Requirement Engineering for Security Issues in Cloud Computing

By

Fiza Saher Faizan

A thesis submitted to the faculty of Computer Software Engineering Department Military College of Signals, National University of Sciences and Technology, Pakistan in Partial Fulfillment of the requirements for degree of MS in Computer Software Engineering.

July 2018

SUPERVISOR CERTIFICATE

This is to certify that **NS Fiza Saher** student of **MSCS-21** Course Reg.No **NUST201463763MMCS25114F** has completed her MS Thesis title **"Requirement Engineering for Security Issues in Cloud Computing"** under my supervision. I have reviewed her final thesis copy and I am satisfied with her work.

Dated: ________________ ___________________________

Thesis Supervisor

(Asst. Prof. Dr. Seemab Latif)

CO-SUPERVISOR CERTIFICATE

This is to certify that **NS Fiza Saher** student of **MSCS-21** Course Reg.No **NUST201463763MMCS25114F** has completed her MS Thesis title **“Requirement Engineering for Security Issues in Cloud Computing”** under my supervision. I have reviewed her final thesis copy and I am satisfied with her work.

Dated: ________________ __________________________

Thesis Co-Supervisor

(Major Athar Mohsin Zaidi)

ABSTRACT

The world is tremendously changing with the advancement in technology. In the world of Information Technology (IT), the most famous technology is Cloud Computing. Cloud computing is an architecture for permitting an appropriate, on-demand network access to a public pool of configurable computing resources for example networks, servers, storage applications and services. The aim of cloud computing is to provide improved usage of distributed resources. With the extent of this new world there are some risks involved in it. The leading risks of cloud computing are availability, security, performance, data confidentiality and auditability and privacy issues. These risks rise due to improper elicitation of requirements of developing cloud system.

The research carried out in this thesis aims to propose a framework which is capable of eliciting functional requirements as well as security requirements of the system which is going to be developed so that the system is secured. To apply the framework, online-banking case study is used. To accomplish the task survey is also conducted and then results are analyzed from survey and proposed framework. The evaluation result shows the utmost concern of system users and the system will be protected from multiple security risks of cloud computing using the proposed framework.

DECLARATION

I hereby declare that this research, neither as a whole nor as a part has been copied out from any source. It is further declared that I have completed this work entirely on the basis of my personal efforts made under the sincere guidance of my supervisor and co-supervisor. If any part of this research work is proved to be copied out or found to be reported, I shall standby the consequences. No portion of the work presented in this research work has been submitted in support of any application for any other degree or qualification of this or any other university or institute of learning.

Fiza Saher Faizan

ACKNOWLEGMENTS

In the name of ALLAH, the most Gracious and the most Merciful, ALHAMDULLILAH, all praises to ALLAH Almighty for his blessings, his kindness to me in all spheres of life and who gave me the strength and determination in completing this thesis.

I am thankful to many people in completion of this thesis as I strongly believe that without their guidance, support and sincere cooperation this achievement would not have been possible. I am grateful to my respected supervisor Dr. Seemab Latif and co-supervisor Major Athar Mohsin Zaidi for their supervision, guidance, and constant help and support. I sincerely thank my supervisor and co-supervisor for their invaluable help of constructive suggestions and comments throughout the research work and thesis writing have contributed to the accomplishment of this research. My special thanks to my committee members: Dr. Naima Iltaf and Dr. Waseem Iqbal for their encouragement and assistance in guiding me through the research and helping me improve the research work presented in this thesis.

Also, I would like to thank all the participants in my survey, for sharing their precious time during the research. Lastly my deepest gratitude goes to my husband and parents for their endless love, prayers, support and always believing on me without them I could not have made it here.

DEDICATION

In the name of ALLAH Almighty, the most glorious, the most merciful. All praise to ALLAH Almighty, for the strength, his blessing and mercy in completing this thesis. Guide us through the right path, path of those to whom you bestowed your blessings. This research work is specially dedicated to ALLAH Almighty, his help makes me able to accomplish this task and his Prophet Muhammad ﷺ, his guidance made me able to do this task.

This research work is also dedicated to my beloved husband, parents, my supervisor, my co-supervisor and my sisters. Their encouragement, faith and motivation gave me strength and confidence to accomplish this research work.

TABLE OF CONTENTS

Chapter # 1: INTRODUCTION

Chapter # 2: **LITERATURE REVIEW**

Chapter # 3: RESEARCH METHODOLOGY

Chapter # 4: **PROPOSED FRAMEWORK**

Chapter # 5: RESULTS AND ANALYSIS

Chapter # 6: CONCLUSION

APPENDIX

REFERENCES

LIST OF TABLES

LIST OF FIGURES

Chapter#1

INTRODUCTION

1.1. Overview

System and software are bounded with each other. When we use term system, software automatically dissolves in it. Systems can be categorized in three types; traditional, cloud-based and real-time systems. In the development of any system, there are five major steps included i.e. gathering requirements, designing, implementation, testing, and then maintenance. To handle or operate systems, software is being present and used by everywhere from scientists, mathematicians, engineers, medical to a common use and specially now in business industry such as cloud computing. Requirement Engineering (RE) is very important part in the development of any system because if there is no requirement then there is no system or system without requirements cannot be create even creatures are born for the purpose of worship. In other words, requirement engineering is the most important part of the system because in the reaction of requirements system is created. But when these requirements are not properly elicited then this may lead toward flaws in the system and sometimes these flaws could be risky as if lack in security requirements. Same is the case in cloud computing, security is major concern. Security issues in cloud computing can be minimize if security threats identified in the requirement elicitation stage and for that purpose a framework can be formulated and proposed to elicit security requirements for cloud-based system. This will help to prevent security threats for the system and increase satisfaction level of customer as well as organization.

1.2. Background

In IT world cloud computing is new trend introduced in 1960 [1]. In 1990s, this trend started in the organizations where communication is on high priority and they need fast communication system so that network transmission minimized. Cloud computing is composed on storage, software and networks placed in a common place which is shared with all relative cloud customers and these resources can be accessed through internet. National Institute of Standards and Technology (NIST) defined cloud computing as “A grid of all resources such as servers and applications are placed in a common place which can be accessed by a network or internet that sets up with minimal efforts and service provider interaction, the user pays only for those resources he used” [2]. Its feature pay-per-use model makes it more attractive. Pay-per-use model means cloud customer pays only for those resources which are being used by him and Service Level Agreement (SLA) assures the availability of these resources.

Besides these benefits, cloud computing is considered risky to adopt and people avoid this practice to implement because there are some flaws exist in cloud system. One of these flaws poor requirement engineering practice in cloud computing because the success rate of cloud system depends upon the accomplishment of requirements and when they are not clear then system may suffer [3]. Therefore, elicitation of requirements plays very important role in the development of the cloud system.

In cloud computing, stakeholders or customers are scattered geographically that is why it is difficult to perform traditional requirement elicitation techniques to discover all requirements for the cloud system. But there are some researches which shows that after modification of traditional techniques they are helpful to elicit requirements and, in some researches, new methods or frameworks are proposed and implement to elicit requirements for cloud-based systems. As discussed above, security is major concern in cloud computing, this is may be due to industrial practice while gathering requirements. In common practice while performing requirement engineering, only functional requirements are considered and all other requirements which helps to fulfill or to maintain system, may be called as non-functional requirements, are ignored and sometimes leave to handle in next stages of system development life cycle i.e. in design and implementation stages. Determining of requirements have a big role on the development process of any system. Therefore, requirement engineering is very important while transforming from traditional system to cloud system.

1.3. Motivation

As requirement engineering plays essential role in cloud computing and to make transformation from traditional to cloud system successful because requirement engineering increases satisfaction level of customer by eliciting or covering all requirements which helps to build system. Security is the top listed issue in cloud computing and security falls in the second category of requirements that is non-functional requirement. A far cry from industrial practice, if security requirements elicit in the initial stage of system development then this helps in designing and implementation stages as well as reduce security threats in cloud systems and increases trust of cloud customer with respective perspective. This can be done by modifying existing frameworks and methods and can be by proposing new techniques.

1.4. Problem Statement

As security is the main issue in cloud computing, if this issue points out in initial stage of development of the system then education rate of this issue can be increase. Therefore, to elicit security requirements for cloud system different approaches, methods etc. introduced either traditional or a specific framework/method for the system. But traditional approaches are not much sufficient to elicit security requirements in cloud computing because problems like inconsistency and scalability still exists.

The purpose of this research work is to study all frameworks/techniques and methods proposed to elicit security requirements for cloud-based system and then devised a framework with improvements to elicit security requirements for cloud systems. Therefore, this research work follows the following three research questions:

1. *What is the role of requirement engineering in cloud computing and what requirement elicitation techniques/ frameworks used to elicit security requirements for cloud systems?*
2. *Can traditional requirement elicitation techniques be used for cloud computing?*
3. *How can Security Requirement Elicitation Assessment and Mechanism technique be scalable?*

1.5. Objectives

The objectives of this research study are as follows:

- Identify the main cause for what cloud computing is not as trusted as it fames.
- Study techniques and frameworks to elicit security requirements in cloud computing.
- Develop a framework to reduce inconsistency and scalability problems to overwhelm security issues in cloud computing.
- Evaluation of proposed work.

1.6. Relevance to National Needs

The research will be helpful for researchers and those organizations that want to transform from traditional system to cloud system so that they save their system from security attack which will happen after implementation of the system and especially financial organizations.

1.7. Advantages of the Research

The research will be helpful for researchers and those organizations that want to transform from traditional system to cloud system as well as it will be also helpful to elicit security requirements for any system.

1.8. Area of Application

This research is helpful for the requirement engineers as well as for financial institutions.

1.9. Structure of Thesis

Chapter 2 illustrates the literature review of the research work which explains related techniques and methodologies. Chapter 3 demonstrates the literature review and research methodologies which is used to conduct this research work. Chapter 4 explains the proposed framework, the main research of this thesis. Results of literature review and proposed framework are analyzed in Chapter 5. Finally, conclusion of the research work with future work is generated in Chapter 6.

Chapter#2

LITERATURE REVIEW

2.1. Introduction

Many researches conduct on requirements elicitation for cloud computing and some on security requirements elicitation for cloud computing. This chapter illustrates those techniques, methods and/or frameworks that are developed to elicit requirements for cloud systems. Therefore, this chapter explains the literature review for this research work. The literature review answers three research questions which are as follows:

RQ1. Is security the utmost issue existing in cloud computing? What kind of threats are there in the cloud?

RQ2. What is the role of requirement engineering in cloud computing and what RE techniques/ frameworks used to elicit security requirements for cloud systems?

RQ3. What are the limitations of these techniques/ frameworks?

2.2. Cloud Computing and Security Issues

Cloud comprises on some important characteristics, service or deployment models according to demand of cloud customers [4]. Cloud computing is classified as private, public, hybrid and community and the basic service or deployment models are Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) [4]. Figure 2.1. depicts classifications and service models of CC. It makes up of two segments; the front-end and the back-end joined through internet [5]. Front-end is referred to as client side and back-end is refer to as cloud service provider. Characteristics of cloud computing are [5, 6, 7, 8]:

i. User can access data, applications and any other services through internet.
ii. Cost reduces as organization has no need to install infrastructure.
iii. A smaller amount IT skill required for execution.
iv. Resourceful consumption of infrastructure.
v. Easy to maintain at front end.
vi. Pay-per-use facilitates for calculating the use of applications regularly.
vii. Keeps an eye on performance and security by back end of cloud.

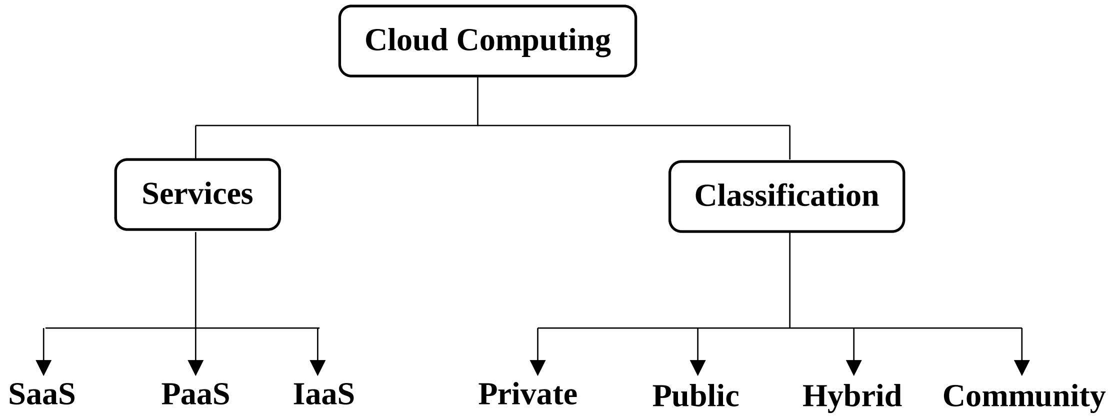


Figure 2.1.: Cloud Computing Classification and Service Models

However, people still hesitate to adopt cloud computing. According to the Forrester Research Consultants who did survey of 11 merchant companies offering cloud services [9]. Their aim was to find why people avoid cloud computing. So, they concluded that mostly cloud customers or stakeholder's needs do not meet with the result of the cloud service provider which causes the loss of customer or stakeholder trust [10]. The factors that cause to lose customer's trust may be security, performance, availability, data loss, data integration, data privacy, not enough ability to customize, network security issues like Denial of Services (DOS) etc. [11, 12].

A research conducted to find out the most focused research topic of cloud computing [13]. The results demonstrated that 182 research conducted on general cloud computing topics and 322 research on security issues in cloud computing out of 504 research topics. According to another review conducted in the year 2014 shows that the security is the most critical concern among other concerns in cloud computing [14].

The Cloud Security Alliance (CSA) considered as the determiner of making sufficient standards for cloud security in the field of IT industry [15]. In last three years, CSA released reports that aims to discover company's concern about cloud security and what tools/methods does these companies used to make secure their systems [16, 17, 18]. The reports are analyzed with respect to the concerns that are related to respondents with the number of members involve in the survey and this information is tabulated in Table 2.1. Figure 2.2. shows the statistics of the analyzed reports and it is clear from this figure that though there are numerous benefits of cloud-based systems, the top listed are flexibility scalability, availability and cost reduction but security is the utmost concern in cloud computing because three major issues are bring out by cybersecurity experts i.e. data loss, data confidentiality and data privacy [16, 17, 18].

Table 2.1.: Analysis of Spotlight Reports by CSA

Year	Members	Use or Plan to Use	Scalable	Availability	Reduction in Cost	Security Concern
2015	250,000	71%	51%	50%	48%	90%
2016	300,000	79%	36%	46%	41%	91%
2017	350,000	76%	47%	43%	36%	81%
Avg.	**300,000**	**75.33%**	**43%**	**46.33%**	**42%**	**87.33%**

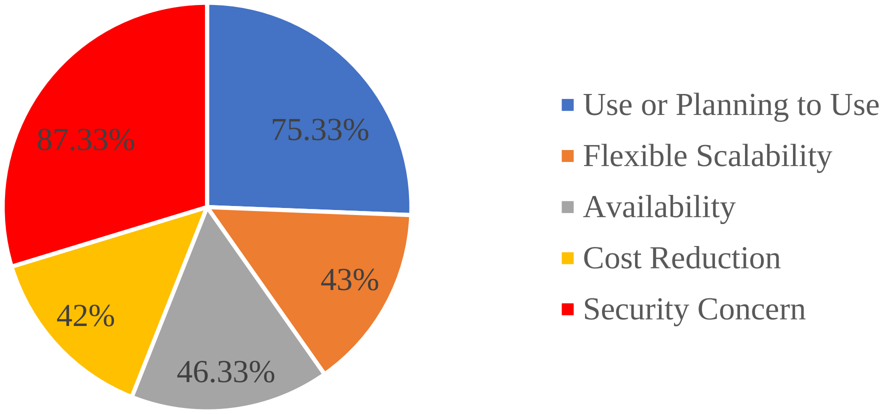


Figure 2.2.: Statistics on Spotlight Reports by CSA

Another analysis on cloud computing security problems describes security issues in each deployment model [19]. Table 2.2. demonstrates associated security issues.

Table 2.2.: Cloud Computing Components and Security Issues

Cloud Computing Components	**Models/ Methods**	**Security Issues**
Service Models	I-a-a-S [20, 21]	Usage and Data Protection from Leakage, Substructure Toughening, Verification and Permission issues
	P-a-a-S [22]	Lack of Interoperability, Susceptible Hosts, No Monitoring on VM
	S-a-a-S [19]	Data Location, Veracity, isolation, privacy and backups.

Network	Cloud Access Methods [19]	Web Browsers, Protocols, Remote connections

Cloud Security Alliance (CSA) reported that highest threats in cloud computing are [20]:

i) Data cracks
ii) Unsatisfactory identity
iii) Credential and access supervision
iv) Uncertain interactions and APIs, structure weaknesses
v) Account hacking
vi) Attack insiders
vii) Data loss
viii) Due diligence
ix) Denial of services
x) Shared technology issues

Hence CSA top threats report, and main results of cloud security surveys shows that security is the primary challenge in cloud computing [16, 17, 18].

2.3. Requirement Engineering

It is known that to develop any system there must be some requirements, so requirement engineering is the process to elicit these requirements of the system to be build [23]. Requirements are categorized in two kinds:

(i) Functional requirements (FR)

These are the user actual requirements or basic requirements that shows the purpose of system to be build [24].

(ii) Non-Functional Requirements (NFR).

The other requirements which are required to build the system or in other words the requirements which supports functions of system are no-functional requirements [24].

Usually industry focuses onto basic requirements and other requirements are left to be handle in design and implementation phases of development of the system which cause serious flaws like inconsistency, ambiguity, security etc. in the system [24]. The success frequency of the system is the “level of fulfillment of requirements to which it was projected", therefore, requirement engineering is the process to find all needs that meets up to get the actual target of the system [23].

2.4. Requirement Engineering for Cloud Computing

The success factor of transformation from traditional system to cloud-based system depends upon meeting of cloud system on cloud customer requirements which means good requirement engineering leads toward successful cloud system [10].

In the result of the survey conducted during the development of requirement elicitation framework shows that requirement engineering is the most important characteristic in the development of cloud system or applications and more research required for this characteristic [25]. Mostly, the proposed frameworks or methods of requirements elicitation in cloud computing are emphasized on different characteristics such as security, availability, privacy etc. [26]. Following sub sections describes the requirement engineering tools, techniques, frameworks and methods used to elicit requirements for cloud systems.

2.4.1. Crowd-Centric Requirement Engineering

A method proposed to elicit requirements in which a group of people supposed to be all users for whom system is going to be developed connected through internet source using a game [27]. In this method crowdsourcing and gamification both methods are connected in a manner such that users are involved to get requirements more deeply. The comparison between traditional requirement elicitation method and crowd-centric requirement engineering method is tabulated in Table 2.3. demonstrates.

Table 2.3:Comparison between Traditional and CCRE

Traditional	CCRE
RE engineers asked for requirements from users for the proposed system at the initial step of the process.	Except requirement specification step the crowd involved throughout the RE process.
Requirements are then analyzed.	Complete set of requirements is repeatedly reviewing to vote and refer requirements according to the involved customer crowd.

Then requirements are prioritized according to acceptance and preference criteria.	Top rated requirements are analyzed to be finalized. Points and badges are awarded to the customer crowd for beneficial response and thus helpful in analysis of requirements.
Finally, requirement specification documented.	Finally, requirement specification documented.

Limitations:

1. A group of users involved which considered as all users.
2. This group suggests some requirements which are assumed to be from all users.
3. Assurance of quality of requirements that are received from group of users is quite difficult.
4. Security requirements are not targeted in this method.

2.4.2 Modeling security requirements for cloud-based system development

Using UML based structures, a method is introducing to elicit security requirements for cloud applications and systems. This method used to progress efficiency in the development of secured cloud application and systems [28]. In this method use case and misuse case strategy applied. Use cases used to demonstrate behavior of the system and misuse cases demonstrate the behavior that is not supposed by the developing system and these misuse cases helps to elicit security requirements for the developing system. Both cases i.e. use case and misuse case, are considered in an interactive state in the proposed method so that these cases are self-sufficient by the technologies presented from cloud provider [29].

Limitations:

1. It can be more useful when designing a system as UML is the modeling language of the system.
2. For cloud system these are not enough to elicit requirements as well as security requirements.

2.4.3 An Improved Requirements Engineering Framework for Cloud Based Application Development

A framework proposed to elicit requirements for cloud systems which is isolated with requirement engineering phases. The basic structure of requirement engineering used as based structure of this framework and different techniques merged with this structure to overwhelm some issues of requirement engineering in cloud system [30].

Limitations:

1. This framework is more useful for justification and supervision of modification of requirements.
2. It focuses only on FRs whereas NFRs are ignored which needs enhancement in this framework.

2.4.4. A Fuzzy Galois Lattices Approach to Requirements Elicitation for Cloud Services

A framework proposed to analyze requirements for cloud service providers and these requirements are generated from cloud customers log files. It named as Fuzzy Galois Lattices Approach [31]. Fuzzy Galois Lattice is a mathematical notation used in various fields of engineering [32]. Input for this algorithm is generated by queries created in log files. This framework cannot be used to elicit requirements for traditional systems. It works with passive participation of users or in other words it uses a marketplace to analyze requirements.

Limitations:

1. Due to mathematical notation there are some boundaries of Fuzzy concept which may not allow to use such kind of methodology for any system to elicit requirements and it may elicit particular requirements [33].
2. Users are passively involved in this methodology.

2.4.5. Requirements Engineering for Cloud Computing Using i*(iStar) Hierarchy Method

The method is based on iStar hierarchy approach and proposed for application handling process in the environment of university [34].

Limitations:

It considers only FRs and NFRs are ignored.

2.4.6. Security Requirements Elicitation and Assessment Mechanism (SecREAM)

A procedure proposed that involves security in initial stage of the development of software system that is requirement stage of the software and this method can be valid for both types of software either traditional or cloud [35]. It is an asset-based ranking method. It means assets are aligned in certain pattern then each stakeholder evaluates it and rank the asset according to the stakeholder's point of view. This method comprises on following components

1. Identify stakeholders and Assets
2. Mapping of assets to relevant stakeholder
3. Familiarization and training
4. Rankings of assets
5. Analysis

This derived information from different stakeholders then gathered on a single board and analyze them. "Bank" is used as case study for experiment to derive results i.e. pension calculation and this case study is a cloud-based system specifically Software-as-a-Service (SaaS).

Limitations:

Inconsistency persists in the method as it is limited on the case study.

2.4.7. Requirements Elicitation Framework for Cloud Applications

A framework proposed which is constitute on audio recordings and storytelling technique and used to develop cloud applications [36]. In this process audio recordings are used in which customer record his requirements using storytelling technique in audio form so that these recordings can be used again when stuck on certain point.

Limitations:

1. Story telling technique cannot be used to elicit cloud requirements for developing a system [33].
2. This method focused only FRs, therefore, NFRs are ignored.
3. It is stated in the paper that ambiguity will be minimized in requirements elicitation process using this approach, but no justification observed in the paper.

2.4.8. Software Security Requirements Management as an Emerging Cloud Computing Service

A framework is proposed to elicit security requirements during the development of cloud system at early stage called as Cloud Software Development Life Cycle (CSDLC) [37]. The framework is consisting on five layers named as storage, service, hypervisor, record and datacenter layers. A technique has been familiarized for security requirement elicitation for cloud systems Integrated-Secure Software Development Life Cycle also introduced and demonstrates for Amazon EC2 service. A set of plans provided through this method on how to secure systems before development or in other words how system could be secure through planning using these set of strategy.

Limitations:

DDoS attack is targeted in this technique.

2.4.9. Cloud security engineering: Early stages of SDLC

Security challenges are causing failure of the system as discussed in [38]. To prevent system from failures, a framework is proposed which is combined with service development life cycle.

Limitations:

This framework also merged throughout the SDLC and Specifically not focused on RE.

2.4.10. Modeling Non-Functional Requirements in Cloud Hosted Application Software Engineering

In this procedure only three NFRs are addressed for the system of "Theater Booking System" and these NFRs are response time, concurrency and user response time [39]. UML notation is used to demonstrates the behavior of the system.

Limitations:

1. Though NFR are focused on this procedure but security is still not considered.
2. This is useful for a specific system.

2.4.11. Exact Requirements Engineering for Developing Business Process Models

This approach is based on Business-Oriented Requirements Engineering (BORE) and Business-driven development (BDD) [40, 41, 42]. Journal paper submission system is used as a case study for evaluation of this approach. Both BORE and BDD are merged in this approach and hence model a composite system.

Limitations:

1. This approach focused on FRs of the system.

Table 2.4. describes the requirement engineering tools, techniques, frameworks and methods used to elicit requirements for cloud systems. This table demonstrates the literature consists in cloud computing and requirement engineering tools and techniques used to elicit functional and non-functional requirements for cloud-based systems.

Table 2.4.: Literature Techniques/Frameworks/Methodologies

Sr. No. Delete this column	Year	Paper Title	Abstract	Tool/Method/ Framework/Technique
1	2014	Cloud Security: Services, Risks, and a Case Study on Amazon Cloud Services [43]	Focused on cloud insights and its security issues. Amazon Web Service case study used to highlight security issues. Current and future status of cloud discussed.	No RE used.
2	2014	Cloud Computing and Security Issues in the Cloud [44]	Cloud insights are focused with its security issues.	No RE used.
3	2014	Crowd-Centric Requirement Engineering [27]	Traditionally all users are not involved during requirement elicitation. To overwhelm this limitation CCRE is proposed. This involves crowdsourcing and gamification procedure to gather requirements.	Framework introduced to elicit requirements for cloud and mobile computation.

4	2014	Modeling security requirements for cloud-based system development [28]	Using UML based structures, a method is introducing to elicit security requirements for cloud applications. This method used to progress efficiency in the development of secured cloud application and systems.	A procedure introduced to elicit security requirements for cloud applications.
5	2015	An Improved Requirements Engineering Framework for Cloud Based Application Development [30]	A framework proposed which is isolated with requirement engineering phases. The basic structure of requirement engineering used as based structure of this framework and different techniques merged with this structure to overwhelm some issues of requirement engineering in cloud system.	A framework proposed to elicit requirements for cloud systems.
6	2015	A Fuzzy Galois Lattices Approach to Requirements	A framework proposed to elicit requirements for purely cloud	A framework proposed to elicit requirements for cloud systems, named as

		Elicitation for Cloud Services [31]	systems. This framework cannot be used to elicit requirements for traditional systems. It works with passive participation of users or in other words it uses a marketplace to analyze requirements.	Fuzzy Galois Lattices Approach.
7	2015	Requirements Engineering for Cloud Computing Using i*(iStar) Hierarchy Method [34]	Requirement engineering method is proposed for university environment. The method is based on iStar hierarchy approach.	i* (iStar) Heirarchy Method introduced for cloud computing.
8	2015	Security in Cloud Computing: Opportunities and Challenges [45]	This paper deals on the survey of current security issues and their solutions for cloud computing. They divide cloud in three sectors: (i) Communication level, (ii) Architectural level, (iii) Contractual and legal levels. Then countermeasures against these issues	No RE used.

			has been discussed and compared with each other.	
9	2015	Security Requirements Elicitation and Assessment Mechanism (SecREAM) [35]	For both traditional and cloud-based systems, a framework introduced to elicit security requirements using asset-based ranking method.	A framework introduced named as SecREAM.
10	2015	Requirements Elicitation Framework for Cloud Applications [36]	An improved requirements elicitation process introduced by proposing a framework constitute on audio recordings and storytelling technique.	A framework introduced for cloud applications named as Elicitation Topic Map (ETM).
11	2016	Software Security Requirements Management as an Emerging Cloud Computing Service [37]	Techniques has been introduced in this research for cloud computing to elicit security requirements. Integrated-Secure Software Development Life Cycle also	A technique has been familiarized for security requirement elicitation for cloud systems.

			introduced and demonstrates for Amazon EC2 service.	
12	2016	A Survey on Security Requirement Elicitation Methods: Classification, Merits and Demerits [47]	A comparison has been done among 15 security requirement elicitation techniques and methods. Merits and demerits are also discussed in this survey.	No new method introduced.
13	2016	Cloud security engineering: Early stages of SDLC [38]	A framework proposed to combine it with SDLC so that systems can be secure from cybercrimes. 103 failed cases discussed there and then a case study used to show the suitability of the framework.	A framework introduced to secure systems from cybercrimes.
14	2016	Modeling Non-Functional Requirements in Cloud Hosted Application Software Engineering [39]	NFRs are the key focus of this paper. NFRs for the theatre booking system are modeled using UML and then transformed to a source code.	No particular technique/ method introduced here.

15	2016	Survey Paper on Trust Management and Security Issues in Cloud Computing [47]	A survey conducted on security issues in cloud computing and concluded that trust is the major problem exists in cloud computing.	No RE used.
16	2016	Reviews on Security Issues and Challenges in Cloud Computing [48]	A survey conducted on cloud architecture, challenges and issue in cloud computing and resolution of these challenges.	No RE used.
17	2017	Analyzing Requirements Engineering for Cloud Computing [49]	A review directed on requirement engineering for cloud area. This review conducted on five directions of cloud computing and explained through example that how to classify the direction of system towards cloud.	A technique introduced for determining cloud direction.
18	2017	Analysis of the Requirements for Offering Industry 4.0 Applications as a Cloud Service [50]	A review conducted to familiarize requirements for market 4.0 proposals and also explore todays status of research on cloud	No technique introduced.

			computing with challenges that can be essentially explored in future by the researcher...	
19	2017	Cloud Computing: Technology, Security Issues and Solutions [51]	Different aspects and weaknesses of cloud computing discussed including security issues and their solutions proposed by researchers. Lastly, some significant strategies proposed to make SLA.	No RE used.
20	2017	Exact Requirements Engineering for Developing Business Process Models [52]	A survey conducted on BORE and BDD and then hybrid these methods to make business model for requirement elicitation. Online case study that is submission of papers to be published used to verify aptitude of proposed method.	A method introduced to elicit requirements for online system.

2.5. Summary

In this chapter it is discussed that security issue is the most important issue in cloud computing and requirement engineering plays very important role to elicit security requirements so that security issues can be highlighted in initial stage of development.

Frameworks, methods and techniques are also discussed in this chapter which are proposed to elicit requirements and few of them are specific to elicit security requirements for cloud systems.

Chapter#3

RESEARCH METHODOLOGY

3.1. Overview of the Chapter

In this chapter, the research methodology is explained as well as the literature review methodology is also described. In this reference, what review methodology has been adopted for this work and how do the proposed framework designed are discussed in this chapter.

3.2. Literature Review Methodology

The literature review method for this research work has been carried out through the method described by Kitchenham [53]. The purpose of this literature is to review all proposed requirement engineering methods, techniques and frameworks presented for cloud systems as discussed in chapter 2. Therefore, the limitation is obtained to define the boundaries of the literature review and these limitations are:

(i) The sources i.e. Journals, conferences and reports

(ii) The period which is from January 2014 to July 2017

The research phases involve in this study are as follows:

3.2.1. Research Questions

The literature review answers the following research questions to determine structure and scope of the literature review, for evaluating the studies and for analyzing their results and these questions are tabulated in Table 3.1. with their motivation.

Table 3.1.: Literature Research RQs and Motivation

ID	Research Questions (RQs)	Motivation
RQ1	Is security the utmost issue existing in cloud computing? What kind of threats are there in the cloud?	Aims to identify either security is the top most issue in cloud and what threats/factors exists in cloud computing so that these can be keep in view while doing requirement elicitation techniques for cloud computing.

RQ2	What is the role of requirement engineering in cloud computing and what RE techniques/ frameworks used to elicit security requirements for cloud systems?	Seeks to address requirement elicitation techniques and frameworks used for cloud-based systems.
RQ3	What are the limitations of these techniques/ frameworks?	The objective of RQ3 is aimed at identifying the limitations of requirements elicitation methods towards the development of cloud systems.
RQ4	Can traditional requirement elicitation techniques be used for cloud computing?	Identify that the techniques which are used in conventional systems can be used in cloud systems.

3.2.2. Search Strategy

To find research papers related to the topic some terms or keywords used. These terms and keywords are “Requirement Engineering for Cloud Computing” + “Requirement Engineering for Security Issues in Cloud Computing” + “Requirement Engineering to solve Security Issues in Cloud Computing” + “Cloud Computing and Requirement Engineering” + “Cloud Computing Security Issues solved by Requirement Engineering” + “Requirement Engineering to solve Security factors in Cloud Computing” + “Requirement Engineering Solutions of Security in Cloud Computing”. More research papers are searched and found from the citation inside the papers.

3.2.3. Search Process

Using the search strings defined above are used to find research papers from different libraries, conferences, reports and journals. Following is the list of databases or sources from where research papers are fetched.

(i) Association for Computing Machinery (ACM) Digital Library
(ii) Springer
(iii) Institute of Electrical and Electronics Engineer (IEEE) Digital Library
(iv) Science Direct (Elsevier)
(v) Scholar Google.

Table 3.2. demonstrates the list of journals with acronyms of whom research papers are selected.

Table 3.2.: Selected Conferences and Journals

Source	Acronym
International Journal of Network Security & Its Applications	IJNSA
International Journal Communications, Network and System Sciences	IJCNSS
International Journal of Engineering Research and General Science	IJERGS
International Journal on Information Sciences	IJIS
International Journal of Information Management	IJIM
International Journal of Applied Engineering Research	IJAER
International Journal on Future Generation Computer Systems	IJFGCS
International Conference on Utility and Cloud Computing	ICUCC
IEEE Student Conference on Research and Development	SCOReD
IEEE Transactions on Services Computing	TSC
International Conference on Advances in Computing, Communications and Informatics	ICACCI
International Conference on Cloud Computing, GRIDs, and Virtualization	ICCCGV
International Conference on Materials Science and Engineering	ICMSE
Symposium on Colossal Data Analysis and Networking	CDAN
IEEE International Symposium on Industrial Electronics	ISIE
International Conference on Anti-Cyber Crimes	ICACC

3.2.4. Inclusion and Exclusion Criteria

Following criteria is considered while filtering research papers:

a) Inclusion Criteria

The research papers which are selected for literature review must be related to:

i) Security issues in cloud computing.

ii) Requirement engineering techniques/ framework apply on cloud computing.

iii) Requirement engineering techniques/ frameworks that elicit security requirements in cloud systems.

iv) Research papers that are related to security issues in cloud computing are not included in survey analysis but only include for getting security factors in cloud systems.

b) Exclusion Criteria

i) Research papers are excluded which are published before January 2014 and after July 2017.

ii) Research papers are excluded in which requirement engineering techniques/ frameworks proposed for traditional system and not for cloud systems.

iii) Journal articles that are not accessible online are excluded.

3.2.5. Quality Assessment

Those research papers which are fall in inclusion criteria are further assessed by quality assessment questions to examine the quality of selected research papers. Following are these quality assessment (QA) questions:

QA1. Does the objective of the paper explain appropriately?

QA2. Does the paper focus on security issue in cloud computing?

QA3. Does the paper used RE framework/ tool/methodology to elicit security issue that may involve later in the development of the cloud system?

These questions were recorded as follows:

QA1: Y (yes), if the abstract of the paper explains the main purpose and the remaining paper revolves around this purpose; P (partly), if the abstract of the paper explains the main purpose and the remaining paper partially around this purpose; N (no), if the purpose of the paper does not explain properly; Unknown (U), if other than above three options.

QA2: Y (yes), if the entire paper discusses security issues in cloud computing; P (partly), if the paper partially define security with other issues of cloud computing; N (no), if security discuss in sub-subsection of the paper; Unknown (U), if other than above three options.

QA3: Y (yes), if the paper introduced requirement engineering framework/tool/methodology to elicit security issue in cloud computing; P (partly), if the paper introduced requirement engineering framework/tool/methodology to elicit requirements in cloud computing; N (no), if no requirement engineering framework/tool/methodology introduced in the paper to elicit requirements in cloud computing; Unknown (U), if other than above three options.

The quality assessment questions scored as Y=1, P=0.5, N or Unknown=0.

3.2.6. Data Collection and Analysis

Following data has been extracted from selected research papers:

i) The source of the paper either journal or conference.

ii) The full reference of the paper.

iii) Main research area of the paper.

iv) Abstract of the paper.

v) Body of the study consists on research questions and the answers.

vi) Whether the study propose any tool/framework/methodology.

vii) Purpose of tool/framework/methodology.

viii) Summary of the study.

The extracted data from the research papers for literature review is used in different scenarios. Table 3.3. shows extracted data and the scenario it is used for.

Table 3.3.: Data and Scenarios

Data	Scenarios
Source of paper	Tabulated to analyze how much research papers conducted from one source then how many are relevant from that source and how many selected.
Full reference	To provide reference in the bibliography of this study.
Research area	Addressing RQ1
Abstract	To evaluate quality
Body of the study	Addressing RQ1 and RQ2
Tool/Framework/methodology	RQ2 and to evaluate quality
Purpose of Tool/ Framework/methodology	Addressing RQ3 and RQ4

3.3. Research Methodology for Proposed Framework

After taking literature review, research work proceeds further to propose a framework. For this purpose, research questions are identified from literature review and then techniques are analyzed (chosen) according to research questions. These research questions (RQs) are defined in Table 3.4. with motivation as well as these RQs are defined in section 1.4, chapter 1.

Table 3.4.: Research RQs with Motivation

ID	Research Questions (RQs)	Motivation
RQ1	How can Security Requirement Elicitation Assessment and Mechanism technique be scalable?	Aims to find either it is scalable or not.
RQ2	Can traditional requirement elicitation techniques be used to elicit security requirements for cloud computing?	Seeks to find traditional techniques that will be suitable for cloud systems.

Two methodologies are selected for this research work. One methodology is used to answer first question and second methodology is used to answer second question but the derived results from first techniques are merged into the second one that will be discuss later in the same section. These techniques are i* hierarchy and Security Requirement Elicitation Assessment and Mechanism (SecREAM). A case study is used to implement these techniques. The case study will be given in the section 3.4 of the same chapter.

i* hierarchy is basically a technique used to elicit functional requirements for traditional systems, but it was used to elicit functional requirements for cloud system [i* BP paper]. Whereas SecREAM is a methodology which can be used to elicit security requirements for any system i.e. traditional systems, cloud-based systems and real-time systems [SecREAM]. This is the reason these techniques are selected and merged together to generate a new technique.

3.3.1. Research Methodology for RQ1

To determine the scalability of SecREAM, as it is mentioned in the research paper that the authors declare not scalable. For that purpose, it is applied on the other case study. Thus, a survey is also conducted to get the results of the technique. These results are analyzed in the chapter 4. Questionnaire that has been used for this research work is given in the Appendix A.

The survey is taken on ground instead of online survey and it is taken from bankers and bank’s customer that is bank account holders who are stakeholders of the system. Almost 11 banks are visited to collect the data. From each bank any two branches are targeted therefore 22 responses are gathered. Branch manager was asked to fill up the questionnaire. The list of the banks from where the response gathered are as follows:

1. United Bank Limited
2. Habib Bank Limited
3. Askari Bank Limited
4. Meezan Bank Limited
5. National Bank of Pakistan
6. Allied Bank Limited
7. Silk Bank Limited
8. Bank Alfalah Limited
9. Muslim Commercial Bank
10. Faysal Bank Limited
11. Standard Chartered Bank Limited

3.3.2. Research Methodology for RQ2

i* hierarchy is focused to derive a specific technique for cloud-based systems. According to the hierarchy, actors are searched out from the case study and from survey and their respective roles on each layer. Then business model process has been derived i.e. the dependency relationship between actors called strategic dependency and the strategic rationale which shows the internal processes of an actor. Two different hierarchies are developed during this research work. First hierarchy is created from case study and second is created after taking survey i.e. from the derived results of survey a new hierarchy is produced. These hierarchies are displayed in diagrams with legends and explanation in chapter 4. The derived research method is verified through the comparison of hierarchies which are discussed in chapter 5.

3.3.3. Methodology to Find Results of Proposed Framework

Assessment criteria is set to derive the results of proposed framework. As it is discussed that traditional technique can be used for cloud computing to elicit requirements also for eliciting security requirements. This criterion to evaluate proposed work is based upon following factors:

1. The method is traditional methodology.
2. The method is used for cloud-based systems.
3. The method is focused on functional requirements for cloud systems.
4. The method is focused on non-functional requirements for cloud systems.

5. Specifically proposed to elicit security requirements for cloud computing.

3.4. Case Study for this Research Work

A certain bank wants to spread out its business through online-banking. Bank uses cloud computing to accomplish this task economically. The bank is considered as potential cloud customer. Following are requirements identified by the bank that must be covered by cloud computing services:

1. Data Storage: Customer's all data that might consist on account number, amount and transaction log history must store in the cloud.
2. Data Processing: Processing of credit transfer processes in cloud.

The bank has an internal development unit that gives software for online-banking service and components like web-server and application-server which works within cloud. The potential cloud provider should only provide cloud services for the finance domain.

3.5. Summary

It is concluded from above all discussion that this research work is based on qualitative research methodology in which descriptive and case study research methodologies are adopted. A survey is taken from multiple banks to verify the technique and then the results of this survey merged in i* hierarchy. Then the comparison of hierarchies verifies new methodology.

Chapter # 4

PROPOSED FRAMEWORK

4.1.Overview of the Chapter

This chapter explains the proposed framework of this research work with the explanation of techniques involved in this framework.

4.2. Baseline Frameworks

The proposed framework is based on i* hierarchy and SecREAM (Security Requirement Elicitation and Assessment Mechanism). iStar is a goal-oriented approach [34]. SecREAM is an asset-based ranking method [35]. To analyze structure of the framework, both models discussed separately and then discussed proposed work i.e. the i* hierarchy is produced with immergence of SecREAM for eliciting security requirements.

4.2.1. i* Hierarchy:

i* hierarchy is a goal-oriented method for gathering requirements [54]. This hierarchy consists upon three layers:

1. Director’s Layer

   This layer consists on the stakeholders who are the directors of company. They have business goals, business plans and strategies to run business and how to achieve these goals [55].

2. Manager’s Layer

   This layer consists on the stakeholders who may be directly associated with the system that is being develop. They have particular Business Rule Model through which they accomplish business goals maintained by directors of the company [55].

3. Administrator’s Layer

   Stakeholders on this layer have more explicit Business Rule Model. They interact more with the system because they execute commands, processes and screens the output of processes [55].

Along with these layers the fundamental concept of i* hierarchy is actor [56]. These actors have some goals and to achieve these goals they need to perform some tasks [56]. While perform their tasks these actors may dependent on each other. When this dependency is outside the existing layer or on the next layer then it is said to be delegation of goals between actors [54]. According to i* hierarchy, each stakeholder who will use the system either owner, developer or user of developing system must be included while gathering requirements because stakeholders are at different level and hence have different requirements [54]. i* hierarchy is being used to gather and analyze requirements from different level of stakeholders.

With respect to the case study used in this research work, bank and cloud provider are the main actors of i* hierarchy. Bank needs to serve online-banking service to its customers. For this purpose, they required cloud computing services which is provided by a certain cloud provider. Let actors of case study be discussed on each layer of i* hierarchy. Table 4.1. shows the layers and the role of actors on each layer according to the case study and figure 4.1 displays the hierarchy.

Table 4.1.: Layers and Roles of Actor

Layers\Actors	**Bank**	**Cloud Provider**
Directors	1. Directors of certain bank involves. 2. Their goal is to provide facilities online-banking services to its customers i.e. ease of access to their accounts. 3. Their task is to report the deployed status of online-banking service to their customers so that accurate actions can be taken for a smooth running of online-banking service.	1. Directors of certain cloud provider. 2. Their goal is to provide cloud services by gathering cloud customer requirements, for instance, they provide cloud services like IaaS, PaaS and SaaS to the bank to create online-banking service. 3. Their task is to report required resources status to its managers so that they fulfill requested services.

Managers	1. Managers of the bank involves. 2. Their goal is to involve administrators to deploy online-banking services properly in the production environment and to monitor this deployment. 3. Their task is to provide resources for deployment of the system to the administrator of bank and report deployed cloud services to the cloud provider manager.	1. Manager of cloud provider involves. 2. Their goal is to fulfill requested services to develop online banking service. 3. Their task is to maintain availability of these cloud services. 4. Their task is to inform resource requirements to the bank manager for a smooth running of cloud services.
Administrators	1. Administrators of the bank involves. 2. Their goal is to deploy online-banking system in production environment. 3. Their task is to inform resource requirements to cloud provider.	1. Managers of the cloud provider involves. 2. Their goal is to provide actual resources like servers, database software etc. to serve the services to cloud customer i.e. bank.

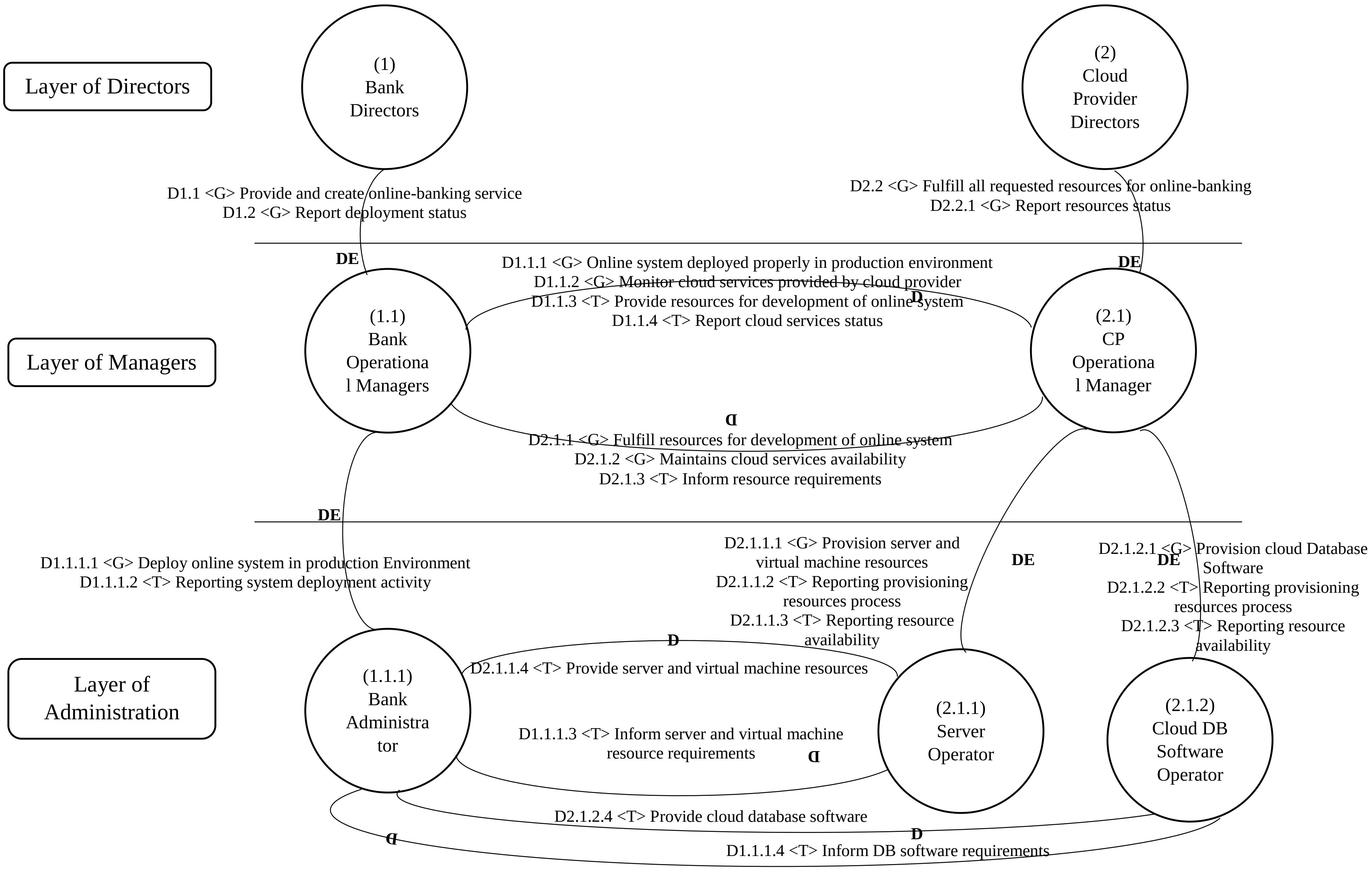

Layer of Directors
Layer of Managers
Layer of Administration
(1) Bank Directors
(2) Cloud Provider Directors
D1.1 <G> Provide and create online-banking service
D1.2 <G> Report deployment status
D2.2 <G> Fulfill all requested resources for online-banking
D2.2.1 <G> Report resources status
DE
DE
D1.1.1 <G> Online system deployed properly in production environment
D1.1.2 <G> Monitor cloud services provided by cloud provider
D1.1.3 <T> Provide resources for development of online system
D1.1.4 <T> Report cloud services status
D
(1.1) Bank Operational Managers
(2.1) CP Operational Manager
D
D2.1.1 <G> Fulfill resources for development of online system
D2.1.2 <G> Maintains cloud services availability
D2.1.3 <T> Inform resource requirements
DE
D1.1.1.1 <G> Deploy online system in production Environment
D1.1.1.2 <T> Reporting system deployment activity
D2.1.1.1 <G> Provision server and virtual machine resources
D2.1.1.2 <T> Reporting provisioning resources process
D2.1.1.3 <T> Reporting resource availability
DE
D2.1.2.1 <G> Provision cloud Database Software
DE
D2.1.2.2 <T> Reporting provisioning resources process
D2.1.2.3 <T> Reporting resource availability
D
D2.1.1.4 <T> Provide server and virtual machine resources
(1.1.1) Bank Administrator
(2.1.1) Server Operator
(2.1.2) Cloud DB Software Operator
D1.1.1.3 <T> Inform server and virtual machine resource requirements
D
D2.1.2.4 <T> Provide cloud database software
D
D
D1.1.1.4 <T> Inform DB software requirements

Figure 4.1.: i* Hierarchy "Strategic Dependency between Actors"

4.2.2. Security Requirement Elicitation and Assessment Mechanism (SecREAM)

It is an asset-based ranking methodology used for requirement elicitation and analysis for security and nonfunctional requirements in both traditional and cloud systems in initial stage of software development [35]. This method consists upon following stages:

1. Recognition of Stakeholders and Assets
2. Relevance of Stakeholders and Assets
3. Ranking of Assets according to the Stakeholders
4. Analysis of Ranking and Generation of Rank Table

The fundamental concept of this methodology are stakeholders, assets and the security parameters related to these assets. Stakeholders and assets of the system are recognized by the requirement engineers then they produce relation between stakeholders and assets. After finding this relation, these stakeholders rank the assets with respect to security parameters so that it can be found that what kind of security is more required by the stakeholder. These security parameters are defined by Forouzan [57].

With respect to the case study, stakeholders of the system are bankers (system handler user) who handles the system and their customer who will use the online-banking system. Though there are some other stakeholders too like cloud providers, the developers and those who will support the services but the above two stakeholders i.e. the banker and bank customers are the particular stakeholders on whom the research work focuses. Assets of the cloud system are data storage and data processing. Stakeholders of the discussing system are related to both assets as they need to store data and they also need to process it when required. This all will be discuss in detail in the description of proposed framework.

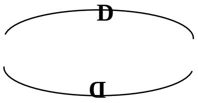
4.3. Proposed Framework:

The goal of this research is to obtain such methodology that will assist requirement engineers to elicit security requirements in early stage of software development so that the system will be secure in future as well as it can be helpful to secure system from disasters. As discussed i* hierarchy is goal-oriented and SecREAM is asset-based methodologies. The proposed work is the combination of both methodologies. It will help to elicit functional as well as security requirements of the developing system.

Actors plays major role in i* hierarchy [46]. Therefore, adding a new actor in this hierarchy can help to elicit security requirements. This new actor is derived from

SecREAM methodology and then merged into i* hierarchy. Figure 4.2. shows new i*hierarchy with this new actor called as “Guard” and Table 4.2. shows its legends.

Table 4.2.: Legends

Symbols	**Description**
▭	Shows the name of layer or layer level
○	Shows the actors of hierarchy
	Shows dependency of one actor to another actor
———	Shows the ending of each layer
(#)	Shows the level number of actor
DE	Shows delegation of actors
<G>	Shows the goal of an actor
<T>	Shows the task of an actor
D(#).1	Means that Dependency (level number of actor). Numbering
⬡	Shows tasks that has to be done by the actors.

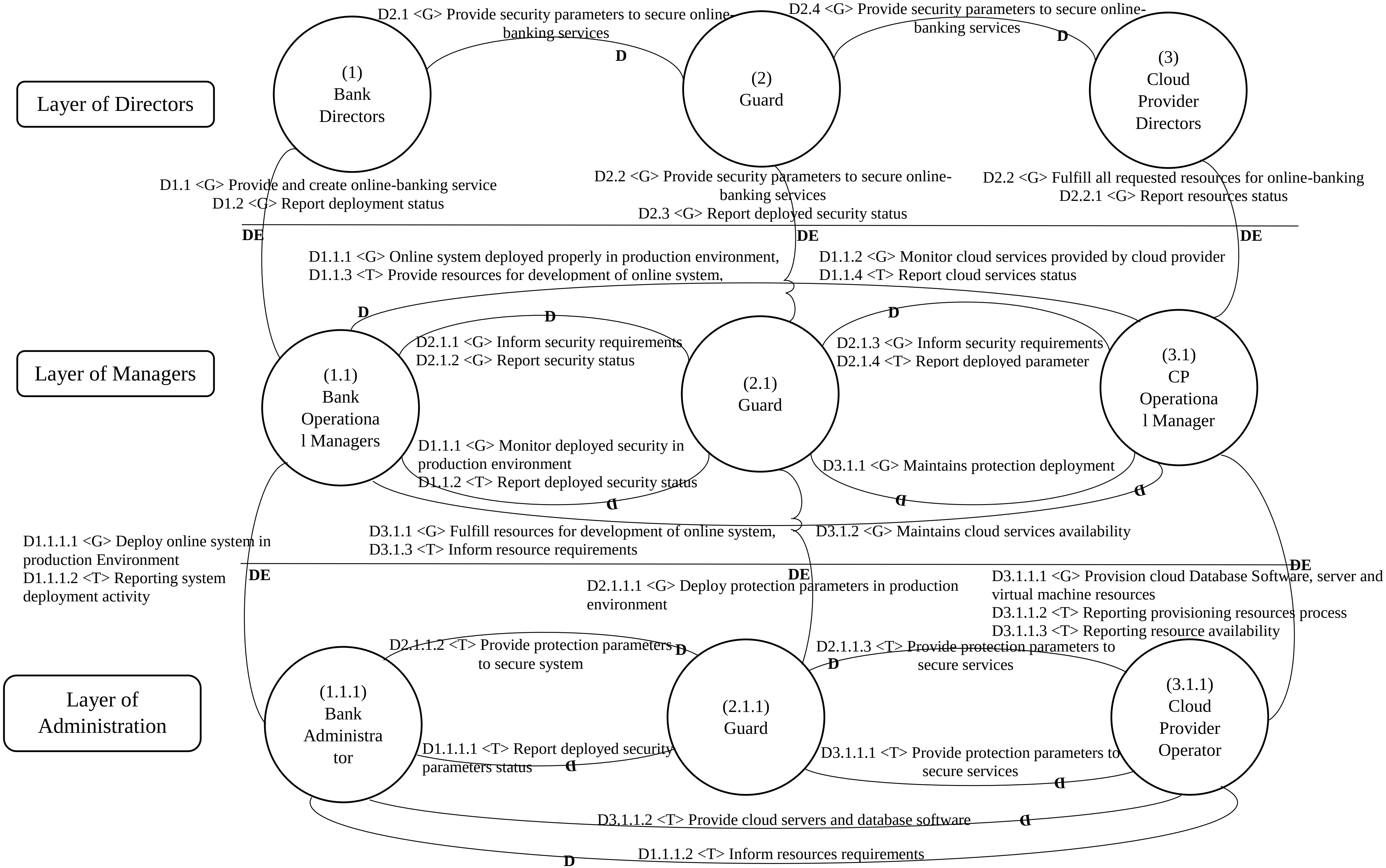

Layer of Directors
Layer of Managers
Layer of Administration
(1) Bank Directors
(2) Guard
(3) Cloud Provider Directors
(1.1) Bank Operational Managers
(2.1) Guard
(3.1) CP Operational Manager
(1.1.1) Bank Administrator
(2.1.1) Guard
(3.1.1) Cloud Provider Operator
D2.1 <G> Provide security parameters to secure online-banking services
D2.4 <G> Provide security parameters to secure online-banking services
D1.1 <G> Provide and create online-banking service
D1.2 <G> Report deployment status
D2.2 <G> Provide security parameters to secure online-banking services
D2.3 <G> Report deployed security status
D2.2 <G> Fulfill all requested resources for online-banking
D2.2.1 <G> Report resources status
DE
DE
DE
D1.1.1 <G> Online system deployed properly in production environment,
D1.1.3 <T> Provide resources for development of online system,
D1.1.2 <G> Monitor cloud services provided by cloud provider
D1.1.4 <T> Report cloud services status
D2.1.1 <G> Inform security requirements
D2.1.2 <G> Report security status
D2.1.3 <G> Inform security requirements
D2.1.4 <T> Report deployed parameter
D1.1.1 <G> Monitor deployed security in production environment
D1.1.2 <T> Report deployed security status
D3.1.1 <G> Maintains protection deployment
D3.1.1 <G> Fulfill resources for development of online system,
D3.1.3 <T> Inform resource requirements
D3.1.2 <G> Maintains cloud services availability
D1.1.1.1 <G> Deploy online system in production Environment
D1.1.1.2 <T> Reporting system deployment activity
DE
DE
DE
D2.1.1.1 <G> Deploy protection parameters in production environment
D3.1.1.1 <G> Provision cloud Database Software, server and virtual machine resources
D3.1.1.2 <T> Reporting provisioning resources process
D3.1.1.3 <T> Reporting resource availability
D2.1.1.2 <T> Provide protection parameters to secure system
D2.1.1.3 <T> Provide protection parameters to secure services
D1.1.1.1 <T> Report deployed security parameters status
D3.1.1.1 <T> Provide protection parameters to secure services
D3.1.1.2 <T> Provide cloud servers and database software
D1.1.1.2 <T> Inform resources requirements
D

Figure 4.2.: i* Hierarchy "Strategic Dependency between Actors with New Actor"

Now this new actor will be discussed in each layer of hierarchy. Providing security is the main goal between role of guard on each layer.

On the layer of directors, its goal is to provide security for an online-banking system. Its second goal is to report deployed security status to its subsequent actor on the next layer. Then guard delegates its goal to the actor on manager layer.

On the layer of managers, guard invokes other actors bank operational manager and cloud provider (CP) operational manager to secure the system. Its main goal is to provide security requirements to bank operational manager and cloud provider operational manager and generate alerts time-by-time for the actors. Now this actor burdens some new responsibilities on other actors existing in the same layer. Bank operational manager has now a new goal i.e. to monitor deployed security measurements taken by bank administrators beneath operational managers and report deployed security status to guard. The purpose of this bank operational manager report related to deployed security status is that guard keeps record of all security measurements that has been taken and then analyze new measurements that will help bank managers to keep their system secure. When guard found new security parameters then it will inform security requirements to the bank as well as cloud provider. Then bank and cloud provider operational manager updates previous security measurements and maintains security deployment of the system. Then guard delegates its role to the actor on administrator layer.

On the layer of administrators, guard provides security parameters to both actors and get reports from them about deployment of security parameters status. Cloud provider administrators reports about satisfaction with the deployed security parameters and bank administrator reports what steps has been taken, which parameters are deployed, and which parameters are left over so that guard invokes bank administrator time-to-time for security deployment to keep system secure.

Strategic rationale is used to look what’s inside an actor i.e. what processes it carries out to accomplish a goal or task [55]. Here strategic rationale of some actors is discussing which shows how an actor completes his goal or task.

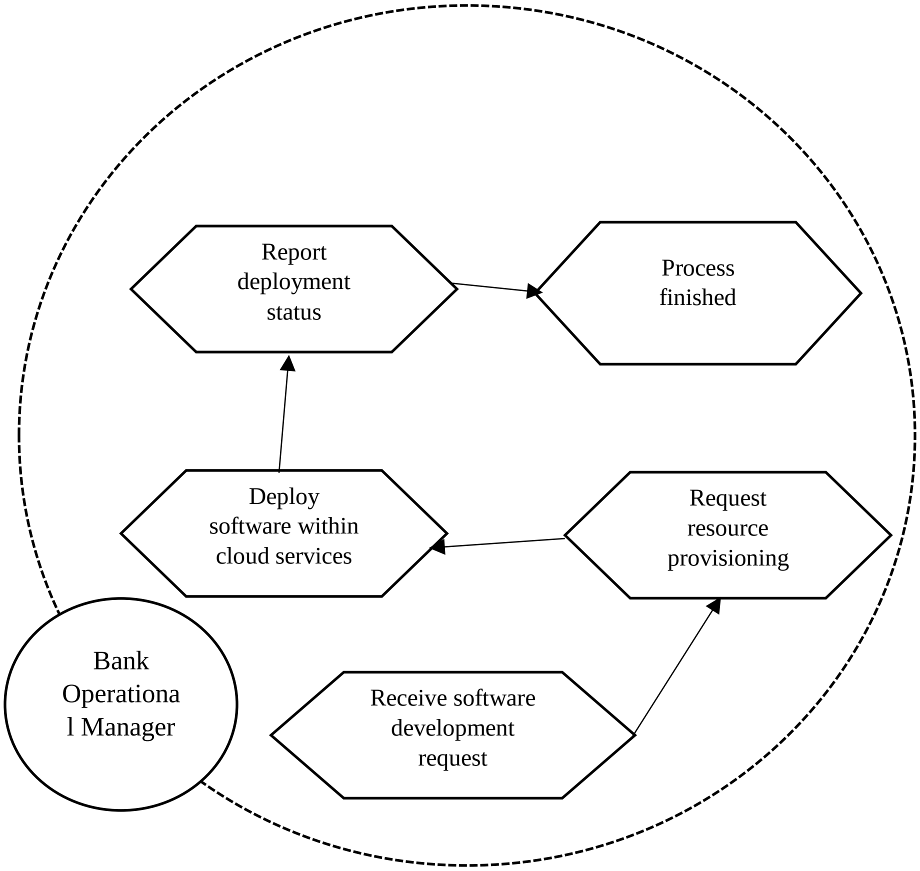

Report deployment status
Process finished
Deploy software within cloud services
Request resource provisioning
Bank Operationa l Manager
Receive software development request

Figure 4.3.: i* Hierarchy "Strategic Rational of Bank Operational Manager"

Figure 4.3. shows strategic rationale of an actor "Bank Operational Manager" at manager layer or layer 2. The purpose of this actor is to manage whole processes to accomplish online-banking services for the bank. In case study, it is given that bank has an internal development unit whose purpose is to provide internal bank software which is installed within cloud services on production environment. In i* hierarchy, bank operational manager is performing the task that is deployment of software within cloud services on production site.

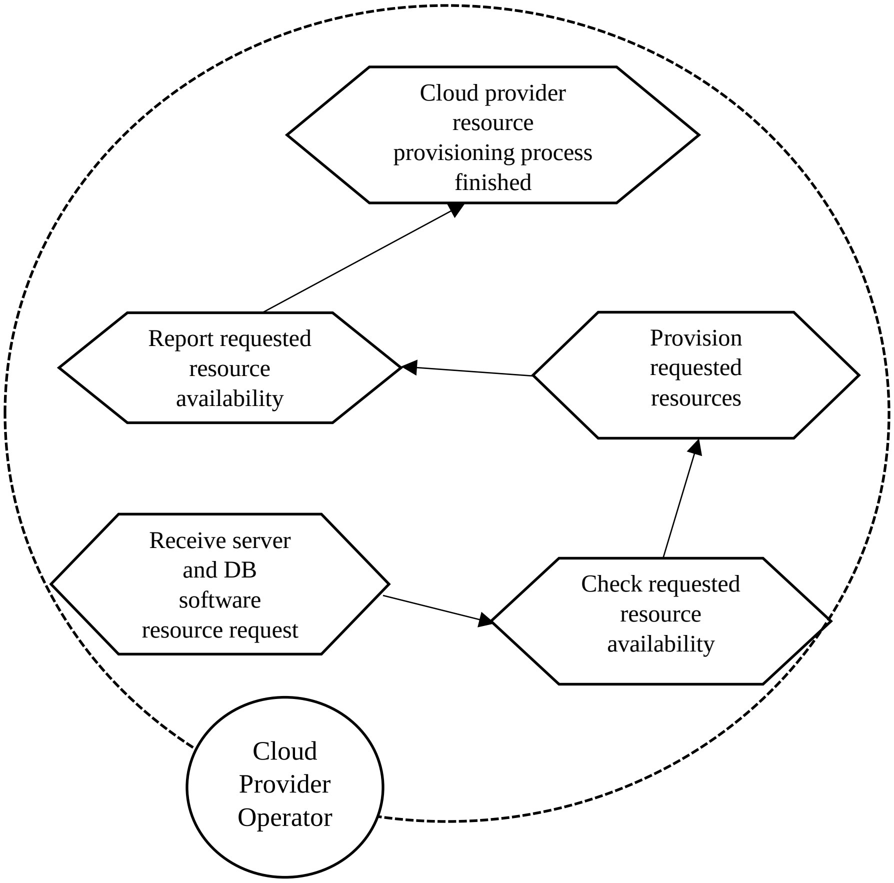

Cloud provider resource provisioning process finished
Report requested resource availability
Provision requested resources
Receive server and DB software resource request
Check requested resource availability
Cloud Provider Operator

Figure 4.4.: i* Hierarchy "Strategic Rational of Cloud Provider Operator"

Figure 4.4. shows strategic rationale of cloud provider operator at administrator layer or layer 3. According to case study the purpose of this actor is to provide cloud resources and their software such as server and database software. It also maintains the availability of resources, for example, is server available at requested domain or not this will be handled by the cloud provider operator or administrator.

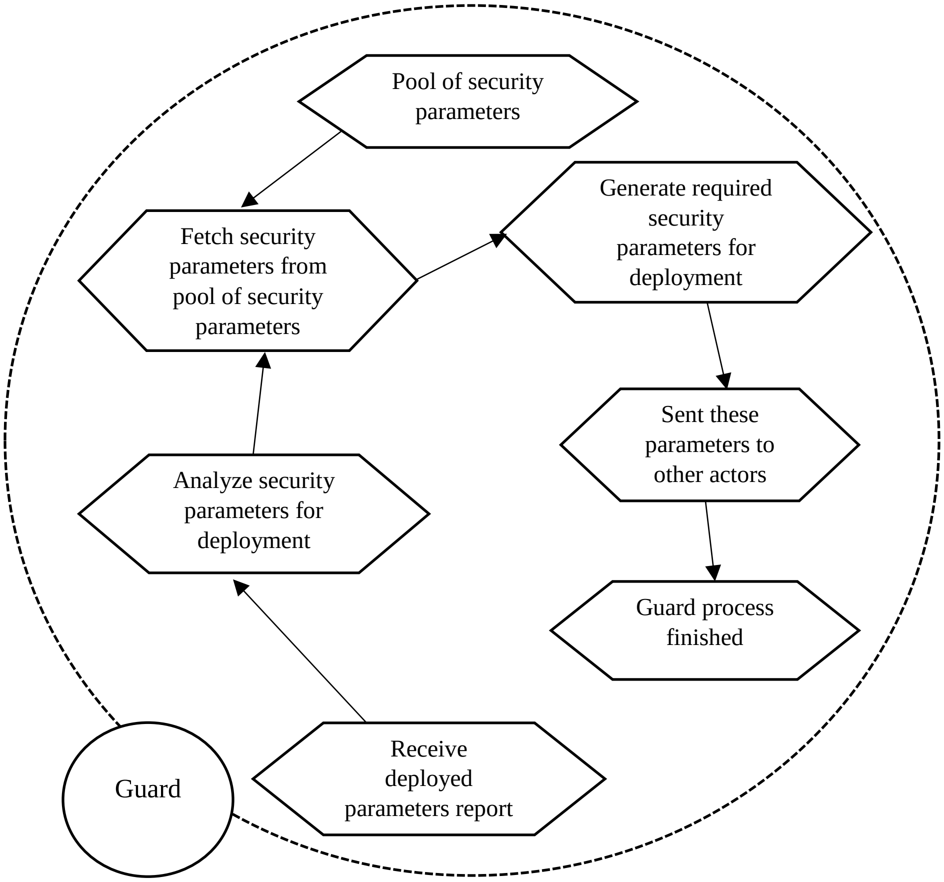

Pool of security parameters
Fetch security parameters from pool of security parameters
Generate required security parameters for deployment
Sent these parameters to other actors
Analyze security parameters for deployment
Guard process finished
Guard
Receive deployed parameters report

Figure 4.5.: i* Hierarchy "Strategic Rational of Guard at Administrator Layer"

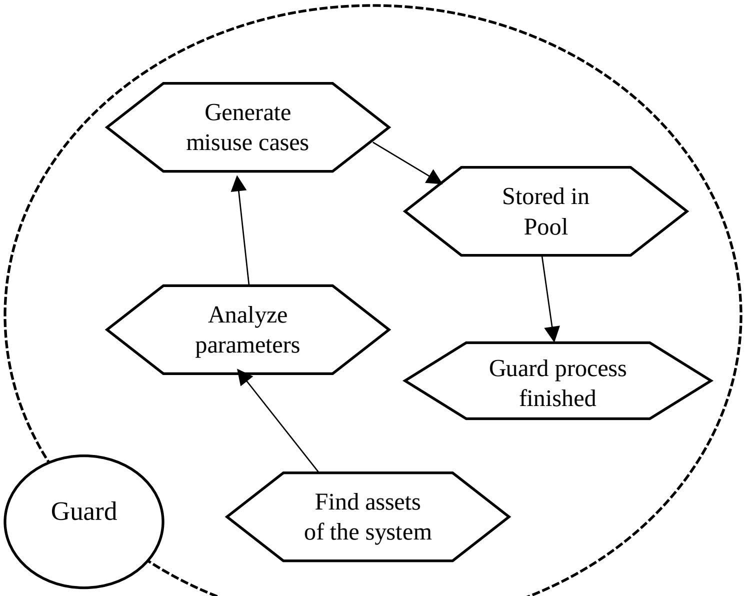


Figure 4.6.: i* Hierarchy "Strategic Rationale of Guard at Manager Layer"

Figure 4.5. shows strategic rationale of an actor guard which is a new actor in this hierarchy in all layer and here it is discussing at administrator layer or layer 3. It contains a pool where all security parameters be located, and these parameters are the results of SecREAM. The purpose of this actor is to invoke other actors and alert them about security issues. When the system is going to be developed there must be an entity which keeps its eye on security issues that might arise in the system, guard will perform this task. Another thing is guard tells about the most important security parameters through which data might be steal as according to case study data processing and data storage is required by the cloud customer i.e. bank. Hence it will handle security issues related to cloud systems.

At the manager layer, the guard finds the assets of the system and then analyze parameters of these assets. Then misuse cases are generated in for each parameter. These misuse cases express the security threats for the system. These parameters are then stored in the pool named as pool of security parameters. This process is demonstrated in Figure 4.6.

Pool of security parameters consists on assets of the system with their respected parameters involved in the system. According to case study the assets of online-banking are data storage and data processing and their parameters are authentication, authorization, availability, maintainability, configuration, scalability and integrity. According to Forouzan these are the security parameters of any system and security requirements are derived from these parameters [47]. Table 4.3. shows the requirements to which these parameters are indicated.

Table 4.3.: Parameters and Security Requirements

Sr. No.	Parameters	Security Requirements
1	Authentication	How do account details access? How do account is protected from unauthorized access? If a fake person with authentic information enters into the system, then how should system resist him?
2	Authorization	Customer view his account details. What things he has allowed?

		What if he tries to view other things?
3	Availability	How much downtime is allowed for the system? When the downtime prolongs then what system should do? When customer tries to access his account and he found message that “System is busy” and he found this message one time or more than one time on different timings then should customer have to take any step?
4	Maintainability	Does system backup it’s data? When the last upgradation of account details has been done? Which architecture is provided by the service provider?
5	Configurability	How an online-banking service provided to the customers? If it is through mobile application, then is it ready to meet with hardware requirements? If it is through web services, then is it capable to deal network security issues? What infrastructure is provided to configure hardware like firewall, proxy server etc.?
6	Scalability	Does system allowed to upgrade to meet technological changes? If so, then are security measures taken for software viruses before upgradation consistent with the change?
7	Integrity	Does data encrypt? Who will decrypt the data and how?

		Is digital signature allowed for customers to add on their account? If so, then how are digital signatures handled by the system?

The guard at layer of administrators, receives deployed parameters report and then evaluate which security parameter is left to be deployed in the system. These deployments of parameters are the security measurements which the developer should take during the development of system. This evaluation report ensures the security of the system.

4.4. Summary

It is concluded that traditional requirement engineering techniques can be used to elicit requirements for cloud-based systems by modifying them because devoted techniques are required for cloud systems.

Chapter # 5

RESULTS AND ANALYSIS

5.1. Introduction

This chapter shows the overall results derived from the literature review, from survey and from proposed framework.

5.2. Results from Literature Review

The results of literature review are discussed here. Literature review comprised on research papers published in past recent years and these are from January 2014 to July 2017. Though not all published research papers are included because of selection criteria created to conduct literature for this research work. Therefore, it includes search strategy, process and paper quality assessment. Following are the derived results search results of search these entities.

5.2.1. Search Results

Table 5.1. shows the search result of the search procedure performed for selection of papers. Figures 5.1, 5.2, 5.3 displays the statistical view of the result of search process that is 148 number of studies found, 60 found relative to this research work. Thus, the research studies which are different in their content, are selected. Hence 20 number of studies selected for literature review.

Table 5.1.: Search Result

Year	Total Papers Found	Relevant Papers	Selected Papers
2014	45	13	4
2015	35	16	6
2016	46	21	6
2017	22	10	4
Total	148	60	20

The raw material takes out from each study and then tabularized in Table A that consists on the parameters such as year, paper title, abstract and the technique it introduces and then this extracted data is used to analyze relative research papers.

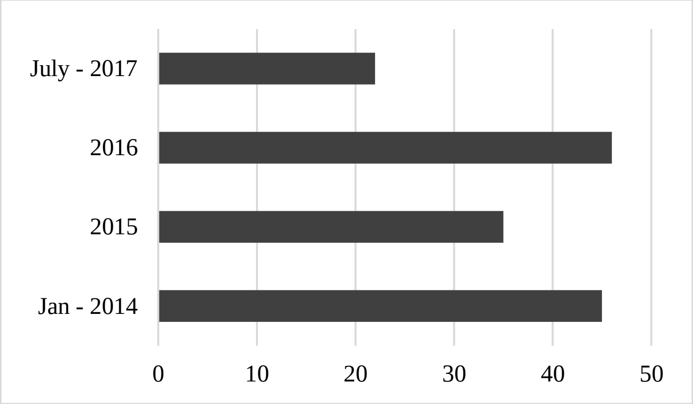


Figure 5.1.: Statistics on Total Papers Found

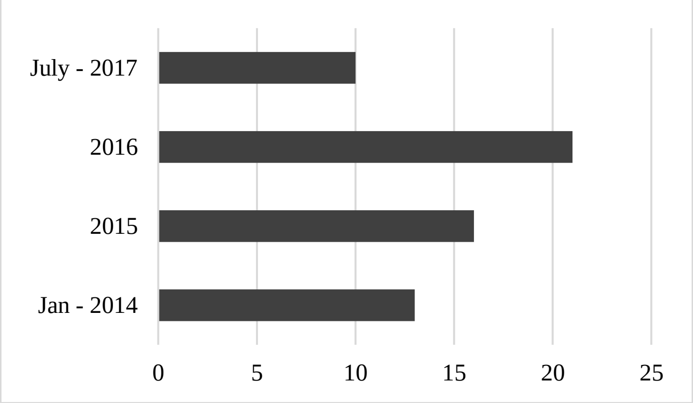


Figure 5.2.: Statistics on Relevant Papers

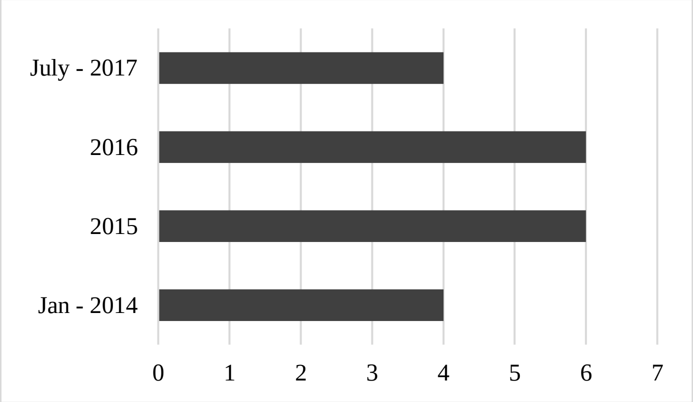


Figure 5.3.: Statistics on Selected Papers

5.2.2. Quality Valuation of Studies

The quality of the papers has been assessed by the quality questions which are describe in section 3.2.5. The outcome of the analysis of studies shows that only three studies scored

3, two studies scored 1 and rest all studies scored 1.5 or more than 1.5. Table 5.2. display the scores of studies respectively. This result demonstrates the need of research in this field i.e. requirement engineering for cloud computing to handle security issues.

Table 5.2.: Quality Valuation of Studies

Study	QA1	QA2	QA3	Total Score
S1	Y	Y	N	2
S2	P	Y	N	1.5
S3	Y	P	P	2
S4	Y	Y	Y	3
S5	Y	P	P	2
S6	Y	N	P	1.5
S7	P	N	P	1
S8	Y	Y	N	2
S9	Y	Y	Y	3
S10	P	P	N	1
S11	Y	Y	Y	3
S12	Y	P	N	1.5
S13	Y	Y	Y	3
S14	Y	P	N	1.5
S15	Y	Y	N	2
S16	Y	P	N	1.5
S17	Y	P	Y	2.5
S18	Y	P	N	1.5
S19	Y	P	N	1.5
S20	Y	N	P	1.5

5.2.3. Quality Factors

Investigation between relationship of year and score has been observed during analysis. Table 5.3. displays the average of quality scores of the studies respectively. This table specifies that the publication number is quite stable in respected years. The average quality score seems to be variant year by year. One important thing is that the last six months of 2017 has been excluded according to criteria set for the literature review, that is why it shows less scoring but if compared with other years then it is concluded that the number of research is increasing on requirement engineering techniques to elicit security issues for cloud computing yet still more research is required in this field.

Table 5.3.: Average Quality Scores by Year

	Year			
	2014	**2015**	**2016**	**2017**
Sum of Studies	4	6	6	4
Average Quality Score	2.11	1.75	2.08	1.17
Standard Deviation	0.39	0.57	0.54	0.7

5.2.4. Results

From the literature review, it is concluded that the techniques/frameworks which are proposed to elicit requirements for cloud systems have following limitations:

1. They focused only on functional requirements.
2. Few of them are used to elicit requirements for specific system.
3. Requirements elicitation is not specifically focused as they are involved throughout the Software Development Life Cycle.
4. Security requirements are not considered in the techniques used to elicit requirements for cloud systems.

Research questions are also derived from this literature review which are also discussed in chapter 3 section 3.3. These questions lead towards to conduct survey and to modify a technique.

5.3. Results from Survey

5.3.1. Survey Analysis from Bankers

The survey is designed that it has two parts. First part is about data storage and second part is about data process. Following Tables and Figures are showing the results of survey.

Table 5.4.: Data Storage (No. of Responses)

Parameters\Ranks	1= High	2= High-medium	3= Medium	4= Medium-low	5= Low
Authentication	15	4	3	0	0
Authorization	12	6	3	0	1
Availability	6	4	7	3	2
Maintainability	6	6	7	1	2
Configuration	5	4	4	4	5
Scalability	4	4	5	5	4
Total %	36.36	21.21	21.97	9.85	9.85

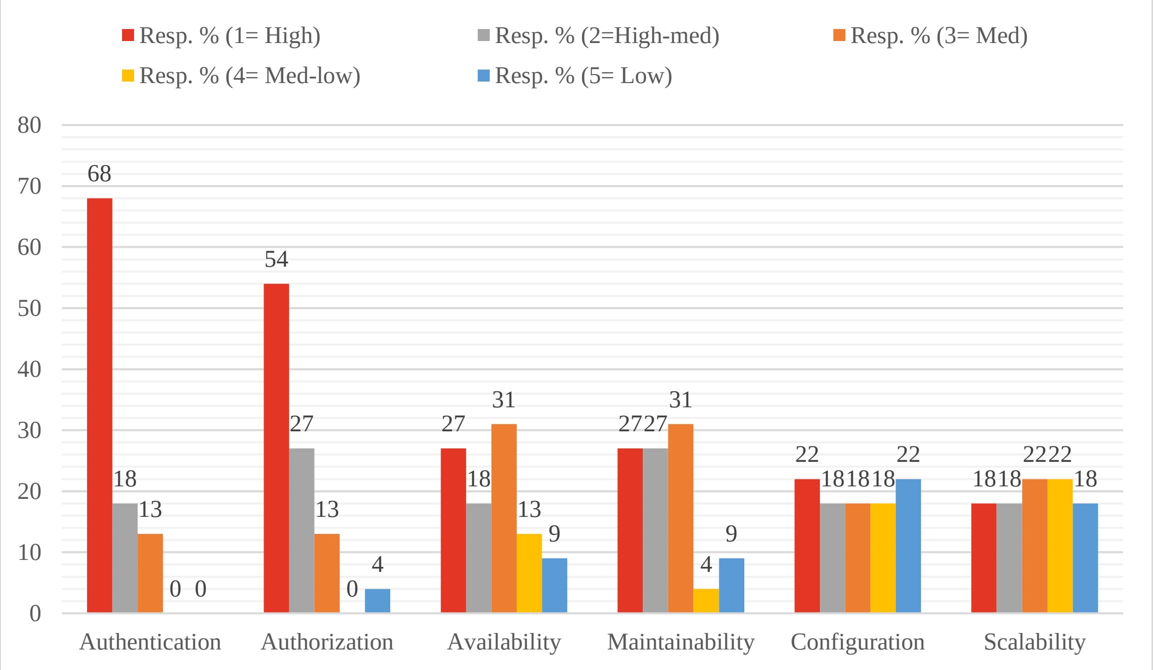


Figure 5.4.: Data Storage Response Percentage Analysis

The Table 5.4. and Figure 5.4. are consists on data storage analysis. In the survey questions are designed to target parameters (listed in first column of the table) in the context of data storage. First parameter authentication ranks highest in its column as well as in row which shows the importance of this parameter in cloud system specially in the case study perspective.

Second parameter i.e. authorization ranks second highest in its column as well as in row which seems that access to data or information is also concerned aspect. Who will access data and how it will be accessed both are very concerned and important and these are authentication and authorization.

Third parameter ranked as medium. It gained 7 votes at rank 3 i.e. medium, therefore, the votes of this parameters are divided into two parts higher part and lower part. Higher part consists on ranks 1, 2 and 3 whereas lower part consists on ranks 3, 4 and 5. Now percentage of each part is calculated and then compared with each other to get the result, so, higher part (percentage of 6, 4 and 7) results in 77.27 % and lower part (percentage of 7, 3 and 2) results in 54.54% which can be seen in the table 7b. This calculation shows that the availability of the system is also a security concerned in the cloud system. Same is the case in forth parameter that is maintainability. By considering third and fourth parameters it can be observed that customers' needs system to be available so that services can be provided to assist users and maintain them time-to-time. Now in next two parameters that is configuration and scalability both are also concerning parameters that may cause security threat in the cloud system.

Table 5.5.: Data Processing (No. of Responses)

Parameters\Ranks	**1= High**	**2= High-medium**	**3= Medium**	**4= Medium-low**	**5= Low**
Authentication	17	3	0	2	0
Authorization	9	6	5	1	1
Availability	7	7	5	2	1
Maintainability	6	7	5	3	1
Configuration	4	6	5	2	5
Scalability	4	1	5	6	6
Total %	35.61	22.73	18.94	12.12	10.61

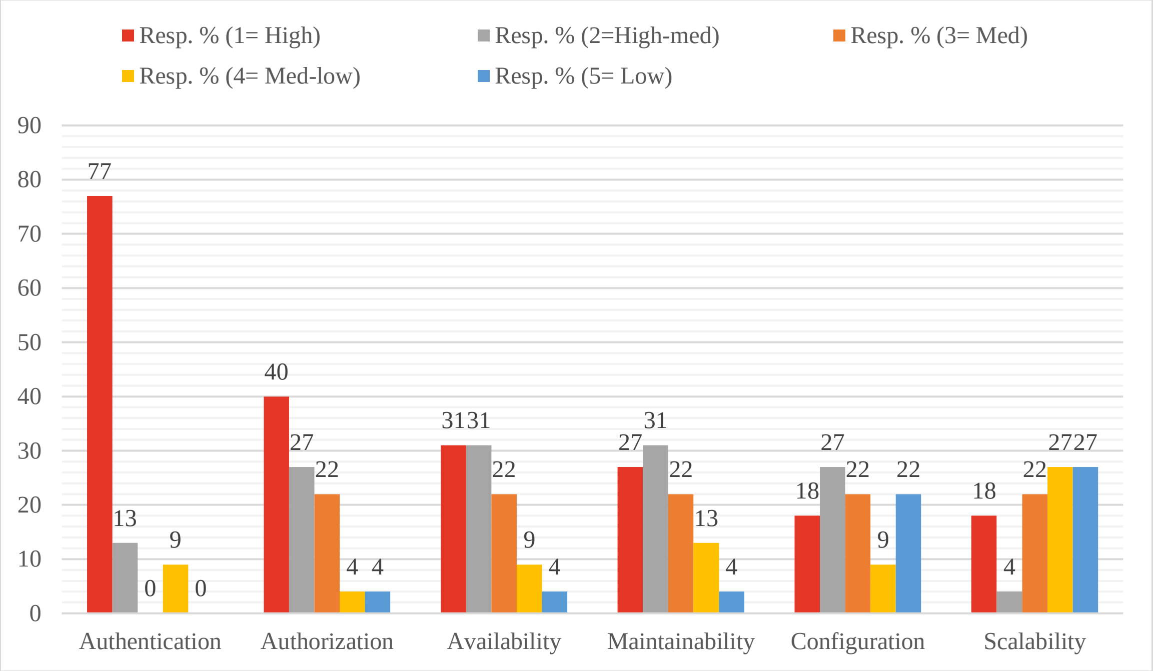


Figure 5.5.: Data Processing Response Percentage Analysis

The Table 5.5. and Figure 5.5. are consists on data processing analysis that is the instant working of online system. In the survey questions are designed to target parameters (listed in first column of the tables) in the context of data processing. First parameter authentication ranks highest in its column as well as in row that is 77% customer rank it as high security aspect which shows the importance of this parameter in cloud system.

Second parameter i.e. authorization ranks second highest that is about 41% customer do not allow others to access their account or account information. Therefore, this parameter must be considered while developing cloud system. It can be seen in the table that third parameter i.e. availability got equal votes (32%) in first two ranks. This shows that the system must be available whenever customer required to access system. This leads that down time of the system should be less than 4 hours in business working days.

The forth parameter got highest votes on rank 2 which shows that cloud system must be maintain either in software that is running to provide services, may be usability and during peak hours. In the case of fifth parameter, it can be observed that rank 2 and rank 3 differs with only one vote which shows customers are not much interested in third party involvement during the use of online applications but if percentage of first three ranks taken considering higher part then it is 68% and on lower part it is about 55%. In the light of percentages comparison configuration is concerning parameter by the customers in security aspect.

The last parameter that is scalability ranks highest at 4 and 5. This shows that scalability for customer is not as such security parameter maybe they are not much aware of how this parameter can be used as security breach.

5.3.2. Survey Analysis from Bank Customers

The survey consists of two parts that is data storage and data processing. Each part has its own parameters according to the case study. Following Tables and Figures are showing the results of survey.

Table 5.6.: Data Storage Analysis (No. of Responses)

Parameters\Ranks	1= High	2= High-medium	3= Medium	4= Medium-low	5= Low
Authentication	19	0	0	1	0
Authorization	17	3	0	0	0
Availability	11	4	4	0	1
Scalability	2	3	6	3	6
Integrity	6	3	4	4	3
Total %	55.00	13.00	14.00	8.00	10.00

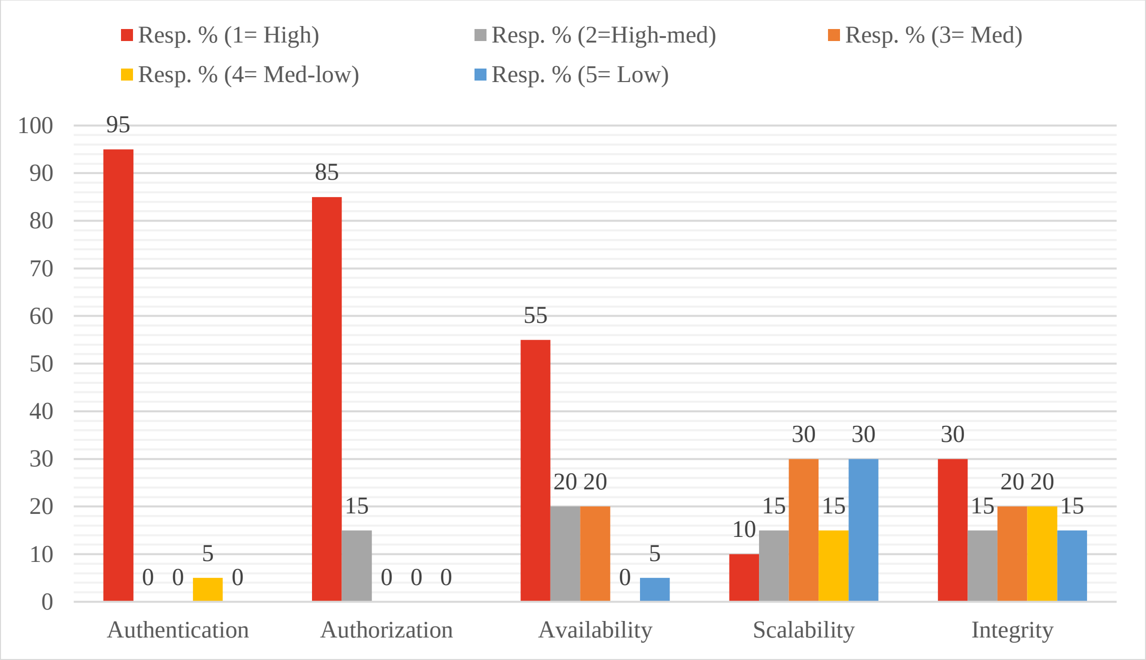


Figure 5.6.: Data Storage Analysis (Response Percentage)

The Table 5.6. and Figure 5.6. consists on data storage analysis. In the survey questions are designed to target parameters (listed in first column of the table) in the context of data storage. The Table 5.6. demonstrates responses on parameter and Figure 5.6. demonstrates response percentages. First parameter authentication indicates that this parameter is very important for the bank customers in the view of security as 95% customers are keen about this parameter. Then they are also concerned about who has access to their data. This is the reason the parameter authorization ranks 85%. The system availability is also important for the customers as the account holders are related from different domains and they need to do transactions monthly or sometimes daily. This is the reason it scored average percentage. The response rate of scalability and integrity are scored less than average percentages but comparatively, integrity is more concerned security aspect by the customers as it ranked higher than scalability.

Table 5.7.: Data Processing Analysis (No. of Responses)

Parameters\Resp. %	Resp. % (1= High)	Resp. % (2=High-med)	Resp. % (3= Med)	Resp. % (4= Med-low)	Resp. % (5= Low)
Authentication	19	0	0	1	0
Authorization	14	5	0	1	0
Integrity	4	5	4	5	2
Total %	61.67	16.67	6.67	11.67	3.33

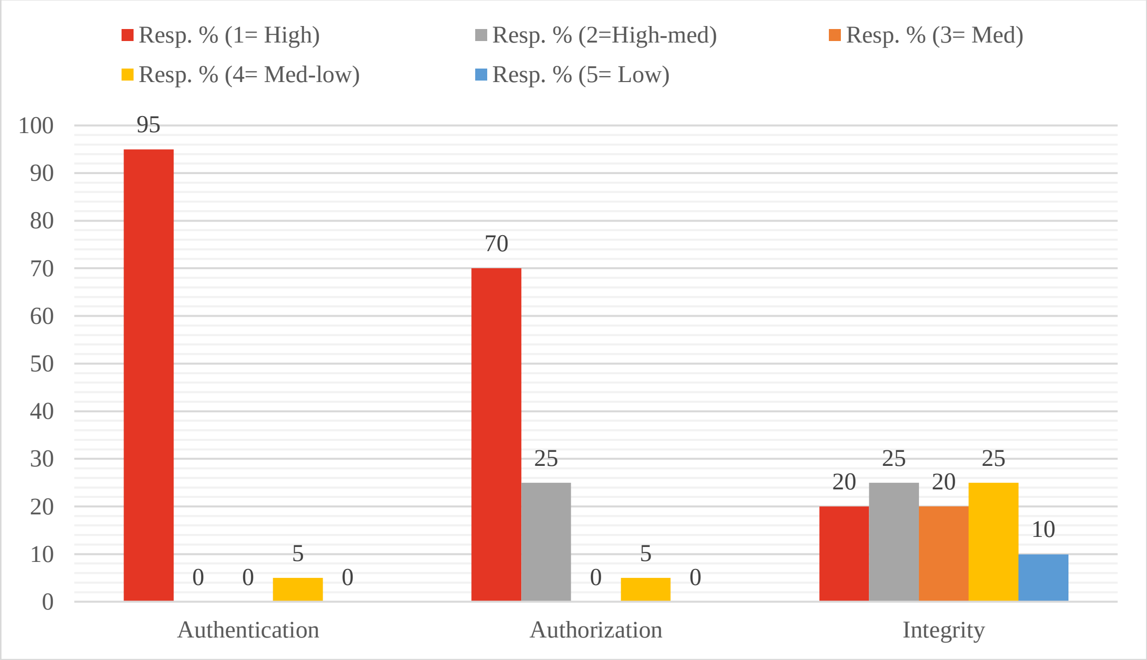


Figure 5.7.: Data Processing Analysis (Response Percentage)

The Table 5.7. consists on data processing analysis this is an instant working of online system. In the survey questions are designed to target parameters (listed in first column of the table) in the context of data processing. The Table 5.7. demonstrates responses on parameter and Figure 5.7. shows response percentages. 95% customers are concerned about their stored information. They do not allow any other except their own selves to access their account, therefore, authorization scores 70%. The last parameter that is integrity ranks 20%. This shows that integrity of their data is not as such security parameter maybe they are not much aware of how this parameter can be used as security breach.

5.4. Results from Proposed Framework

The parameters which are considered as security parameters indicated in Table 4.3. demonstrated the targeted security threats.

Table 5.8.: Parameters and Targeted Security Threats

Sr. No.	Parameters	Security Threat
1	Authentication	Verification and Permission issues
2	Authorization	Usage and Data Protection from Leakage
3	Availability	Denial of Service
4	Maintainability	Veracity (Accuracy), privacy and backups
5	Configurability	Web Browsers, Protocols, Remote connections
6	Scalability	Technological issues,
7	Integrity	Malicious attacks,

In the result of these parameters, the system should be secure from data loss, account hijacking, denial of services, inside attacks and shared technology issues.

It is derived from the proposed framework that a traditional technique can be modified to elicit requirements for cloud-based systems and it depends upon the technique that how much it is capable to cover stakeholders as much that the proper requirements can be elicited to develop the system.

Crowd-centric requirement engineering technique involves group of the users and their requirements assumes from all users whereas in the proposed framework all stakeholders are involved during requirement elicitation process [27]. Use cases and misuse cases are used to elicit functional and security requirements of the system [28]. Misuse cases generates against use cases and use cases are generated to show the functionality of the system. Hence misuse cases against use cases generates only for the function of the system. Whereas in proposed framework, requirements are gathered from each level of hierarchy of the system i.e. directors, manager and administrators. Security alerts are involved in each layer of the hierarchy. To analyze parameters of the systems with respect to security a method is required which digs out the security threat against a parameter. Therefore, misuse cases are involved in the proposed framework when parameters are required to analyze and then produce security alert as discussed in Table 4.3. Parameters and Requirements. The methodology proposed software security requirement engineering and management as an emerging cloud service (SSREMaaES) suggest rules and methods to secure system and the targeted threat in the method is DoS. Whereas Table demonstrates the threats covered by the proposed framework of this research work [37].

The existing techniques and proposed framework are evaluated with respect to the following factors to derive the results of proposed framework and hence displayed in Table 5.9.

1. The method is traditional methodology.
2. The method is used for cloud-based systems.
3. The method is focused on functional requirements for cloud systems.
4. The method is focused on non-functional requirements for cloud systems.
5. Specifically proposed to elicit security requirements for cloud computing.

Table 5.9.: Comparison of Frameworks

Techniques	**1**	**2**	**3**	**4**	**5**
Crowd Centric Requirement Engineering	√	√	×	×	×
UML based Structure	√	√	√	×	×
Improved RE Framework for Cloud		√	√	×	×
Requirement Elicitation Cloud Framework	√	√	√	×	×
Software Security RE and Management as an Emerging cloud Service	×	√	√	×	√
Proposed Framework	√	√	√	√	√

Hence, it is derived from the proposed framework that a traditional technique can be modified to elicit requirements for cloud-based systems. the proposed framework elicits functional as well as non-functional requirements of the system.

5.5. Summary

The proposed method can be used for traditional as well as cloud computing systems. Traditional requirement engineering techniques can be used to elicit requirements for cloud-based systems by modifying them because devoted techniques are required for cloud systems.

Chapter # 6

CONCLUSION

6.1.Overview of the Chapter

This chapter describes the conclusion of the overall work which are carried out during this research work.

6.2. Conclusion

Cloud computing has changed the world of information technology. The cloud system is considered to be very strong so that data cannot be access by hackers, attackers or something like these entities. For that purpose, researchers suggest that this thing that is security must be considered at initial stage of the development of the system and this is the stage of requirement engineering.

This research work is carried out for the initial stage of development i.e. requirement elicitation process. A survey is also taken to examine what is the most demanding requirement for the users and the security parameters of the system that will be used by the customers. The result of the survey shows security is the most demanding requirement with multiple parameters which can cause data breach. When security is handled at early stage of cloud system development then it can prevent system from security threats. For cloud computing dedicated requirement elicitation techniques are required and this research work proposed a framework which is performed such task.

The proposed framework is based on i* hierarchy which helps to understand functional requirements because of hierarchies involved in it. This will help to elicit functional requirements with the most demanding requirement i.e. security requirements as it describes the role at each level which will be consider in development stages so that the system is save from security issues. An online-banking case study is used to manipulate this work. This framework elicits both functional and non-functional requirements as security is in non-functional requirements category. The proposed framework concentrates on requirement elicitation process; hence, it is not involved all processes of requirement engineering.

It is derived from the proposed framework that a traditional technique can be modified to elicit requirements for cloud-based systems and it depends upon the technique that how much it is capable to cover stakeholders as much that the proper requirements can be elicited to develop the system.

6.3. Future Work

In future the proposed work will be apply on different domains and make it appropriate to involve all processes of requirement engineering which are (i) requirement analysis, (ii) requirement prioritization and (iii) requirement specification. Some other traditional techniques will be modified for cloud-based systems.

Appendix - A

Questionnaire for Bank Customers

I am student of MS (Computer Software Engineering) from NUST (National University of Science and Engineering). I am working in the field of "Requirement Engineering for Cloud Computing". I have selected "Online Banking" as my case study. In this regard I have taken two tasks i.e. data storage and data process that are carried out on cloud. From this survey I will be analyzing security issues that need to be considered in development stage.

This survey is divided into two parts. First part is about data storage and second part is about data process. Kindly choose the option that describes your best answer.

Note: This information is only used for research purposes.

How often do you use internet banking? Which features of internet banking do you use? Fill the following grid.

You use online banking for	Yes/No	Daily	Weekly	Twice in a week	Monthly	Yearly
Pays utility bills						
Check the account details						
Transfer money between accounts						
Mini Statements						
Order cheque books						

1. **Data Storage:**

   It is the space where customer's all data that might consist on account number, amount and transaction log history must store in the cloud.

   a. **Authentication**

   How would you like to access your data?

   ○ User name and password
   ○ Only password
   ○ Only username
   ○ Finger prints
   ○ Pin codes

   b. **Authorization**

   What do you think, who can access your personal information\data?

   ○ Authorized persons
   ○ Employees
   ○ Technical support
   ○ All of above
   ○ Only authorized persons and employees

   c. **Availability**

   How much do you access your bank account data?

   ○ Daily
   ○ Twice in a week
   ○ Weekly
   ○ Monthly
   ○ Yearly

   d. **Scalability**

   Do you upgrade mobile application to meet technological changes?

   ○ Yes
   ○ No
   ○ May be
   ○ Not at all
   ○ Don't know

e. Integrity

Are you satisfied with current features of online banking?

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree

2. Data Process:

It is the processing of credit transfer processes in cloud.

a. Authentication

How would you like to access your data?

- User name and password
- Only password
- Only username
- Finger prints
- Pin codes

b. Authorization

Do you have digital signatures or something alike when perform transactions?

- Yes
- No
- May be
- Not at all
- Don’t know

c. Integrity

What do you think, security and ease of use both are important?

- Yes
- No
- May be
- Not at all
- Don’t know

In your view, how much these factors contribute towards security? Rank them with the meaning of these numbers: 1= high, 2= high – medium, 3= medium, 4= medium – low and 5= low

Parts\Parameters	**Authentication**	**Authorization**	**Availability**	**Maintainability**	**Configuration/Integrity**	**Scalability**
Data Storage						
Data Processing						

Appendix - B

Questionnaire for Bankers

I am student of MS (Computer Software Engineering) from NUST (National University of Science and Engineering). I am working in the field of "Requirement Engineering for Cloud Computing". I have selected "Online Banking" as my case study. In this regard I have taken two tasks i.e. data storage and data process that are carried out on cloud. From this survey I will be analyzing security issues that need to be considered in development stage.

This survey is divided into two parts. First part is about data storage and second part is about data process. Kindly choose the option that describes your best answer.

Note: This information is only used for research purposes.

3. **Data Storage:**

   It is the space where customer's all data that might consist on account number, amount and transaction log history must store in the cloud.

   f. **Authentication**

      How is data protected from unauthorized access?

      ○ Through user name and password

      ○ Through only password

      ○ Through digital signatures

      ○ Through finger prints

      ○ Through pin codes

   g. **Authorization**

      Who has access to data?

      ○ Authorized persons

      ○ Employees

      ○ Technical support

      ○ All of above

      ○ Only authorized persons and employees

h. Availability

What is your service level agreement (SLA) for uptime?

- ○ 0-4 hours (during business hours) for issues classified as High priority
- ○ 0-8 hours (during business hours) for issues classified as High priority
- ○ Within 48 hours for issues classified as Medium priority
- ○ Within 2 working days for issues classified as Low priority
- ○ Within 5 working days for issues classified as Low priority

i. Maintainability

Do you back-up your data?

- ○ Daily
- ○ Once in a week
- ○ Twice in a week
- ○ Once in month
- ○ Once in a year

j. Configuration

Do you allow advertisement of third parties during usage of online banking application?

- ○ Yes
- ○ No
- ○ May be
- ○ Not at all
- ○ Don’t know

k. Scalability

Do you upgrade online banking application to meet technological changes?

- ○ Yes
- ○ No
- ○ May be
- ○ Not at all
- ○ Don’t know

4. Data Process:

It is the processing of credit transfer processes in cloud.

d. Authentication

Which customer verification system is used?

- User name and password
- Only password
- Only username
- Finger prints
- Pin codes

e. Authorization

Do you encrypt all data transmissions including server-to-server and data centers?

- Yes
- No
- May be
- Not at all
- Don’t know

f. Availability

What is your service level agreement (SLA) for uptime?

- 0-4 hours (during business hours) for issues classified as High priority
- 0-8 hours (during business hours) for issues classified as High priority
- Within 48 hours for issues classified as Medium priority
- Within 2 working days for issues classified as Low priority
- Within 5 working days for issues classified as Low priority

g. Maintainability

Which security tasks are carried out by the provider?

- No one allowed to access data without username and password
- Check on transactions
- Limit on payment transaction
- Check on more than one account
- Check on locations from where data is accessed

h. Configuration

How increase of usage or peaks handled?

- ○ Limits access
- ○ Use more resources to provide access to the data
- ○ Drop connections with third parties
- ○ Divert traffic
- ○ No policy to handle such situation

i. Scalability

Do you upgrade online banking application to meet technological changes?

- ○ Yes
- ○ No
- ○ May be
- ○ Not at all
- ○ Don't know

In your view, how much these factors contribute towards security? Rank them with the meaning of these numbers: 1= high, 2= high – medium, 3= medium, 4= medium – low and 5= low

Parts\Parameters	**Authentication**	**Authorization**	**Availability**	**Maintainability**	**Configuration**	**Scalability**
Data Storage						
Data Processing						

REFERENCES

[1] F. A. Alvi1, B. S. Choudar, N. Jaferry, and E.Pathan, "A review on cloud computing security issues & challanges", ISSN: 2278-8735.Volume 9, Issue 1, Ver. V. pp 28 – 35, IOSR Journals Feb. 2014.

[2] Janakiram MSV Cloud Computing Strategist, "Demystifying the Cloud An introduction to Cloud Computing", Version 1.0 – March 2010.

[3] H. Schrodl and S. Wind, "Requirements Engineering for Cloud Computing", Journal of Communication and Computer Vol. 8 pp. 707-715 2011.

[4] Peeyush Mathur, Nikhil Nishchal, "Cloud Computing: New challenge to the entire computer industry", 2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010).

[5] Y. Jadeja and K. Modi, "Cloud Computing – Concepts, Architecture and Challenges", International Conference on Computing, Electronics and Electrical Technologies (ICCEET) 2012.

[6] http://www.computerweekly.com/ArticlesI2009/02124/234988/googlemail-collapses.htm

[7] "Security of virtualization, cloud computing divides IT and security pros". http://www.networkworld.com/newsI2010/02221O-virtualizationc1oud-security-debate.html

[8] F. Sabahi, "Cloud Computing Security Threats and Responses", International Conference on Cloud Computing IEEE 2011.

[9] Forrester, TechRadar for infrastructure & operations professionals, Cloud Computing, Forrester (2009).

[10] H. Schrodl and S. Wind, "Requirements Engineering for Cloud Computing", Journal of Communication and Computer Vol. 8 pp. 707-715 2011.

[11] Chang, L, Ti ; Chin L; Chang, A.Y.; Chun J, C;(2010), " Information Security Issue of Enterprises Adopting the Application of Cloud Computing", IEEE 2010 Sixth International Conference on Networked Computing and Advanced Information Management (NCM), pp 645, 16-18 Aug. 2010.

[12] P. Jain, "Security Issues and their solution in Cloud Computing", International Journal of Computing and Business Research ISSN (Online) 2229-6166 2012.

[13] Diogo A. B. Fernandes, Liliana F. B. Soares, Joao V. Gomes, Mario M. Freire and Pedro R. M. Inacio, "Security issues in cloud environments: a survey", International Journal of Computer Trends and Technology, Vol. 138, pp. 113-117, 2014.

[14] O. Harfoushi, B. Alfawwaz, N. A. Ghatasheh, R. Obiedat, M. M. Abu-Faraj, H. Faris, "Data Security Issues and Challenges in Cloud Computing: A Conceptual Analysis and Review", International Journal of Communicationa and Network, Vol. 6, pp. 15-21, 2014.

[15] A. Kaur and N. Bhagat, "A Review on Cloud Computing Security Issues", International Journal of Advance Research on Computer Science, Vol. 5, No. 7, 2014.

[16] H. Schulze, "Cloud Security" 2015 Spotlight Report powered by Cloud Passage Information Security Community on LinkedIn.

[17] H. Schulze, "Cloud Security" 2016 Spotlight Report powered by Cloud Passage Information Security Community on LinkedIn.

[18] H. Schulze, "Cloud Security" 2017 Spotlight Report powered by Cloud Passage Information Security Community on LinkedIn.

[19] M. Al Morsy, J. Grundy, I. Muller, "An Analysis of the Cloud Computing Problem", Swinburne University of Technology, Australia, 2014.

[20] P. Thakur, S. Awasthi, "Infrastructure as a Service (IaaS) Security Issues in Cloud Computing", International Journal on Emerging Technologies, Volume 8, No. 2, 2017.

[21] P.R. Jaiswal, A.W. Rohankar, "Infrastructure as a Service (IaaS) Security Issues in Cloud Computing", International Journal of Computer Science and Information Technology, Vol. 3, Issue 3, 2014.

[22] T. Devi, R. Ganesan, "Platform-as-a-Service (PaaS): Model and Security Issues", Indonesian Journal of Electrical Engineering, Vol. 15, No. 1, 2015.

[23] B. Nuseibeh and S. Eaterbrook, "Requirements Engineering: A Roadmap", International Symposium on Requirements Engineering (RE-01), Toronto, Canada, 2001.

[24] P. Zave, "Classification of Research Efforts in Requirements Engineering," ACM Computing Surveys, vol. 29, no. 4, pp. 315–321, Dec. 1997.

[25] M. E. Rana, J. Dauren and S. Kumaran, “An Improved Requirement Engineering Framework for Cloud Based Application Development”, IEEE Student Conference on Research and Development, 2015.

[26] H. Mouratidis, S. Islam, C. Kalloniatis and S. Gritzalis, “A Framework to Support Selection of Cloud Providers based on Security and Privacy Requirements”, International Journal of Systems and Software, 86(9):2276-2293, 2013.

[27] R. Snijders, F. Dalpiaz, M. Hosseini, A. M. Shahri and R. Ali, “Crowd-Centric Requirements Engineering”, IEEE/ACM International Conference on Utility and Cloud Computing, 2014.

[28] M. Ficco, F. Palmieri and A. Castiglione, “Modeling Security Requirements for Cloud-based System Development”, Special issue Paper, 2014.

[29] Rak.M, Ficco M, Battista E, Casola V, Mazzocca N. Developing Secure Cloud Application. Scalabale Computing: Practice and Experience 2014; 15(1):49-62.

[30] M. E. Rana, J. Dauren and S. Kumaran, “An Improved Requirements Engineering Framework for Cloud Based Application Development”, IEEE Student Conference on Research and Development (SCOReD), 2015.

[31] I. T.Koitz and M. Glinz, “A Fuzzy Galois Lattice Approach to Requirements Elicitation for Cloud Services”, IEEE Transaction on Services Computing, 2015.

[32] A. Jaoua, F. Alvi, S. Elloumi, S. BenYahia, "Galois connection in fuzzy binary relations: applications for discovering association rules and decision making", *In Proceedings of the Intl. Conference RELMICS'2000*, no. 5, pp. 141-149, 10–14 January 2000.

[33] Daniel McNeill & Paul Freiberger, Fuzzy Logic: The Revolutionary Computer Technology that Is Changing Our World. New York: Simon & Schuster, 1994, pp. 47-48.

[34] Sandfreni, N. R. Oktadini and K. Surendro, “Requirement Engineering for Cloud Computing Using i* (iStar) Hierachy Method”, International Journal of Information Science and Applications, 2015.

[35] R. Goel, M. C. Govil and G. Singh, “Security Requirements Elicitation and Assessment Mechanism (SecREAM)”, IEEE International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2015.

[36] J. Vijayashree, Dr. P. U. Ivy and J. Jayashree, “Requirement Elicitation Framework for Cloud Applications”, International Journal of Engineering Research and General Science, Vol. 3, Issue 1, 2015.

[37] M. Ramachandran, “Software Security Requirements Management as an Emerging Cloud Computing Service”, International Journal of Information Management, Vol. 36, pp 580-590, 2016.

[38] S. A. Aljawarneh, A. Alawneh and R. Jaradat, “Cloud Security Engineering: Early Stages of SDLC”, International Journal of Future Generation Computer Science, 2016.

[39] S. Devata and A. Olmsted, “Modeling Non-Functional Requirements in Cloud Hosted Application Software Engineering”, International Conference on Cloud Computing, GRIDs, and Virtualization, 2016.

[40] M. Nosrati, “Exact Requirements Engineering for Developing Business Process Models”, IEEE International Conference on Web Research, 2017.

[41] A. Przybyłek, “A Business-Oriented Approach to Requirements Elicitation,” in Proceedings of the 9th International Conference on Evaluation of Novel Software Approaches to Software Engineering (ENASE’14), pp. 152-163, 2014.

[42] S. Faulk and R. Dorfman, “Software Requirements: A Tutorial”, Software Requirements Engineering. IEEE Computer Society press 1997.

[43] P. Mosca, Y. Zhang, Z. Xiao, Y. Wang, “Cloud Security: Services, Risks, and a Case Study on Amazon Cloud Services”, International Journal of Communications, Network and System Sciences, Vol. No. 7, pp. 529-535, 2014.

[44] M. Ahmed and M. A. Hossain, “Cloud Computing and Security Issues in the Cloud”, International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014.

[45] M. Ali, S. U. Khan and A. V. Vasilakos, “Security in Cloud Computing: Opportunities and Challenges”, International Journal of information Sciences, pp. 357-383, 2015.

[46] M. R. R. Ramesh and Dr. Ch. S. Reddy, “A Survey on Security Requirement Elicitation Methods: Classification, Merits and Demerits”, International Journal of Applied Engineering Research ISSN 0973-4562 Vol. 11, No. 1, pp. 64-70, 2016.

[47] S. Harbajanka and Dr. P Saxena, “Survey Paper on Trust Management and Security Issues in Cloud Computing”, IEEE Symposium on Colossal Data Analysis and Networking (CDAN), 2016.

[48] Y. Z. An, Z. F. Zaaba and N. F. Samsudin, “Reviews on Security Issues and Challenges in Cloud Computing”, International Engineering Research and Innovation Symposium (IRIS), 2016.

[49] Zalazar A.S., Ballejos L., Rodriguez S. (2017) Analyzing Requirements Engineering for Cloud Computing. In: Ramachandran M., Mahmood Z. (eds) Requirements Engineering for Service and Cloud Computing. Springer, Cham.

[50] W. A. Khan, L. Wisniewski, D. Lang and J. Jasperneite, “Analysis of the Requirements for Offering Industrie 4.0 Applications as a Cloud Service”, International Symposium on Industrial Electronics, 2017.

[51] N. Ahmad, “Cloud Computing: Technology, Security Issues and Solutions”, International Conference on Anti-Cyber Crimes, 2017.

[52] M. Nosrati, “Exact Requirements Engineering for Developing Business Process Models”, IEEE International Conference on Web Research, 2017.

[53] B. A. Kitchenham, “Guidelines for performing Systematic Literature Reviews in Software Engineering”, Version 2.3, EBSE Technical Report, Software Engineering Group School of Computer Science and Mathematics Keele University, EBSE-2007-01.

[54] Eric Yu, Tutorial presented at the One-Day Symposium “Modelling Your System Goals –The i* Approach” London, UK -April 20, 2005.

[55] K. Surendro and C. Martini, “Hierarchical i* Modeling in Requirement Engineering”, International Journal of TELKOMNIKA (Telecommunication Computing Electronics and Control), Vol.14, No.2, June 2016.

[56] Yu E.S. (2009) Social Modeling and *i**. In: Borgida A.T., Chaudhri V.K., Giorgini P., Yu E.S. (eds) Conceptual Modeling: Foundations and Applications. Lecture Notes in Computer Science, vol 5600. Springer, Berlin, Heidelberg

[57] B. Forouzan, Data Communication and Networking.: Tata McGraw Hill, 2010.