CLOUD COMPUTING SECURITY ISSUES AND SELECTION OF DEPLOYMENT MODEL AND SERVICE MODEL ACCORDING TO SECURITY REQUIREMENTS

A MASTER'S THESIS

IN

SOFTWARE ENGINEERING

ATILIM UNIVERSITY

by

ARDA SEZEN

JANUARY 2015

CLOUD COMPUTING SECURITY ISSUES AND SELECTION OF DEPLOYMENT MODEL AND SERVICE MODEL ACCORDING TO SECURITY REQUIREMENTS

A THESIS SUBMITTED TO

THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

OF

ATILIM UNIVERSITY

BY

ARDA SEZEN

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE OF PHILOSOPHY

IN

THE DEPARTMENT OF SOFTWARE ENGINEERING

JANUARY 2015

Approval of the Graduate School of Natural and Applied Sciences, Atılım University.

_____

Prof. Dr. İbrahim Akman

Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

_____

Prof. Dr. Ali Yazıcı

Head of Department

This is to certify that we have read the thesis Cloud Computing Security Issues and Selection of Deployment Model and Service Model According to Security Requirements submitted by Arda Sezen and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

_____	_____
Asst. Prof. Dr. Atila Bostan	Prof. Dr. Ali Yazıcı
Co-Supervisor	Supervisor

Examining Committee Members

Prof. Dr. Ali Yazıcı	_____
Assoc. Prof. Dr. Murat Koyuncu	_____
Assoc. Prof. Dr. Osman Abul	_____
Asst. Prof. Dr. Çiğdem Turhan	_____
Asst. Prof. Dr. Atila Bostan	_____

Date: 27.01.2015

I declare and guarantee that all data, knowledge and information in this document has been obtained, processed and presented in accordance with academic rules and ethical conduct. Based on these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last name: Arda Sezen

Signature:

ABSTRACT

CLOUD COMPUTING SECURITY ISSUES AND SELECTION OF DEPLOYMENT MODEL AND SERVICE MODEL ACCORDING TO SECURITY REQUIREMENTS

Sezen, Arda

M.S., Software Engineering Department

Supervisor: Prof. Dr. Ali Yazıcı

Co-Supervisor: Asst. Prof. Dr. Atila Bostan

January 2015, 89 pages

This thesis reviews the necessity of X.800 Recommendation service categories for different cloud service models and cloud deployment models together with some security solution approaches in cloud computing.

The thesis evaluates the solution approaches to show that technical and non-technical approaches need to be handled together to produce comprehensive solutions. Six technical solution approach have been included to evaluate the fulfilment of X.800 Recommendation service categories.

Eventually, twelve hypotheses have been formulated, tested, and accepted based on the survey data to understand the necessity of X.800 Recommendation service categories for different cloud service models and cloud deployment models.

Keywords: Cloud security, X.800, Information privacy, Cloud standardization, Trust in cloud.

ÖZ

BULUT BİLİŞİM GÜVENLİK SORUNLARI VE GÜVENLİK GEREKSİNİMLERİNE GÖRE DAĞITMA MODELİ İLE HİZMET MODELİ SEÇİMİ

Sezen, Arda

Yüksek Lisans, Yazılım Mühendisliği Bölümü

Tez Yöneticisi: Prof. Dr. Ali Yazıcı

Ortak Tez Yöneticisi: Yrd. Doç. Dr. Atila Bostan

Ocak 2015, 89 sayfa

Bu tez, X.800 Tavsiyesi içinde bulunan hizmet kategorilerinin gerekliliğini, farklı bulut hizmet modelleri ve bulut dağıtım modelleri için, bazı güvenlik çözümü yaklaşımlarıyla birlikte incelemektedir.

Tezde sunulan çözüm önerileri, teknik ve teknik olmayan yaklaşımların kapsamlı çözümler üretmek için birlikte ele alınması gerektiğini göstermektedir. Altı teknik çözüm yaklaşımı, X.800 Tavsiyesi içinde bulunan hizmet kategorilerinin yerine getirilmesini değerlendirmek üzere bu çalışmaya dâhil edilmiştir.

Sonunda, X.800 Tavsiyesi içinde bulunan hizmet kategorilerinin gerekliliğini, farklı bulut hizmet modelleri ve bulut dağıtım modelleri için anlamak ve anlamlı farklılaşmaları ortaya koymak adına on iki hipotez, anket verilerine dayanarak, formüle, test ve kabul edilmiştir.

Anahtar Kelimeler: Bulut güvenliği, X.800, Bilgi gizliliği, Bulut standardizasyonu, Bulut'da güven.

To My Fiancée Seba, My Mother, and My Brother

ACKNOWLEDGMENTS

I express sincere appreciation to my supervisor Prof. Dr. Ali Yazıcı for his guidance and insight throughout the research. Thanks also go to my co-supervisor Asst. Prof. Dr. Atila Bostan. The technical assistance of Dr. Salih Akyürek and assistance of Yusuf Evren Aykaç is gratefully acknowledged. To my fiancée, Seba, I offer sincere thanks for her continuous support and patience during this period.

TABLE OF CONTENTS

LIST OF TABLES

TABLE

LIST OF FIGURES

FIGURES

LIST OF ABBREVIATIONS

ABI	-	Allied Business Intelligence
AES	-	Advanced Encryption Standard
ANOVA	-	Analysis of Variance
API	-	Application Programming Interface
BLS	-	Boneh-Lynn-Shacham
CA	-	Certification Authority
CAGR	-	Compound Annual Growth Rate
CIA	-	Confidentiality, Integrity and Availability
CPU	-	Central Processing Unit
CSA	-	Cloud Security Alliance
CTA	-	Cloud Trust Authority
Dec	-	Decryption
DS	-	Distributed Server
EC	-	European Community
EIU	-	Economist Intelligence Unit
Enc	-	Encryption
FE	-	File Encryption
FHE	-	Fully Homomorphic Encryption
GDP	-	Gross Domestic Product
HDFS	-	Hadoop Distributed File System

IaaS	-	Infrastructure as a Service
ICT	-	Information & Communications Technology
IDC	-	International Data Corporation
IEC	-	International Electrotechnical Commission
IETF	-	Internet Engineering Task Force
INFOSEC	-	The U.S. National Information Systems Security
I/O	-	Input/Output
IS	-	Information System
ISO	-	International Organization for Standardization
IT	-	Information Technology
ITIL	-	Information Technology Infrastructure Library
ITU	-	International Telecommunication Union
MD5	-	Message Digest algorithm 5
MHT	-	Markle Hash Tree
MPNR	-	Multi-party Nonrepudiation Protocol
NRO	-	Non-Repudiation of Origin
NRR	-	Non-Repudiation of Receipt
OVF	-	Open Virtualization Format
P2P	-	Peer to Peer
PaaS	-	Platform as a Service
PDP	-	Provable Data Possession
PKI	-	Public Key Infrastructure
PoR	-	Proof of Retrievability
QoS	-	Quality of Service

R&D	-	Research and Development
RSA	-	Ron Rivest, Adi Shamir and Leonard Adleman
SA	-	Security Architecture
SaaS	-	Software as a Service
SACS	-	Security Access Control Service
SAP	-	SSL Authentication Protocol
SHA	-	Secure Hash Algorithm
SLA	-	Service Level Agreement
SME	-	Small and Medium-sized Enterprises
SP	-	Service Provider
SPSS	-	Statistical Package for the Social Sciences
SSF	-	Store Small Files
SSL	-	Secure Sockets Layer
STAR	-	Security, Trust & Assurance Registry
SW	-	Software
SWOT	-	Strengths, Weaknesses, Opportunities, and Threats
TC	-	Trusted Computing
TCG	-	Trusted Computing Group
TCP	-	Trusted Computing Platform
TDZ	-	Technology Development Zone
TPA	-	Third Party Auditing
TurkStat	-	Turkish Statistical Institute
TÜBİSAD	-	Turkish Informatics Industry Association
TV	-	Television

UA	-	User Authentication
VPN	-	Virtual Private Network
YASED	-	International Investors Association

CHAPTER 1

INTRODUCTION

1.1. Thesis Scope

Generation of data has increased in this information era, as well as in storing, distributing and processing needs. These needs can be satisfied by the paradigm known as cloud computing. Another increasing and critical requirement for information systems (IS) is security. In this work, we investigated technical and non-technical solutions of implementing and using a secure cloud computing environment by examining the literature reviews mostly published after 2010. Also survey approach is adopted to get empirical data about the security requirements of different cloud computing service delivery models and cloud computing types for further analysis and comparison.

The aim of the work and the research questions are described in the following parts of this thesis and structure of the thesis is analyzed. Methodologies that are used in the thesis will be given in the relevant section. At the end, the data which we obtain during this study will be analyzed in detail.

1.2. Research Objectives and Statement of the Problem

In information technology (IT), protection of data has utmost importance among other things. By the contribution of portable devices, internet became sine qua non in our lives. Data we share, data we hold is judged as assets which can easily be turned into material gains or material injury.

When pioneer companies discover that they do not need full potential of their information technology resources all the time, they start to think on a model which reduces daily expenses at daily IT operations and also gain profit from using it.

Combination of existing technologies but presenting them in a different way lies beneath cloud computing therefore this trendy term inherits existing gaps and also creates its own security problems [1].

This study proposes a cloud computing security requirements evaluation to understand which ones are considered as a must and which ones are optional. To our best of knowledge there are not many existing studies that have been specifically focusing on various cloud computing service delivery models and cloud computing types.

The objectives of the study are:

- Review the security challenges associated with adopting cloud computing
- Explore technical and non-technical solutions of implementing more secure cloud computing
- Analyze the strength of information security requirements for different cloud computing types and service delivery models.

By aiming the objectives above, the study will address the following questions which are needed to be answered for better understanding of the security problem in the presence of adopting cloud computing. According to IDC survey, security concerns ratio of the cloud (87.5%) took the first place [2]. This data can be supported by using Google trends which provides interest over time graph for a search term. To demonstrate, two terms are searched by Google trends. These terms are cloud computing and cloud computing security. The results based on these two terms show, while there is a decrement for the term cloud computing after 2011, the term cloud computing security protects its interest from that year until now. Therefore, there is a necessity for more research in the security area of cloud computing at least according to current trends and survey results.

The study will address the following questions:

- What are the possible technical solutions and non-technical aspects to implement or use cloud computing infrastructure by addressing the security issues?
- Which security services should we use to form a more secure cloud computing platform?

- What type of problems do we face considering the current regulations associated with cloud computing?

To accomplish the adaptation of cloud computing smoothly researchers realized that focusing on different aspects of cloud computing together with technical side is crucial. Although technical solutions provide some easing on the subject, "The Future of Cloud Computing 3rd Annual Survey 2013" [3] is a proof to such easing which shows that 18% easing on security concerns stated between 2012 and 2013, but clearly far to be a complete solution by itself. Therefore, we aim at a better understanding about the security requirements and trust issue in this study with the hope of contribution to the related field.

1.3. Thesis Outline

This thesis has been organized as follows: In Chapter 1 the source of the problem and motivation factors for this study are mentioned. The scope of the thesis is determined by these research objectives. Detailed outline is described by the structure of the thesis that is prepared within the specified scope.

Chapter 2 states background information and literature survey that includes technical and non-technical solution approaches together with general information about cloud computing paradigm and security concept. Most of the terms and definitions used in this document are in this section. In addition, existing research and more related work will be analyzed.

Chapter 3 provides statistical information about status of ICT sector in Turkey and draws an economical perspective which is necessary to understand cloud computing, also known as an economical model as well as technological model.

Chapter 4 consists of methodologies to conduct this research and limitations that we face during the thesis process. Details of the survey that prepared for this study to obtain required data sample which will be used in the next section is given too.

Chapter 5 is dedicated to evaluate the survey results and producing hypotheses in respect to data sample. Findings will be discussed throughout this chapter with relevant graphics.

In Chapter 6, we summarize the thesis to conclude and a discussion is held for further research opportunities.

CHAPTER 2

BACKGROUND INFORMATION AND LITERATURE SURVEY

2.1. Information Security Concept

The U.S. National Information Systems Security (INFOSEC) Glossary defines "information systems security" as the protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service attacks, including those measures necessary to detect, document, and counter such threats [4].

Also, there are other definitions for information security such as the definition in US Code Title 44, Chapter 35, Subchapter III that presents an appropriate delineation to provide integrity, which means guarding against unauthorized modification of data; confidentiality, which means guarding against unauthorized disclosure of data; and availability; which means reliable access to data in time is guaranteed. Furthermore, these three (confidentiality, integrity, and availability) are known as CIA triangle of security in the literature.

Today, processes and operations are redefined by the help of information security. Systems hold many valuable information about customers or blueprints about new products. To understand the gravity of this concept, some daily life examples caused by security breach or improper security settings/ configurations/ usage are given below:

- A job portal known as Monster was hacked and confidential details of more than 1.3 million people were stolen in 2007 [5]. As a consequence, all the people registered in Monster at that time faced the risk of being masqueraded.

- In FlexiScale which is a cloud service provider, an engineer accidentally deleted one of the main storage volumes. Processing and networking services were unavailable until restoration of the lost data to a brand new disk structure was completed [6].
- An indexing system at Zoho resulted in one user being able to read other users' documents in an unauthorized way [7].
- A tax collector improperly accessed private tax files of hundreds of individuals [8]. Cases such as this one, clearly demonstrates the need for access control policies.

As shown from the examples above, data protection is vital and protecting these information assets includes integrity, availability and confidentiality of data and services which are commonly mentioned and accepted as the CIA triad. Usage of standardization is important in the area of security too because of the quality provided by these standards, interoperability, effectiveness of products and services can only be guaranteed with the help of standards. There is not a single standard which covers all aspects of security, among them is X.800 Recommendation [9] (ITU-T X.800 Recommendation). Security services are divided into five categories in X.800 Recommendation which are authentication (provides confirmation by using information such as user name-password, digital certificate), access control (protection against unauthorized use of resources), data confidentiality (protection against unauthorized disclosure of data), data integrity (protection against unauthorized modification of data) and nonrepudiation (protection against denial of one of the entities involved in a communication) [10]. Publisher of this recommendation is a highly reputable organization known as International Telecommunication Union (ITU) which currently has a membership of 193 countries and over 700 private-sector entities and academic institutions. In this study, we perform our security requirements research based on X.800 Recommendation.

2.2. Literature Survey

2.2.1. Some Definitions

There are many definitions for cloud computing in literature. For instance:

Definition 1: “The cloud itself is a set of hardware, networks, storage, services, and interfaces that enable the delivery of computing as a service” [11].

Definition 2: “Applications and services that run on a distributed network using virtualized resources and accessed by common Internet protocols and networking standards” [12].

Definition 3: “A large pool of easily usable and accessible virtualized resources (such as hardware, development platforms and/or services). These resources can be dynamically reconfigured to adjust to a variable load (scale), allowing also for an optimum resource utilization. This pool of re-sources is typically exploited by a pay-per-use model in which guarantees are offered by the Infrastructure Provider by means of customized SLAs” [13].

Basically, presenting resources as a service manner and obtaining profit from it lies behind these definitions. Therefore, cloud computing is a business paradigm as well as technological paradigm.

Cloud computing derives benefit from virtualization. Because, virtualization prevents complexity of hardware and software presentation by abstraction (allows to create an abstraction layer) such as storage virtualization which does this between the server side applications and the storage they use. At the bottom of the cloud computing architecture physical resources take place. Cloud computing uses the power of virtualization technologies in the virtual resource layer to virtualize systems which are constructed in the physical resource layer by pooling and sharing resources. In other words, cloud computing gathers physical resources and presents them as virtual resources.

Cloud computing architecture is needed to be examined in two different layers; one is the layer of resources and the other one is the layer of services. Resource layer is divided into two which are the physical resource layer and virtual resource layer. Three different service models in the architecture are as follows:

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)

In Figure 2.1 the Cloud Computing Architecture is given.

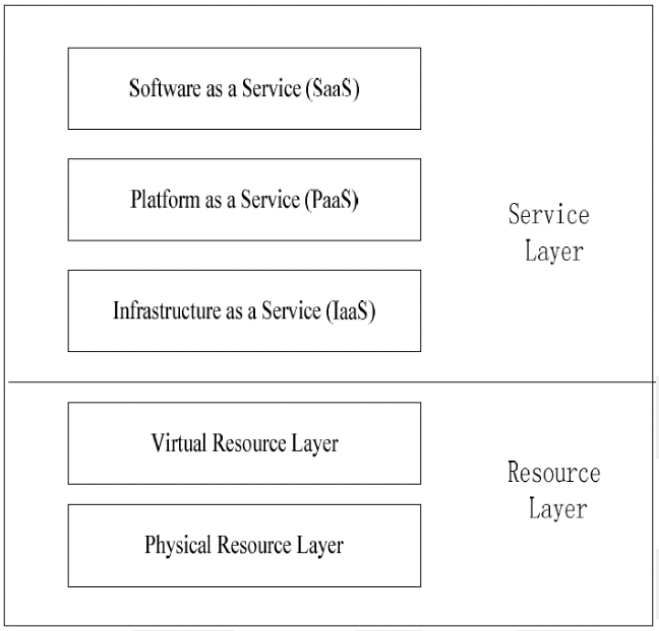


Figure 2.1: Cloud computing architecture [14]

Some details of these cloud services are given below:

IaaS: Infrastructure as a Service is a provision model based on the need for equipment outsourcing to support daily operations. This service model provides virtual machines, virtual storage, virtual infrastructure and other hardware assets as resources. In this model, service provider is responsible for managing all the infrastructure. On the other hand, some responsibilities exist for the clients which are operating system, applications and user interaction with the system.

PaaS: Platform as a Service is a provision model based on the need for computing platform and solution stack. Provision of virtual machines, operating systems, development frameworks describes the goal of PaaS. Service provider responsibilities are managing cloud infrastructure, the operating system and enabling software. Clients responsibilities can be listed as application deployment or application use supported by PaaS, installing and managing the application.

SaaS: Software as a Service is a software licensing and delivery model. This service model is a complete operating environment with applications, management and user interface. In SaaS, service provider is responsible for everything from the application down to the infrastructure. Clients are responsible for entering and managing its data and user interaction in this service model.

Clouds are not only classified by considering service models but also considering deployment types too. There are three deployment models for cloud computing which are:

- Public cloud: These type of clouds are owned by an organization. Point of interest is selling cloud services.
- Private cloud: These type of clouds are operated for the exclusive use of an organization. Either managed by that organization or a third party.
- Hybrid cloud: These type of clouds are combination of both public and private.

Due to the multiuser and resource sharing structure, there are various security requirements for cloud computing. The following proposed models are some technical solution approaches for cloud computing security that we have seen in literature. There are various examples similar or completely different than these approaches but for a better understanding of X.800 service categories compliance and to examine these proposed models in detail, we pick six studies randomly.

2.2.2. Security Access Control Service (SACS)

In their study Jing, and Jian-jun [14] proposed a technical solution approach. Customized services are the backbone of cloud computing's service delivery nature. All services are supported by the resource layer and upper layer services require some security measures to ensure that only the right person is able to use specific services safely by having access to this environment [1] [14].

Combining Access Authorization, Security Application Programming Interface (Security API), and cloud connection security with the existing architecture of cloud computing, underlies at the bottom of the examined approach which referred as SACS model [1]. Shown in Figure 2.2 [14].

According to this model [1] [14],

1. In an effective period of time, certification need arises for secure authentication as the first step of SACS model.
2. During the second step, the user's task becomes a trigger at the beginning. While the application checks out whether the user's certificate is expired or still valid, a mutual authentication takes place between the user agent and the specific application.
3. A list of service resource is created by the cloud application. Figure 2.2 shows a Security API (in this model achieved with SSL) that a user agent has to pass through for the connection of specific services.
4. While resources are provided by the resource layer, Secure Sockets Layer (SSL) method is used together with Virtual Private Network (VPN) method to establish cloud connection security ensuring that resources are provided safely.

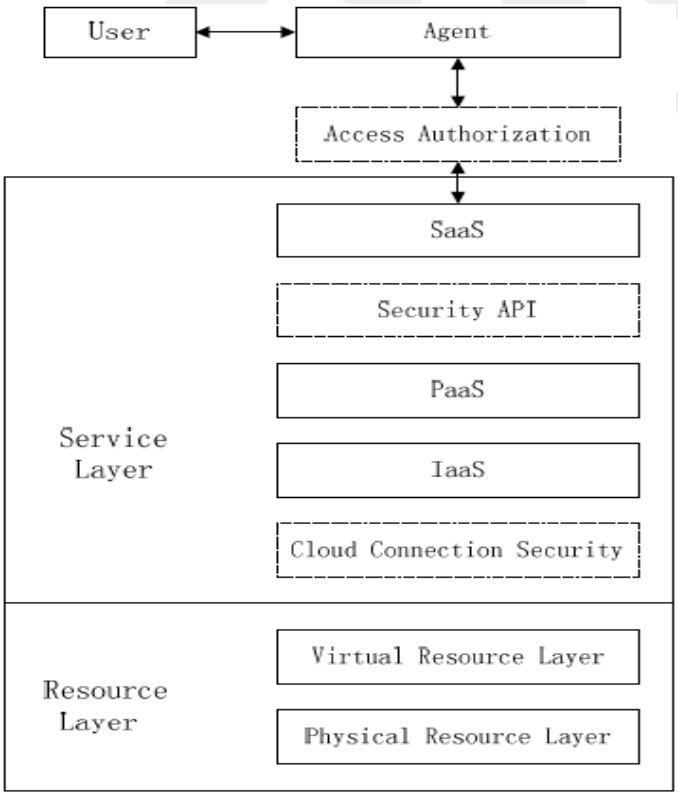


Figure 2.2: A security model of cloud computing [14]

As an advantage, this model provides authentication and access control via certification and a list of derivable service resources. Although the model provides communication confidentiality, this alone is not enough to accept as a competent proposal in terms of data confidentiality.

2.2.3. Fully Homomorphic Encryption

Homomorphic encryption is a form of encryption and is defined as following [15].

"Allows specific types of computations to be carried out on ciphertext and generate an encrypted result which, when decrypted, matches the result of operations performed on the plaintext. This is a desirable feature in modern communication system architectures. Homomorphic encryption would allow the chaining together of different services without exposing the data to each of those services, for example a chain of different services from different companies could 1) calculate the tax 2) the currency exchange rate 3) shipping, on a transaction without exposing the unencrypted data to each of those services. Homomorphic encryption schemes are malleable by design. The homomorphic property of various cryptosystems can be used to create secure voting systems, collision-resistant hash functions, and private information retrieval schemes and enable widespread use of cloud computing by ensuring the confidentiality of processed data."

Fully homomorphic encryption is an encryption technique and can be done on ciphertexts. Satisfying data confidentiality is accepted as one of the major problems not only for cloud computing but also other information systems as well. Cloud computing provides computing power to its beneficiaries; files can be encrypted and stored in the cloud but if one can use the benefits of the cloud like computing power, the cloud service provider has to hold the keys [1].

Main idea lies behind fully homomorphic encryption technique is mirroring. Certain operations done on the ciphertexts mirrored to the corresponding operations on the plaintexts such as plain RSA, condition of simple homomorphic encryption is satisfied where there is just one operation on the plaintext that has a corresponding operation on the ciphertext [1] [16]. The following example is taken from Ryan (2013) [16].

Suppose plaintext z1 is encrypted with public key pk, the result is c1 and ciphertext c2 is the encryption under the same key of plaintext z2; that is

$$c1 = enc(pk, z1) \text{ and } c2 = enc(pk, z2)$$

Then multiplication result of the ciphertexts is identical to the multiplication result of the plaintexts. Suppose dk is the decryption key which corresponds to pk; that is

$$z1 \times z2 = dec(dk, c1 \times c2)$$

As an example, plain RSA is not suitable in practice because of insecurity. On the other hand, Pallier encryption and Elgamal encryption can be given for secure encryption techniques that have the homomorphic property. This seems a complete solution in theory but there are some drawbacks [1] [16]:

- The result of operations on ciphertexts is also an encryption of the actual result. Therefore, the cloud cannot take any action based on the result or the information itself such as sort, search, and etc.
- The other one is inefficiency, because of key sizes and the encryption.
- The proposed model offers transaction without risking data confidentiality but provides nothing in other security service categories of X.800 Recommendation.
- Also, the important problem here is the usage of the same public key to encrypt the data. Sharing information becomes impossible because of this problem.

2.2.4. Trusted Computing Platform

Standard Web services tools and software are the fundamental part of today's security model of cloud computing in terms of transportation and manipulation of security messages and secured messages. However, this structure has some disadvantages that it has hardware shortage, and it does not have enough secure certificate creation and protection or performance of cryptographic computation process, for example. Integrating data security into the core operations plays the main role in Trusted Computing[1] (TC), rather using add-on applications for implementation [1] [17].

[1] Trusted Computing is a technology developed by Trusted Computing Group (TCG). TCG acts as a successor to the Trusted Computing Platform Alliance which is an initiative started by AMD, Cisco, Hewlett-Packard, IBM, Intel, Microsoft and Wave Systems Corp to implement Trusted Computing.

In their study Shen, and Tong [17] proposed Trusted Computing Platform (TCP) for authenticated boot and encryption. Mechanism is shown in Figure 2.3 [1].

To quote Sezen, Bostan and et al. [1]:

1. At first, the system requires hardware as an audit logger for the boot process.
2. After that, a service called authenticated boot service monitors the booted operating system to provide drastic information for applications.

Basically, Trusted Computing Platform uses combination of hardware/software duo. Therefore, manufacturers add some new hardware to each computer to support TC functions.

A special TC operating system mediates between the hardware and any TC-enabled application. In another way, certification of a known operating system is done by TC and then that operating system can certify the configuration of the application.

Here are some benefits to be gained by adopting this system:

- A better security token by using hardware for random key generation.
- As a benefit, relieves some computation power from the CPU.
- Traceability improvement as a result of user's personal key usage based on hardware integration.
- Necessity for additional hardware cost is a disadvantage to TC.
- There are some security service categories that cannot be achieved by this proposed approach in its current state such as access control and nonrepudiation.

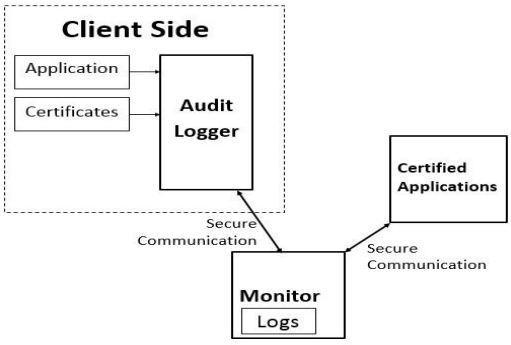


Figure 2.3: A general view of the system [1]

2.2.5. A New Fair Multi-Party Non-Repudiation Protocol

According to Feng, et al. [18], proposing a new fair multi-party non repudiation (MPNR) protocol, Non-Repudiation of Receipt (NRR) or Non-Repudiation of Origin (NRO) is data transmission information in each message. For the encryption part of this approach, block cipher is applied while each block is encrypted with a different key. With this way, the user has keys only to access to authorized ciphertext blocks [1] [18]. Rounds are shown in Figure 2.4 [18]. Owner is the person who owns the file with all its rights such as reading, writing, and modifying. Provider is the entity or person who provides cloud services such as storage. Users are natural and legal persons who download the files from the provider.

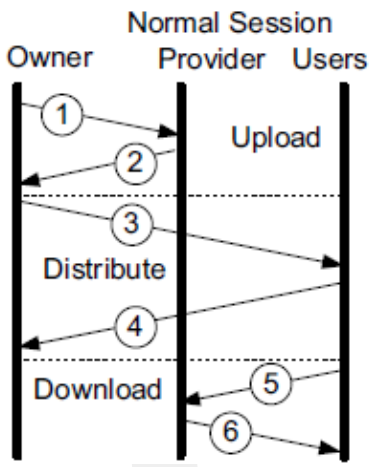


Figure 2.4: Normal Session Rounds [18]

To quote Sezen, et al. [1] the working principle behind the rounds is as follows:

1. Owner uploads data to storage with NRO_{OP} message, where the message direction is from owner to service provider (OP).
2. SP checks the message and identifies the owner. If it is valid which means the data is uploaded by the owner himself or herself, SP responds with NRR_{PO} message. Otherwise, it responds with an error message. Validity condition here is that the uploaded data owner and the owner in the NRO_{OP} message have to be the same person.

3. On receiving the NRR_{PO} message, the owner sends both NRO_{OP} message and NRR_{PO} message to user groups by group encryption with a NRO_{OU} message, where all the messages direction is from owner to user.
4. If the message is valid which means all messages are received on the same transfer, users respond with NRR_{UO} message. If not, users send back an error message.
5. Any user can send download request to SP with NRR_{UP} message.
6. If the message is valid which means the SP can able to recognize the user. Also, the recognized user and the user in the NRR_{UP} message have to be same for validity. After that, SP responds with NRR_{PU} message and data. Otherwise, it responds with an error message.

2.2.6. Storage Security in Cloud Computing

In their study Rajathi, and Saravanan [19] revealed advantages and drawbacks of several existing cloud computing storage frameworks and techniques.

In their study the following techniques are given as storage techniques in cloud computing:

1. Implicit Storage Security to Data in Online: It is based on data partitioning. In the scheme, partitioned data is saved on randomly chosen cloud servers for storing, and these data pieces can only be reached by one who has specific knowledge such as passwords and storage locations of partitioned pieces for retrieval [19] [20].
2. Identity-Based Authentication: Signature and encryption scheme is proposed as an alternative to SSL Authentication Protocol (SAP) for cloud communication security [19] [21].
3. Public Auditing with Complete Data Dynamics Support: The existent proofreading scheme such as PDP or PoR is improved by spoofing the basic Markle Hash Tree (MHT) to accomplish dynamic data support. This technique targets verification of data integrity at unreliable servers [19] [22].
4. Efficient Third Party Auditing (TPA): Usage of bilinear aggregate signature technique is the backbone of batch auditing. For error correction Reed-Solomon technique is used. This scheme tries to achieve multiple batch

auditing to perform multiple auditing tasks for different users at the same time [19] [23].

5. Way of Dynamically Storing Data in Cloud: It uses a data reading algorithm with a new protocol system to help the clients to check the data security with multi server data comparison and overall data calculation in each update [19] [24].
6. Effective and Secure Storage Protocol: Behind the curtain, this protocol is constructed by using Elliptic curve cryptography and Sobol Sequence to confirm the data integrity arbitrarily [19] [25].
7. Storage Security of Data: This technique tries to establish a secure cross platform by using SHA Hash algorithm for encryption, GZIP algorithm for compression and SFSPL algorithm for splitting files [19] [26].
8. Secure and Dependable Storage Services: By using Homomorphic token with Reed-Solomon erasure correcting code technique which ensures the correctness and also identifying misconducting servers, this mechanism allows users to audit the cloud data storage [19] [27].
9. Optimal Cloud Storage Systems: Focuses on storage service optimality by adopting a taxonomic approach. According to the proposed scheme, contribution of storage system definition, storage optimality, ontology for storage service and controller architecture for storage are the main requirements [19] [28].
10. Process of access and Store Small Files with Storage: Instead of adopting database storage this technique prefers distributed file system to store the data. Researchers gave Hadoop distributed file system (HDFS) [19] [29] as an example which is used by Google, too. HDFS is preferable for cloud because of the functioning on clusters property.
11. File Storage Security Maintenance: Two types of servers exist in this technique which are master and slave. Master server holds the clients file in the form of tokens. Slave servers hold the chunked files for file recovery. Client's requests are handled by the master server. The aim for this technique is to achieve correctness insurance and data availability by using Token generation algorithm with homomorphic token and merging algorithm [19] [30].

According to Rajathi, and Saravanan advantages and restrictions of storage schemes are shown in Table 2.1 [19].

Table 2.1 Advantages and Restrictions of Storage Schemes

Storage Scheme	Advantages	Restrictions
1. Implicit Storage Security to Online data	Partitioned data pieces cannot bring out any user information.	In case user forgot where the data stored, it will become difficult for users.
2. Identity-Based Authentication	Weightless and more expeditious.	Only certificate communication is taken into account.
3. Public Auditing with Complete Data Dynamics support	Basic Markle Hash Tree (MHT) is manipulated for block tag authentication.	Computation cost of BLS scheme is prominent.
4. Efficient Third Party Auditing (TPA)	Auditor performs auditing jobs for different users at the same.	Unable to support both public verification and dynamic data correctness.
5. Way of Dynamically Storing Data in Cloud	Integrity can be verified before and after data insertion.	TPA is not considered for integrity checking process.
6. Effective and Secure Storage Protocol	Block level data dynamic operations are also used to maintain the same security assurance.	Elliptic Curve Cryptography scheme is only suitable for devices with restricted low power.
7. Storage Security of Data	Provided data backups for data recovery. Includes essential security services such as authentication, encryption and decryption and compression.	Data backups are available at multiple servers. So there is a chance for servers to behave unreliably.
8. Secure and Dependable Storage Services	Guaranteed the correctness insurance and also identified immoral server behavior.	Gross overhead approximately stays equal with other.
9. Optimal Cloud Storage Systems	Proposed generic architecture served as blueprint for optimal storage controller.	Need to integrate with frontends for future research.
10. Process of access and Store Small Files with Storage	Improves the access ability of small files. Cut-off point is measured to improve I/O performance.	Formula for cut-off point not available.

Table 2.1 (cont.)

11. File Storage Security Maintenance	File chunking operation is carried out to provide data backups in case of server failure.	Data chunks are stored in slave server will lead to an opportunity of corrupting data by servers.

When we prepare Models versus X.800 Table (Table 2.2) we select number 10 storage scheme (Process of access and Store Small Files with Storage) because of distributed storage architecture and cluster usage. Its importance not only comes from storage but also from a popular term big data which goes hand-in-hand with cloud computing paradigm.

One of the prerequisite conditions of being an information society is to process large sets of data which are consumed in milliseconds. Capturing, storing, processing and indexing these large data sets are changing the way of traditional database management systems approach. When thinking that the main aim of engineering is to improve the quality of life by making creations better and stronger, developing alternative solutions is an infinite process. Cloud computing and distributed file systems were born somewhere inside this process.

2.2.7. User Authentication, File Encryption and Distributed Server Based Security Architecture

Nafi, et al. [31], proposed a cost effective security architecture for cloud computing by using high ranked security algorithms for providing secured communication process instead of using secured channel for communication. For file encryption, researchers prefer to adopt AES algorithm in which keys are generated randomly by the system. Distributive server concept lies at the center of this model. This model is also suggested by the researchers for secured communication between the users and the servers because of the RSA algorithm.

Connection to data establish via the main server. Only the main server has relation with other storage systems which can be servers or storage devices. Therefore all users need to pass through a secured channel which is connected to the main server. The users' request for a file is responded from the cloud service provider by encrypting the

file via RSA encryption algorithm using the user's public key. After receiving an encrypted file, the user's browser will decrypt it with RSA algorithm using the user's private key [31].

From this point everything is appropriate about this scheme but there is a sentence in the article that raises questioning to the usefulness of the proposed approach which is "Similarly when the system receives an encrypted file from the user it will immediately decrypt it using its private key. As a result, the communication becomes secured between the user and the system" [31]. According to the literature, the communication is safe between the user and the system but one should ask, what is the point of encrypting the file with your private key if the system already knows your private key? This means anyone inside the system or intruding into the system can decrypt your encrypted file.

Authentication procedure of this approach is wearisome. Whenever a user logs in in the system, the system randomly generates a new password for the next login and sends it to the users who is authorized by mail account. By this way researchers believe in doing validity check of the user. So what happens if the user cannot reach his or her mail account at that moment? The proposed approach clearly states that only the passwords retrieved from the authorized mail accounts are valid for login process. The system has a gap in this point, at least one alternative approach for the login process is needed.

Newly generated password is restored in the system after MD5 hashing and we are faced with another problem. As authors mentioned MD5 hashing is irreversible and it will be a challenge for an unauthorized or unknown party to get password information but what is the point of it if you already use one time password in your system? Also there is another gap in here; if the system stores user password in MD5 form, how will the system understand user password when the user tries to login? There is no conversion system in the login process that the system will check with the converted version of the password.

It is pointless to give further details about this article because unless the researchers do not fix the gaps that we mentioned so far, the proposed architecture does not work. Still, it is helpful to examine such an approach at least to see that not all the accepted

and published papers are hundred percent true and to behave a skeptical paradigm for what is generally accepted in the literature as it is.

In the evaluation part of technical solution approaches according to X.800, we include "User Authentication, File Encryption and Distributed Server Based Security Architecture" in the table (Table 2.2) as an examined approach but we do not make any evaluation for this one because of those gaps and logic errors.

2.2.8. Evaluation of Technical Approaches with X.800

In Recommendation X.800 there are five main service categories that has to be taken into consideration for open system interconnections, these are:

- Authentication: In this category, when technical solution approaches given in this chapter are examined, management privilege of the authentication database were kept in mind with many other issues that researchers mentioned in their studies.
- Access Control: Policy oriented access control was searched among technical solution approaches.
- Data Confidentiality: In this one, storage encryption and communication encryption are two parameters prior to confirm data confidentiality but only storage encryption was chosen as an evaluation criteria.
- Data integrity: From examined researches, we tried to understand data changes only in response to authorized transactions.
- Nonrepudiation: This category is checked whether a nonrepudiation protocol is offered for that approach or not.

The revealed security service categories from technical solution proposals are shown in Table 2.2 [1].

In this section, various technical approaches about cloud computing security from assorted research have been associated with X.800 service categories. Several research suggest that technical measures should be enough to maintain the cloud security. On the other hand, Table 2.2 shows that none of the existing technical proposals are able to fulfill all service categories. Even if all properties of X.800 are complete in theory,

current technology limits the daily practices, such as ineffectiveness of fully homomorphic encryption.

Table 2.2 Models versus X.800

Approaches	**Security Access Control Service**	**FHE**	**TCP**	**A New Fair MPNR Protocol**	**Process of access & SSF with Storage**	**UA, FE & DS Based SA[2]**
Cloud Service Models	**SaaS**	**SaaS IaaS**	**SaaS PaaS IaaS**	**SaaS**	**PaaS IaaS**	
Authentication	✓	-	✓	-	-	
Access Control	✓	-	-	-	✓	
Data Confidentiality	-	✓	✓	-	✓	
Data Integrity	-	-	✓	-	✓	
Nonrepudiation	-	-	-	✓	-	

2.2.9. Standardization and Legal Concerns

Due to the nature of cloud computing, combining existing technologies and presenting differently, various standards can be applied in this field. It is too hard to construct a big picture which can be a standard or act as a suggestion. Instead, there are many of them that focus on specific parts of cloud computing. Field of IT has some difficulties such as nonstandard material usage and impalpable processes. Cloud computing inherits these difficulties also adds new ones onto them. Therefore, understanding the gravity of communities for pooling best practices and gathering stakeholders are musts in this era of information.

An eye catching structure comes with Open Virtualization Format (OVF). Deployment-platform free characteristic of OVF should count as an advantage because of different virtualization platforms. On the other hand, secure service provisioning is another critical subject for cloud computing. Information Technology Infrastructure Library (ITIL) and ISO/IEC 27001/27002 are such examples which focus on ensuring

[2] User Authentication, File Encryption and Distributed Server Based Security Architecture is examined as a proposed technical solution approach but not taken into evaluation because of errors.

secure service provisioning. Communities like Cloud Security Alliance (CSA) allows non-profit organizations and individuals to enter into discussion. Thus, they become a part of solution itself [1] [32].

Because of cloud computing's nature of combining and presenting several type services under one roof, examination of current regulations clearly shows that there is an incompetency on privacy protection according to the following issues [1] [33]:

- Under certain circumstances, service providers are obliged to disclose customers' information in United States. This is permitted by "The Stored Communications Act" legislation. According to the same legislation service provider type is unimportant which is electronic communication service provider or remote computing service provider.
- The problem here is cloud computing service providers may be qualified either as an electronic communication service provider or a remote computing service provider. Therefore, a legal misuse may be observed by utilizing this gap.

Information privacy protection in European Community seems to have more solid ground than United States because of the following reasons [1] [33]:

- In Directive 95/46/EC there is a manifest which includes a personal data disclosure that racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and data concerning health or sex must be protected with certain exceptions.
- Public electronic communications networks and services including telecom operators, mobile phone communication service providers, internet access providers, providers of the transmission of digital TV content, and other providers of electronic communication services that are offered to the public are bound to provide the notification of information security breach through Directive 2002/58/EC. In other words, service providers have to assure the information security breach report for any accident which is expected from related authorities.
- Also, there is an article in 95/46/EC states restrictions for transfer of personal data outside the European Community.

2.2.10. Measuring Trust in the Cloud

There is a relationship between cloud service providers and cloud service users when the users require some type of service from the cloud. Trust is a vital factor here as in every other relationship type. Because of various services and customer needs, "establish trust" in the cloud environment is not an easy task. Therefore identifying the trust and trust kinds are good starting points to understand the unseen face of the iceberg.

In [34] [35] [36] definition of trust is given as: "Generally, an entity can be said to 'trust' a second entity when the first entity makes the assumption that the second entity will behave exactly as the first entity expects".

Another definition is given by [37]: "Trust (or, antonym, distrust) is a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action, both before he can monitor such action (or independently or his capacity ever be able to monitor it) and in a context in which it affects his own action".

Third definition [38] is used by many articles: "Trust is a mental state comprising: (1) expectancy – the trustor expects a specific behavior from the trustee (such as providing valid information or effectively performing cooperative actions); (2) belief – the trustor believes that the expected behavior occurs, based on the evidence of the trustee's competence, integrity, and goodwill; (3) willingness to take risk – the trustor is willing to take risk for that belief".

Trust relations involve two different kind of entities which are trustor and trustee. In case of cloud computing trustee can be defined as the provider of required services and trustor can be assumed as the customer of these services provided by the trustee. Previous interactions between trustor and trustee are used for trust establishment.

Also trust is divided into two classes: direct trust and recommended trust [34] [39] [40] [41]. They differ based on the interaction type; if trustor and trustee have a direct relationship that both of them can be able to construct their own experience, it is called direct trust. Otherwise they need to build their relationship via some third party (the

trust relationship is established by another entity's recommendation) which is called recommended trust.

Several trust properties were introduced [35] [42] and are used to obtain models [34] for the management of trust:

- Asymmetry: If first entity trusting second entity, this does not mean that second entity trusts first entity. Therefore a trust relation is asymmetric.
- Reflexivity: Each entity in a trust relationship trusts itself.
- Context dependence: Trust depends on specific actions on specific contexts, cannot be generalized.
- Scalability: Trust may evolve during interaction according to time and experience.
- Partial Transitivity: A first entity recommends second entity to a third entity if and only if third entity trusts first entity and first entity trusts second entity.
- Subjective: Trust is a level of subjective probability.
- Uncertainty: Nature of trust relationships between entities are complex.
- Space based: If trust is evolved from reputation such as recommended trust.
- Time based: If trust is evolved over a period of time such as direct trust.

Trust management models are categorized under three classes: reputation based models, policy based models and evidence based models. "Each individual in a society has to place trust in some basic parts of the society" [43]. Because of that, societal trust lies at the core of all trust models.

Reputation based trust: Reputation based trust systems rely on measuring reputation to evaluate the trust [34], because reputation of an entity presents joint opinion of a community towards that entity [43]. Reputation based evaluation is inherited from e-commerce and P2P networks, instantly adapted to cloud. Usually, high reputation equivalent to high trust level which is a judgment factor on a trustee in these type of systems. One major gap of these systems is general opinion representing a cumulative approach towards a service which can be mirrored to the other services of the service provider. Maybe a cloud service provider has low trust level but in one or two services it may be better than a cloud service provider that has a high trust level.

There are some trust mechanisms such as SLA verification, cloud transparency, and trust as a service to assist for the judgment process:

SLA verification: First step after establishing the initial trust, verification and reevaluation of the trust is needed. As a legal contract between a cloud user and a cloud service provider, service level agreement and its verification are important tasks. There are two major concerns existing about SLA verification. One of them is that SLA mostly includes functional properties of a cloud service and leaves out non-functional aspects such as security and privacy. The other one is lack of user capability to do SLA verification on their own [43] [44] [45].

Cloud transparency: Transparency is a recognized criteria to build trust. "Security, Trust & Assurance Registry (STAR)" program [46] is a free, publicly accessible registry launched by Cloud Security Alliance (CSA) [43]. The aim of STAR is to allow cloud service providers to publish their security controls in defined formats. Cloud users must remember that data presented on the STAR is a self-assessment. The problem here is dishonest cloud service providers can easily change the data because they are the ones who created the data.

Trust as a service: In [43] Huang and Nicol state that Cloud Trust Authority (CTA), as a cloud service, provides a single point for configuring and managing security of cloud services from multiple providers. Basically, the CTA is a specialized tool on cloud trust management.

Another trust management model class is Policy based trust: PKI technology is a good example for employing formal trust mechanisms to support digital signature, key certification and validation. According to Huang and Nicol [43] "trust in a certification authority (CA) with respect to issuing and maintaining valid public key certificates is based on the CA's conformance with certain certificate policies. Certificate policies play a central role in PKI trust. We call this trust mechanism as policy based trust."

The third one is Evidence based trust: In this class of trust, belief of the one entity (trustor) is based on the evidence about attributes of the other entity (trustee) such as competency, goodwill, and integrity. [43] suggests two-dimension space for attribute organization:

1. Expectation domain: aspects of performance, security and privacy.
2. Trust source: competency (capability), integrity[3] (consistency in performance and principles) and goodwill[4] (motivation or intension).

To quote Huang and Nicol [43] the connection between evidence based trust and policy based trust is as follows:

"The belief that an entity conforms to a trusted policy implies the belief that the entity has a set of attributes associated with that policy."

The last part about evidence based trust is the source of attributes which is needed to be tracked for a healthy trust judgment. Source of cloud attribute is provided by the study of Huang and Nicol [43] in detail and listed below:

- Cloud user observation: Direct interaction experience advantage but the disadvantage is that the data collected are due to the range of cloud service usage.
- Opinions of other peer users: Other peer users' opinions is an important source because direct experience has limits.
- Social network based approach: Combine personal trust opinion with the opinions of trusted friends.
- Reputation based approach: Based on service ratings.
- Statements from cloud service provider: The attributes of the service stated in a SLA are the promises of that service provider to that user.
- Assessment of cloud auditor/accreditor[5]: Independent assessment.
- Observation of cloud brokers: Provide real-time cloud service performance monitoring and feedback from many peer users.
- Attribute certification: Standards might be used for cloud attribute certification such as IETF X.509 AC.

[3] "A trustee's historical behavior might reflect integrity" [43].
[4] "Goodwill might be quantified as performance improvements are measured, and cloud users' feedback" [43]
[5] "Accreditation focuses on the qualification of the accredited entity with respect to conducting a specific type of professional services; audit focuses on assessing the performance of the audited entity with respect to the common requirements of a society and/or the professional standards of a professional community." [43]

Generating models for trust management is crucial to gain a further step in the area of cloud computing and in non-functional security requirements. There are models in the literature which focus formalizing trust in the cloud domain and which use independent evaluators for a solution alternative. Such a model is proposed by Prajapati, et al. [34] for recommended trust, based on space variant evaluation and direct trust, based on time variant evaluation. The proposed model can be used with past experience and without any past interaction with the service. Additionally, the reputation factor of trust is included in the model for the calculation of direct trust. Also satisfaction level (depends on service level agreements of the services resides in the cloud environment) is considered for the calculation of recommended trust. Decay function lies at the core of the model to estimate the trust value.

The model components [34] are given below for a better understanding of the model structure:

- Trust degree: From a set of possible trust values, trust degree variable is used to evaluate the degree of trust. Trust degree has value between 0 and 1 and is calculated using direct trust or recommended trust.
- Trust relation: For two types of trust relationship (direct trust and recommended trust), trust relation is the relationship between trustor and trustee from the trusted set.
- Trust levels: Represents the trustworthiness using trust degree.
- Trust chain: Based on the partial transitive properties to form a trust chain.
- Trust model: TM = (trustor, trustee, trust relationship between trustor and trustee, nth service, trust reputation factor, time).
- Direct trust: Each entity holds the values for all other entities in direct trust table.
- Recommended trust: Values constructed by other entities are hold in recommended list table (updated dynamically). If direct trust value is not available, entity checks recommended list table.

Even trust is formalized that it needs to be judged. However, this is not an easy task especially considering the capabilities of cloud users. In their study [43] Huang and Nicol contribute to the literature by giving the tips of judgment for different actors in

the cloud environment. This thesis uses those tips to present a trust judgment assistance table (Table 2.3).

Table 2.3 Trust Judgment Assistance

Judgment on / Information Source	**Cloud Auditor**	**Cloud Broker**	**Cloud Service Provider**	**Cloud Service**
Accreditation	✓	✓	✓	
Policy compliance audit	✓	✓	✓	✓
Certified attributes	✓	✓	✓	✓
Assessed attributes		✓	✓	✓
Self-assessment and information revealing		✓	✓	✓
Reputation / recommendation		✓	✓	✓
Trust based on the service provider				✓
QoS monitoring and SLA verification				✓

CHAPTER 3

STATUS OF ICT SECTOR IN TURKEY

To understand cloud computing and security investments, an important direction passes through a sector analyses. According to the findings based on the report on Information & Communications Technology (ICT) provided by Deloitte Consulting in Turkey, which is an investment support and promotion agency, the ICT sector has a promising future in Turkey because of a stable growth and a positive correlation between GDP (Gross domestic product) and ICT. Therefore, cloud investors are able to see the big picture based on economy. At the same time, this positive correlation assists by highlighting important trends. Also, clearly focuses on economic infrastructure provides vision that can easily be turned into investment opportunities. Between the years of 2012 and 2017, with regards to the recent data, the Turkish IT market promises to grow by 7.4%, although the whole region including both the Middle East and Africa are expected to grow by 9.6% [47].

Future strategies developed by authorities is required to clarify the blurred picture in front of cloud computing in our country. The Turkish government is focused on the goal of achieving an improvement of the ICT market size of USD 160 billion and sector share of 8% of the GDP by 2023. This is not an optimistic vision when seeing that Turkey currently has 129 ICT related Research and Development centers with a goal of building more. The major technological investments are demonstrated by the spending in the hardware market, corresponding to more than 2/3 of the Turkish ICT market. Although hardware holds outweighing, it is promised that total ICT spending will grow by USD 53.5 billion in 2017 from 20 billion in 2009, with a compound annual growth rate of 12.65% [47]. This means other markets will merge into the picture more effectively in the near future.

In Figure 3.1 Turkish Statistical Institute (TurkStat)'s "ICT Usage Survey in Households and Individuals 2014" results are given for information society statistics. Ratio increment can be seen year by year but the most remarkable result is in the category "Households with access to the internet" with %60.2 and the escalation between 2013 and 2014 is %11.1, especially considering total population of Turkey is over 76 million, these values represent significance for cloud computing should gain more ground in Turkey.

Similarly, based on Gartner forecasts, Turkey's ICT spending is expected to grow in parallel to the positive trend in the GDP in the future. For example, it is expected that IT spending in hardware, software, IT services and telecommunication services in Turkey will grow by over USD 25 billion in 2016 with a parallel growth to its GDP growth between 2013 and 2016 (see Figure 3.2) [47]. So far, it is not possible to distinguish security related cloud investments from other cloud investments because of the following reasons:

- Cloud Service Providers keep that information confidential,
- A few number of Private Cloud Providers in Turkey produces a generalization about security costs. Also, sensitive information is a problem in here too.
- The public sector is still behind the cloud adaptation process because of legal issues and regulations mainly.

Information Society Statistics, 2004-2014 %

	2004	2005	2006 (*)	2007	2008	2009	2010	2011	2012	2013	2014
ICT Usage in Enterprises											
Computer Usage	-	87.8	-	88.7	90.6	90.7	92.3	94.0	93.5	92.0	
Internet Access	-	80.4	-	85.4	89.2	88.8	90.9	92.4	92.5	90.8	
Having Website	-	48.2	-	63.1	62.4	58.7	52.5	55.4	58.0	53.8	
ICT Usage in Households and Individuals											
Computer Usage (Total)	23.6	22.9	-	33.4	38.0	40.1	43.2	46.4	48.7	49.9	53.5
Male	31.1	30.0	-	42.7	47.8	50.5	53.4	56.1	59.0	60.2	62.7
Female	16.2	15.9	-	23.7	28.5	30.0	33.2	36.9	38.5	39.8	44.3
Internet Usage (Total)	18.8	17.6	-	30.1	35.9	38.1	41.6	45.0	47.4	48.9	53.8
Male	25.7	24.0	-	39.2	45.4	48.6	51.8	54.9	58.1	59.3	63.5
Female	12.1	11.1	-	20.7	26.6	28.0	31.7	35.3	37.0	38.7	44.1
Households with access to the Internet	7.0	8.7	-	19.7	25.4	30.0	41.6	42.9	47.2	49.1	60.2

Figure 3.1: Information society statistics [56]

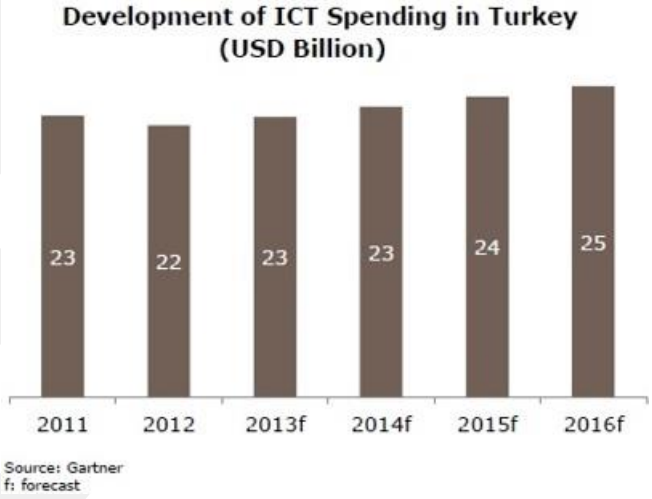


Figure 3.2: Gartner forecast (ICT Spending) [47]

The increasing importance of IT in business and market has led to a large number of Turkish firms to invest heavily in IT to gain a competitive advantage. According to Gartner forecast, the spending in the information and communication technology sub-sectors, including telecommunication services, devices, IT services, software, data center systems, are expected to grow by over USD 25 billion in 2016 (see Figure 3.3) [47].

According to recent research, software has been a major component of technology spending in Turkey. Deloitte report points out that there is an immense opportunity in packaged software sales in Turkey as the economy grows. Today, packaged software sales are 0.1% of the GDP in Turkey, while it was approximately TL 2.24 billion with a growth of 28% with respect to 2011. Software sales in enterprise applications and infrastructure software are expected to grow by USD 4.56 billion in 2016. The parallel growth between GDP and the IT sector offers great potential when thinking from SaaS structure of the cloud [47].

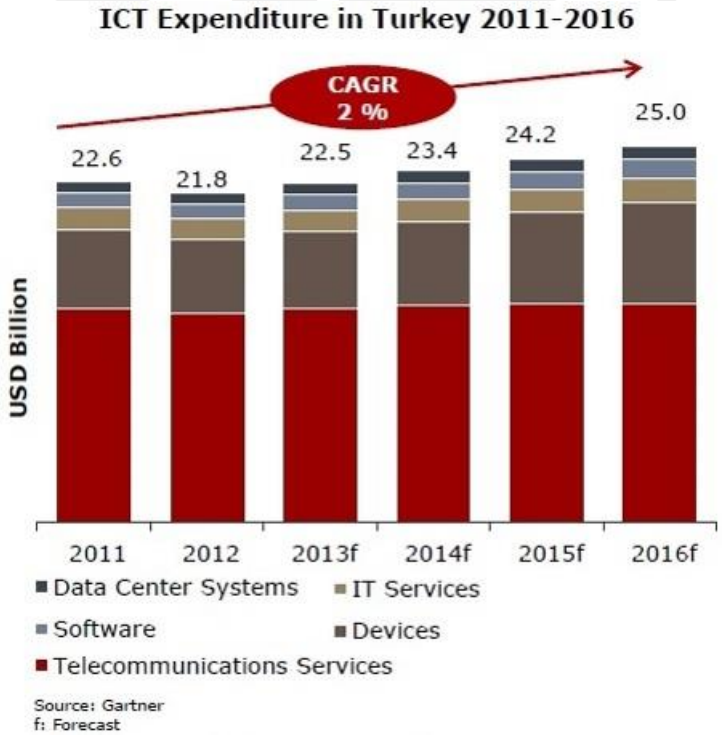


Figure 3.3: Gartner forecast (ICT Expenditure) [47]

The total shares of sub-sectors, including ICT services and the software sector in Turkey, are less than one quarter of Turkey's total ICT market, while their combined share in the global ICT market is around 70%. Most of the Turkish companies are expected to accelerate their spending on software packages for their respective business requirements in the near future [47].

Another major component of technology spending in Turkey has been in hardware. According to the Turkish Informatics Industry Association (TÜBISAD) analysis, as Deloitte report highlights, the hardware sub-sector is composed of more than two thirds of the IT market, excluding the communications sector. The total technology spending in Turkey is expected to be approximately USD 53.5 billion in 2017, with a CAGR of 12.65% between the years 2009 and 2017 [47].

Use of internet and its potential are increasing in Turkey which is a trigger factor for the usage of cloud computing. As Deloitte report indicates, if there is a better infrastructure, internet subscriptions may increase and accelerate the developments in rural areas. Today, internet usage in Turkey is approximately 42% and it is expected to increase by over 47% in 2017. Based in EIU analysis, in 2017 the number of internet subscriptions is expected to triple [47]. Moreover, the significance of rising in internet subscriptions has a positive effect on the increase in the development of business that benefited from cloud computing.

According to a study in 2010, Turkish firms find 46% of new business markets and customers via internet. Furthermore, broadband internet subscriptions, mobile internet subscriptions and internet retailing are expected to increase more because of high young population, high interest in usage of internet, expected spending and popularity of internet usage in mobile phones, tablets and personal computers show that the sector is expected to continue growing [47]. In Figure 3.4 TurkStat's "ICT Usage Survey in Households and Individuals 2014" results are given for individuals using the computer and internet by age groups.

Individuals using the computer and Internet in the last 3 months by age groups (%)

		Age group																	
		16 - 24			25 - 34			35 - 44			45 - 54			55 - 64			65 - 74	
	Year	Total	Male	Female	Total	Male	Female	Total	Male	Female	Total	Male	Female	Total	Male	Female	Total	Male
Computer	2004	32.2	44.4	21.1	19.8	26.4	13.1	13.1	19.2	7.1	7.9	12.9	2.8	2.3	4.0	0.7	0.4	0.8
	2005	34.1	43.8	25.0	20.9	27.8	13.9	13.2	19.2	7.1	8.8	14.2	3.3	3.1	5.0	1.2	1.2	2.2
	2007	54.6	67.3	40.7	35.1	44.7	25.5	26.8	36.6	17.1	17.1	28.8	7.5	6.0	9.6	2.0	1.5	2.2
	2008	57.9	69.6	47.0	43.3	54.8	31.8	31.6	41.6	21.5	20.4	28.3	12.5	7.4	12.6	2.5	1.8	3.0
	2009	62.2	76.4	49.1	46.6	58.6	34.5	31.8	42.1	21.3	20.2	28.9	11.6	6.7	10.6	3.1	2.2	3.2
	2010	65.2	78.5	52.7	52.0	62.4	41.6	36.9	46.9	26.9	23.2	33.6	12.7	8.3	13.5	3.4	2.7	4.1
	2011	67.7	77.9	58.3	57.1	67.5	46.7	41.7	52.6	30.6	24.1	34.3	13.9	11.2	17.2	5.4	3.0	5.0
	2012	68.5	81.1	56.4	59.1	70.0	48.1	43.6	54.3	32.7	26.7	36.3	17.0	12.5	19.1	6.1	3.8	6.9
	2013	70.6	82.0	59.5	59.6	70.0	49.1	47.0	58.2	35.6	28.1	38.2	15.9	11.9	18.2	5.8	4.4	7.8
	2014	70.3	79.6	61.0	63.3	71.3	55.3	51.0	61.9	40.0	30.6	40.5	20.6	15.4	21.9	9.1	5.0	8.8
Internet	2004	28.6	38.3	15.9	15.7	21.5	9.9	9.4	13.9	4.9	5.5	9.3	1.7	1.8	2.7	0.8	0.4	0.9
	2005	27.8	37.4	18.8	16.7	22.5	10.6	9.7	14.3	5.0	6.3	10.1	2.4	2.3	3.8	0.9	0.9	1.8
	2007	50.4	63.5	36.2	32.3	41.5	23.1	23.8	33.2	14.4	14.8	23.2	6.5	4.8	7.5	1.8	1.4	2.1
	2008	54.8	67.1	43.4	41.4	52.3	30.4	29.3	37.7	20.8	19.4	27.1	11.6	6.9	11.9	2.2	1.6	2.5
	2009	59.4	74.1	46.0	45.1	57.2	32.9	30.2	40.3	19.9	18.6	26.7	10.5	6.2	9.5	3.1	2.0	3.1
	2010	62.9	76.6	49.9	50.6	60.9	40.2	34.7	43.5	25.7	22.4	31.9	12.9	7.8	12.6	3.2	2.7	4.2
	2011	65.8	76.5	55.9	55.1	65.4	44.9	39.7	50.4	28.9	22.7	32.1	13.2	10.4	16.0	5.0	2.7	4.5
	2012	67.7	80.6	55.4	58.5	69.6	47.2	42.6	53.3	31.8	25.5	34.8	16.2	11.9	18.5	5.6	3.6	6.4
	2013	68.7	80.1	57.5	58.8	69.1	48.4	45.6	56.7	34.4	24.9	34.7	15.1	11.1	16.8	5.7	4.2	7.5
	2014	73.0	82.8	63.2	67.1	76.8	57.4	52.0	63.7	40.2	30.4	40.7	20.0	15.3	21.5	9.3	5.0	8.8

Figure 3.4: Computer and internet usage [56]

TurkStat Information and Communication Technology (ICT)'s analysis on the usage survey in households and individuals in Turkey between the years of 2004 and 2014 states that the demand on technological devices is increasing drastically including both rural and urban areas such as mobile phones, rising by 96.1% in 2014 (see Figure 3.5).

Availability of devices in households (%)

	Year	Desktop computer	Portable computer (Laptop, Tablet PC)	Portable computer (Laptop, netbook,	Tablet computer	Mobile phone (incl. smart	Television (including satellite dish, cable	Smart TV	Fixed line telephone	Game console	Handheld computer	Digital camera/photography	DVD / VCD / DivX player	Printer	Scanner	Fax	Multi function device (including two or more functions like printer,scanner,fax,etc.)	Other	None of above
Turkey	2004	10.0	0.9	.	.	53.7	92.2	.	81.6	2.9	0.1	.	.	.	.	.	.	.	2.3
	2005	11.8	1.1	.	.	72.8	97.7	.	81.3	2.9	0.1	.	.	.	.	.	.	.	1.1
	2007	24.0	5.6	.	.	87.4	.	.	72.7	3.7	0.4	16.9	40.8	9.7	3.5	1.2	1.3	.	.
	2008	28.1	9.1	.	.	88.1	.	.	68.4	3.9	0.5	20.0	42.6	12.1	4.5	1.1	1.1	1.3	2.8
	2009	30.7	11.2	.	.	87.6	.	.	61.9	3.7	0.6	20.4	42.7	12.4	3.4	1.1	1.8	.	3.6
	2010	33.8	16.8	.	.	90.5	.	.	56.1	3.1	0.7	23.8	40.6	13.9	3.5	1.1	2.5	2.4	2.9
	2011	34.3	22.6	.	.	91.9	.	.	51.4	3.8	1.2	27.8	40.5	14.0	3.9	0.8	3.2	3.3	0.2
	2012	31.8	27.1	.	.	93.2	.	.	46.5	4.6	1.4	27.1	36.0	.	.	.	16.0	0.0	2.9
	2013	30.5	.	31.4	6.2	93.7	.	7.3	37.9	5.0	.	28.1	30.6	.	.	.	.	.	3.1
	2014	27.6		40.1	.	96.1	.	12.4	.	5.6	.	27.2	29.2	.	.	.	.	0.0	1.8
Urban	2004	14.2	1.2	.	.	62.4	93.9	.	84.5	4.1	0.2	.	.	.	.	.	.	.	1.2
	2005	16.1	1.6	.	.	79.9	99.0	.	83.6	3.7	0.2	.	.	.	.	.	.	.	0.4
	2007	30.0	7.2	.	.	90.3		.	74.2	4.5	0.6	19.9	47.4	12.2	4.1	1.5	1.7	.	.
	2008	33.7	11.4	.	.	90.2	.	.	68.9	4.5	0.6	24.3	49.2	14.5	5.4	1.4	1.4	0.4	2.2
	2009	37.1	14.3	.	.	89.6	.	.	63.1	4.5	0.8	24.6	48.6	15.1	4.2	1.3	2.0	.	2.6
	2010	40.6	20.4	.	.	92.8	.	.	58.8	3.7	0.9	28.6	47.4	16.8	4.4	1.4	3.1	2.2	2.0
	2011	41.0	27.9	.	.	93.6	.	.	55.1	4.9	1.5	34.2	48.2	17.0	4.8	0.9	4.2	2.1	0.2
	2012	38.2	33.5	.	.	95.1	.	.	47.4	5.8	1.7	33.2	42.0	.	.	.	20.0	0.1	1.9
	2013	38.2	.	37.9	8.1	95.8	.	9.5	40.8	6.8	.	34.7	38.8	.	.	.	.	.	1.8
	2014	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
Rural	2004	2.8	0.2	.	.	38.8	89.3	.	76.5	0.8	0.0	.	.	.	.	.	.	.	4.1
	2005	3.7	0.3	.	.	59.9	95.6	.	77.4	1.4	0.0	.	.	.	.	.	.	.	2.4
	2007	8.9	1.8	.	.	80.1	.	.	68.9	1.5	0.1	9.2	23.6	3.5	1.8	0.4	0.2	.	.
	2008	13.6	3.2	.	.	82.8	.	.	67.0	2.2	0.3	9.1	25.7	5.8	2.1	0.3	0.5	3.6	4.5
	2009	15.2	3.6	.	.	82.9	.	.	59.9	1.8	0.3	10.2	25.9	6.0	1.3	0.4	0.8	.	6.1
	2010	16.6	7.8	.	.	85.0	.	.	49.4	1.5	0.2	11.7	23.4	6.5	1.1	0.5	0.9	3.0	5.3
	2011	17.4	9.2	.	.	87.7	.	.	41.9	1.3	0.3	11.7	21.0	6.7	1.5	0.3	0.8	6.2	0.3
	2012	16.3	11.8	.	.	88.5	.	.	40.9	1.7	0.5	12.4	18.0	.	.	.	6.4	0.0	5.2
	2013	17.0	.	15.6	1.5	89.1	.	1.9	31.5	1.4	.	12.3	16.2	.	.	.	.	.	6.3
	2014	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.

Figure 3.5: Availability of devices in households [56]

Technical education requirement is another aspect during cloud adoption process. In Turkey, the engineering fields related to ICT sector in universities are one of the most popular undergraduate and graduate studies. Every year, a significant young population chooses to study under the ICT-related programs that make a contribution with a high-quality workforce. According to Deloitte report, 115,528 undergraduate and 140,713 graduate students chose to enroll in associate programs, growing by 29% in 2012 compared to 2011. Related to this, the quality of engineering departments is improving as well as the quantity of the students in associate fields [47]. Moreover, as the figure shows that technology development zones (TDZs) in Turkey have been considered as "strategic investments" since the early 1990s (see Figure 3.6) [47].

Figure 3.6: TDZ progress [47]

There are several regulations and incentive programs, which support ICT sector investments and initiatives. In 2012, half of the ICT companies benefitted from them. According to Deloitte report, TÜBITAK-TEYDEB Program's incentives have the largest total share [47].

Deloitte report sums up 2023 ICT targets in Turkey in terms of three different fields [47]:

1. Industrial Strategy of the Ministry of Science, Industry & Technology:

   The goal is to increase the number of companies that constantly develop their skills within the economy; to increase the number of medium and high technology sectors in production and export; to transit products with high added value in low-technology sectors; and to increase the sector's share in the GDP from 2.9% to 8% in 2023.

2. Communication Strategy of The Ministry of Transport, Maritime Affairs & Communications:

   The goal is to have 120 million mobile subscribers; to have 30 million broadband subscriptions; to provide internet connections for 14 million houses at a speed of 1000Mbs; and to reach an ICT sector size of USD 260 billion that requires a market growth of around 15% each year.

3. R&D Strategy of the Supreme Council of Science and Technology:

   The goal is to increase the number of researchers from 135,000 to 300,000; to reach a number of 180,000 private sector researchers from 39,000, to increase the R&D expenditure to GDP ratio to 3% from 0.85%; and to increase private sector R&D expenditure of the GDP ratio to 2%.

These targets are also relevant for the future of cloud computing in Turkey. Security investments in the cloud should not be done without considering the ICT sector in general. IT services in Turkey have accelerated its speed drastically with an increasing amount of investments each year. Software integration has been increasing within the public domain, freeware and shareware programs over the years. International companies such as IBM, Hewlett Packard, Dell, Siemens, Cisco and NCR have invested in Turkey's IT services sector. Some international firms joined the market via acquisition, such as Soitron's acquisition of Sekom. According to Gartner forecasts, spending on IT services in Turkey reached USD 1.4 billion and is expected to rise in the following years. Business IT services turn to be around 70% of the IT services sector, and the rest 30% is in IT product support [47].

It is also important to discover where we lose or why we lose for a better understanding of where and how we win in terms of Turkey's unique conditions. Therefore,

International Investor Association's (2012) SWOT analysis is presented in this study as an efficacious point to perceive the challenges that will be useful for cloud computing too. Firstly, the strengths of the ICT sector in Turkey are young population apt to technology consumption, young and inclined to improve workforce, the trend of a fast growth rate in sectors, and strong economic indicators and growth tendency. The weaknesses are high tax rates, predictability of the regulations, cost-oriented auction politics, lack of initiative funding, intellectual property right related intrusions, and slow bureaucracy. The opportunities of ICT sector in Turkey are consumers fast adaptable to innovations, its closeness to developing and advanced markets, the existence of virgin markets, the capacity of growing qualitative workforce, constant increase in innovative products, the Government's positive attitude and the importance it gives to the sector, and the interest of international investors into the sector. Lastly, the threats are tendency of a decrease in profit margins and investment because of cost-oriented high competition, lack of a sufficiently developed collaboration culture at the fields of R&D and innovativeness, macro-economic ambiguities, such as current deficit, exchange rate, inflation, etc., lack of a broad vision on product and branding, and lack of necessary educational politics for qualitative workforce and researchers (see Table 3.1) [48].

Analyzing the ICT sector's effect on efficiency by increasing in productivity and economic growth, the empirical studies suppose that ICT sector can contribute in three ways [49]. First of all, it is emphasized that investments in ICT sector has a direct role in increasing in productivity and economic growth by contributing to capital deepening. Second, the studies try to show the role of the fast developments in technologies, which are used in the production of information and communication technology products and services, on the sectors producing information and communication technologies that are seen as having an increasing efficiency. Lastly, there are studies to analyze the effects on the efficiency in the whole economy and the innovative tendency as a result of the spread of ICT sector in a broad field in the economy [49].

Table 3.1 SWOT Analysis of ICT Sector in Turkey

Strengths	**Weaknesses**
- Young population apt to technology consumption - Young and inclined to improve workforce - Trend of a fast growth rate in sectors strong economic indicators and growth tendency	- High tax rates - Predictability of the regulations - Cost-oriented auction politics - Lack of initiative funding - Intellectual property right related intrusions - Slow bureaucracy
Opportunities	**Threads**
- Consumers fast adaptable to innovations - Its closeness to developing and advanced markets - The existence of virgin markets - The capacity of grow qualitative workforce - Constant increase in innovative products - The Government's positive attitude and the importance it gives to the sector - The interest of international investors into the sector	- Tendency of a decrease in profit margins and investment because of cost-oriented high competition - Lack of a sufficiently developed collaboration culture at the fields of R&D and innovativeness - Macro-economic ambiguities, such as current deficit, exchange rate, inflation, etc. - Lack of a broad vision on product and branding - Lack of necessary educational politics for qualitative workforce and researchers

Cloud computing does not correspond to a particular technology, but means a new approach and use of model of device, independent from technology and capacity, where various access and information technology infrastructure are gathered and stored in a "cloud"; where the devices are used instead of data and software that is processed and stored on a server; and where access is provided via the Internet. Based on the strategic report prepared by the US CIO Council, Cloud computing is the main factor that will enable and accelerate the transformation, provided by cheap and developing technological devices and mobility, and lead to currently unpredictable job opportunities. Cloud computing is expected to make major changes on business and use of models like the way internet did on our communication, socialization and working styles. Nowadays, a lot of people have already been using several services over the cloud computing infrastructure. Many Internet users are actually benefitting from the cloud computing by using products of companies like Facebook, Google,

Apple and Yahoo!, which are kind of public cloud products. According to ABI Research, until the year of 2014, the number of users accessing to the "cloud" based applications with mobile devices will reach 1 billion. In addition to this, various surveys, conducted over the businesses which have already cloud computing, show that it can provide an improvement of around 60% in terms of total cost of ownership. With these developments, many users' –large or small– IT adaptation will also speed up.

According to Yased, the most important benefits of Cloud Computing can be sorted in four ways [48]:

- Freedom of mobility provided by freedom of application and file usage independent from devices and their technological features (processor, memory, etc.)
- Cost advantage with "pay as you use" business model, with the help of its shared resource pools and common usage and the increase in the utilization rates.
- Advantage of accessing the recent technology that allows the recent and upgraded IT resources to be easily bought from the common pools as a service.
- Advantage of flexibility provided by the systems that offers instant solutions according to the capacity needs due to periodical and temporary changes.

Singapore offers incentives to all businesses, including SMEs, by giving education related to Cloud Computing, providing tax exemption in R&D expenditures and developing to support Cloud Computing-like structures via an investment agency. Besides, universities open selective courses that train graduates who will adopt and develop cloud computing. With the help of studies, improvements and the vision set forth, Amazon, Fujitsu, Microsoft, OpSource, My Salesforce.co, Tata, Canon, HP, IBM, and International companies such as Oracle and Parallels have opened Cloud Computing service center in Singapore, aiming for being the center of Cloud Computing in Asia [48].

In the following years, there will be more new projects in the fields of "cloud computing", "smart applications", "mobile Internet" and "Internet of Things" (Machine to Machine-M2M) in IT sector. In 2012, investments in cloud computing

has increased fast around the world, reaching by USD 109 billion. Cloud computing investments are expected to be USD 150 billion in 2013. In Turkey, 8% of SMEs are positive about favoring cloud computing. This percentage means an over of 200,000 businesses [50].

Similarly, Deloitte sees cloud computing as a high potential business line along with other emerging IT service practices, such as cybercrime, data centers, mobility and analytics. According to ABI Research, cloud based application users through mobile devices will be 1 billion by 2014. Turkey is expected to be a major player in this market. Infrastructure investments of companies dealing with cloud computing became more than USD 11 billion in 2011, although there was relatively a small number of cloud service suppliers, which was around 50 in 2008 and raised to 100 by the end of the year of 2011. In Turkey, cloud computing services is expected to grow by about 54% in 2013. 31% of companies and organizations were dealing with cloud computing in 2011, while %40 of them are planning to adopt cloud; conversely Turkey's adoption rate is 4th-largest in the world. At the same time, the oil and gas sector and public sector are positive about investing in cloud computing infrastructure. Cloud services have started to be provided by Telecom operators that give several signs that Turkey could be an attractive destination for cloud facilities [47]. As cloud products prove their effectiveness and convenience by spreading throughout the market in Turkey, there will be a high percentage interest in software-as-a-service and cloud offerings.

CHAPTER 4

RESEARCH METHODOLOGY AND SURVEY

4.1. Research Method

In order to summarize the current situation of security in cloud computing to serve as a background for the study, a literature review of the examined studies that have been performed in the technical domain, X.800 services categories compliance for strengthening security on the cloud and the necessity of generating new solutions by considering non-technical aspects are carried out. In addition, preparing a questionnaire is the adopted approach for data collection in this study.

After producing research questions as motivation factors of this study, we started to define categories for search terms which are “Set A”, “Set B”, and “Set C”. Then each search term is placed into one category as follows:

- Set A: security, cloud computing security, security cloud computing, secure data generation, secure data storage, secure service provisioning, secure cloud.
- Set B: recommendation X.800, X.800, authentication, access control, data confidentiality, data integrity, nonrepudiation, trust.
- Set C: technical, non-technical, legal, standardization.

Defining an exclusion criteria is an important part. The excluded studies are: Do not relate to; cloud computing security, technical solution proposals, non-technical solution proposals, cloud computing legal issues, cloud computing standardization. The studies which are not describing any of X.800 service categories except the studies related to trust. Later, six study is randomly chosen to present several technical solution proposals.

Technical solution proposals are examined with respect to X.800 service categories (Authentication, Access Control, Data Confidentiality, Data Integrity, and Nonrepudiation) for the following criteria:

- Authentication: Management privilege of the authentication database.
- Access Control: Policy oriented access control.
- Data Confidentiality: Storage encryption was chosen as an evaluation criteria.
- Data Integrity: Data changes only in response to authorized transactions.
- Nonrepudiation: This category is checked whether a nonrepudiation protocol is offered for that approach or not.

According to the examination, which solution proposal has which X.800 service category or categories is shown in a Table (Table 2.2) together with cloud service models. For the decision of cloud service models we use definitions of IaaS, PaaS, and SaaS.

Standardization and legal concerns are given by comparing different regions such as United States and European Union. Trust is highlighted as one of the major problem in cloud environment and for better understanding of this intangible asset we tried the following steps:

- Step 1: Give the definitions of trust in general,
- Step 2: List trust properties and give definitions,
- Step 3: Categorize trust types and examine decision support systems under them,
- Step 4: Examine trust management models for formalization,
- Step 5: Formalize trust,
- Step 6: Prepare a table to help trust judgment.

Status of ICT sector is directly related with cloud computing and security investments. Therefore, a whole chapter is committed to give statistical data from Turkish Statistical Institute, Investment Support and Promotion Agency, International Investors Association, Informatics Industry Association, Informatics Association of Turkey, Deloitte, and Gartner about market, technology adaptation, IT spending, etc.

Also survey methodology is applied to prioritize the security requirements for different cloud computing types and service delivery models. It is often employed in many empirical research studies and is defined as following [51].

"A single survey is made of at least a sample, a method of data collection and individual questions or items that become data that can be analyzed statistically. A single survey may focus on different types of topics such as preferences, opinions, behavior, or factual information, depending on its purpose. Survey methodology as a scientific field seeks to identify principles about the sample design, data collection instruments, statistical adjustment of data, and data processing, and final data analysis."

A questionnaire is prepared by considering the above-mentioned description. We try to find IT professionals who have general knowledge about cloud computing and security concept to complete the questionnaire and achieve accurate data from it. Searching cloud computing work groups constituted under broad organizations were the first step that needs to be accomplished for survey methodology.

By the help of this questionnaire, the thesis points out which X.800 service categories are taken into consideration as a must and which are optional for public cloud, private cloud and hybrid cloud together with delivery models (IaaS, PaaS, SaaS). We decided to apply the questionnaire to both private and public sector IT executives. Consequently, the Cloud Computing Security Requirements Survey is applied to 73 participants during the 31st National Informatics Meeting in 2014 accommodating a satisfactory sample set and distribution among IT professionals and people in related work groups from the workshops; "Cloud IT: Will the future be more cloudy?" and "Big Data".

In the survey, there were 15 questions, some of which Likert-type (that is, the scale of 1 being 'strongly disagree' up to 5 as 'strongly agree'), the others are open-ended and constrained questions. All questions in the survey are mainly formulated by us. At the beginning of the second part of the survey, cloud service models, cloud types, Recommendation X.800 categories is also provided as a textual introductory material. All answer required questions are marked with a star to the left side of the question number in the survey. The survey is composed of two main sections: Information in

the first part (“Demographic Information” part) is gathered through 7 questions. In the second part, “Priority, Requirements and Necessity of X.800 Service Categories”, it is aimed to gather the opinions of the participants about security (general and specific to X.800) with cloud computing including various cloud types and cloud service models by asking 8 questions. Table 4.1 shows survey questions and choices in detail.

The purpose is to prioritize X.800 service categories regarding participant opinions and the statistical data is carried out by providing 12 hypotheses. During the detailed evaluation, in addition to the overall percentage distributions, mean[6] of the relations among the responses are studied and examined with the hypothesis tests. The hypotheses are generated based on a statistically significant difference that occurred from the point of view of this thesis and is tested with the 0.05 significance level. The tests for hypotheses are conducted by Pearson Correlation where a statistically significant correlation between two variables is searched. Also, One-way ANOVA is applied when comparing means between groups is needed to understand any significant difference.

[6] mean = sum of elements in set / number of elements in set

Table 4.1 Survey Questions and Choices

***1. Gender:**					
Male			Female		
***2. Age:**					
18-25	26-33	34-41	42-49	50-58	59 +
***3. Education:**					
High School	University		Master	PhD	
***4. Work Sector:**					
Public	Private		University	Unemployed	
5. Your task in the sector you work:					
IT Manager	IT Software Employee	IT Hardware Employee	Academic	Sales and Marketing	Project Management	Other + Text Field for Other
6. Years of experience:					
1-5	6-10	11-15	16-20	21-25	26+
7. Number of employees in your organization:					
1-9	10-50	51-250	>250		
***8. Do you have a general knowledge about data security?**					
Yes	No				
***9. Do you have a general knowledge about cloud computing?**					
Yes	No				
***10. Which cloud type do you use more intense than others?**					
Public Cloud	Private Cloud	Hybrid Cloud	I do not use cloud services		

Table 4.1 (cont.)

11. Which cloud services do you use? (You can select more than one)							
Data storage	Database and services	File sharing	Messaging	Office / Functional software applications	Computing power	Application development	Other + Text Field for Other

***12. How important is the privacy and security of data process and the protection of personal information for you? Please rate. (1: Nothing, 5: Enormous)**							
Data storage	Database and services	File sharing	Messaging	Office / Functional software applications	Computing power	Application development	Other (If you filled in Q11)

***13. How necessary is the following service categories for Infrastructure as a Service (IaaS)? Please rate. (1: Nothing, 5: Enormous)**				
Authentication	Access Control	Data Confidentiality	Data Integrity	Nonrepudiation

***14. How necessary is the following service categories for Platform as a Service (PaaS)? Please rate. (1: Nothing, 5: Enormous)**				
Authentication	Access Control	Data Confidentiality	Data Integrity	Nonrepudiation

***15. How necessary is the following service categories for Software as a Service (SaaS)? Please rate. (1: Nothing, 5: Enormous)**				
Authentication	Access Control	Data Confidentiality	Data Integrity	Nonrepudiation

4.2. Research Limitation

Although the research has achieved its goal to explore the necessity of X.800 Recommendation security service categories for different cloud deployment models and cloud service delivery models, also to reveal the standardization, legal, trust issues of cloud computing security, there were some unavoidable limitations:

- There is few literature related to our current X.800 service categories in cloud computing security study for the comprehensive investigation.
- Regarding the necessities of more non-technical specifications and challenges to our general thinking about security related to cloud computing, there are still a great many open issues in the adoption of cloud computing.
- There are some restrictions to get access to IT professionals such as time restrictions, networking, hypersensitivity (even in an anonymous survey) to any research because their sensitive information could make them vulnerable to political or legal harm.
- Gathering as many people as possible who has high interest about the related field is a difficult task. Therefore, we had to wait a related meeting which is organized in Turkey.
- People are reluctant to contribute in an academic research, the survey have been opened on the internet but none of the cloud related groups, that we wrote and requested to fill the survey, return to our call.
- Classification of an approach was a difficult task to accomplish because of various usage methods.
- Entering the data collected from the survey to a statistical tool, learning the tool for detailed analysis with appropriate statistical test methods, and interpret statistical results is a challenge because of extra knowledge which is needed from a different major area.

CHAPTER 5

EVALUATION OF SURVEY RESULTS

5.1. Findings

Digitalization of data obtained from 73 participants is done by using Google Documents. In the first spreadsheet participant numbers, question numbers and their choices are entered together with selected choices and codes of choices (See Appendix A). Selected choices are entered as 1 in related fields for the sum of each choice and represented as total at the last row. At the same time, another spreadsheet (See Appendix B) is prepared for the data entry process and further analysis with IBM SPSS Statistics 20. By using cross-check technique 17 entry errors are caught and corrected. After that 23 participants are excluded from the study and placed on another spreadsheet (See Appendix C) because of the following reasons:

- Three participant are excluded because they do not have general knowledge about either data security or cloud computing. To get meaningful results, at least general knowledge about these areas are mandatory.
- The other participants (17 participant) are excluded because of inconsistent or unsatisfactory data. Such as, some participants answered question #10 as "I do not use cloud services" and in question #11 they selected one or more cloud services that they use or some participants selected multiple choices for one choice only question which is question #10 or some participants' survey results are empty.

Remaining sample number from the survey is 53. In this stage, data is transferred from Google Documents to IBM SPSS Statistics 20 tool as variables together with their values.

Demographic characteristics/distribution of the data is as follows; According to the results, 90.6% (48 people) of the participants of the survey are male and 9.4% (5 people) of the participants are female (see Table 5.1 & Figure 5.1).

Table 5.1 Gender Frequency

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	48	90,6	90,6	90,6
	Female	5	9,4	9,4	100,0
	Total	53	100,0	100,0	

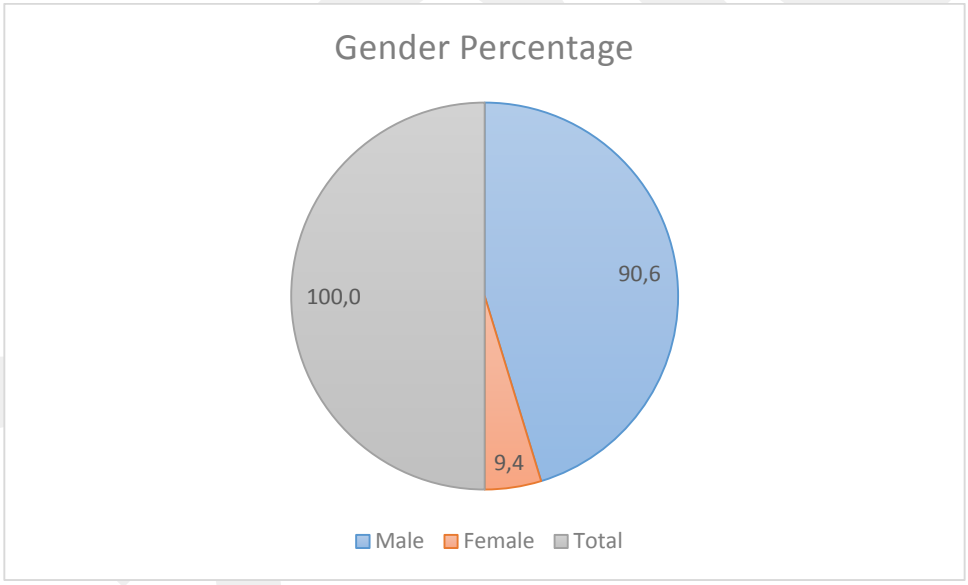


Figure 5.1: Gender distribution of the participants

The age distribution results that 7.5% of the participants of the survey are between 18 and 25 years old. The other 7.5% of the participants are between 50 and 58 years old. The highest percentage belongs to the group between years 26 and 33 with 32.1% (see Table 5.2 & Figure 5.2).

Table 5.2 Age Frequency

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	18-25	4	7,5	7,5	7,5
	26-33	17	32,1	32,1	39,6
	34-41	15	28,3	28,3	67,9
	42-49	13	24,5	24,5	92,5
	50-58	4	7,5	7,5	100,0
	Total	53	100,0	100,0	

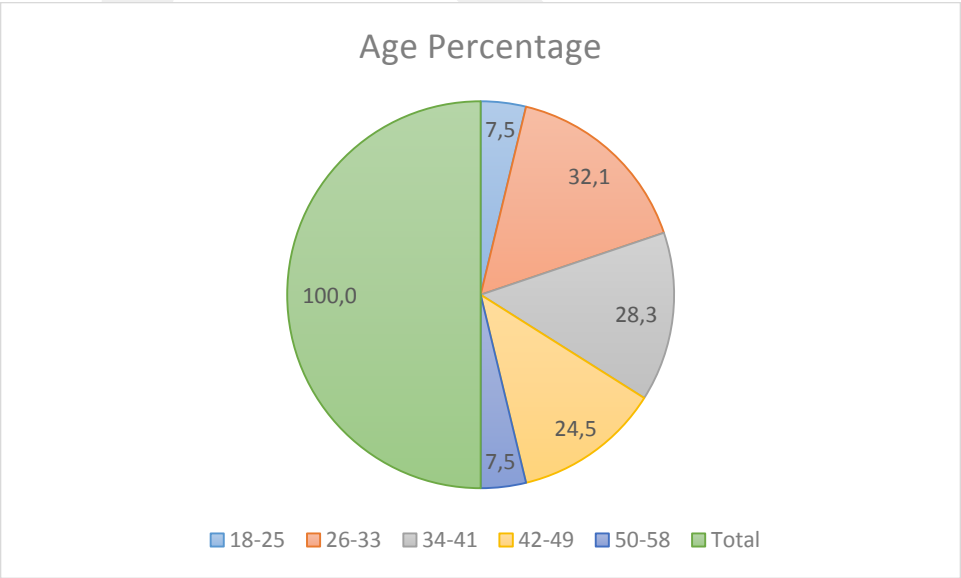


Figure 5.2: Age distribution of the participants

In terms of education, 60.4% of the participants hold either a MSc or a PhD degree (see Table 5.3 & Figure 5.3).

Table 5.3 Education Frequency

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	High School	2	3,8	3,8	3,8
	University	19	35,8	35,8	39,6
	Master	21	39,6	39,6	79,2
	PhD	11	20,8	20,8	100,0
	Total	53	100,0	100,0	

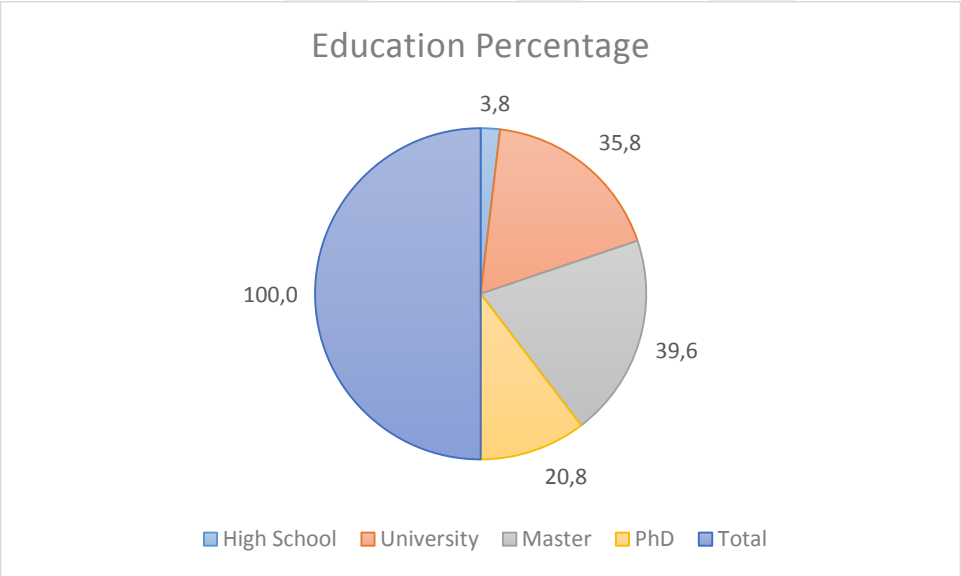


Figure 5.3: Educational distribution of the participants

It is observed that 50.9% of the participants are public representatives, 32.1% of the participants are from private sector, 15.1% of the participants are from University, and 1.9% of the participants are unemployed or retired (see Table 5.4 & Figure 5.4).

Table 5.4 Sector Frequency

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Public	27	50,9	50,9	50,9
	Private	17	32,1	32,1	83,0
	University	8	15,1	15,1	98,1
	Unemployed	1	1,9	1,9	100,0
	Total	53	100,0	100,0	

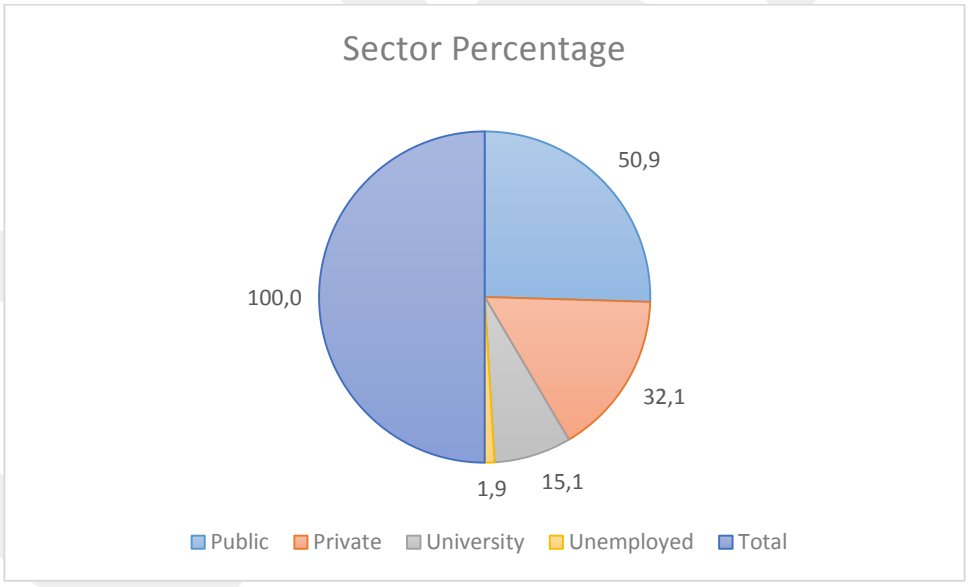


Figure 5.4: Sectorial distribution of the participants

From occupations' point of view, IT software employee, Academic, and Project Management are dominant among participants with 15.1%. Also, there are other jobs that participants (35.8%) describe by selecting the other option and entering text field (see Table 5.5 & Figure 5.5).

Table 5.5 Occupation Frequency

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	IT Manager	4	7,5	7,7	7,7
	IT Software Employee	8	15,1	15,4	23,1
	IT Hardware Employee	3	5,7	5,8	28,8
	Academic	8	15,1	15,4	44,2
	Sales and Marketing	2	3,8	3,8	48,1
	Project Management	8	15,1	15,4	63,5
	Other	19	35,8	36,5	100,0
	Total	52	98,1	100,0	
Missing	System	1	1,9		
Total		53	100,0		

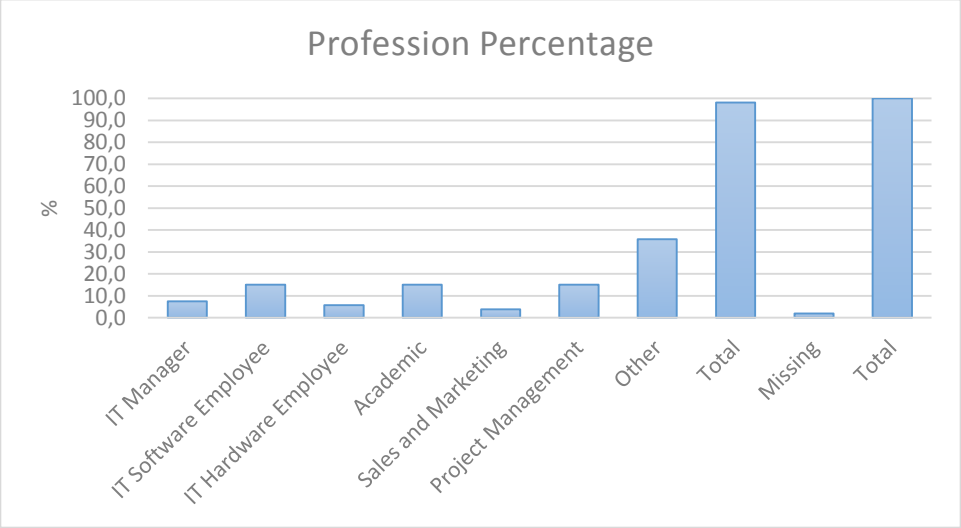


Figure 5.5: Occupational distribution of the participants

During the detailed evaluation, the generated hypotheses are based on a statistically significant difference as mentioned in the Research Methodology chapter (Chapter 4) of this thesis. Statistical significance is often employed in many survey analysis and is defined as following [52].

"Statistical significance is the low probability of obtaining at least as extreme results given that the null hypothesis is true. It is an integral part of statistical hypothesis testing where it helps investigators to decide if a null hypothesis can be rejected. These tests are used to determine whether the outcome of a study would lead to a rejection of the null hypothesis based on a pre-specified low probability threshold called p-values, which can help an investigator to decide if a result contains sufficient information to cast doubt on the null hypothesis. P-values are often coupled to a significance or alpha (α) level, which is also set ahead of time, usually at 0.05 (5%). Thus, if a p-value was found to be less than 0.05, then the result would be considered statistically significant and the null hypothesis would be rejected."

In IBM SPSS Statistics 20 statistical analysis tool variable names is given due to their respective coding equivalents. They are listed as follows:

- Q13a: Authentication necessity in Infrastructure as a Service.
- Q14a: Authentication necessity in Platform as a Service.
- Q15a: Authentication necessity in Software as a Service.
- Q13b: Access Control necessity in Infrastructure as a Service.
- Q14b: Access Control necessity in Platform as a Service.
- Q15b: Access Control necessity in Software as a Service.
- Q13c: Data Confidentiality necessity in Infrastructure as a Service.
- Q14c: Data Confidentiality necessity in Platform as a Service.
- Q15c: Data Confidentiality necessity in Software as a Service.
- Q13d: Data Integrity necessity in Infrastructure as a Service.
- Q14d: Data Integrity necessity in Platform as a Service.
- Q15d: Data Integrity necessity in Software as a Service.
- Q13e: Nonrepudiation necessity in Infrastructure as a Service.
- Q14e: Nonrepudiation necessity in Platform as a Service.

- Q15e: Nonrepudiation necessity in Software as a Service.
- Q10r1: 1 = "Public Cloud"; 2 = "Private/Hybrid Cloud".
- Q10r2: 1 = "Public/Private Cloud"; 2 = "Hybrid Cloud".
- Q10r3: 1 = "Public/Hybrid Cloud"; 2 = "Private Cloud".
- Q10r4: 1 = "Public/Private/Hybrid Cloud"; 4 = "I do not use cloud services".

The hypotheses (from H1 to H12) and their propositions are as follows:

- H1: There is a positive, significant and strong correlation between the necessity of authentication and the necessity of access control in Infrastructure as a Service.
- H2: There is a positive, significant and strong correlation between the necessity of authentication and the necessity of access control in Platform as a Service.
- H3: There is a positive, significant and strong correlation between the necessity of authentication and the necessity of access control in Software as a Service.
- H4: There is a statistically significant difference between Public Cloud users and other cloud users for the necessity of nonrepudiation in Infrastructure as a Service.
- H5: There is a statistically significant difference between Public Cloud users and other cloud users for the necessity of access control in Platform as a Service.
- H6: There is a statistically significant difference between Public Cloud users and other cloud users for the necessity of data confidentiality in Platform as a Service.
- H7: There is a statistically significant difference between Hybrid Cloud users and other cloud users for the necessity of data integrity in Software as a Service.
- H8: There is a statistically difference between Private Cloud users and other cloud users for the necessity of data integrity in Software as a Service.
- H9: There is a statistically difference between non-cloud users and cloud users for the necessity of data confidentiality in Infrastructure as a Service.
- H10: There is a statistically difference between non-cloud users and cloud users for the necessity of access control in Platform as a Service.

- H11: There is a statistically difference between non-cloud users and cloud users for the necessity of authentication in Software as a Service.
- H12: There is a statistically difference between non-cloud users and cloud users for the necessity of access control in Software as a Service.

For hypotheses #1, #2, and #3, an exploration of the linear relationship between two variables is needed, such as authentication and access control in IaaS (Q13a and Q13b). Q14a and Q14b represents same variables in PaaS. Q15a and Q15b are SaaS representations. Therefore, Pearson Correlation is selected to perform a correlational analysis with 2-Tailed value that is useful to tell if there is a statistically significant correlation between two variables. Also, statistical significance is tested in two directions by this approach (Table 5.6, Table 5.7, and Table 5.8).

When Pearson's Correlation coefficient is applied to a sample, it is commonly represented by the letter r [53].

Table 5.6 Correlations in IaaS

		Q13a	Q13b	Q13c	Q13d	Q13e
Q13a	**Pearson Correlation**	1	,850**	,844**	,750**	,525**
	Sig. (2-tailed)		,000	,000	,000	,000
	N	53	53	53	53	53
Q13b	**Pearson Correlation**	,850**	1	,809**	,721**	,480**
	Sig. (2-tailed)	,000		,000	,000	,000
	N	53	53	53	53	53
Q13c	**Pearson Correlation**	,844**	,809**	1	,795**	,566**
	Sig. (2-tailed)	,000	,000		,000	,000
	N	53	53	53	53	53
Q13d	**Pearson Correlation**	,750**	,721**	,795**	1	,635**
	Sig. (2-tailed)	,000	,000	,000		,000
	N	53	53	53	53	53
Q13e	**Pearson Correlation**	,525**	,480**	,566**	,635**	1
	Sig. (2-tailed)	,000	,000	,000	,000	
	N	53	53	53	53	53

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

Table 5.7 Correlations in PaaS

		Q14a	Q14b	Q14c	Q14d	Q14e
Q14a	**Pearson Correlation**	1	,819**	,715**	,656**	,518**
	Sig. (2-tailed)		,000	,000	,000	,000
	N	53	53	53	53	53
Q14b	**Pearson Correlation**	,819**	1	,672**	,591**	,554**
	Sig. (2-tailed)	,000		,000	,000	,000
	N	53	53	53	53	53
Q14c	**Pearson Correlation**	,715**	,672**	1	,777**	,543**
	Sig. (2-tailed)	,000	,000		,000	,000
	N	53	53	53	53	53
Q14d	**Pearson Correlation**	,656**	,591**	,777**	1	,526**
	Sig. (2-tailed)	,000	,000	,000		,000
	N	53	53	53	53	53
Q14e	**Pearson Correlation**	,518**	,554**	,543**	,526**	1
	Sig. (2-tailed)	,000	,000	,000	,000	
	N	53	53	53	53	53

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

Table 5.8 Correlations in SaaS

		Q15a	Q15b	Q15c	Q15d	Q15e
Q15a	**Pearson Correlation**	1	,903**	,591**	,514**	,318*
	Sig. (2-tailed)		,000	,000	,000	,020
	N	53	53	53	53	53
Q15b	**Pearson Correlation**	,903**	1	,678**	,523**	,251
	Sig. (2-tailed)	,000		,000	,000	,070
	N	53	53	53	53	53
Q15c	**Pearson Correlation**	,591**	,678**	1	,743**	,291*
	Sig. (2-tailed)	,000	,000		,000	,034
	N	53	53	53	53	53
Q15d	**Pearson Correlation**	,514**	,523**	,743**	1	,390**
	Sig. (2-tailed)	,000	,000	,000		,004
	N	53	53	53	53	53
Q15e	**Pearson Correlation**	,318*	,251	,291*	,390**	1
	Sig. (2-tailed)	,020	,070	,034	,004	
	N	53	53	53	53	53

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

- For H1, r and p values are: r = 0.850; p = 0.000 and p < 0.01

  This hypothesis (H1) is accepted.

- For H2, r and p values are: r = 0.819; p = 0.000 and p < 0.01

  This hypothesis (H2) is accepted.

- For H3, r and p values are: r = 0.903; p = 0.000 and p < 0.01

  This hypothesis (H3) is accepted.

For hypotheses #4, #5, and #6, public and other cloud users are differentiated into two groups by the help of variable Q10r1 (Table 5.9). Comparing means between these groups is the motivation factor to understand any significant difference. Therefore, the one-way Analysis of Variance (One-way ANOVA) is applied to examine equality of population means for a quantitative outcome (Table 5.10).

Separation of cloud users into two groups is important because of the nature of this technique. When there are two means to compare, the t-test and the F-test applied under One-way ANOVA are equivalent (F column in the following tables represents the ratio of two groups' variances). Variance is used to measure how far a set of number is spread out. Also, standard deviation can be used for measurement which is the square root of the variance.

Table 5.9 Public Cloud Users versus Other Cloud Users

		N	Mean	Std. Deviation
Q13a	**Public Cloud**	17	4,59	,870
	Private/Hybrid Cloud	25	4,68	,748
	Total	42	4,64	,791
Q13b	**Public Cloud**	17	4,53	,800
	Private/Hybrid Cloud	25	4,80	,500
	Total	42	4,69	,643
Q13c	**Public Cloud**	17	4,71	,686
	Private/Hybrid Cloud	25	4,92	,277
	Total	42	4,83	,490
Q13d	**Public Cloud**	17	4,35	,786
	Private/Hybrid Cloud	25	4,56	,821
	Total	42	4,48	,804
Q13e	**Public Cloud**	17	4,00	1,225
	Private/Hybrid Cloud	25	4,64	,700
	Total	42	4,38	,987
Q14a	**Public Cloud**	17	4,59	,795
	Private/Hybrid Cloud	25	4,68	,690
	Total	42	4,64	,727
Q14b	**Public Cloud**	17	4,53	,624
	Private/Hybrid Cloud	25	4,96	,200
	Total	42	4,79	,470
Q14c	**Public Cloud**	17	4,53	,624
	Private/Hybrid Cloud	25	4,92	,400
	Total	42	4,76	,532
Q14d	**Public Cloud**	17	4,65	,493
	Private/Hybrid Cloud	25	4,64	,700
	Total	42	4,64	,618
Q14e	**Public Cloud**	17	4,18	1,131
	Private/Hybrid Cloud	25	4,60	,645
	Total	42	4,43	,887
Q15a	**Public Cloud**	17	4,88	,332
	Private/Hybrid Cloud	25	4,80	,577
	Total	42	4,83	,490

Table 5.9 (cont.)

Q15b	**Public Cloud**	17	4,65	,606
	Private/Hybrid Cloud	25	4,80	,645
	Total	42	4,74	,627
Q15c	**Public Cloud**	17	4,76	,437
	Private/Hybrid Cloud	25	4,80	,500
	Total	42	4,79	,470
Q15d	**Public Cloud**	17	4,59	,618
	Private/Hybrid Cloud	25	4,68	,627
	Total	42	4,64	,618
Q15e	**Public Cloud**	17	4,35	1,057
	Private/Hybrid Cloud	25	4,48	,823
	Total	42	4,43	,914

Table 5.10 ANOVA Results of Table 5.9

		F	**Sig.**
Q13a	**Between Groups**	,133	,717
Q13b	**Between Groups**	1,825	,184
Q13c	**Between Groups**	1,981	,167
Q13d	**Between Groups**	,666	,419
Q13e	**Between Groups**	4,636	,037
Q14a	**Between Groups**	,158	,693
Q14b	**Between Groups**	10,430	,002
Q14c	**Between Groups**	6,129	,018
Q14d	**Between Groups**	,001	,972
Q14e	**Between Groups**	2,383	,131
Q15a	**Between Groups**	,281	,599
Q15b	**Between Groups**	,596	,445
Q15c	**Between Groups**	,056	,815
Q15d	**Between Groups**	,219	,642
Q15e	**Between Groups**	,192	,664

- For H4, F and p values are: F = 4.636; p = 0.037 and $p < 0.05$

  This hypothesis (H4) is accepted.

  Mean (Public Cloud Users): 4.00; Mean (Private/Hybrid Cloud Users): 4.64

- For H5, F and p values are: F = 10.430; p = 0.002 and $p < 0.01$

  This hypothesis (H5) is accepted.

  Mean (Public Cloud Users): 4.53; Mean (Private/Hybrid Cloud Users): 4.96

- For H6, F and p values are: F = 6.129; p = 0.018 and p < 0.05

  This hypothesis (H6) is accepted.

  Mean (Public Cloud Users): 4.53; Mean (Private/Hybrid Cloud Users): 4.92

For hypothesis #7, hybrid and other cloud users are differentiated into two groups by the help of variable Q10r2 (Table 5.11). One-way ANOVA is applied to examine equality of population means for a quantitative outcome (Table 5.12).

Table 5.11 Hybrid Cloud Users versus Other Cloud Users

		N	Mean	Std. Deviation
Q13a	**Public/Private Cloud**	32	4,63	,833
	Hybrid Cloud	10	4,70	,675
	Total	42	4,64	,791
Q13b	**Public/Private Cloud**	32	4,72	,634
	Hybrid Cloud	10	4,60	,699
	Total	42	4,69	,643
Q13c	**Public/Private Cloud**	32	4,78	,553
	Hybrid Cloud	10	5,00	0,000
	Total	42	4,83	,490
Q13d	**Public/Private Cloud**	32	4,44	,840
	Hybrid Cloud	10	4,60	,699
	Total	42	4,48	,804
Q13e	**Public/Private Cloud**	32	4,25	1,078
	Hybrid Cloud	10	4,80	,422
	Total	42	4,38	,987
Q14a	**Public/Private Cloud**	32	4,63	,793
	Hybrid Cloud	10	4,70	,483
	Total	42	4,64	,727
Q14b	**Public/Private Cloud**	32	4,72	,523
	Hybrid Cloud	10	5,00	0,000
	Total	42	4,79	,470
Q14c	**Public/Private Cloud**	32	4,69	,592
	Hybrid Cloud	10	5,00	0,000
	Total	42	4,76	,532
Q14d	**Public/Private Cloud**	32	4,66	,602
	Hybrid Cloud	10	4,60	,699
	Total	42	4,64	,618

Table 5.11 (cont.)

Q14e	**Public/Private Cloud**	32	4,34	,971
	Hybrid Cloud	10	4,70	,483
	Total	42	4,43	,887
Q15a	**Public/Private Cloud**	32	4,81	,535
	Hybrid Cloud	10	4,90	,316
	Total	42	4,83	,490
Q15b	**Public/Private Cloud**	32	4,69	,693
	Hybrid Cloud	10	4,90	,316
	Total	42	4,74	,627
Q15c	**Public/Private Cloud**	32	4,81	,397
	Hybrid Cloud	10	4,70	,675
	Total	42	4,79	,470
Q15d	**Public/Private Cloud**	32	4,75	,508
	Hybrid Cloud	10	4,30	,823
	Total	42	4,64	,618
Q15e	**Public/Private Cloud**	32	4,47	,915
	Hybrid Cloud	10	4,30	,949
	Total	42	4,43	,914

Table 5.12 ANOVA Results of Table 5.11

		F	**Sig.**
Q13a	**Between Groups**	,067	,797
Q13b	**Between Groups**	,255	,617
Q13c	**Between Groups**	1,540	,222
Q13d	**Between Groups**	,306	,583
Q13e	**Between Groups**	2,452	,125
Q14a	**Between Groups**	,079	,780
Q14b	**Between Groups**	2,847	,099
Q14c	**Between Groups**	2,737	,106
Q14d	**Between Groups**	,062	,805
Q14e	**Between Groups**	1,235	,273
Q15a	**Between Groups**	,239	,628
Q15b	**Between Groups**	,872	,356
Q15c	**Between Groups**	,430	,516
Q15d	**Between Groups**	4,377	,043
Q15e	**Between Groups**	,255	,617

- For H7, F and p values are: F = 4.377; p = 0.043 and p < 0.05

  This hypothesis (H7) is accepted.

  Mean (Hybrid Cloud Users): 4.30; Mean (Public/Private Cloud Users): 4.75

For hypothesis #8, private and other cloud users are differentiated into two groups by the help of variable Q10r3 (Table 5.13). One-way ANOVA is applied to examine equality of population means for a quantitative outcome (Table 5.14).

Table 5.13 Private Cloud Users versus Other Cloud Users

		N	Mean	Std. Deviation
Q13a	**Public/Hybrid Cloud**	27	4,63	,792
	Private Cloud	15	4,67	,816
	Total	42	4,64	,791
Q13b	**Public/Hybrid Cloud**	27	4,56	,751
	Private Cloud	15	4,93	,258
	Total	42	4,69	,643
Q13c	**Public/Hybrid Cloud**	27	4,81	,557
	Private Cloud	15	4,87	,352
	Total	42	4,83	,490
Q13d	**Public/Hybrid Cloud**	27	4,44	,751
	Private Cloud	15	4,53	,915
	Total	42	4,48	,804
Q13e	**Public/Hybrid Cloud**	27	4,30	1,068
	Private Cloud	15	4,53	,834
	Total	42	4,38	,987
Q14a	**Public/Hybrid Cloud**	27	4,63	,688
	Private Cloud	15	4,67	,816
	Total	42	4,64	,727
Q14b	**Public/Hybrid Cloud**	27	4,70	,542
	Private Cloud	15	4,93	,258
	Total	42	4,79	,470
Q14c	**Public/Hybrid Cloud**	27	4,70	,542
	Private Cloud	15	4,87	,516
	Total	42	4,76	,532
Q14d	**Public/Hybrid Cloud**	27	4,63	,565
	Private Cloud	15	4,67	,724
	Total	42	4,64	,618
Q14e	**Public/Hybrid Cloud**	27	4,37	,967
	Private Cloud	15	4,53	,743
	Total	42	4,43	,887
Q15a	**Public/Hybrid Cloud**	27	4,89	,320
	Private Cloud	15	4,73	,704
	Total	42	4,83	,490

Table 5.13 (cont.)

Q15b	**Public/Hybrid Cloud**	27	4,74	,526
	Private Cloud	15	4,73	,799
	Total	42	4,74	,627
Q15c	**Public/Hybrid Cloud**	27	4,74	,526
	Private Cloud	15	4,87	,352
	Total	42	4,79	,470
Q15d	**Public/Hybrid Cloud**	27	4,48	,700
	Private Cloud	15	4,93	,258
	Total	42	4,64	,618
Q15e	**Public/Hybrid Cloud**	27	4,33	1,000
	Private Cloud	15	4,60	,737
	Total	42	4,43	,914

Table 5.14 ANOVA Results of Table 5.13

		F	**Sig.**
Q13a	**Between Groups**	,021	,886
Q13b	**Between Groups**	3,529	,068
Q13c	**Between Groups**	,106	,747
Q13d	**Between Groups**	,115	,736
Q13e	**Between Groups**	,551	,462
Q14a	**Between Groups**	,024	,877
Q14b	**Between Groups**	2,375	,131
Q14c	**Between Groups**	,901	,348
Q14d	**Between Groups**	,034	,855
Q14e	**Between Groups**	,320	,575
Q15a	**Between Groups**	,972	,330
Q15b	**Between Groups**	,001	,971
Q15c	**Between Groups**	,686	,413
Q15d	**Between Groups**	5,759	,021
Q15e	**Between Groups**	,816	,372

- For H8, F and p values are: F = 5.759; p = 0.021 and p < 0.05

  This hypothesis (H8) is accepted.

  Mean (Private Cloud Users): 4.93; Mean (Public/Hybrid Cloud Users): 4.48

For hypotheses #9, #10, #11, and #12, the participants who do not use cloud services and the participants who use one type of cloud (public, private, hybrid) are differentiated into two groups by the help of variable Q10r4 (Table 5.15). Again, One-

way ANOVA is applied to examine equality of population means for a quantitative outcome (Table 5.16).

Table 5.15 Non-Cloud Users versus Cloud Users

		N	Mean	Std. Deviation
Q13a	**Public/Private/Hybrid Cloud**	42	4,64	,791
	I do not use cloud services	11	4,27	1,618
	Total	53	4,57	1,010
Q13b	**Public/Private/Hybrid Cloud**	42	4,69	,643
	I do not use cloud services	11	4,18	1,601
	Total	53	4,58	,929
Q13c	**Public/Private/Hybrid Cloud**	42	4,83	,490
	I do not use cloud services	11	4,09	1,640
	Total	53	4,68	,894
Q13d	**Public/Private/Hybrid Cloud**	42	4,48	,804
	I do not use cloud services	11	4,09	1,446
	Total	53	4,40	,968
Q13e	**Public/Private/Hybrid Cloud**	42	4,38	,987
	I do not use cloud services	11	4,36	1,120
	Total	53	4,38	1,004
Q14a	**Public/Private/Hybrid Cloud**	42	4,64	,727
	I do not use cloud services	11	4,00	1,732
	Total	53	4,51	1,031
Q14b	**Public/Private/Hybrid Cloud**	42	4,79	,470
	I do not use cloud services	11	3,91	1,700
	Total	53	4,60	,927
Q14c	**Public/Private/Hybrid Cloud**	42	4,76	,532
	I do not use cloud services	11	4,18	1,601
	Total	53	4,64	,879
Q14d	**Public/Private/Hybrid Cloud**	42	4,64	,618
	I do not use cloud services	11	4,09	1,375
	Total	53	4,53	,846

Table 5.15 (cont.)

Q14e	**Public/Private/Hybrid Cloud**	42	4,43	,887
	I do not use cloud services	11	4,27	1,191
	Total	53	4,40	,947
Q15a	**Public/Private/Hybrid Cloud**	42	4,83	,490
	I do not use cloud services	11	4,00	1,732
	Total	53	4,66	,939
Q15b	**Public/Private/Hybrid Cloud**	42	4,74	,627
	I do not use cloud services	11	3,91	1,868
	Total	53	4,57	1,047
Q15c	**Public/Private/Hybrid Cloud**	42	4,79	,470
	I do not use cloud services	11	4,45	1,214
	Total	53	4,72	,690
Q15d	**Public/Private/Hybrid Cloud**	42	4,64	,618
	I do not use cloud services	11	4,27	1,421
	Total	53	4,57	,844
Q15e	**Public/Private/Hybrid Cloud**	42	4,43	,914
	I do not use cloud services	11	4,64	,674
	Total	53	4,47	,868

Table 5.16 ANOVA Results of Table 5.15

		F	**Sig.**
Q13a	**Between Groups**	1,175	,283
Q13b	**Between Groups**	2,699	,107
Q13c	**Between Groups**	6,669	,013
Q13d	**Between Groups**	1,393	,243
Q13e	**Between Groups**	,003	,960
Q14a	**Between Groups**	3,558	,065
Q14b	**Between Groups**	8,995	,004
Q14c	**Between Groups**	4,015	,050
Q14d	**Between Groups**	3,920	,053
Q14e	**Between Groups**	,232	,632
Q15a	**Between Groups**	7,750	,008
Q15b	**Between Groups**	5,987	,018
Q15c	**Between Groups**	2,049	,158
Q15d	**Between Groups**	1,700	,198
Q15e	**Between Groups**	,494	,485

- For H9, F and p values are: F = 6.669; p = 0.013 and p < 0.05

  This hypothesis (H9) is accepted.

  Mean (Cloud Users): 4.83; Mean (Non-Cloud Users): 4.09

- For H10, F and p values are: F = 8.995; p = 0.004 and p < 0.01

  This hypothesis (H10) is accepted.

  Mean (Cloud Users): 4.79; Mean (Non-Cloud Users): 3.91

- For H11, F and p values are: F = 7.750; p = 0.008 and p < 0.01

  This hypothesis (H11) is accepted.

  Mean (Cloud Users): 4.83; Mean (Non-Cloud Users): 4.00

- For H12, F and p values are: F = 5.987; p = 0.018 and p < 0.05

  This hypothesis (H12) is accepted.

  Mean (Cloud Users): 4.74; Mean (Non-Cloud Users): 3.91

One of the initial goals for this thesis is to provide a priority analysis inside X.800 Recommendation elements which are authentication, access control, data confidentiality, data integrity, and nonrepudiation. According to Tables 5.17, 5.18, and 5.19, participants find all these security requirements a must without distinction of cloud service models (IaaS, PaaS, SaaS) or cloud deployment models (Public, Private, Hybrid). Therefore, creating a suggestion table listing which security requirements are must and which are optional for different cloud service models and cloud deployment models is not possible at this stage because of comparable and high order means (minimum 4.38, maximum 4.72) which are calculated from the Likert scale questions; question #13, question #14, and question #15.

Table 5.17 Question #13 Statistics

		Q13a	Q13b	Q13c	Q13d	Q13e
N	Valid	53	53	53	53	53
	Missing	0	0	0	0	0
Mean		4,57	4,58	4,68	4,40	4,38
Median		5,00	5,00	5,00	5,00	5,00
Mode		5	5	5	5	5
Std. Deviation		1,010	,929	,894	,968	1,004
Variance		1,020	,863	,799	,936	1,009

Table 5.18 Question #14 Statistics

		Q14a	Q14b	Q14c	Q14d	Q14e
N	Valid	53	53	53	53	53
	Missing	0	0	0	0	0
Mean		4,51	4,60	4,64	4,53	4,40
Median		5,00	5,00	5,00	5,00	5,00
Mode		5	5	5	5	5
Std. Deviation		1,031	,927	,879	,846	,947
Variance		1,062	,859	,773	,716	,898

Table 5.19 Question #15 Statistics

		Q15a	Q15b	Q15c	Q15d	Q15e
N	Valid	53	53	53	53	53
	Missing	0	0	0	0	0
Mean		4,66	4,57	4,72	4,57	4,47
Median		5,00	5,00	5,00	5,00	5,00
Mode		5	5	5	5	5
Std. Deviation		,939	1,047	,690	,844	,868
Variance		,882	1,097	,476	,712	,754

The hypotheses formulated so far, the p-values, and the analysis techniques are summarized in Table 5.20 at the end of this section.

Table 5.20 Summary for Formulated Hypotheses

	Analysis Technique	p-value
H1	Pearson Correlation with 2-Tailed	0.000
H2	Pearson Correlation with 2-Tailed	0.000
H3	Pearson Correlation with 2-Tailed	0.000
H4	One-way ANOVA	0.037
H5	One-way ANOVA	0.002
H6	One-way ANOVA	0.018
H7	One-way ANOVA	0.043
H8	One-way ANOVA	0.021
H9	One-way ANOVA	0.013
H10	One-way ANOVA	0.004
H11	One-way ANOVA	0.008
H12	One-way ANOVA	0.018

5.2. Discussion

Our results provide evidence of the importance given to security service categories of X.800 Recommendation. While some of our results confirm correlation between these security service categories in different cloud service delivery models other results highlight statistically significant difference between various cloud users (e.g. Public versus Private/Hybrid) and also between cloud users and non-cloud users.

If we look at the first three hypothesis, we see that a positive correlation between the necessity of authentication and the necessity of access control in IaaS, PaaS, and SaaS. This correlation suggests a linear relationship between these necessities which means the participants who select high necessity of authentication also select high necessity of access control. There can be many reason behind such a relationship. Today more and more technical solution approaches are proposed for cloud computing security and may be some of them focused on authentication and access control duo as a solution alternative. As we evaluated in Chapter 2 of this thesis, Security Access Control Service [14] is such an example. Even though the participants have general knowledge

about security, may be differentiating these two security service categories was a challenging task for participants and both of them may be selected with high necessity degree is another possibility. During our research we found that authentication is handled together with access control under Section 11 in the ISO/IEC 27002:2005 outline [54] which indicates a correlation footprint to our findings.

In hypotheses #4, #5, and #6, we observe a statistically significant difference between public cloud users and other cloud users (private/hybrid users) for the necessity of nonrepudiation in IaaS, the necessity of access control in PaaS, and the necessity of data confidentiality in PaaS respectively. According to our analysis, other cloud users find the necessity of nonrepudiation in IaaS more than public users with 0.64 mean difference in hypothesis #4. Same direction is observed in hypothesis #5 and hypothesis #6 with 0.43 and 0.39 mean difference respectively. In hypotheses #7, there is a statistically significant difference between hybrid cloud users and other cloud users (public/private users) for the necessity of data integrity in SaaS. Other cloud users find the necessity of data integrity in SaaS more than hybrid users with 0.45 mean difference. Also, a statistically significant difference is observed for the same X.800 Recommendation security service category and cloud service delivery model between private cloud users and other cloud users (public/hybrid users) in hypothesis #8. Up to now, none of the separated cloud users group transcends other cloud users group but in hypothesis #8 we see such an occurrence with 0.45 mean difference. From Figure 3.3 [47] of Chapter 3, we know that most of ICT expenditure is done in telecommunication services but we observe few representatives from telecommunication sector in the workshops. This may cause a possibility why we see such differences because of sector-specific impact on ICT market. We think that further statistical studies can gain detailed results if this stakeholder type contribution is achieved much more. Another point from Chapter 3 of this thesis which may be count as another possibility is computer and internet usage for different age groups. According to Figure 3.4, age group 16-24 has the top percentages for computer and internet usage with 63.3% and 67.1% respectively. On the other hand, our survey results show 32.1% in age group 26-33 and 28.3% in age group 34-41 as first two percentage distribution. Also, in Chapter 2 we highlighted the importance of the trust management models for the trust judgment process in cloud computing. During the

analysis of the survey results we notice that none of the participants stated services such as a broker service in the other option of cloud services used question (Q11). Therefore, without considering trust management models by participants for different cloud deployment models and cloud service delivery models may end up such differences which we have seen so far.

For hypotheses #9, #10, #11, and #12, we observe a statistically difference between non-cloud users and cloud users (public/private/hybrid users) for the necessity of data confidentiality in IaaS, the necessity of access control in PaaS, the necessity of authentication in SaaS, and the necessity of access control in SaaS respectively. According to our analysis, cloud users find the necessity of data confidentiality in IaaS more than non-cloud users with 0.74 mean difference in hypothesis #9. Same direction is observed for the hypothesis #10, hypothesis #11, and hypothesis #12 with 0.88, 0.83, and 0.83 mean difference respectively. In here, we believe that the main cause for mean difference is participant distribution. According to survey results, we have 17 public cloud user, 15 private cloud user, and 10 hybrid cloud user. The total number of cloud users become 42. On the other hand, the number of non-cloud users is 11.

Based on our findings, we made comparisons of the necessity of X.800 Recommendation security service categories between different cloud users or between cloud users and non-cloud users. However, statistically this does not mean one X.800 Recommendation security service category is more necessary than other because of comparable and high order mean values. Also, participant distribution is another major factor for this as we seen in hypotheses #9, #10, #11, and #12.

In addition to evaluated technical solution proposals in Chapter 2, there are other studies which highlight one or more X.800 Recommendation security service category for different cloud deployment models and cloud service delivery models, [55] is such an example. In their study, Gharat and Motwani underline the increasing demand for data security in hybrid models. As a matter of fact, we found 4.30 mean in hybrid cloud users for the necessity of data integrity in SaaS which indicates a relation for the hybrid user expectations from X.800 Recommendation security service categories in cloud.

CHAPTER 6

CONCLUSION AND FUTURE WORK

In this thesis, background information for cloud computing is provided with some technical solution approaches in the literature which are examined from the security perspective of cloud computing, and evaluation of these technical approaches is given according to X.800 Recommendation. Also, a number of studies in the literature have been reviewed to present standards and regulations in cloud computing area by aiming our first and second research questions which are "What are the possible technical solutions and non-technical aspects to implement or use cloud computing infrastructure by addressing the security issues?" and "What type of problems do we face considering the current regulations associated with cloud computing?". Based on our research, none of the examined technical approaches fulfill all of the X.800 Recommendation service categories. Even if all properties of X.800 Recommendation security service categories are satisfied in theory, current technology limits the daily practices, such as ineffectiveness of fully homomorphic encryption. Although technical solution approaches achieve easing on cloud computing security concerns, it seems current technological progress does not permit to embrace them as a complete solution. Therefore, we continued with the trust concept as a non-technical solution approach in cloud computing. Even though there are technical aspects inside the trust concept, such as measuring the trust, we handle the trust as a non-technical approach as well as standards and regulations. While examining non-technical side of security, we discovered more challenges, such as multi-functioned cloud computing services may be misjudged or may use regulation gaps. There is not a single standard which covers all aspects of cloud computing and working with nonstandard materials, and invisible processes are additional challenges of non-technical aspects. Cloud computing, interoperability and other recent trends make these challenges more

visible. For the trust part, a trust judgment assistance table is prepared based on the studies in the literature to gain an insight for the selection of cloud auditor, cloud broker, cloud service provider, and cloud service. Until come up to that point, definitions of trust, trust types and trust properties are given to support the understanding of trust management models. Cloud computing is also a matter of global business. Constructing a win-win system which covers various aspects of cloud computing is crucial for the future of cloud computing and security concerns. Therefore, current status of ICT sector in Turkey together with investments are given in detail to view from above. By gaining such a perspective, which sectors have influence in the ICT market is revealed. Also supervision of newly configured support programs is critical when growth rate of ICT market and strategic plans are considered in Turkey. For the further evaluation of necessity of X.800 Recommendation service categories in different cloud service models and cloud deployment models, the survey method is adopted in this thesis by aiming the third research question which is "Which security services should we use to form a more secure cloud computing platform?".

Twelve hypotheses are formulated, tested, and accepted. Three accepted hypotheses show us a positive correlation between the necessity of authentication and the necessity of access control in Infrastructure as a Service, Platform as a Service, and Software as a Service. The other nine hypotheses highlight a statistically significant difference between various cloud users and also between cloud users and non-cloud users for different cloud service models. As one of the motivation factors in this thesis, we wanted to distinguish the necessity of X.800 Recommendation service categories for different cloud service models and cloud deployment models but according to the participants, necessity of X.800 Recommendation service categories are too close to each other and all of them are considered as a must.

Future work issues are identified as follows:

- Although the participants have interest related to our study domain, the hypotheses are produced on limited dataset. We invited researchers to provide further quantitative data on the necessity of X.800 Recommendation service categories for different cloud service models and cloud deployment models: are there regional, geographical, or cultural differences, etc.

- The unexpected result of being unable to distinguish the necessity of X.800 Recommendation service categories for different cloud service models and cloud deployment models will serve as inspirations for further research to uncover any other alternative research approach.
- A study combined with our newly formulated hypotheses is planned to be initiated.
- Another area that is worth investigation is studying the effect of uncertainties in laws, and regulations which may create security concerns.

REFERENCES

[1] Sezen, A., Bostan, A., & Yazici, A. 6 [2014] "Security issues of cloud computing and alternative approaches", International Conference on Advanced Technology & Sciences Conferences, 2014.

[2] F. Gens. (2009)New IDC IT cloud services survey: Top benefits and challenges on homepage IDC eXchange. [Online]. Available: http://blogs.idc.com/ie/?p=730

[3] (2013) The NORTH BRIDGE website. [Online]. Available: http://www.northbridge.com/2013-cloud-computing-survey

[4] National information systems security (INFOSEC) glossary. (1997). Fort George G. Meade, Md.: National Security Agency.

[5] Millions hit by Monster site hack. (2007, August 24). BBC NEWS. Retrieved July 28, 2014, from http://news.bbc.co.uk/2/hi/6961880.stm

[6] Engineer accidentally deletes cloud. (2008, August 28). The Register. Retrieved August 28, 2014, from http://www.theregister.co.uk/2008/08/28/flexiscale_outage/

[7] Mansfield-Devine, S. (2008). Cloud Security: Danger in the clouds. 2008(12), Pages 9-11.

[8] Data breach demonstrates need for access control policies. (2010, August 17). NETWORKWORLD. Retrieved July 28, 2014, from http:// http://www.networkworld.com/article/2216448/security/data-breach-demonstrates-need-for-access-control-policies.html

[9] Recommendation X.800. (1991). In Security architecture for open systems interconnection for CCITT application. Geneva.

[10] W. Stallings, Cryptography and Network Security: Principles and Practice, 5th ed., Marcia Horton, Ed. New York, America: Prentice Hall, 2011.

[11] Hurwitz, J. (2010). Cloud computing for dummies (p. 9). Hoboken, NJ: Wiley Pub.

[12] Sosinsky, B. (2011). Cloud computing bible. Indianapolis, IN: Wiley;

[13] Rhoton, J. (2009). Cloud computing explained (2nd ed.). London: Recursive Press.

[14] J. Xue and J. Zhang, "A brief survey on the security model of cloud computing," Int. Symp. on Distributed Computing and Applications to Business, Engineering and Science, 2010, pp. 475-478.

[15] Homomorphic encryption. (2014, November 14). Retrieved August 28, 2014, from http://en.wikipedia.org/wiki/Homomorphic_encryption

[16] M.D.Ryan, "Cloud computing security: The scientific challenge, and a survey of solutions," The Journal of Systems and Software., vol. 86, pp. 2263–2268, Mar. 2013.

[17] Z. Shen, and Q. Tong, "The security of cloud computing system enabled by trusted computing technology," in Proc. ICSPS'10, 2010, p. V2-11-V2-15.

[18] J. Feng, Y. Chen, D. Summerville, W-S Ku, and Z. Su, "Enhancing cloud storage security against roll-back attacks with a new fair multi-party non-repudiation protocol," in Proc. IEEE CCNC'11, 2011, p. 521-522.

[19] Rajathi, A., & Saravanan, N. (2013). A Survey on Secure Storage in Cloud Computing. Indian Journal Of Science And Technology, 6(4), 4396-4401.

[20] Parakh A, and Kak S (2009). Online data storage using implicit security, Information Sciences, vol 179(19), 3323-3331.

[21] Li H, Dai Y et al. (2009), Identity-Based Authentication for Cloud Computing, M. G. Jaatun, G. Zhao, and C. Rong (Eds.): Cloud Computing, Lecture Notes in Computer Science, vol 5931, 157-166.

[22] Wang Q, Wang C et al. (2011). Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing, IEEE Transactions on Parallel and Distributed Systems, vol 22(5), 847-859.

[23] Balakrishnan S, Saranya G, et al. (2011). Introducing Effective Third Party Auditing (TPA) for Data Storage Security in Cloud, International Journal of Computer Science and Technology, vol 2(2), 397-400.

[24] Dinesh C (2011). Data Integrity and Dynamic Storage Way in Cloud Computing, Distributed, Parallel, and Cluster Computing.

[25] Kumar S P, Subramanian R (2011). An efficient and secure protocol for ensuring data storage security in Cloud Computing, International Journal of Computer Science Issues, vol 8(6), No 1, 261-274.

[26] Sajithabanu S, Raj E G P (2011). Data Storage Security in Cloud, International Journal of Computer Science and Technology, vol 2(4), 436-440

[27] Wang C, Wang Q et al. (2012), Toward Secure and Dependable Storage Services in Cloud Computing, IEEE Transactions on Services Computing, vol 5(2), 220-232.

[28] Spillner J, Müller J et al. (2012), Creating optimal cloud storage systems, Future Generation Computer Systems, vol 29(4), 1062-1072.

[29] Dong B, Zheng Q et al. (2012). An optimized approach for storing and accessing small files on cloud storage, Journal of Network and Computer Applications, 35 (6), 1847-1862.

[30] Deshmukh P M, Gughane A S et al. (2012). Maintaining File Storage Security in Cloud Computing, International Journal of Emerging Technology and Advanced Engineering, vol 2(10), 2250-2459.

[31] Wazed, K., Shekha, T., Anisul, S., & M., D. (2012). A Newer User Authentication, File encryption and Distributed Server Based Cloud Computing security architecture.International Journal of Advanced Computer Science and Applications, 3(10), 181-186.

[32] K. Popovic, and Z. Hocenski, "Cloud computing security issues and challenges," in Proc. MIPRO'10, 2010, p. 344-349.

[33] F-C. Cheng, and W-H. Lai, "The impact of cloud computing technology on legal infrastructure within internet-focusing on the protection of information privacy," Procedia Engineering., vol. 29, pp. 241–251, 2012.

[34] Somesh Kumar Prajapati, Suvamoy Changder, Anirban Sarkar, "Trust Management Model for Cloud Computing Environment", International Conference on Computing Communication and Advanced Network, India, PP 1-5, March 15-17, 2013

[35] R. Abassi, S. G. El Fatmi, "Towards A Generic Trust Management Model", 19th International Conference on Telecommunication (ICT), pp. 1 – 6, 2012.

[36] International Telecommunication Union: ITU-T Recommendation X.509, March 2000

[37] D. Gambetta, "Can We Trust Trust?" in Gambetta, Diego (ed.) Trust: Making and Breaking Cooperative Relations, electronic edition, Department of Sociology, University of Oxford, chapter 13, pp. 213-237, 2000.

[38] Huang J, Nicol D (2010) A formal-semantics-based calculus of trust. Internet Comput IEEE 14(5): 38–46. doi:10.1109/MIC.2010.83

[39] H. Zhu, B. Feng, R.H. Deng, "Computing of trust in distributed networks", http://eprint.iacr.org/2003/056, 2003.

[40] Alfarez Abdul Rahman, Stephen Hailes, "Supporting Trust in Virtual Communities". 33rd Hawaii International Conference on System Sciences, 2000.

[41] F. Azzedin, M.Maheswaran, "Towards Trust-Aware Resource Management in Grid Computing Systems", 2ndIEEE/ACM International Symposium on Cluster Computing and the Grid, pp. 452, 2002.

[42] Q. Guo, D. Sun, G. Chang, L. Sun, X. Wang. "Modeling and evaluation of trust in cloud computing environments", 3rd Intl. Conf. on Advanced Computer Control, pp. 112-116, 2011.

[43] Huang, J., & Nicol, D. (2013). Trust mechanisms for cloud computing. Journal of Cloud Computing: Advances, Systems and Applications, 9-9.

[44] Haq IU, Alnemr R, Paschke A, Schikuta E, Boley H, Meinel C (2010) Distributed trust management for validating sla choreographies. In: Wieder P, Yahyapour R, Ziegler W (eds). Grids and service-oriented architectures for service level agreements. Springer, US. pp 45–55. http://dx.doi.org/10.1007/978-1-4419-7320-7_5

[45] Pawar P, Rajarajan M, Nair S, Zisman A (2012) Trust model for optimized cloud services(Dimitrakos T, Moona R, Patel D, McKnight D, eds.). Springer, Berlin Heidelberg. pp 97–112. http://dx.doi.org/10.1007/978-3-642-29852-3_7

[46] CSA (2011) STAR (security , trust and assurance registry) program. Cloud Security Alliance. https://cloudsecurityalliance.org/star/. Accessed on 16 Aug. 2014

[47] Information & Communications Technology. (n.d.). Retrieved September 19, 2014, from http://www.invest.gov.tr/en-US/infocenter/publications/Documents/ICT.INDUSTRY.pdf

[48] YASED - International Investors Association of Turkey. (n.d.). Retrieved September 11, 2014, from http://www.yased.org.tr/webportal/English/Pages/MainPage.aspx

[49] TÜBİSAD Informatics Industry Association. (n.d.). Retrieved September 11, 2014, from http://www.tubisad.org.tr/Tr/Sayfalar/default.aspx

[50] Evaluation Report. (2013, January 1). Retrieved August 29, 2014, from http://www.tbd.org.tr/usr_img/temp/2013_TBD_Degerlendirme_Raporu.pdf

[51] Survey methodology. (2014, November 27). Retrieved November 29, 2014, from http://en.wikipedia.org/wiki/Survey_methodology

[52] Statistical significance. (2014, November 27). Retrieved November 29, 2014, from http://en.wikipedia.org/wiki/Statistical_significance

[53] Pearson product-moment correlation coefficient. (2014, November 27). Retrieved November 29, 2014, from http://en.wikipedia.org/wiki/Pearson_product-moment_correlation_coefficient

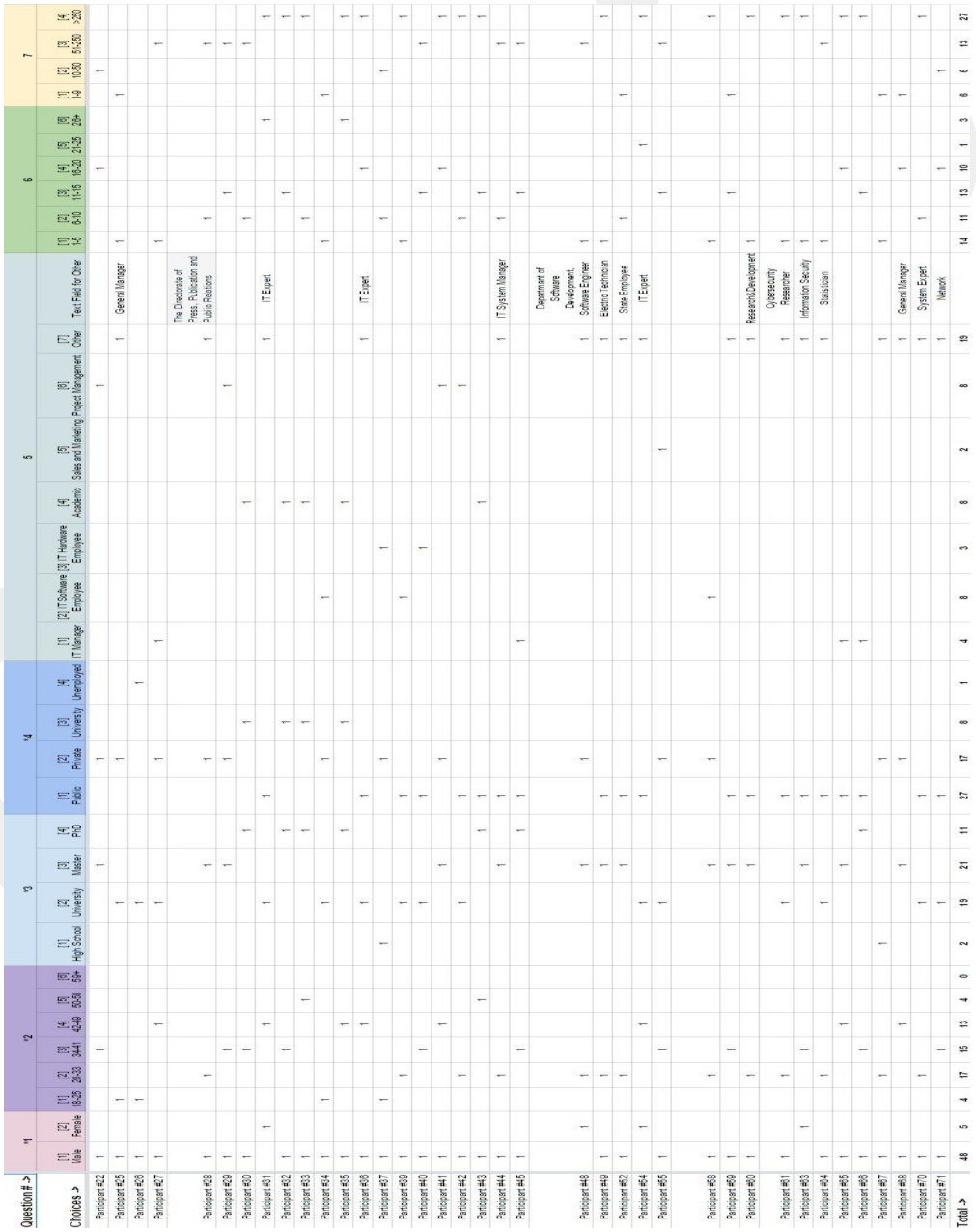
[54] ISO/IEC 27002-2005 Outline. (2007, November 28). Retrieved December 10, 2014, from http://www.docucu.com/Structure-and-contents-of-ISO/IEC-27002.doc

[55] Gharat, M.P., & Motwani, D. (2013). Survey on establishing trust, data security and authentication in hybrid cloud computing. International Journal of Engineering Research & Technology, 2-11.

[56] ICT Usage in Households and Individuals 2014. (2014, March 20). Retrieved August 29, 2014, from http://www.tuik.gov.tr/PreTablo.do?alt_id=1028

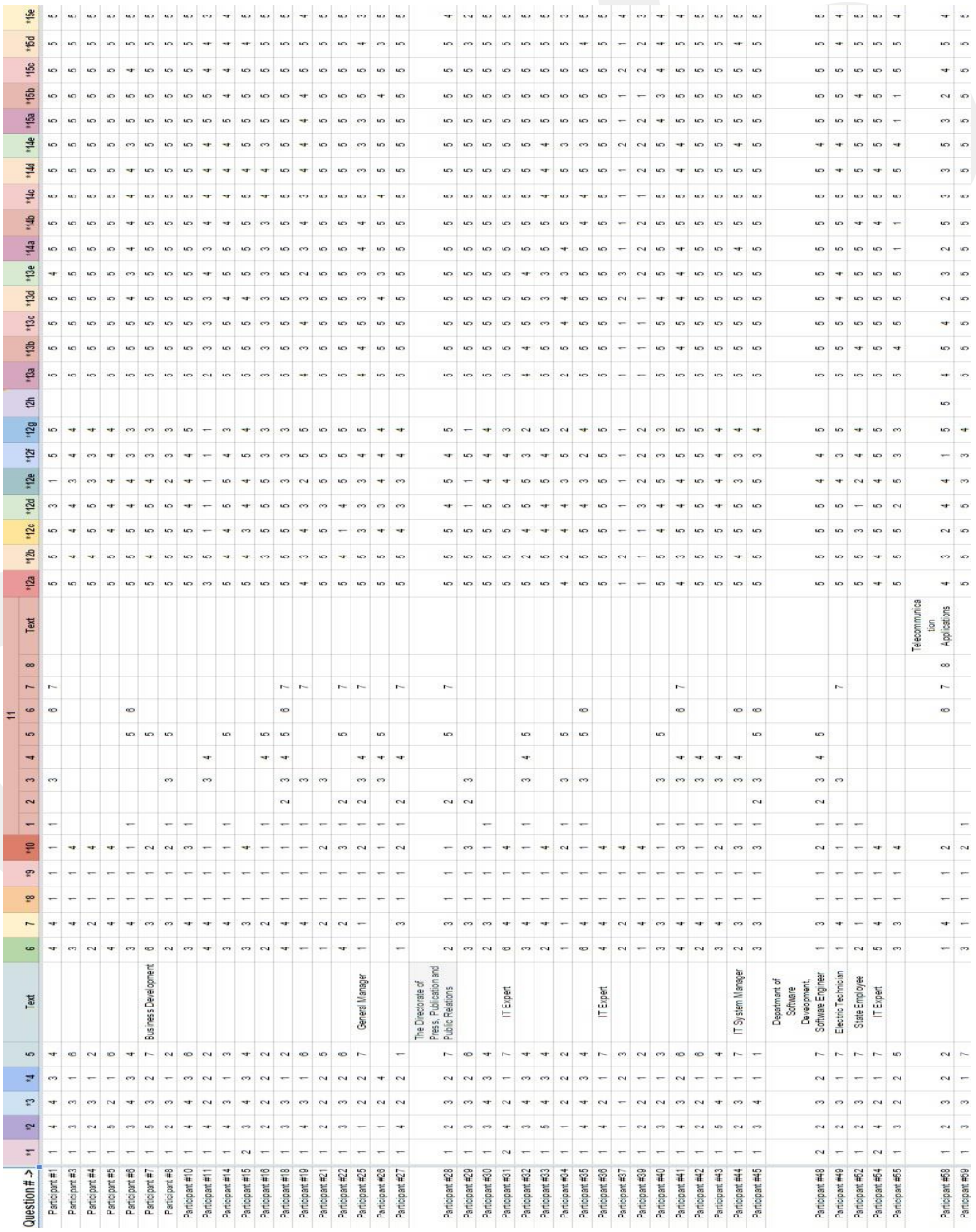
APPENDIX A

Partial presentation of the survey data (full data can be reached from https://docs.google.com/spreadsheets/d/1uh3buGfpMX6doliSJ9EHRB80GxKyvCl-FmDcwTCLS2s/edit?usp=sharing)



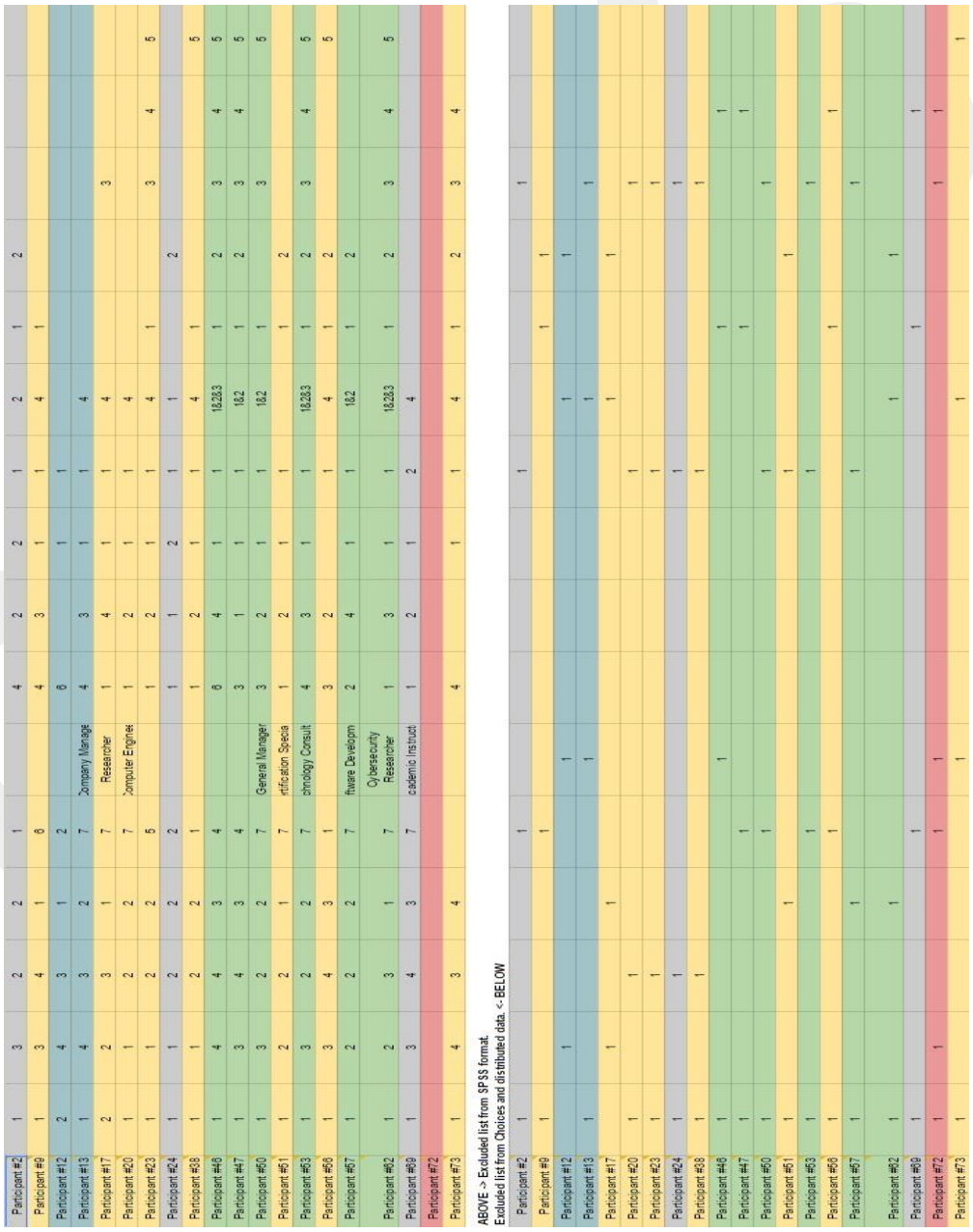
APPENDIX B

Partial presentation of the survey data in SPSS format (full data can be reached from https://docs.google.com/spreadsheets/d/1uh3buGfpMX6doliSJ9EHRB80GxKyvCl-FmDcwTCLS2s/edit?usp=sharing)



APPENDIX C

Partial presentation of the excluded list (full list can be reached from https://docs.google.com/spreadsheets/d/1uh3buGfpMX6doliSJ9EHRB80GxKyvCl-FmDcwTCLS2s/edit?usp=sharing)



APPENDIX D

Complete Form of Table 5.10

		Sum of Squares	df	Mean Square	F	Sig.
Q13a	**Between Groups**	,085	1	,085	,133	,717
	Within Groups	25,558	40	,639		
	Total	25,643	41			
Q13b	**Between Groups**	,741	1	,741	1,825	,184
	Within Groups	16,235	40	,406		
	Total	16,976	41			
Q13c	**Between Groups**	,464	1	,464	1,981	,167
	Within Groups	9,369	40	,234		
	Total	9,833	41			
Q13d	**Between Groups**	,434	1	,434	,666	,419
	Within Groups	26,042	40	,651		
	Total	26,476	41			
Q13e	**Between Groups**	4,145	1	4,145	4,636	,037
	Within Groups	35,760	40	,894		
	Total	39,905	41			
Q14a	**Between Groups**	,085	1	,085	,158	,693
	Within Groups	21,558	40	,539		
	Total	21,643	41			
Q14b	**Between Groups**	1,876	1	1,876	10,430	,002
	Within Groups	7,195	40	,180		
	Total	9,071	41			
Q14c	**Between Groups**	1,544	1	1,544	6,129	,018
	Within Groups	10,075	40	,252		
	Total	11,619	41			
Q14d	**Between Groups**	,001	1	,001	,001	,972
	Within Groups	15,642	40	,391		
	Total	15,643	41			
Q14e	**Between Groups**	1,815	1	1,815	2,383	,131
	Within Groups	30,471	40	,762		
	Total	32,286	41			
Q15a	**Between Groups**	,069	1	,069	,281	,599
	Within Groups	9,765	40	,244		
	Total	9,833	41			

Table 5.10 (cont.)

Q15b	**Between Groups**	,237	1	,237	,596	,445
	Within Groups	15,882	40	,397		
	Total	16,119	41			
Q15c	**Between Groups**	,013	1	,013	,056	,815
	Within Groups	9,059	40	,226		
	Total	9,071	41			
Q15d	**Between Groups**	,085	1	,085	,219	,642
	Within Groups	15,558	40	,389		
	Total	15,643	41			
Q15e	**Between Groups**	,163	1	,163	,192	,664
	Within Groups	34,122	40	,853		
	Total	34,286	41			

Complete Form of Table 5.12

		Sum of Squares	**df**	**Mean Square**	**F**	**Sig.**
Q13a	**Between Groups**	,043	1	,043	,067	,797
	Within Groups	25,600	40	,640		
	Total	25,643	41			
Q13b	**Between Groups**	,107	1	,107	,255	,617
	Within Groups	16,869	40	,422		
	Total	16,976	41			
Q13c	**Between Groups**	,365	1	,365	1,540	,222
	Within Groups	9,469	40	,237		
	Total	9,833	41			
Q13d	**Between Groups**	,201	1	,201	,306	,583
	Within Groups	26,275	40	,657		
	Total	26,476	41			
Q13e	**Between Groups**	2,305	1	2,305	2,452	,125
	Within Groups	37,600	40	,940		
	Total	39,905	41			
Q14a	**Between Groups**	,043	1	,043	,079	,780
	Within Groups	21,600	40	,540		
	Total	21,643	41			
Q14b	**Between Groups**	,603	1	,603	2,847	,099
	Within Groups	8,469	40	,212		
	Total	9,071	41			
Q14c	**Between Groups**	,744	1	,744	2,737	,106
	Within Groups	10,875	40	,272		
	Total	11,619	41			
Q14d	**Between Groups**	,024	1	,024	,062	,805
	Within Groups	15,619	40	,390		
	Total	15,643	41			

Table 5.12 (cont.)

Q14e	**Between Groups**	,967	1	,967	1,235	,273
	Within Groups	31,319	40	,783		
	Total	32,286	41			
Q15a	**Between Groups**	,058	1	,058	,239	,628
	Within Groups	9,775	40	,244		
	Total	9,833	41			
Q15b	**Between Groups**	,344	1	,344	,872	,356
	Within Groups	15,775	40	,394		
	Total	16,119	41			
Q15c	**Between Groups**	,096	1	,096	,430	,516
	Within Groups	8,975	40	,224		
	Total	9,071	41			
Q15d	**Between Groups**	1,543	1	1,543	4,377	,043
	Within Groups	14,100	40	,353		
	Total	15,643	41			
Q15e	**Between Groups**	,217	1	,217	,255	,617
	Within Groups	34,069	40	,852		
	Total	34,286	41			

Complete Form of Table 5.14

		Sum of Squares	**df**	**Mean Square**	**F**	**Sig.**
Q13a	**Between Groups**	,013	1	,013	,021	,886
	Within Groups	25,630	40	,641		
	Total	25,643	41			
Q13b	**Between Groups**	1,376	1	1,376	3,529	,068
	Within Groups	15,600	40	,390		
	Total	16,976	41			
Q13c	**Between Groups**	,026	1	,026	,106	,747
	Within Groups	9,807	40	,245		
	Total	9,833	41			
Q13d	**Between Groups**	,076	1	,076	,115	,736
	Within Groups	26,400	40	,660		
	Total	26,476	41			
Q13e	**Between Groups**	,542	1	,542	,551	,462
	Within Groups	39,363	40	,984		
	Total	39,905	41			
Q14a	**Between Groups**	,013	1	,013	,024	,877
	Within Groups	21,630	40	,541		
	Total	21,643	41			
Q14b	**Between Groups**	,508	1	,508	2,375	,131
	Within Groups	8,563	40	,214		
	Total	9,071	41			

Table 5.14 (cont.)

Q14c	**Between Groups**	,256	1	,256	,901	,348
	Within Groups	11,363	40	,284		
	Total	11,619	41			
Q14d	**Between Groups**	,013	1	,013	,034	,855
	Within Groups	15,630	40	,391		
	Total	15,643	41			
Q14e	**Between Groups**	,256	1	,256	,320	,575
	Within Groups	32,030	40	,801		
	Total	32,286	41			
Q15a	**Between Groups**	,233	1	,233	,972	,330
	Within Groups	9,600	40	,240		
	Total	9,833	41			
Q15b	**Between Groups**	,001	1	,001	,001	,971
	Within Groups	16,119	40	,403		
	Total	16,119	41			
Q15c	**Between Groups**	,153	1	,153	,686	,413
	Within Groups	8,919	40	,223		
	Total	9,071	41			
Q15d	**Between Groups**	1,969	1	1,969	5,759	,021
	Within Groups	13,674	40	,342		
	Total	15,643	41			
Q15e	**Between Groups**	,686	1	,686	,816	,372
	Within Groups	33,600	40	,840		
	Total	34,286	41			

Complete Form of Table 5.16

		Sum of Squares	**df**	**Mean Square**	**F**	**Sig.**
Q13a	**Between Groups**	1,194	1	1,194	1,175	,283
	Within Groups	51,825	51	1,016		
	Total	53,019	52			
Q13b	**Between Groups**	2,255	1	2,255	2,699	,107
	Within Groups	42,613	51	,836		
	Total	44,868	52			
Q13c	**Between Groups**	4,805	1	4,805	6,669	,013
	Within Groups	36,742	51	,720		
	Total	41,547	52			
Q13d	**Between Groups**	1,294	1	1,294	1,393	,243
	Within Groups	47,385	51	,929		
	Total	48,679	52			
Q13e	**Between Groups**	,003	1	,003	,003	,960
	Within Groups	52,450	51	1,028		
	Total	52,453	52			

Table 5.16 (cont.)

Q14a	**Between Groups**	3,602	1	3,602	3,558	,065
	Within Groups	51,643	51	1,013		
	Total	55,245	52			
Q14b	**Between Groups**	6,699	1	6,699	8,995	,004
	Within Groups	37,981	51	,745		
	Total	44,679	52			
Q14c	**Between Groups**	2,933	1	2,933	4,015	,050
	Within Groups	37,255	51	,730		
	Total	40,189	52			
Q14d	**Between Groups**	2,656	1	2,656	3,920	,053
	Within Groups	34,552	51	,677		
	Total	37,208	52			
Q14e	**Between Groups**	,212	1	,212	,232	,632
	Within Groups	46,468	51	,911		
	Total	46,679	52			
Q15a	**Between Groups**	6,053	1	6,053	7,750	,008
	Within Groups	39,833	51	,781		
	Total	45,887	52			
Q15b	**Between Groups**	5,991	1	5,991	5,987	,018
	Within Groups	51,028	51	1,001		
	Total	57,019	52			
Q15c	**Between Groups**	,956	1	,956	2,049	,158
	Within Groups	23,799	51	,467		
	Total	24,755	52			
Q15d	**Between Groups**	1,194	1	1,194	1,700	,198
	Within Groups	35,825	51	,702		
	Total	37,019	52			
Q15e	**Between Groups**	,376	1	,376	,494	,485
	Within Groups	38,831	51	,761		
	Total	39,208	52			