gcloud users is presented.These security requierments must be identified by them before taking services and forming a service level agreement. This not only fills a gap of engineering security requirements in cloud computing architecture for Gcloud users having classified data/resources. Steps 5.3.1, 5.3.2, 5.3.4, 5.3.5 & 5.3.9 in SRSFGCU are basic steps for SRE frameworks proposed in [1] and [5], where as conducting harm/risk analysis, prioritizing assets, identifying CSP capabilities, identifying services to migrate to cloud and SR checklist w.r.t cloud computing are unique steps specific to this framework. Following these steps will help Gcloud users in achieving secure cloud

services hence ensuring smooth and secure running of its application and data on cloud service provider infrastructure.

The proposed work is comparable to SRE framework proposed in [1] [5] [7] [13] [11] [14]. In their work by Haley's and his colleagues,the first three steps i.e. Identification of functional requirements, identication of security goals and identification of security requirements; of this framework are same as to our framework, which emphasize the need of identifying security goals along with business goals of a system [1]. It identifies security goals by identifying assets and applying management principles to them, it does not emphasize on doing harm/risk analysis for these identified assets, where as our SRSFGCU pays attention to conducting a harm/risk analysis of each asset and determine their security level, a criticality value is assigned to each asset and then management principles for each of them are proposed to apply thus determining security goals. This framework does not provide any idea of how it can be used by Gcloud users in moving their data to cloud. Moreover, no generic security requirements checklist is provided to Gcloud users and its left open for users.

A similar framework is given by P.Salini and S.Kanmani in this framework again does not provide any information on how it can be used by Gcloud users in adopting cloud services [5].

This paper does not provide any information about security requirements for each of cloud service models i.e.; SaaS, PaaS or IaaS, nor it provide need of engineering the security requirements forGcloud users, the framework provided is not specific i.e.; it is generalized for cloud users and CSP's [7]. The modeling language and processes involved in this framework doesnot clearly mention which steps to follow in order to adopt cloud services by cloud users or vice versa. Overview of

necessary possible security requirements checklist is not given. Move over, a complex structure is proposed to meet security and privacy in cloud deployment.

David G. Rosado, Rafael Gómez, Daniel Mellado and Eduardo Fernández-Medina reveals cloud security concerns and security issues with its deployment models, but a systematic framework for step by step adoption for Gcloud users by considering Gcloud users specific security requirements is missing [13].

NIST and Oracle CSC have discussed cloud adoption by several governments including US,UK and Australia but identifying in detailed security requirements of Gcloud users for cloud computing projects and engineering these requirements in a form of framework has not yet been analyzed [11] [14].

The framework provided here is rather simple and can easily be adopted by classified cloud users. It covers all necessary steps and requirements related to subject in a form of framework. None of papers gone through my sight so far provide a comprehensive framework that provides such security assurance steps to government sector classified cloud users in moving their systems to cloud.

6.4 Summary

In this chapter evaluation of proposed framewok is done by taking a case study project given to ACW. Each step is elaborated with respect to government organization's functional and security requirements, allowing them to follow a step by step process that finally leads to fulfillment of their business and security goals. At the end of this chapter a comparison is done of the proposed SRSFGCU framework with similar work related to this topic.

Chapter 7

Conclusion and Future Work

7.1 Introduction

The field of Security Requirements Engineering and cloud computing is rapidly progressing. Researchers have realized that cloud being a vibrant technology and amazing advantages does have serious security issues. This security being top most concern needs to be addressed, thus they are in a process of incorporating into this field with new ideas and methodologies. Incorporating SRE concept in cloud computing systems is an emerging field. Moreover, how a Gcloud users can decide to migrate their process to cloud with all necessary security requirements being in place, needs to be discovered.This research works tries to fill this gap and adds some worth to this unexplored area.

This chapter provides an overview of work done andthe goals we have achieved. At the end, this research work is concludedand future work is proposed.

7.2 Overview of Research Work

We have carried this research work in two steps, the first step was to find literature review on this topic. We have analysed that although many researchers have addressed security requirements engineering, security requirements, security concerns and challenges faced by cloud users and few provide guidelines for necessary requirements checklist to its government for availing cloud services. Cloud computing architecture with its security concerns are given in detail in order to let new Gcloud users to have indepth knowledge of the technology they are going for adoption. This provides them with know how of all layers, service and deployment models and security requirements of each deployment model that they might ask their CSP.

The second step was to explore the need to SRE and why it is needed for Gcloud users, SRE is done and a security requirements specified framework is proposed to Gcloud users in taking services from CSP. Based on an extensive study; the framework presented would help users to identify security requirements of their assets and specify the level of security and privacy they required for their systems that they would run on cloud infrastructure. This framework is then evaluated onto a case study porjects and a comparison is done with work related to this topic.

7.3 Achievements

We have analyzed two very important concepts SRE and Cloud computing. The goals we have set in the beginning of our research have been successfully met. A new field is explored that integrated SRE concept in cloud computing for Gcloud users. It successfully provide them asecurity requirements specified framework SRSFGCU to Gcloud users for cloud computing projects.

SRE being a methodology that fulfills specific security requirements and business and security goals of a system, provide them with security solutions, security specifications and policies, protect their assets, define level of security required and overall built a system that is trustworthy to use with adequate security needs and requirements being in place. Cloud computing being an emerging outsoursed resource sharing technology provides it users on demand storage, applications, infrastructure, platform and network access [6]. It has separated users from their physical hardware needs thus providing them with more flexible and scalable IT services [2] [4] [5]. In the process of integrating them we have found that SRE is done by providing a framework to its users. Cloud computing security challenges are kept in mind and a security requirements checklist is chalked out along with necessary migration requirements to cloud available in literature and by discussions and interviews. This

finally helped us in proposing a SRSFGCU framework. This framework is easy to use and helps in providing steps to its users for obtaining cloud services.

7.4 Future Work

The framework proposed is based on discussions and interviews with personals of government organizations, intellectuals and material available on engineering security requirement subject. For details Appendix-A is refered. Future work can be to devise a test and validate for the development of real time secure cloud systems for government sector cloud users. This work can also be extended to devise a framework for developing a private classified cloud service provider, which can be used specifically only for top secret missions where need of cloud services are inevitable.

7.5 Conclusion

Engineering Security Requirements for Gcloud users is a open field for research that has been addressed in detail. Based on an extensive study; the framework is presented that would provide step by step practical approach to Gcloud users in moving their system to CSP. It will also help users to identify security requirements of their assets and specify the level of security and privacy they required for their systems that they would run on cloud infrastructure.

We have explained cloud computing architecture, critical security challenges that the user might face in adapting cloud environment. Cloud service models, their use and security requirements for each is discussed in detail so that they must select an appropriate service that fits well to their specific environment. This will help GCloud users in understanding cloud's different layers and determine where they need which type of security requirements for their data that will reside in CSP's

premises. This framework helps in the security enforcement mechanisms incorporated in system's functional requirements and to counter security challenges. With this, our research work is concluded.

Appendix-A

QUESTIONNAIRE

SECURITY REQUIREMENTS SPECIFICATION FRAMEWORK FOR GOVERNMENT SECTOR CLOUD USERS FOR CLOUD COMPUTING PROJECTS

Dear Sir/Madam,

I am currently doing research on the above topic mentioned above. I request you to kindly fill out this questionnaire. Your response will be kept confidential and your integrity will not be disclosed to anyone. This information will be used only for academic research purpose only.

Surveyor: Rida Naveed

University: NUST (MS-Information Security)

Name/Designation: _____

Department/Qualification: _____

1. What is the security level of data you are currently handling in your organization?

Restricted	Confidential	Public

2. Is there any procedure and policy available in you department about taking cloud services?

Yes	No

3. Is there any cloud service provider you can trust for sensitive data handling? If Yes kindly name it_____

Yes	No

4. Are you aware of security concerns related to cloud computing architecture?

Yes	No

5. Kindly pen down few security issues faced by cloud computing.

_____

_____

6. What points you would consider in selecting a cloud service provider?

_____

_____

7. Are they responsible for providing you quality of service or security of service or both?

_____

_____

8. How to categorize security level of you assets?

_____

_____

9. Is there any measuring tool of determining which asset is to move on cloud and which should not?

_____

_____

10. Is there any framework that is available in your organization that tells you steps for secure cloud adoption?

Yes	No

11. What goals you consider in taking cloud services and how you measure if they are satisfied?

12. Do you have any concept of security requirements of a system?

Yes	No

13. At what stage security requirements are considered for any system?

Starting Phase	Parallel	Ending Phase

14. Are you aware of security requirements for each of cloud service models i.e; SaaS, PaaS and IaaS?

Yes	No

15. If yes name few security requirements of each cloud service model?

16. How important is the location of CSP you select?

17. Is there any back up plan available for your selected CSP of their services and hardware in case of failure?

18. What you expect will happen to your service and available bandwidth as the number of users increases?

19. As no. of users using cloud services increases, the BW utilized by each users will decrease, will this also effect billing?

Yes	No

20. What planning has done by your CSP for uninterrupted services in case of no. of users increase?

_____

_____

21. Where is your data located in CSP architecture?

_____

_____

22. Do you trust them for handling your sensitive information without any security controls in place?

Yes	No

23. Is you data accessible to you at all times? Can other users can also access your data?

Yes	No

24. Are controls properly placed and implemented in your CSP?

Yes	No

25. In which format our data is placed in CSP?

Plain Text	Encrypted

26. Who must be a focal person that you may contact to inquire about your data processing, storage and in case you lost your data or service failure?

_____

_____

27. How security of your data must be done?

_____

_____

28. Do you have any concept of all technical terms above?

Yes	No	Few

29. Have you clearly read and demanded security in SLA you made with your cloud service provider?

Yes	No

30. Is this questionnaire thought provoking for you to consider security requirements which dealing with CSP?

Yes	No

Thankyou for your valuable time

Partially Based on this survey and discussions from we have proposed security requuirements of cloud service models and have identified security requirements for Gcloud users when adopting cloud technology.

BIBLIOGRAPHY

[1] Haley, Charles B. Laney, Robin Moffett, Jonathan D. and Nuseibeh, Bashar (2008). Security Requirements Engineering: A Framework for Representation and Analysis. IEEE Transactions on Software Engineering, 34(1), pp. 133–153,

[2] Haralambos Mouratidis: Guest editorial: security requirements engineering: past, present and future. Requir. Eng. 15(1): 1-5 (2010),

[3] Stefan Wind and Holger Schrödl. Requirements Engineering for Cloud Computing: A Comparison Framework.

[4] Mouratidis H, Giorgini P, Manson G (2005) When security meets software engineering: a case of modelling secure information systems. Inf Syst 30(8):609–629 Elsevier.

[5] Salini, P. Kanmani, S. 2011. "A model based security requirements engineering framework applied for online trading system" by Recent Trends in Information Technology (ICRTIT), 2011 International Conference on Digital Object Identifier: 10.1109/ICRTIT.2011.5972266 Publication Year: 2011 , Page(s): 1195 – 1202.

[6] D. Zissis and D. Lekkas. Addressing cloud computing security issues, Future Gener. Comput. Syst., vol. 28, no 3, p. 583-592, 2012.

[7] Christos Kalloniatis, Haralambos Mouratidis, Shareeful Islam(2013) Evaluating cloud deployment scenarios based on security and privacy requirements by Received: 10 November 2012 / Accepted: 18 March 2013 / Published online: 4 April 2013_ Springer-Verlag London 2013

[8] Islam S, Mouratidis H, Weippl E (2012) A goal-driven risk management approach to support security and privacy analysis of cloud-based system.

[9] Pearson S, Benameur A (2010) Privacy, security and trust issues arising from cloud computing. In: 2nd IEEE International conference on cloud computing technology and science, IEEE Computer Society, UK, pp 693–702

[10]. Iliana Iankoulova, Maya Daneva: Cloud computing security requirements: A systematic review. RCIS 2012: 1-7

[11] . NIST, Cloud Computing Security Working Group, Challenging Security Requirements for US Government Cloud Computing Adoption (Draft) (Nov. 2011) .

[12] 5. Grobauer B, Walloschek T, Stocker E (2011) Understanding cloud computing vulnerabilities. IEEE Security Priv Mag9(2):50–57

[13] David G. Rosado, Rafael Gómez, Daniel Mellado and Eduardo Fernández-Medina. Security Analysis in the Migration to Cloud Environments Received: 20 December 2011; in revised form: 23 April 2012 / Accepted: 24 April

2012 / Published: 8 May 2012 future internet ISSN 1999-5903 www.mdpi.com/journal/futureinternet.

[14] Oracle CSC. Building on the Cloud: Why You Should Consider Moving Your Application Platform to the Public, Private, or Hybrid Cloud white paper by Oracle CSC.

[15] Traian Andrei , Cloud Computing Challenges and Related Security Issues

[16] Adeela Waqar, Asad Raza, Haider Abbas, Muhammad Khurram Khan A framework for preservation of cloud users' data privacy using dynamic reconstruction of metadata, Journal of Network and Computer Applications, Volume 36, Issue 1, January 2013, Pages 235–248

[17] Eric Dubois, Haralambos Mouratidis: Guest editorial: security requirements engineering: past, present and future. Requir. Eng. 15(1): 1-5 (2010).

[18] K. Ren, C. Wang, and Q. Wang, Security Challenges for the Public Cloud, Internet Comput. IEEE, vol. 16, no 1, p. 69 -73, 2012.

[19] W. Venters and E. A. Whitley, A critical review of cloud computing: researching desires and realities, J. Inf. Technol., vol. 27, no 3, p. 179-197, 2012.

[20] M. Jensen, J. Schwenk, N. Gruschka, and L. L. Iacono, On Technical Security Issues in Cloud Computing, in IEEE Int. Conf. on Cloud Computing (CLOUD'09), 2009, p. 109 -116.

[21] Rida Naveed, Haider Abbas, "Security Specification Framework for Cloud Users for Cloud Computing Projects" Springer, September 2013.

[22] Y. Chen, V. Paxson, and R. H. Katz, What's New About Cloud Computing Security?, EECS Department, University of California, Berkeley, USA, UCB/EECS-2010-5, 2010.

[23] H. Yu, N. Powell, D. Stembridge, and X. Yuan, Cloud computing and security challenges, in Proceedings of the 50th Annual Southeast Regional Conference, New York, NY, USA, 2012, p. 298–302.

[24] LeeBadger, Tim Grance, RobertPatt-Corner, JeffVoas, Draft-NIST-SP800-146-NIST Draft Cloud Computing Synopsis and Recommendations, Recommendations of the National Institute of Standards and Technology, Available at http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf (Accessed on 12-09-2012).

[25] James Cebula ,The Basics of Cloud Computing" USCERT

[26] Cloud Security Alliance, March 2010.Cloud Security Alliance, Top Threats to Cloud Computing, V1.0 by Cloud Security Alliance, March 2010.

[27] David G. Rosado, Daniel Mellado, Security Engineering for Cloud Computing: Approaches and Tools, IGI Global Snippet 2012.

[28] David C. Wyldl, The cloudy future of government IT: Cloud Computing and Public Sector Around the World, International Journal of Web & Semantic Technology (IJWesT), Vol 1, Num 1, January 2010.

[29] Randy Marchany, Conducting a Risk Analysis, Chapter 3,Computer and Network Security in Higher Education, A publication of Educause, Copyright 2003 Jossey-Bass Inc.

[30] Inger Anne Tondel, Martin Gilje Jaatun, and Per Hakon Meland, "Security Requirements for the Rest of Us: A Survey" IEEE Software Published by the IEEE Computrt Society, 0740-7459/08/2008 IEEE.

[31] J.D. Moffett, J.G. Hall, A. Coombes, and J.A. McDermid, "A Model for a Casual Logic for Requirements Engineering," Requirements Eng.,vol. 1, no.1, pp. 27-46, Mar. 1996.

[32] Grace Lewis, Carnegie Mellon, "Basics about cloud computing", Software Engineering Institues, September 2010.

[33] Opinion 05/2012 on cloud computing, Adopted July 1st 2012, Article 29 Data Protection working party 01037/12/EN WP 196.

[34] Lewis, Grace. Cloud Computing: Finding the Silver Lining, Not the Silver Bullet.

[35] Dormann, Will & Rafail, Jason. Securing Your Web Browser. (2006).

[36] Jansen, Wayne & Grance, Timothy. Guidelines on Security and Privacy in Public Cloud Computing. National Institute of Standards and Technology, 2011.

[37] Strowd, Harrison & Lewis, Grace. T-Check in System-of-Systems Technologies: Cloud Computing (CMU/SEI-2010-TN-009). Software Engineering Institute, Carnegie Mellon University, 2010.

[38] Lewis, Grace. Basics About Cloud Computing.

[39] Lee Badger, Tim Grace, Robert Patt-Corner, Jeff Voas, NIST Draft Cloud Computing Synopsis and Recommendations, Recommendations of National Institute of Standards and Technology, NIST Special Publication 800-146.

[40] NIST Special Publication 500-299, NIST Cloud Computing Security Reference Architecture.

[41] NIST Special Publication 800-35, Guide to Information Technology Security Services by Tim Grace, Joan Hash, Marc Stevens, Kristofor O'Neal, Nadya Bartol.

[42] “Addressing Data Security Challenges in the Cloud.pdf” A Trend Micro White Paper | July 2010.

[43] Traian Andrei. “Cloud Computing Challenges and Related Security Issues” A Survey Paper

[44] David G. Rosado, Rafael Gómez, Daniel Mellado and Eduardo Fernández-Medina. “Security Analysis in the Migration to Cloud Environments”

[45] Oscar Rebollo, Daniel Mellado and Eduardo Fernández-Medina. A Systematic Review of Information Security Governance Frameworks in the Cloud Computing Environment. Journal of Universal Computer Science, vol. 18, no. 6 (2012), 798-815 submitted: 15/10/11, accepted: 15/2/12, appeared: 28/3/12 © J.UCS

[46] Fei Hu1, Meikang Qiu, Jiayin Li, Travis Grant, Draw Tylor, Seth McCaleb, Lee Butler and Richard Hamner. A Review on Cloud Computing:Design Challenges in Architecture and Security.

[47] Rosado DG, Mellado D, Ferna´ndez-Medina E, Piattini M (eds) Security engineering for cloud computing:approaches and tools. IGI Global Publication, Hershey