

**Cloud-based Services Users and Trust Issues - A Comparative Study  
of Gender and National Culture Perspectives**

Chetan Sharma Kandel

University of Tampere  
Faculty of Natural Sciences  
Degree Programme in Software Development  
M. Sc. thesis  
Supervisor: Eleni Berki  
November 2017

University of Tampere

Faculty of Natural Sciences

Degree Programme in Software Development

Chetan Sharma Kandel: Cloud-based Services Users and Trust Issues - A Comparative Study of Gender and National Culture Perspectives

M.Sc. thesis, 50 pages, 3 appendix pages

November 2017

---

Cloud-based services are becoming increasingly popular for different purposes such as data storage, application deployment, testing and development, data backup and other such purposes which may include very sensitive and confidential data. Several articles related to cloud services have been published. However, none of them have studied cloud-based services usage and trust issues in cloud-based services from gender and national-culture perspectives. Since sensitive data are stored in the cloud services, there is risk of data theft and other such attacks. There were some serious incidents about information leakage and data theft in cloud services in recent years. Therefore, it is crucial to understand how trustworthy these services are and if not, what are the trust issues and what measures can be applied while using cloud services to secure the data in cloud.

The purpose of this thesis is to identify the trust issues in cloud services and to present the data about cloud usage, reasons for not using cloud services and security considerations while using cloud services by future information technology (IT) professionals in five countries, namely, China, Finland, Greece, Nepal and UK from gender and national culture perspective. It discusses the cloud trust issues and solutions to overcome those issues. These findings would be useful for the higher-level institutions to redesign the curriculum in a way that students would be aware of cloud services, their advantages and challenges and security measures. It also presents the reasons for not using cloud services which could be useful for the cloud service providers to consider while providing services to consumers.

The future IT professionals and other cloud service users should have more Cryptography-based knowledge, which should be taught through Curricula, and that knowledge could result in cloud services and online consumers using encryption technology more, which, on the other hand, will facilitate the relationship of trust between cloud-based services and service consumers.

Key words and terms: Cloud Services, Trust, Security Issues, Cloud Users.

## **Acknowledgement**

I would like to express my gratitude and appreciation to Dr. Eleni Berki, my thesis supervisor for helping me for choosing the topic, providing the constant support and motivation and inspiring me for doing the excellent research in the topic. This work would not have been possible without her guidance. I am very much grateful to Dr. Sunil Chaudhary and Dr. Juri Valtanen for their great guidance and for showing me the right direction in my thesis work.

I would also like to sincerely thank Language Teacher, Susan Gamache, for helping me to get familiar with the academic writing rules. My sincere thanks also go to Prof. Zheyang Zhang and all the participants in “Master’s Thesis Seminar in Software Development” course for their constructive feedback and suggestions.

Chetan Sharma Kandel  
19<sup>th</sup> November 2017  
Tampere

## Table of Contents

<b>1. Introduction .....</b>	<b>1</b>
1.1 Introduction to Cloud Computing.....	1
1.2 Cloud Usage and Growth.....	3
1.3 Research Questions .....	6
1.4 Related Work .....	6
1.5 Structure of Thesis .....	7
<b>2. Methodologies .....</b>	<b>7</b>
2.1 Questionnaire Survey.....	7
2.2 Systematic Literature Review .....	10
<b>3. Data Analysis Results .....</b>	<b>11</b>
3.1 Cloud Users and Non- users by Gender.....	11
3.2 Cloud Users and Non-users by Country.....	11
3.3 Reasons for not using Cloud .....	12
3.4 Reasons for not using Cloud by Gender .....	13
3.5 Reasons for not using Cloud by Country.....	14
3.6 Considerations while using cloud services by Gender.....	15
3.6.1 Putting confidential data into cloud.....	15
3.6.2 Trusting service provider will handle data with good care.....	16
3.6.3 Encrypting data before storing into cloud.....	16
3.7 Considerations while using cloud services by Country .....	17
3.7.1 Putting confidential data into cloud.....	17
3.7.2 Trusting service provider will handle data with good care.....	18
3.7.3 Encrypting data before storing into cloud.....	19
<b>4. Literature Review Findings .....</b>	<b>20</b>
<b>5. Discussion .....</b>	<b>25</b>
<b>6. Conclusion and Recommendations.....</b>	<b>33</b>
<b>7. Further Enhancements.....</b>	<b>35</b>
<b>References.....</b>	<b>36</b>

## Appendix

## List of Figures

Figure 1: NIST Model of Cloud Computing .....	1
Figure 2: Data Collected by Country .....	8
Figure 3: Data Collected by Gender .....	9
Figure 4: Data Categorization by Country.....	10
Figure 5: Categorization of Cloud users by Country.....	11
Figure 6: Cloud Users and Non-users in five Countries.....	12
Figure 7: Reasons for not using Cloud services .....	13
Figure 8: Reasons for not using Cloud by Gender.....	14
Figure 9: Reasons for not using Cloud by Country .....	14
Figure 10: Data about putting confidential data into Cloud by Gender.....	15
Figure 11: Data about trusting service provider by Gender.....	16
Figure 12: Data about encrypting data before storing into Cloud by Gender.....	17
Figure 13: Data about putting confidential data into Cloud by Country .....	18
Figure 14: Data about trusting servic provider by Country .....	19
Figure 15: Data about encrypting data before storing into Cloud by Country.....	20
Figure 16: Trust Management Perspectives .....	23

**List of Tables**

Table 1: Worldwide Public Cloud Services Forecast (billions of dollars) .....	4
Table 2: Survey Results by Gender and Country.....	26
Table 3: National Culture Dimensions in five countries .....	28

**List of Abbreviations**

API	Application Programming Interface
EU	European Union
IT	Information Technology
NIST	National Institute of Science and Technology
SaaS	Software as a Service
IaaS	Infrastructure as a Service
PaaS	Platform as a Service
CSP	Cloud Service Provider
DoS	Denial of Service
VM	Virtual Machine
PocT	Policy as a Trust Management Technique
PrdT	Prediction as a Trust Management Technique
RecT	Recommendation as a Trust Management Technique
RepT	Reputation as a Trust Management Technique

## 1. Introduction

### 1.1. Introduction to Cloud Computing

Cloud computing is internet-based computing which allows the sharing of computer resources and data to computers and other devices on demand. National Institute of Standards and Technology (NIST) defines cloud computing as follows [Mell and Grance, 2011]:

*“Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”*

Cloud services are the services based on cloud computing mechanism and are delivered over the internet by the service provider and accessible by the users globally through internet.

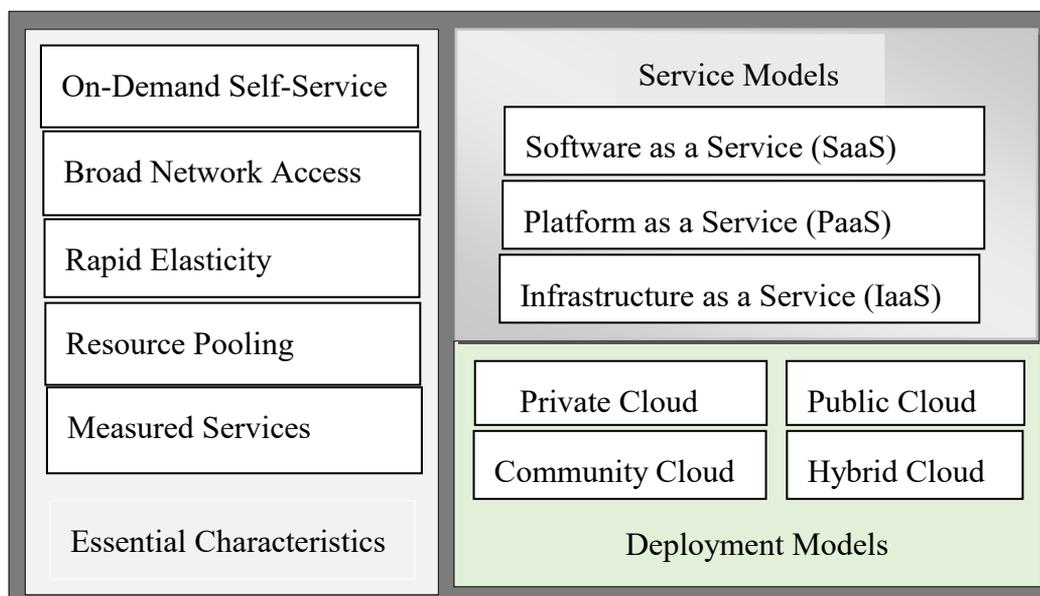


Figure 1: NIST Model of Cloud Computing

The essential characteristics of cloud model are as follows [Kotha, 2015]:

- **On-demand self-service:** The cloud users can gain access to the data and resources as demanded without having any human interaction with service providers.
- **Broad network access:** Users can access the cloud services from computers, mobile phones and such other devices. The users only need the interface to access services (usually web interface) and internet.

- **Rapid elasticity:** The usage of cloud resources can easily be increased or decreased by the users based on their requirements.
- **Resource pooling:** Users can gain access to pooled resources like data, storage, etc. through virtualization on demand.
- **Measured Services:** Both service providers and cloud users can measure, control and monitor the use of cloud resources transparently.

There are basically three cloud service models which are as follows [Kotha, 2015]:

- **Software as a Service (SaaS)**

In SaaS, users can use the provider's applications running on the cloud infrastructure. In such service models, the users do not manage underlying cloud infrastructure including servers, networks, storage or operating systems. E.g.: Microsoft Office 365 [Microsoft, 2017], Salesforce [Salesforce, 2017].

- **Platform as a Service (PaaS)**

In PaaS, users can deploy the user-created or acquired applications onto the cloud infrastructure. To deploy onto the cloud infrastructure, programming language, libraries and tools used to create the applications should be supported by the service provider. In such service model, users do not manage the underlying cloud infrastructure including servers, networks, storage or operating systems but has control over the deployed applications. E.g.: Google App Engine [Google Cloud, 2017], Force.com [Force, 2017].

- **Infrastructure as a Service (IaaS)**

In IaaS, users are provided with the processing, network, storage, and other computing resources where the users can deploy and run the arbitrary software, which can include applications and operating systems. The users do not manage the underlying cloud infrastructure but have control over storage, operating system, deployed applications and limited control over network components. E.g.: Microsoft Azure [Microsoft Azure, 2017], Amazon Elastic Compute Cloud (Amazon EC2) [Amazon, 2017].

The cloud deployment models are of four types [Mell and Grance, 2011]:

- i. **Public Cloud:** In public cloud deployment model, the cloud service provider makes the cloud infrastructure available to public over the internet. It may be owned, managed, operated and controlled by a government, business or academic organization.

- ii. Private Cloud: In such cloud deployment model, the cloud infrastructure is made available for a single organization. It may be owned, managed, operated and controlled by the organization or a third party.
- iii. Community Cloud: Community cloud is used by the community of consumers with shared concerns in community cloud deployment model. It may be owned, managed, operated and controlled by one or more organizations.
- iv. Hybrid Cloud: It is a combination of two or more cloud infrastructures (private, community, or public).

## **1.2. Cloud Usage and Growth**

Cloud usage refers to the use of various cloud services by the users for different purposes. Due to various advantages such as cost reduction, greater flexibility, elasticity and optimal resource utilization, cloud services are becoming popular for various usage such as test and development, big data analytics, file storage, disaster recovery and backup [Ferkoun, 2014].

Worldwide Public Cloud Services Market is growing so rapidly that it will grow by 18 Percent in 2017. Table 1 shows the projected growth of worldwide public cloud services in upcoming years. Its total market of \$209.2 billion dollars in 2016 is expected to grow to \$246.8 billion in 2017, \$287.8 billion in 2018, \$332.7 billion in 2019 and \$383.3 billion in 2020. Cloud application infrastructure services (platform as a service [PaaS]) is projected to grow by 23.4 % in 2017. Similarly, cloud application services (software as a service [SaaS]) is expected to grow by 20.13 % in 2017. The highest growth will be in cloud system infrastructure services (infrastructure as a service [IaaS]), which is projected to grow by 36.82% in 2017. [Gartner, 2017]

	2016	2017	2018	2019	2020
Cloud Business Process Services (BPaaS)	40.81	43.77	47.56	51.65	56.18
Cloud Application Infrastructure Services (PaaS)	7.17	8.85	10.62	12.58	14.80
Cloud Application Services (SaaS)	38.57	46.33	55.14	64.87	75.73
Cloud Management and Security Services	7.15	8.77	10.43	12.16	14.00
Cloud System Infrastructure Services (IaaS)	25.29	34.60	45.56	57.90	71.55
Cloud Advertising	90.26	104.52	118.52	133.57	151.09
Total Market	209.25	246.84	287.83	332.73	383.35

Table 1: Worldwide Public Cloud Services Forecast (billions of dollars) [Gartner,2017]

Regarding the cloud usage in European Union (EU), Finland is on the top position where one in every two enterprises is using some forms of cloud computing service. Italy is in second place where two in every five enterprises use some form of cloud computing services. In Italy, the most prevalent use of cloud computing is for email services. With 39% of enterprises using cloud computing, Sweden is in third place. Denmark is in the fourth place with 38% of enterprises use cloud computing. File storage is the most prevalent use of cloud computing in Denmark. With equal 28% of enterprises using some form of cloud computing, Netherlands and Ireland are in fifth and sixth position. The most common use of cloud computing in Netherlands is for hosting databases whereas storage of files is its common use in Ireland. UK is in seventh position for cloud computing where 24 % of enterprises use cloud computing in one or other form. With 22% of enterprises using cloud, Croatia is in eighth place where email service is the most prevalent use of cloud computing followed by Belgium where the primary use of cloud computing is file storage. Slovakia is in tenth position where 19 % of enterprises use cloud computing and the most common use of cloud is for email services. [Cummins, 2015]

International Trade Administration (ITA) published a report which provides a ranking for the top twenty cloud computing export markets for 2016 out of which six are Asian countries (Japan, South Korea, India, China, Singapore and Malaysia), eight European countries (United Kingdom, Germany, Switzerland, France, Netherlands, Italy, Sweden and Spain), two North American countries(Canada and Mexico), two South American countries(Brazil and Chile), one African country(South Africa) and one Australian country(Australia) [Pardo, Flavin and Rose, 2016].

There are several cloud service providers providing cloud services worldwide. For instance, Alibaba cloud, which is one of those CSP which is China's largest and the

fourth largest worldwide public cloud service provider that has 1,011,000 paying customers and more than 2,300,000 customers worldwide [Alibaba, 2017]. Alibaba cloud offers elastic computing, storage and content delivery products, networking, database management, security, resource management, domain and websites management, analytics and big data, application services and media services [Alibaba Cloud, 2017].

Despite of having so many advantages, there are still several individuals and organizations not using cloud services which can also be seen from the data about cloud usage presented above. The cloud usage is growing every year (as shown in table 1). However, the growth is not in the significant amount. Trust issues may be one of the reasons for such growth as trust between the cloud service provider and cloud users is one of the main issues in cloud services [Kaur and Kaur, 2015]. CNET stated trust as the biggest cloud computing issue [CNET, 2009]. There may be several elements related to trust issues in cloud computing. Different data breach incidents are one of the factors that impacts the user's trust towards cloud services.

Data breach can be as *“an incident in which sensitive, protected, or confidential data has potentially been viewed, stolen, or used by an individual unauthorized to do so.”* Data breaches may involve personal health information (PHI), payment card information (PCI), personally identifiable information (PII), trade secrets, or intellectual property.” [Lord, 2017]

Microsoft experienced data breach in 2010 that allowed non-authorized users of cloud service to access the contact information of employee in their offline address books. In 2012, cloud-based file sharing giant, Dropbox experienced data breach in which the hackers tapped into more than 68 million user accounts including email addresses and passwords. National Electoral Institute of Mexico was the victim of a breach in which over 93 million voter registrations were compromised. The reason behind that incident was that the institute was using insecure, illegally hosted Amazon cloud server outside of Mexico to store the data. LinkedIn experienced data breaches twice. Initially, 6 million user's passwords were stolen and published on a Russian forum in 2012. Later, in May 2016, hackers stole an estimated 167 million LinkedIn email addresses and password and posted for sale on the dark web. Apple suffered the one of the largest high-profile cloud security breach which involved the online leakage of some celebrities' private photos in Apple iCloud. [Bradford, 2017]

Recently, in Australia, nearly 50,000 personal records related to government employees, employees of two banks and a utility were exposed on internet due to a misconfiguration in Amazon cloud storage server which was used to store the backup data [Kirk, 2017]. In 2016, hackers breached an Australian domestic national security contractor and stole data related to military projects [Schwartz, 2017]. With the increment of data in cloud, the number of data breaches is also increasing every year.

Therefore, this research focuses on the different trust related issues in cloud based services including data breaches and discusses the other reasons for not using cloud by future IT professionals. It also presents the data about cloud usage and security considerations while using cloud by future IT professionals from five countries namely, China, Finland, Greece, Nepal and UK.

### 1.3. Research Questions

The purpose of this thesis is to review the trust issues in cloud services and to present the data about cloud usage, reasons for not using cloud and security considerations while using cloud services by future information technology (IT) professionals in five countries namely China, Finland, Greece, Nepal and UK.

The main research questions are as follows:

- RQ1: What are the trust issues and trust-building methods in cloud based services?
- RQ2: How is the cloud services usage by future IT professionals in those five countries?
- RQ3: What are the reasons for not using cloud services by future IT professionals in those countries? Is trust one of those reasons?
- RQ4: What are the security issues future IT professionals consider while using cloud services in those countries?
- RQ5: How does the national culture and gender affect the usage of cloud services, reasons for not using cloud services and security considerations while using cloud services?

### 1.4. Related Work

Most of the studies about cloud computing focuses on its technical aspect whereas some of them focuses on trust issues and management in cloud computing.

[Grandison and Sloman, 2003] has presented the trust management toolkit for the specification, analysis and monitoring of trust specifications. In their work, [Artz and Gil, 2007] have presented different trust definition from different research and they have also categorized trust research into four major groups as policy-based trust, reputation-based trust, general models of trust and trust in information resources. [Sherchan *et al.*, 2013] has presented the comprehensive review of trust in social and computer science literature. The authors have also discussed the definition of trust from psychology, sociology and computer science perspectives and also described different facets of trust: calculative, relational, emotional, cognitive, institutional and dispositional. There were few surveys which focus on reputation-based trust management systems. For instance, [Sabatar and Sierra, 2005] has presented the overview about computational trust and reputation models. It also presents the

classification of computational trust and reputation models based on different perspectives, such as, conceptual model, information sources and model's granularity.

[Marti and Garcia-Molina, 2006] has provided a taxonomy technique for the classification of different reputation-based trust management system. [Silaghi *et al.*, 2007] has reviewed reputation-based trust systems and investigated how those trust management systems can be applied to grid computing. It has also discussed some guidelines which can be useful for the development of trust management systems in grids.

This research provides the overview of the trust issues and discusses the factors that have impact on the trust in cloud based services. It also compares the trust issues related findings through literature review with the results of analysis of data collected through questionnaire survey.

### **1.5. Structure of Thesis**

The thesis is organized as follows. Section 2, Methodologies, discusses two methodologies used in the thesis, Questionnaire Survey and Systematic Literature Review. Section 3, Data Analysis Results, describes the analysis of data collected through questionnaire survey. Section 4, Literature Review Findings, provides the findings through Systematic Literature Review. Section 5, Discussion, presents the analysis of findings through these two methodologies. Section 6, Conclusions and Recommendations, presents the conclusion of the thesis and finally the section 7, Future Enhancements, presents the issues which are not covered in the thesis and can be studied later.

## **2. Methodologies**

This thesis uses two research methodologies, questionnaire survey and systematic literature review. The previously published articles were reviewed to identify the trust issues in cloud services. Therefore, systematic literature review methodology was used to answer the research question RQ1. The data collected through questionnaire survey were analyzed to find out the cloud services usage by future IT professionals, the reasons for them not using cloud services and the security issues they consider while using cloud services. Therefore, research questions RQ2, RQ3, RQ4, RQ5 were answered by using questionnaire survey.

### **2.1. Questionnaire Survey**

An offline survey questionnaire consisting of closed-ended questions in the form of Likert scale, multiple-choice questions as well as some open-ended questions, was designed in Finland with the participation of all the members of our international research team on cyber-security. After conducting pilot survey and publishing the results, questionnaires were translated into different languages and distributed in five

countries: China, Finland, Greece, Nepal and UK. Data were collected from higher-level (Bachelor's and Master's degree final year or about to graduate) universities students having computer science as a major subject. Students were asked to answer the questions during the studies in classroom.

There were altogether 29 questions in the questionnaire out of which only following questions relevant to this research were taken for this thesis work [Chaudhary, 2016].

- Please choose your gender
- Please select the country where you are currently enrolled as a student
- Please select your current level of education
- Please mention the subject you are majoring in college/university
- Do you use Cloud Services (e.g., Dropbox, Google Drive, Microsoft OneDrive, Apple iCloud, Tencent, Yunpan 360 etc.)?
- What are the reasons behind not using Cloud Services?
- What kind of security issues you consider while using your Cloud Services?

In total, 270 students from the aforementioned five countries participated in the survey. After the data collection process, data was inserted in Microsoft Excel. Among the collected data, 6 were invalid or incomplete. After removing those invalid/incomplete data, the final dataset was formed consisting of 264 data which was analyzed taking different variables into consideration.

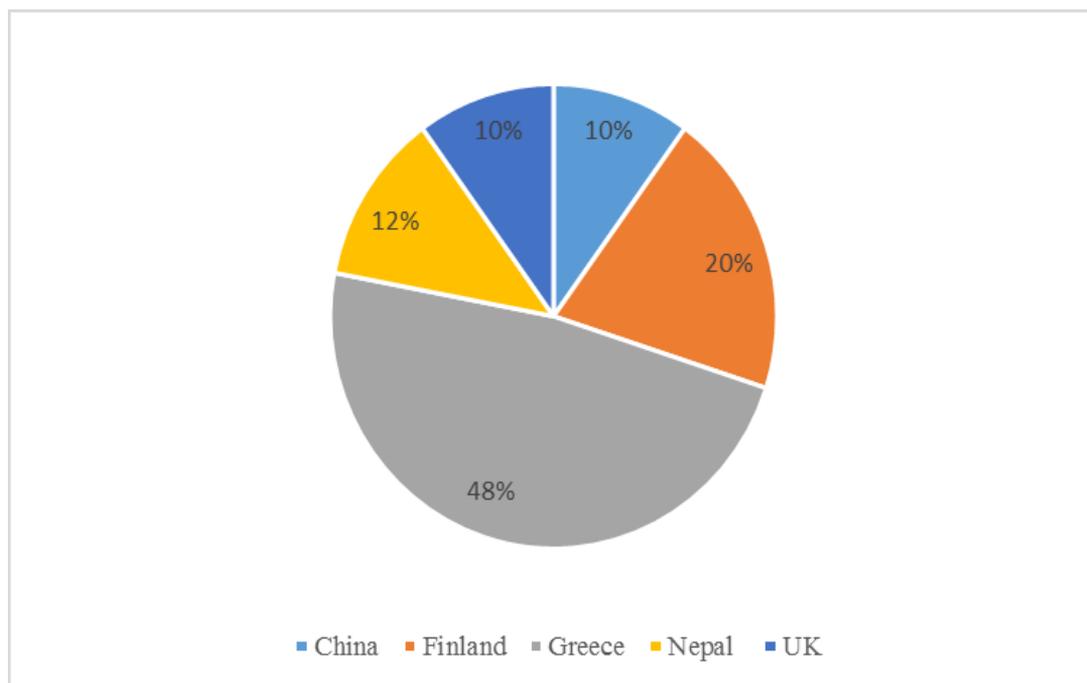


Figure 2: Data Collected by Country

Figure 2 shows the percentage of data collected from each five countries. As shown in figure, the dataset contains the largest number of data from Greece. 48% of data in dataset is from Greece, 20% from Finland, 12% from Nepal and equal 10 % from both China and UK.

The number of male participants is much greater than the number of female participants as shown in figure 3. Among the total participants, 71.59% participants were male and 28.41% were female.

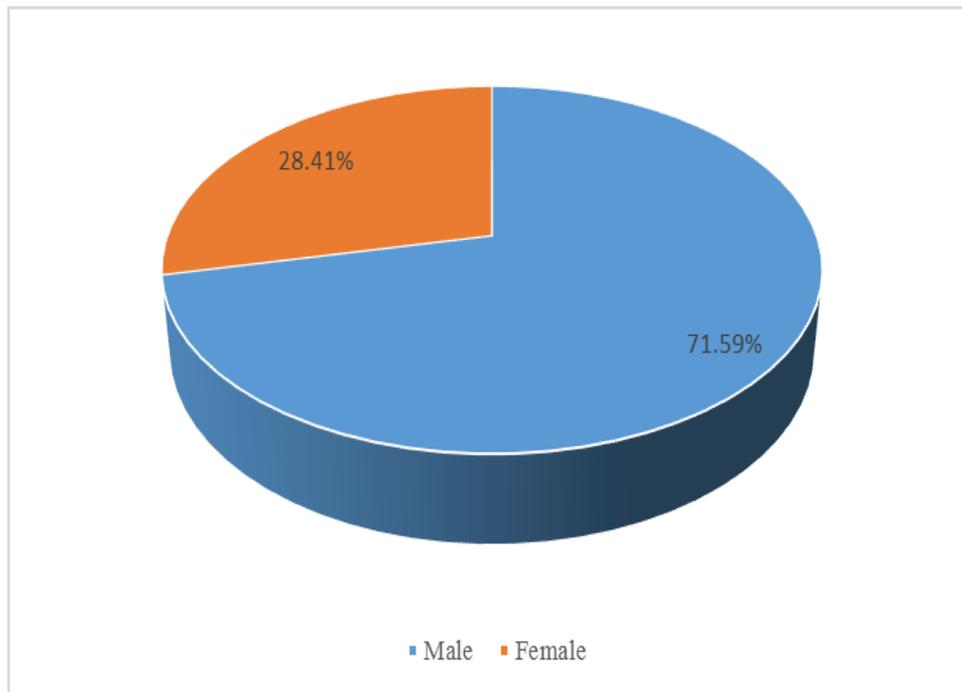


Figure 3: Data collected by gender

Figure 4 presents the categorization of data by gender in five countries. The number of male participants is greater than that of female participants in every country.

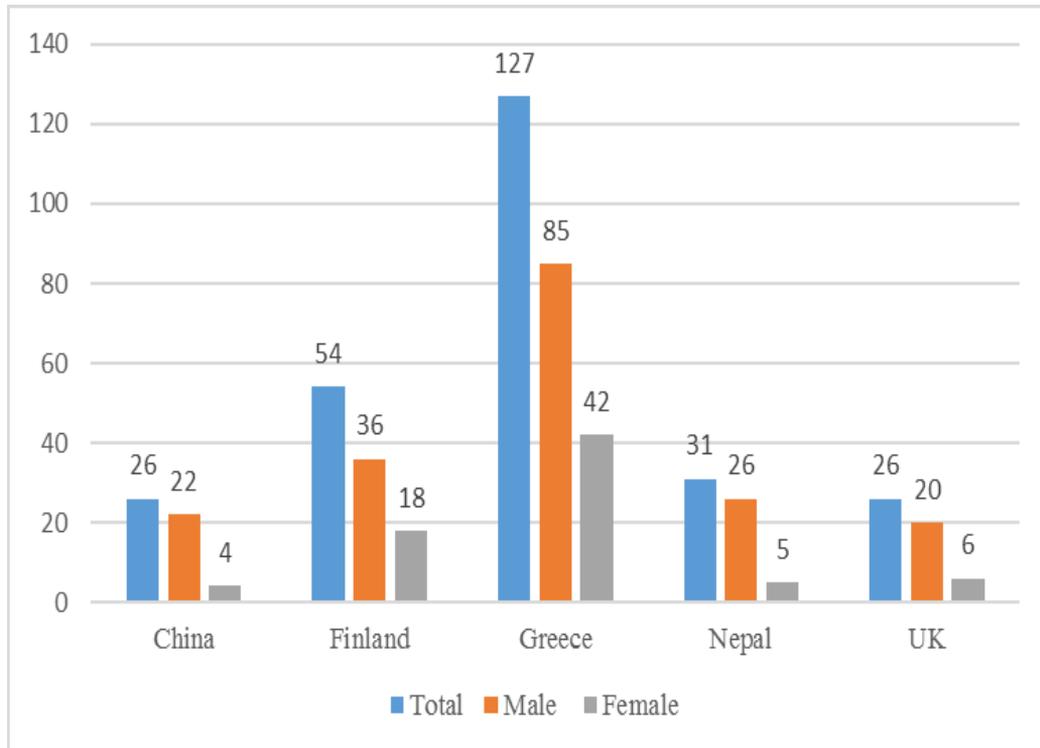


Figure 4: Data categorization by country

Data were collected from 26 participants in China, out of which 22 participants were male and 4 were female as shown in figure 4. In Finland, we collected data from 54 participants consisting of 36 males and 18 females. Data from 127 participants was collected in Greece where the data set contains 85 male participants and 42 female participants. A total of 31 participants gave the available data from Nepal. The data commented here were collected from a set consisting of 26 male participants and 5 female participants. The data collected in UK was given by 26 valid questionnaire respondents, comprising of 20 males and 6 female participants, as shown in figure 4.

## 2.2. Systematic Literature Review

Initially, the search keywords were constructed for searching the literatures related to cloud trust issues. Those search keywords were *cloud trust* and *cloud computing trust issues*. Boolean operators were also used to connect those search keywords. The search expression after using Boolean operator was *cloud computing trust issues OR cloud trust*. After constructing the search keywords, following digital libraries were used to search the literatures: IEEE Explore, ACM Digital Library, ScienceDirect and Springer Link. Those digital libraries were selected as they are very good sources for quality technical literatures. Since, these libraries have their own search mechanism, searching were done accordingly. While searching the literatures, the following inclusion criteria were used:

- Conference Proceedings, Journals and Magazines since 2004

- Studies focused on trust issues and trust management in cloud environment

Initially, there were total 362 literatures in IEEE Explore library, 49 literatures in ACM Digital Library, 211 literatures in ScienceDirect and 251 literatures in Springer Link were found. Out of those results, more closely related literatures were selected and reviewed.

### 3. Data Analysis Results

This section presents the results from analysis of the data collected through questionnaire survey. It provides information about cloud users and non-users, reasons for not using cloud and user's considerations while using cloud services. It discusses every finding from gender and country perspective.

#### 3.1. Cloud users and non-users by gender

Figure 5 shows the categorization of cloud users and non-cloud users by gender. Out of total 189 male participants, 150 are cloud users whereas the remaining 39 do not use it. Similarly, 64 female participants out of 75 use cloud and 11 do not use it.

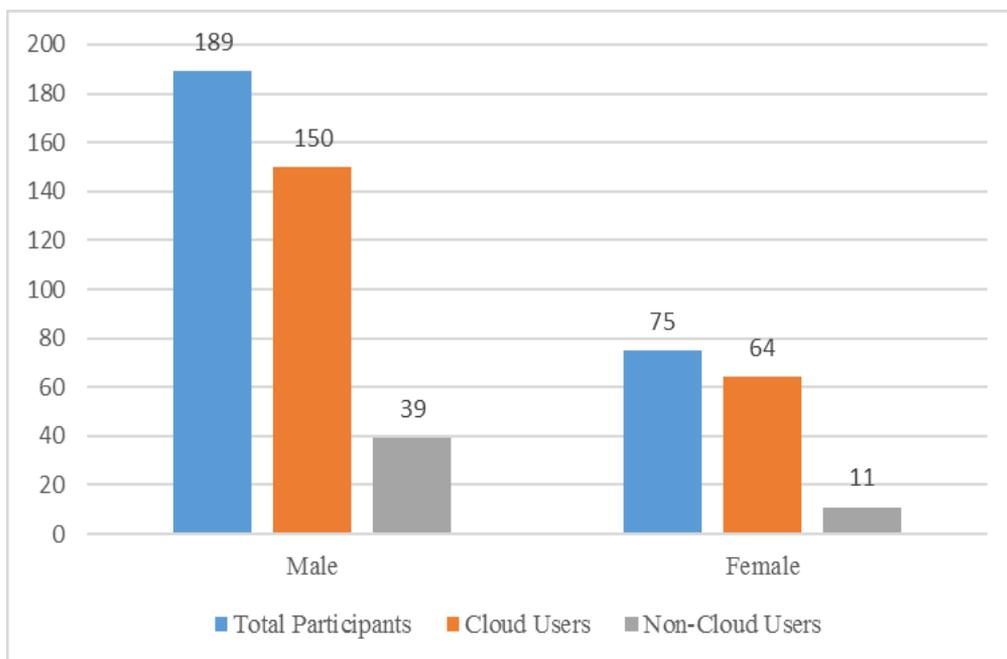


Figure 5: Categorization of cloud users by gender

#### 3.2. Cloud users and non-users by country

Figure 6 illustrates the number of cloud users and non-cloud users in those five countries. Out of 26 participants from China, 16 use cloud whereas the remaining 10 do not use it. Similarly, 51 out of 54 participants use cloud and 3 do not use cloud in Finland. In Greece, 105 participants out of 127 total participants use cloud whereas 22 do not use it. 19 participants use cloud in Nepal whereas the remaining 12 do not use

cloud. In UK, out of 26 participants, 23 use cloud and 3 do not use it as shown in the figure 6.

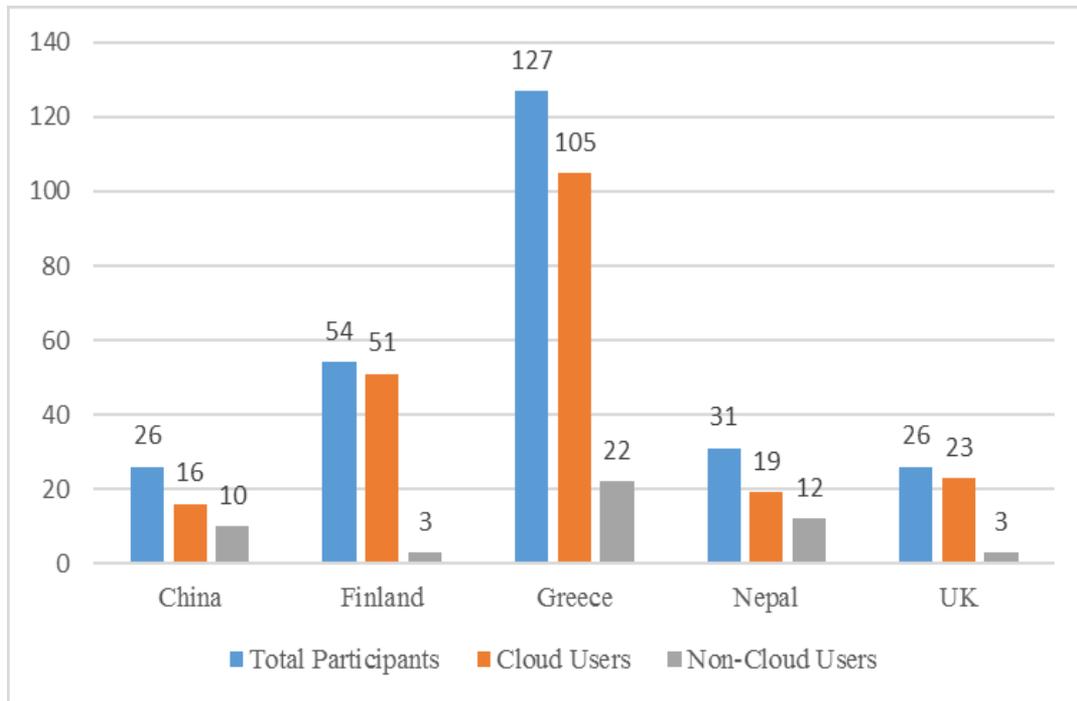


Figure 6: Cloud users and non-users in five countries

### 3.3. Reasons for not using cloud

There was a specific question in the questionnaire about the reasons for not using cloud. For this question, we didn't get any data from China. Based on the data collected from Finland, Greece, Nepal and UK, there appeared to be several reasons for not using cloud in those countries which is plotted in figure 7.

The reason '*I never needed*' is the most common reason for not using cloud with a 50% percentage, whereas the answer '*I don't trust*' is the second most common reason. Similarly, other reasons include '*I don't know how to use them*', '*no access*', '*I never heard*' and *other reasons*.

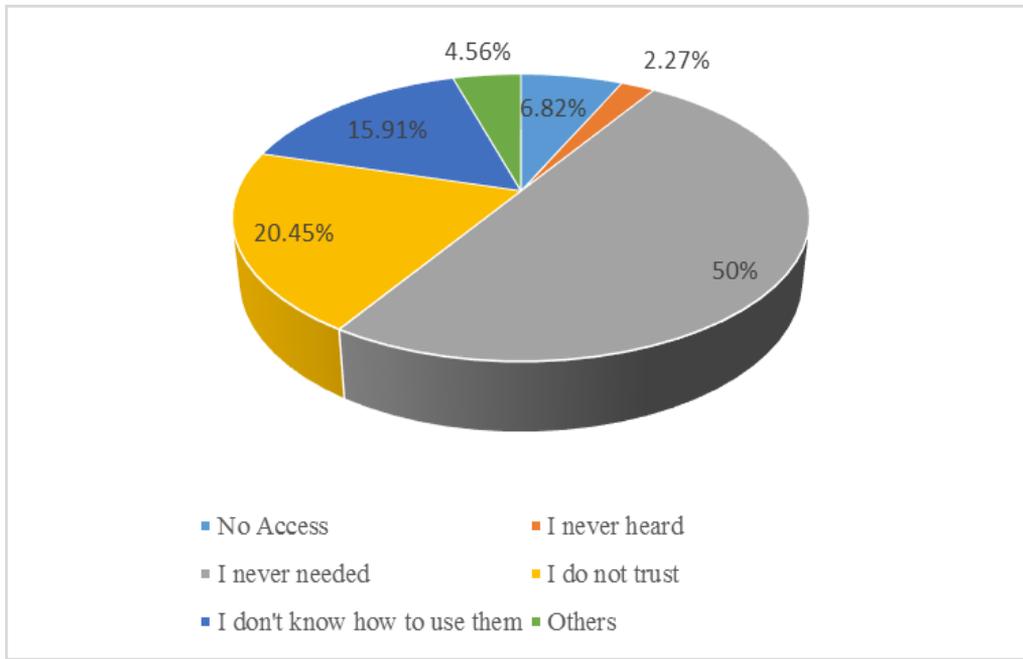


Figure 7: Reasons for not using cloud services

### 3.4. Reasons for not using cloud by gender

Out of 50 non-cloud users, 39 were male and 11 were female. 31 (79.9 %) male and 6 (54.55 %) female non-cloud users answered the question about reasons for not using cloud.

Figure 8 presents the reasons for not using cloud from gender-perspective. Not having the need of cloud is common reason for majority of male and female non-cloud users. As shown in the figure, it is the reason for 51.61 % male and 66.67 % female for not using cloud. Not having knowledge of using cloud is second most common reason for 16.13 % male and 33.33 % female for not using it. Not trusting the cloud is another major reason for not using it for 16.13 % male non-cloud users.

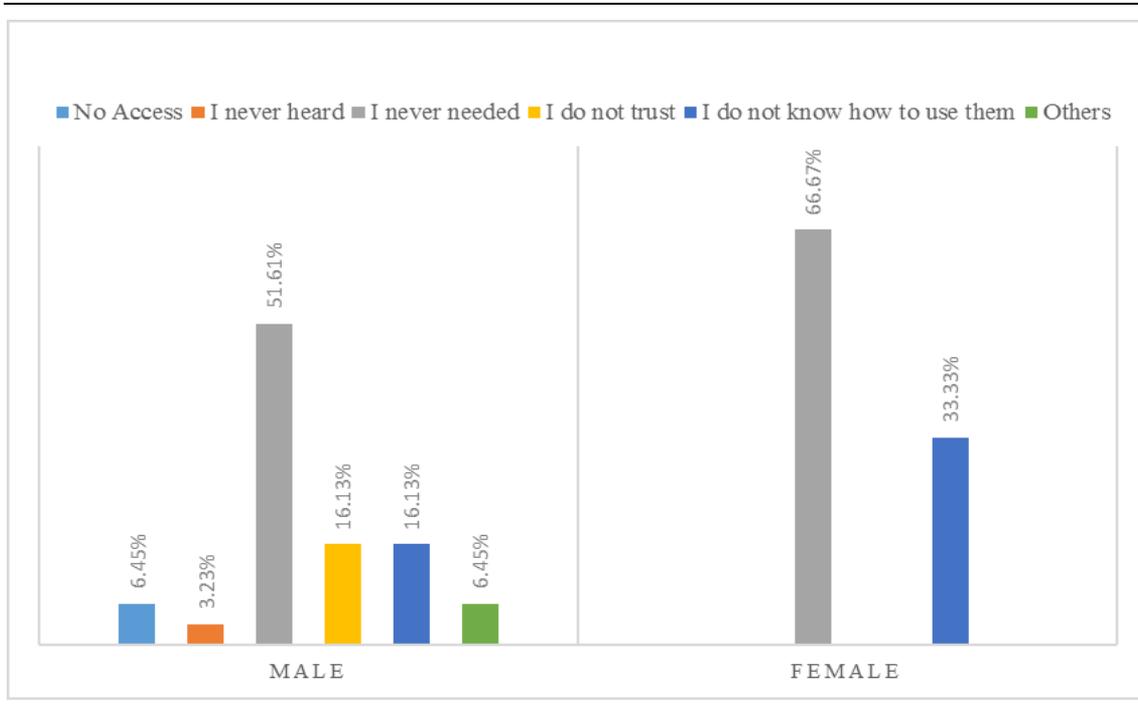


Figure 8: Reasons for not using cloud by gender

### 3.5. Reasons for not using cloud by country

Among total 50 non-cloud users, 44 non-cloud users from other countries except China have answered this questions about the reasons for not using cloud services. These reasons for not using cloud have also been categorized based on the countries of the data samples as shown in figure 9.

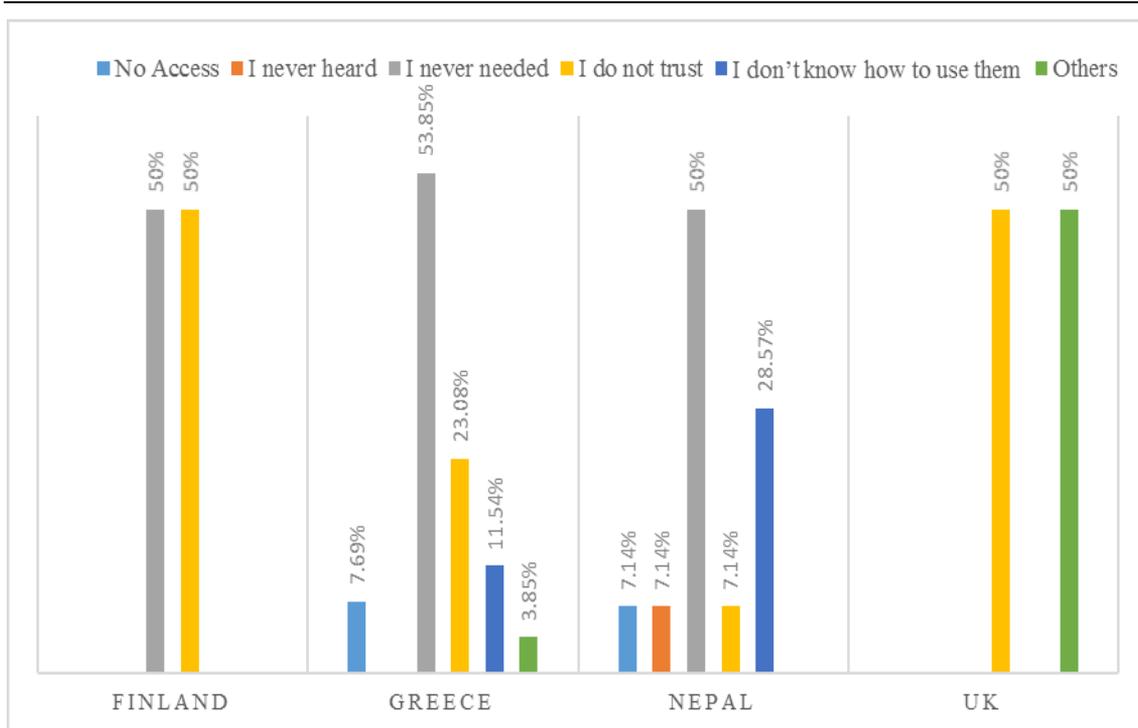


Figure 9: Reasons for not using cloud by country

Not trusting is the common reason for not using cloud services in all four countries. Among the answers from non-cloud users, it is the reason for 50 % non-cloud users in Finland, 23.08 % non-cloud users in Greece, 7.14 % non-cloud users in Nepal and 50 % non-cloud users in UK for not using cloud services. ‘No need to use cloud services’ is second common reason for not using cloud services. The later has the highest percentage in Greece, where 53.85% of the non-cloud users selected this reason for not using cloud services. ‘Never heard’ is the least common reason for not using cloud services which is the reason for the 7.14 % of non-cloud users from Nepal.

### 3.6. Considerations while using cloud services by gender

Data about security considerations while using cloud services were collected through questionnaire survey. There were some considerations while using cloud services and the participants had to select one answer among five options: *never*, *rarely*, *sometimes*, *very often* and *always*.

#### 3.6.1. Putting confidential data into cloud

One of those concerns was putting confidential data in cloud. 232 out of total 264 participants answered this question. Data collected through this question can be categorized by gender- perspective which is shown in figure 10. Total 162 males and 70 female participants answered this question. Among those male participants who answered, 27.78% answered *never*, 20.99% answered *rarely*, 25.31% answered *sometimes*, 18.52% answered *very often* and 7.41% answered *always* whereas among those female participants who answered this question, 25.71% answered *never*, 30% answered *rarely*, 14.29% answered *sometimes*, 17.14% answered *very often* and 12.86% answered *always* as shown in figure 10.

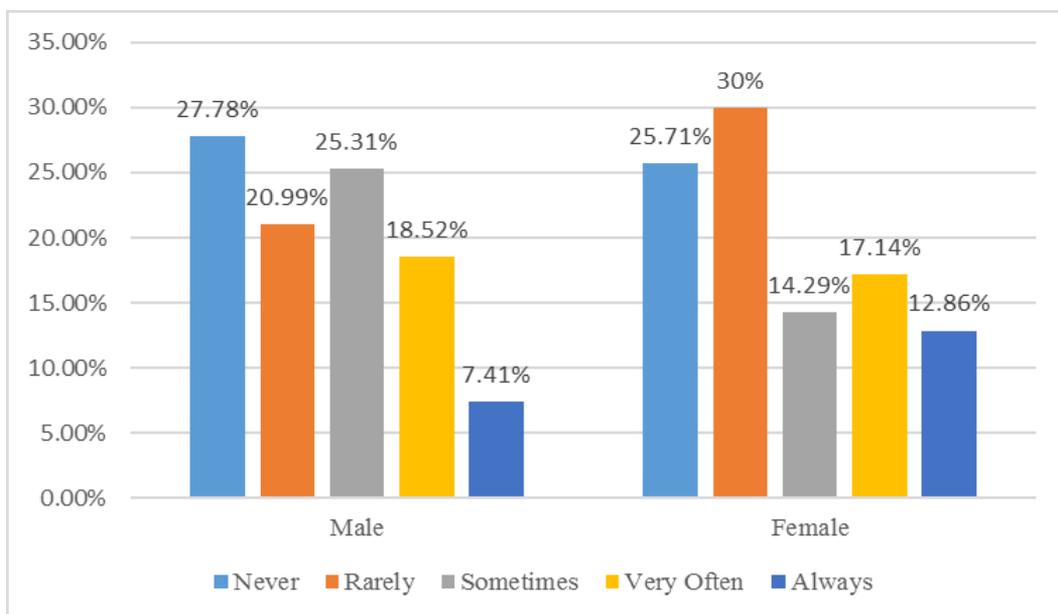


Figure 10: Data about putting confidential data in cloud by gender

### 3.6.2. Trusting service provider will handle data with good care

Another security consideration participants were asked to answer were about trusting the cloud service provider will handle their data with good care.

As shown in figure 11, data about trusting the service provider can also be categorized by gender. This question was answered by 164 males and 70 female participants. Among those male participants, 12.20% answered *never*, 15.85% answered *rarely*, 35.37% answered *sometimes*, 24.39% answered *very often* and 12.20% answered *always*. Similarly, out of those female participants who answered, 10% answered *never*, 18.57% answered *rarely*, 24.29% answered *sometimes*, 34.29% answered *very often* and 12.86% answered *always*.

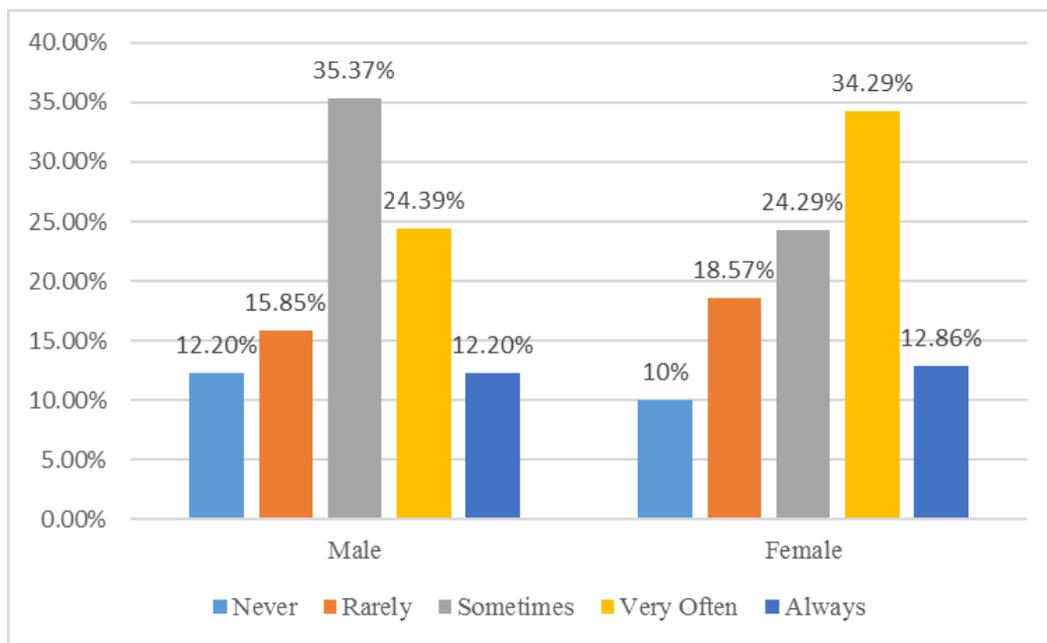


Figure 11: Data about trusting service provider by gender

### 3.6.3. Encrypting data before storing into cloud

The third security concern was encrypting data before storing into cloud. Total 234 participants answered this question. Among the participants who answered this question, 164 were males and 70 were females. Out of those male participants, 31.71% answered *never*, 23.78% answered *rarely*, 23.17% answered *sometimes*, 12.80% answered *very often* and 8.54% answered *always*. Similarly, among those female participants, 38.57% answered *never*, 27.14% answered *rarely*, 15.71% answered *sometimes*, 12.86% answered *very often* and 5.71% answered *always* as shown in figure 12.

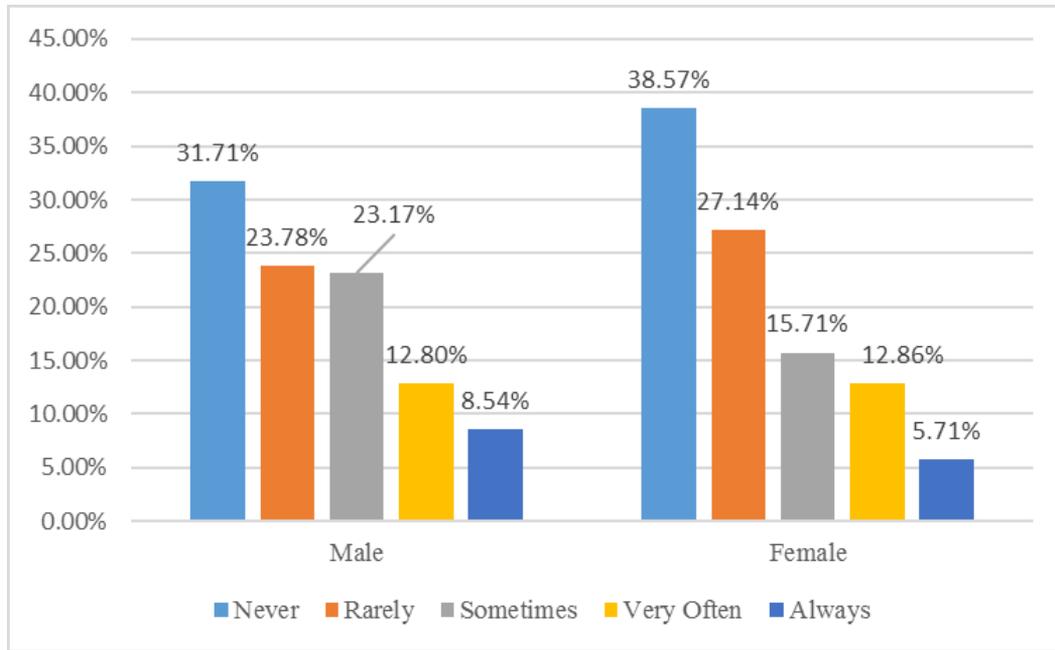


Figure 12: Data about encrypting data before storing into cloud by gender

### 3.7. Considerations while using cloud services by country

#### 3.7.1. Putting confidential data into cloud

The total of 232 participants answered the question whether they put confidential data into cloud. Out of 20 participants who answered the question in China, 40 % of them *rarely* put confidential data in cloud whereas 25 % answered *sometimes*, 20% answered *very often* and 15% answered *always*. Similarly, out of 52 participants from Finland who answered this question, equal 23.08% answered *never*, *rarely* and *sometimes* whereas 21.15% answered *very often* and 9.62% answered *always*. 115 participants answered this question in Greece out of which 40.87% answered *never*, 20.87% answered *rarely*, 17.39% answered *sometimes*, 16.52% answered *very often* and 4.35% answered *always*. In Nepal, 21 participants answered the question where 9.52% answered *never*, 14.29% answered *rarely*, 19.05% answered *sometimes*, 33.33% answered *very often* and 23.81% answered *always*. Similarly, out of 24 participants answered this question in UK, 8.33% answered *never*, 3.33% answered *rarely*, 41.67% answered *sometimes*, 4.17% answered *very often* and 12.50% answered *always* as shown in figure 13.

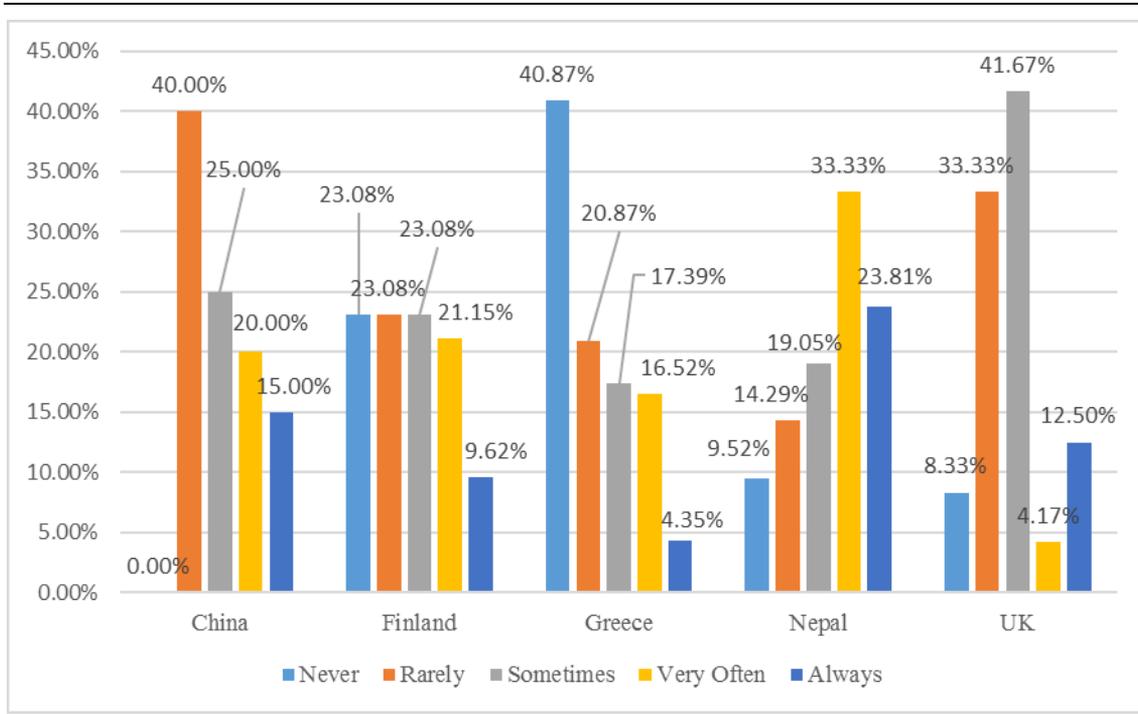


Figure 13: Data about putting confidential data in cloud by country

### 3.7.2. Trusting service provider will handle data with good care

Out of total 264 participants, 234 answered whether they trust service provider will handle their data with good care. Out of 21 participants from China who answered this question, 4.76% answered *never*, 28.57% answered *rarely*, 47.62% answered *sometimes*, 4.76% answered *very often* and 14.29% answered *always*. Similarly, 52 participants from Finland answered this question where 1.92% answered *never*, 11.54% answered *rarely*, 26.92% answered *sometimes*, 48.08% answered *very often* and 11.54% answered *always*. In Greece, 115 participants answered this question, out of which 17.39% answered *never*, 20.87% answered *rarely*, 31.30% answered *sometimes*, 20.87% answered *very often* and 9.57% answered *always*. Total 22 participants answered this question in Nepal where 4.55% answered *never*, 13.64% answered *rarely*, 40.91% answered *sometimes*, 22.73% answered *very often* and 18.18% answered *always*. Similarly, 24 participants answered this question in UK, out of which 16.67% answered *never*, 25% answered *sometimes*, 37.5% answered *very often* and 20.83% answered *always* as shown in figure 14.

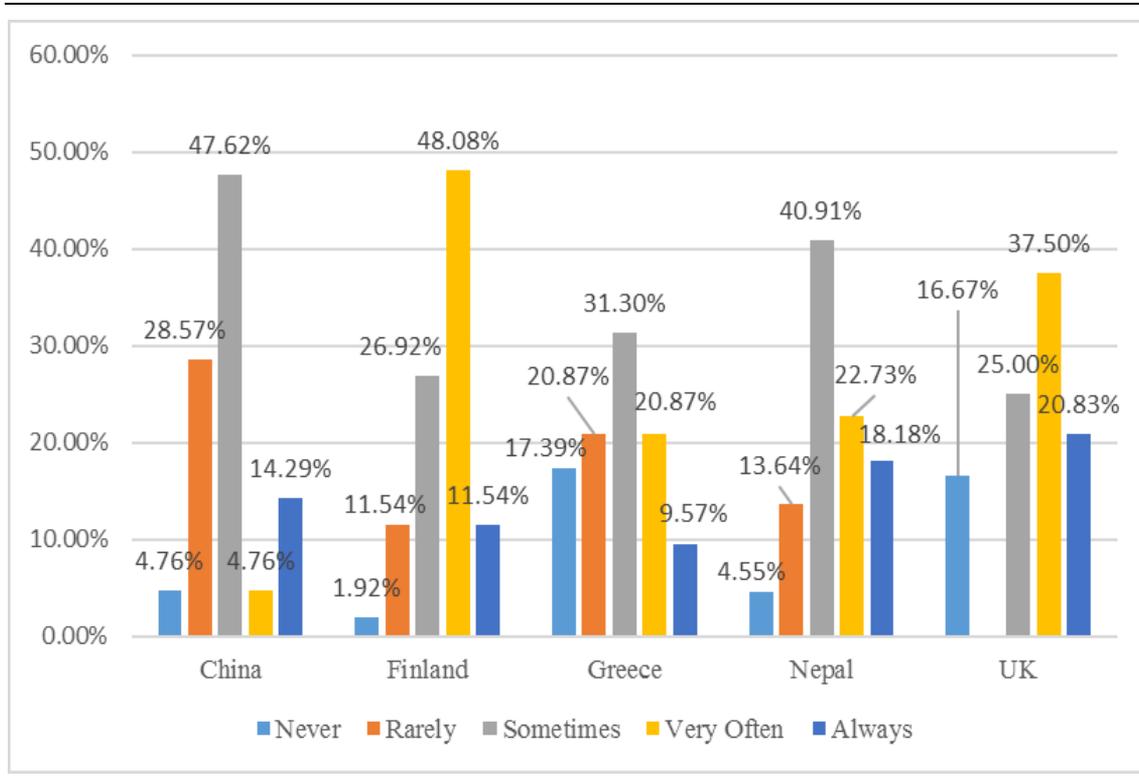


Figure 14: Data about trusting service provider by country

### 3.7.3. Encrypting data before storing into cloud

Out of 21 participants from China who answered this question, 9.52% answered *never*, 14.29% answered *rarely*, 42.86% answered *sometimes*, 19.05% answered *very often* and 14.29% answered *always*. The total of 52 participants from Finland answered this question where 48.08% answered *never*, 18.85% answered *rarely*, 17.31% answered *sometimes* and 5.77% answered *very often*. Among 115 participants in Greece who answered this question, 35.65% answered *never*, 24.35% answered *rarely*, 17.39% answered *sometimes*, 14.78% answered *very often* and 7.83% answered *always*. In Nepal, 22 participants answered this question out of which equal 22.73% answered both *never* and *rarely*, 27.27% answered *sometimes* and equal 13.64% answered *very often* and *always*. In UK, 24 participants answered this question where 25% answered *never*, 29.17% answered *rarely*, 20.83% answered *sometimes* and equal 12.50% answered *very often* and *always* as shown in figure 15.

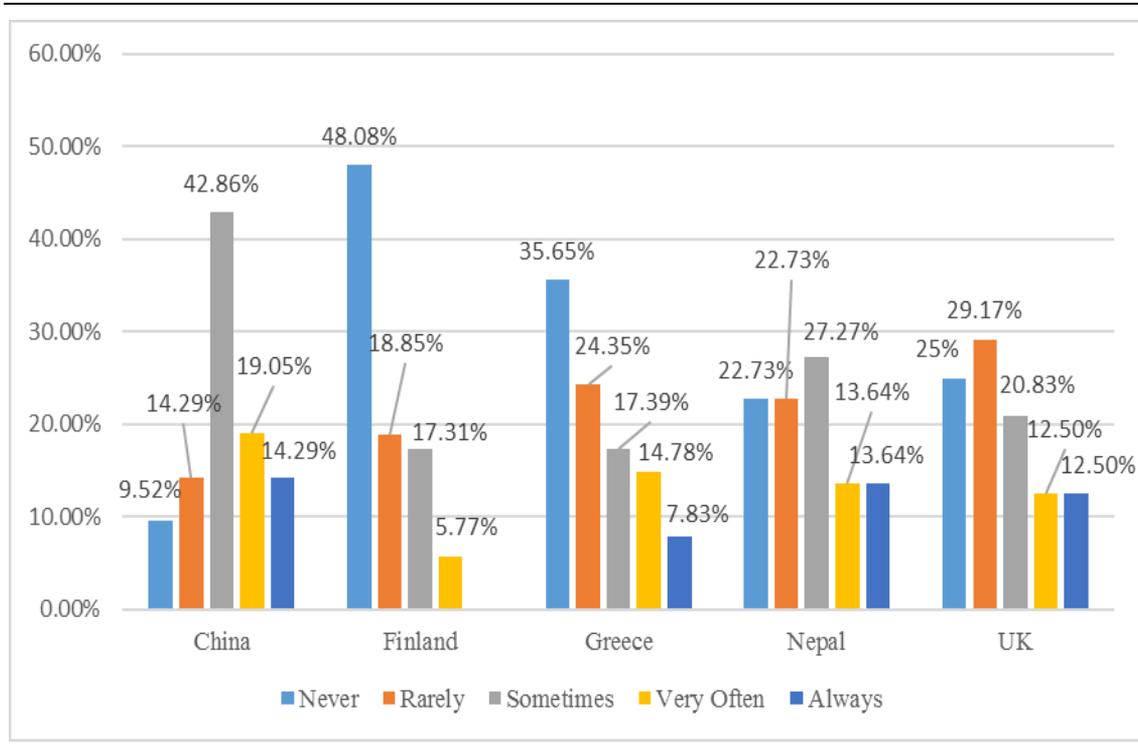


Figure 15: Data about encrypting data before storing into cloud by country

#### 4. Literature Review Findings

As the use of internet is growing rapidly, it requires large request processing in server which is very difficult to handle with traditional computing. Therefore, cloud computing is the new trend that offers huge computational and storage capabilities over internet. Data outsourcing is common concept in cloud computing. When users want to store their data in cloud, but that cloud service provider may not have the whole requested space to store that data, the service provider contracts other service provider to store their data. Therefore, data outsourcing increases the risk of security threats as multiple organizations have access to user's data. It also raises the trust issues as users are concerned about their data storage location and who can access their sensitive or confidential information. [Harbajanka and Saxena, 2016]

Trust management is one of the key challenges in cloud computing [Noor *et al.*, 2013]. "*Trust is a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another*" [Pearson and Benameur, 2010]. Trust is the most complex relationship among entities as it is non-symmetric, context-dependent, uncertain and extremely subjective [Sun *et al.*, 2011].

While talking about trust, there are two basic entities, truster and trustee. Truster may be an individual or an organization, and the trustee may be a person, organization or a specific IT artifact. [Lansing and Sunyaev, 2016] Trust in cloud computing refers to the bi-directional trust between cloud service provider (CSP) and cloud users. It also

sometimes refers to trust between cloud service provider and their employees. [Khorshed *et al.*, 2011]

It is important for CSPs that their clients fully trust them in terms of confidentiality, integrity and availability [Brandenburger *et al.*, 2015]. According to the researchers at UC Berkeley, trust management and security are ranked among the top 10 obstacles for adopting cloud computing. This is because of privacy issues (e.g., the leakage of Apple's iPad subscribers' information), security issues (e.g., the mass email deletions of Gmail), and dependability issues (e.g., Amazon Web Services outage that took down lots of business Web sites).[Noor *et al.*, 2013]

There may be trust issue with the CSPs that the service provider will use less secured infrastructure than agreed to store user's information and use untested or poor data retention practices which also result into data loss or leakage [Khorshed *et al.*, 2011]. Other issue is ensuring that the users have control over the lifecycle of their data. For instance, for a particular deletion of data, it is difficult for a user to be sure that the data is deleted, and cloud service provider will not be able to recover that data. It all relies on trust between user and cloud service provider. [Pearson and Benameur, 2010]

When the individuals don't understand why their personal information is requested and how and by whom the information will be processed, then there arises the suspicion which ultimately leads to distrust. There may also be security concern of whether the data will be protected or not. The users may not use cloud if they feel such risks for their data in service provided by the cloud service provider. [Pearson and Benameur, 2010]

[Bose *et al.*,2013] has compared the trust between cloud service providers and cloud service users with trust between banks and their customers. It states that the cloud users need to trust the service provider in a same way as the customers trust banks to put their money. Similarly, the cloud service providers should be able to demonstrate that they are trustworthy so that service users are confident in using that service. There was a time where people didn't trust banks to deposit their money and other tangible assets. The two-way trust building process between banks and the customers took long time which may be similar in the trust building process between cloud service providers and users. Trust management in cloud services is even more challenging due to dynamic, distributed and non-transparent nature of cloud services [Noor *et al.*, 2013]. After winning the user's trust, users will confidently store their data in cloud as they are confident about their money in the bank. However, banking security systems comprise of several levels and components such as physical security, transaction security and electronic security whereas cloud services are often offered in open virtual environment which increases the risk of various attacks. Therefore, it is crucial for the service provider to identify such possible attacks and implement the security processes to provide the secured services. [Bose *et al.*,2013]

The CSPs are responsible for storage and processing of user data. The data are stored and processed using machines in which user has no control which results into trust issues in cloud services as there may be risk of theft, misuse of the user's data. There may also be risk of service provider gaining benefits from unauthorized secondary use of user's data. Cloud services combining outsourcing and offshoring may raise more complex issues. The movement of data inside cloud and outsourcing of data for processing increases risk factors. Due to dynamic nature of cloud, it is unclear about who is responsible for ensuring the legal requirements for data handling are followed. It may also be unclear to identify trustworthiness of the subcontractors involved in data processing. [Pearson and Benameur, 2010]

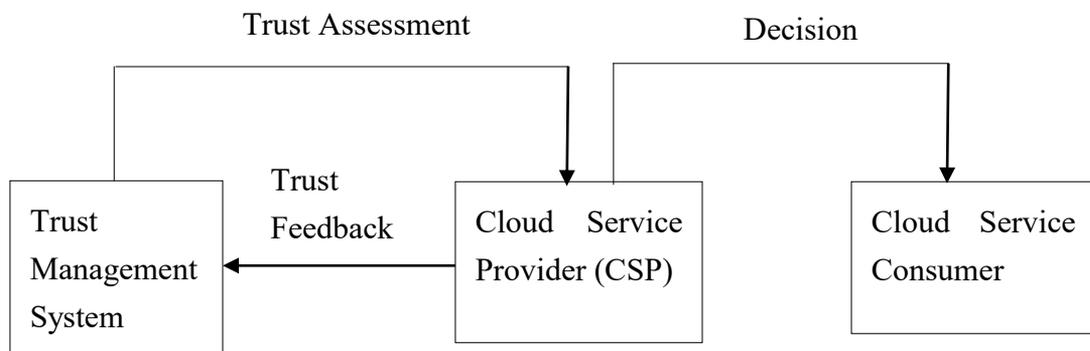
There may be various ways to establish online-trust. Security may be one of these ways. However, some argue that security is not related to trust and level of security does not affect trust whereas some believe that trust increases with increasing security as the service users trust the service providers if they provide encryption of their personal information. Reputation is another factor for trust [Pearson and Benameur, 2010]. Trusting the cloud services depends on the reputation of cloud service provider. The users trust the cloud service provider which has good reputation. Reputation can be defined as "the extent to which firms and people in the industry believe a supplier is honest and concerned about its customers" [Lansing and Sunyaev, 2016].

The reputation of the cloud service provider has direct impact on the user's choice for that service. The cloud users need to re-evaluate and verify the trust after building the initial trust with the service provider. Therefore, quality of service (QoS) monitoring and service level agreement (SLA) is one of the basis for trust management in cloud computing. However, SLA focuses on visible cloud service performance elements but does not focus on elements such as privacy and security. Another issue with SLA is that users need a professional third party to provide QoS monitoring and SLA services as most of the cloud users may not be able to perform these services on their own. [Huang and Nicol, 2013]

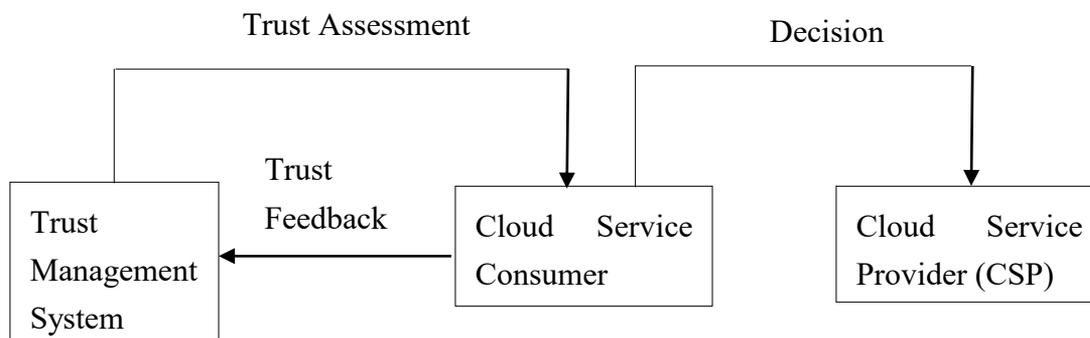
While thinking about the reputation of the service provider, users can consider how secure are the services provided by that service provider, where there any security related issues with that service provider in past. If there are any such cases with service provider, it may be difficult to regain the user's trust. There are some examples where some cloud service provider faced such security issues not because of security attacks but due to some malfunction in service provider such as software malfunction. Such data breach occurred in Google Docs in March 2009. Similarly, users experienced silent data corruption in Amazon S3 due to service provider's malfunctions. A cloud storage-provider named LinkUp (MediaMax) went out of business after losing 45% of stored client data due to system administrator's error. [Cachin *et al.*, 2009]

Implementing user authentication before providing access the data may be helpful to build trust with the users. If the user need to be authenticated before accessing the data, it ensures the user that the data can be accessed by him only and no other can access that data. It helps to build the user trust towards that cloud service. [Harbajanka and Saxena, 2016] As many cloud service providers are offering similar cloud services, it may be difficult for the organizations to choose the service provider. There are also other elements in addition to the reputation of the service provider resources which the organizations need to take care while selecting the service provider, such as, size of the service provider company in terms of employees, market share as well as other organizational elements. [Rad *et al.*, 2017]

An effective trust management system is required for the cloud service provider and consumers in order to fully utilize the benefits offered by cloud services. Trust management can be classified using two perspectives, service provider's perspective (SPP) and service requester's perspective (SRP) [Noor *et al.*, 2013].



(a) Service Provider's Perspective (SPP)



(b) Service Requester's Perspective (SRP)

---

Figure 16: Trust Management Perspectives [Noor *et al.*, 2013]

In service provider's perspective (SPP), the service provider assesses the trust worthiness of service consumer whereas the trust worthiness of cloud service consumer

is assessed by service provider in service requester's perspective (SRP) as shown in figure.

The trust management techniques can be categorized into four categories: Policy as a Trust Management Technique (PocT), Recommendation as a Trust Management Technique (RecT), Reputation as a Trust Management Technique (RepT), and Prediction as a Trust Management Technique (PrdT) [Noor *et al.*, 2013].

Policy as a Trust Management Technique (PocT) is one of the traditional and most popular way to establish trust among the parties in cloud environment which uses a set of policies, each of which assuming several roles that control authorization levels and specifying a minimum trust threshold in order to authorize access. In PocT, trust thresholds are based on the credentials or trust results. Recommendation as a trust management technique (RecT) is one of the popular techniques used in cloud computing, which uses the participant's knowledge about trusted parties. Recommendations can be of several types such as transitive recommendation and explicit recommendation. When a cloud service user trusts a cloud service because one or some of his trusted relations trust the service, it is called transitive recommendation. In explicit recommendation, cloud service user recommends that particular cloud service to his well-trusted relations such as friends. Reputation as a Trust Management Technique (RepT) is other important technique for trust management in cloud computing. The reputation of a cloud service can be influenced dramatically by the feedback of the service users as the positive feedback has positive impact and negative feedback has negative impact in the service's reputation. Similarly, the reputation of cloud service influences its trustworthiness directly or indirectly. Prediction as a trust management technique (PrdT) is also another technique for managing trust in cloud services. It is usually useful in situations where there is no prior information about the cloud services such as history of records and previous interactions. The basic idea behind PrdT is that cloud users (similar minded entities) are more likely to trust each other. In [Noor *et al.*, 2013], the authors have also proposed a generic analytical framework for trust management in cloud environments.

Security is also a major obstacle in adopting and utilizing the full benefit from cloud computing. Availability, confidentiality and integrity are the main dimensions of security. [Sun *et al.*,2011] Security techniques, such as, encryption may be helpful to preserve the confidentiality of the stored data, but it may not be able to prevent the malicious attacks and data modifications [Brandenburger *et al.*, 2015].

Data integrity is another crucial factor in cloud. Data can be damaged in service provider or during transmission. There can be risks of malicious attacks from inside or outside the service provider. For example, the servers of the Red Hat Linux distribution were attacked, and the intruder introduced a vulnerability and even sign some packages of the Linux operating-system distribution. [Cachin *et al.*, 2009]

In case of single client, integrity of the data can be verified by locally keeping a short cryptographic hash value for the outsourced data and comparing this value with the data returned by cloud service provider. However, the situation becomes very much complicated with multiple disconnected clients where neither hashing nor digital signatures works sufficiently. One of the reasons is malicious service provider violating the data consistency. The malicious service provider may pretend to one group of clients that some operations by other group of clients did not occur. The clients will not be able to detect such types of attacks until they communicate directly with each other. [Brandenburger *et al.*, 2015]

## **5. Discussion**

Table 2 shows the analysis of the collected data from country and gender perspective. The comparison of male and female cloud users and non-users in those five countries shows that the percentage of male cloud users is higher than that of female cloud users in China and Nepal (Asian countries) while opposite is true for Finland, Greece and UK (European countries). In case of Finland and UK, every female participant use cloud as shown in the table below.

	China		Finland		Greece		Nepal		UK	
	M	F	M	F	M	F	M	F	M	F
Cloud Users (%)	68.18	25	91.67	100	80	88.10	65.38	40	85	100
Reasons for not using cloud services (in %)										
No Access	0	0	0	0	6.25	0	9.09	0	0	0
I never heard	0	0	0	0	0	0	9.09	0	0	0
I never needed	0	0	50	0	62.5	66.67	45.45	66.67	0	0
I don't trust	0	0	50	0	12.5	0	9.09	0	50	0
I don't know how to use them	0	0	0	0	12.5	33.33	27.27	33.33	0	0
Others	0	0	0	0	6.25	0	0	0	50	0
Security considerations while using cloud services										
1. Putting confidential data into cloud (in %)										
Never	0	0	23.53	22.22	44	35	11.11	0	11.11	0
Rarely	41.18	33.33	14.71	38.89	18.67	25	16.67	0	27.78	50
Sometimes	23.53	33.33	29.41	11.11	20	12.5	16.67	33.33	50	16.67
Very often	23.53	0	20.59	22.22	14.67	20	38.89	0	5.56	0
Always	11.76	33.33	11.76	5.56	2.67	7.5	16.67	66.67	5.56	33.33
2. Trusting the cloud service provider will handle data with good care (in %)										
Never	5.56	0	2.94	0	17.33	17.5	5.26	0	22.22	0
Rarely	22.22	66.67	11.76	11.11	21.33	20	10.53	33.33	0	0
Sometimes	55.56	0	32.35	16.67	32	30	36.84	66.67	33.33	0
Very often	5.56	0	44.12	55.56	18.67	25	26.32	0	27.78	66.67
Always	11.11	33.33	8.82	16.67	10.67	7.5	21.05	0	16.67	33.33
3. Encrypting data before putting into cloud (in %)										
Never	11.11	0	47.06	50	34.67	37.5	26.32	0	16.67	50
Rarely	16.67	0	23.53	38.89	26.67	20	15.79	66.67	27.78	33.33
Sometimes	38.89	66.67	23.53	5.56	16	20	31.58	0	27.78	0
Very often	22.22	0	5.88	5.56	14.67	15	10.53	33.33	11.11	16.67
Always	11.11	33.33	0	0	8	7.5	15.79	0	16.67	0

Table 2: Survey Results by Gender and Country (M = Male and F = Female)

The survey results also show that Finland has the highest percentage of male cloud users while Nepal has the least percentage of male cloud users. Finland and UK have the highest percentage of female cloud users. China has least percentage of female cloud users among all those countries. The reason behind this is that men are more interested in technological studies than women and less women has technical background [Kandel *et al.*, 2017]. It is also supported by [Alejos *et al.*, 2014] which states that, while there is rise in labour demand in ICT sector, there is a declination in the presence of women in both the student and professional levels.

The analysis of reasons for not using cloud services shows that trust is the common issue in all those four countries. Trust issue can also be seen from the data analysis results of security considerations while using cloud services. This proves that trust issue is one of the major issue in cloud services which is also supported by several literature review findings, for instance, [Noor *et al.*, 2013], which has stated trust as one of the challenging issue in cloud computing.

No need of cloud services is second common reason for both male and female participants in all those countries. Not having knowledge of using cloud services is other reason in both male and female participants. These results show that there is lack of knowledge about cloud services, its benefits and ways to use cloud services in IT students in higher educational institutions.

Cloud services are being used to store and process sensitive, confidential data which can also be seen from data analysis results in table 2 which show that most of the participants (both male and female) from all countries put confidential data in the cloud.

Encrypting data before uploading into cloud services is one of the way to protect confidential data in cloud from unauthorized access. From the survey results, it can be clearly seen that some participants are using encryption mechanism before uploading data into cloud. However, its usage does not look satisfactory. Therefore, the usage of various encryption mechanisms should be promoted so that the sensitive information could be protected from various attacks.

The influence of national culture in using cloud services is studied using Hofstede's dimensions of national culture. Professor Geert Hofstede conducted a study on how workplace values are influenced by culture. He defines culture as "the collective programming of the mind distinguishing the members of one group or category of people from others". Based on the research by Geert Hofstede and the team, there are six dimensions of national culture as follows [Hofstede *et al.*, 2010] [Hofstede, 2001]:

- Power Distance Index (PDI)
- Individualism versus Collectivism (IDV)
- Masculinity versus Femininity (MAS)
- Uncertainty Avoidance Index (UAI)
- Long Term Orientation versus Short Term Normative Orientation (LTO)

- Indulgence versus Restraint (IND)

The score for each cultural dimension for those five countries can be found in [Hofstede Insights, 2017] which is shown in the table below.

	<b>China</b>	<b>Finland</b>	<b>Greece</b>	<b>Nepal</b>	<b>UK</b>
Power Distance Index (PDI)	80	33	60	65	35
Individualism versus Collectivism (IDV)	20	63	35	30	89
Masculinity versus Femininity (MAS)	66	26	57	40	66
Uncertainty Avoidance Index (UAI)	30	59	100	40	35
Long Term Orientation versus Short Term Normative Orientation (LTO)	87	38	45	N/A	51
Indulgence versus Restraint (IND)	24	57	50	N/A	69

Table 3: National Culture Dimensions in five countries [Hofstede Insights, 2017]

As shown in the table 3, Finland and the UK have the highest scores both in Individualism versus Collectivism (IDV) and Indulgence versus Restraint (IND) which is in accordance with the fact that the students from Finland and the UK had the highest rate of using cloud services. Both Finland and the UK have the lowest answer rate in 'I never heard' or 'I don't know how to use them' for the question about reasons for not using cloud services. This may also imply that the main reasons for adopting new methods or technology are their motivation and initiative. Among all countries, Greece has the highest score in Uncertainty Avoidance Index among all other countries. This can also be seen from the answers "*I do not trust*" towards question about the reason for not using cloud by Greek students. The ratio of this answer by Greek students is much more than that from other countries. The answers '*I never needed*' by the Greek students can also be explained in a similar way in which 53.85% of Greek students had selected this answer, which is higher than the 2nd highest percentage (50 %) in Finland and Nepal, where Uncertainty Avoidance value is 59 and 40 respectively.

There are still many higher educational IT students who are using cloud services in one or other way but due to lack of knowledge of cloud services, they do not know that they are using it. This may be one of the reasons why certain percentage (18.94%) of

total participants answered that they do not use cloud. There may be several reasons for not using cloud services. One of those reasons could be unawareness of cloud services and its benefits. There may be a group of people or organizations not having knowledge of benefits of using cloud services. Nowadays, cloud services are being used in one or other way in our daily activities. There may also be a group using cloud services in some way but not having idea about using it.

These results about the cloud usage can also be discussed in a relation to the usability of cloud services. As the main concern while using cloud services is security, the cloud service provider may tend to provide the best secured services and may not think about the usability of the services which may result into the services which are good from security perspective but not good from usability perspective. The cloud service users may not use such services which are not easy to use even though they are secured.

The most common reason for not using cloud from the participants was not having the need to use cloud. There may be some students who are using cloud services, but they may have misconception about cloud, for instance, some may think of Dropbox as cloud and they think they do not use cloud if they do not use Dropbox. There may also be some students who really do not need cloud services, but this number may be very small as cloud services nowadays are closely related to our various daily activities. Not trusting the cloud service provider is second most common reason for future IT professionals which is also supported by [Harbajanka and Saxena, 2016] which states that trust is very important factor in cloud computing technology. This is one of the serious issues in cloud services as users are storing their sensitive or confidential information on cloud and they don't know about the data storage location and they do not have control over their data's lifecycle. Reputation of cloud service provider and adequate security in the services offered are some elements for trusting the cloud service provider. As, security is one of the factor to build the trust, service provider can use cryptographic solutions to their services as cryptography provides protection to user's data as it uses encrypted data [Harbajanka and Saxena, 2016]. When data is outsourced and stored on cloud server, it should be stored in encrypted format so that data cannot be accessed by unauthorized person even if it is lost during transmission [Cachin *et al.*, 2009].

While considering the data analysis results, there are only two reasons for not using cloud by female participants, not having the need to use cloud and having no idea of how to use cloud whereas there are several reasons for not using cloud by male participants. Not trusting the cloud services is one of the reasons for the male participants for not using cloud. Trust issue is the common reason for not using cloud services in all the four countries. It shows that the trust issue is one of the major issues in cloud computing. Not everyone trusts cloud security as the biggest risk lies on giving

the full control of your sensitive data and information to someone in remote location. There may be various factors for not trusting cloud services. Having knowledge of different cloud security issues may be one of those factors. Individuals and organizations may be afraid to use cloud after knowing the cloud security issues. Not having idea of how data is handled in cloud by service provider may be other factor for not trusting cloud. As users puts very sensitive data in cloud, it is difficult to trust cloud if they don't know how service provider will take care of their data. Lack of knowledge about different cloud security measures is another factor for not trusting cloud. If the users have idea of those security measures, users can be sure that their sensitive, confidential data is safe in cloud.

Cloud security issues are one of the major reasons for not trusting cloud. As sensitive and confidential data and information are moved into the cloud, security is the major concern in cloud services. Security is viewed as a composite notion, namely “the combination of confidentiality, the prevention of the unauthorized disclosure of information, integrity, the prevention of the unauthorized amendment or deletion of information, and availability, the prevention of the unauthorized withholding of information” [Avizienis, 2004]. There are also cloud service provider's trust issues towards cloud users. Regarding the service provider's trust towards the cloud users, service provider may not be completely sure that the users only use the services as provided by the provider and do not perform any such activities which may create security threats for other users and service providers. However, this study focuses on cloud user's trust towards the service provider.

Several research and articles have already been published in cloud security issues. Since cloud computing involves various components and technologies such as resource allocation, virtualization, cloud networks, operating systems, databases and memory management, there may occur numerous security issues if each cloud component and technology used is not secure. [Kaur and Kaur, 2015]. For instance, if the cloud network is not secure, there would be network based issues such as man-in-middle attacks. Similarly, virtualization, resource allocation and memory management may result in numerous issues if not performed in secure way. There may be cloud security issues such as denial of service (DoS) attack, account or service traffic hijacking, Man-in-the-Middle attacks, replay attack, session hijacking, signature wrapping attack and cloud malware injection attack [Kotha, 2015]. Data access control, data integrity, data loss, data theft, privacy issues, user level issues and security issues are the other security issues in cloud computing [Kaur and Kaur, 2015].

The attackers can get access to the sensitive and confidential data in cloud and may misuse the data. Therefore, controlling the unauthorized access to cloud data is one of the issues in cloud computing. There may also be issues while entering the data, transmitting it or due to hardware malfunctions. Since, several organizations are

adopting cloud for handling sensitive data such as banking or business information, there comes a serious challenge not only to protect data from unauthorized access but also from data loss and data theft. Since the cloud users use external servers for storing the information, there may be privacy issues associated with it. In some cases, some user's action while using cloud may cause data loss or problem in accessing data for other users. The users should be aware of such actions while accessing cloud. The cloud service provider should make sure that the cloud server is secure from all the external security threats. These cloud security attacks can also be categorized based on different cloud components: storage-based attacks, network-based attacks, virtual machine-based attacks and application-based attacks [Khan, 2016]. Cloud Security Alliance (CSA) has identified the twelve cloud security issues [CSA, 2016]: data breaches, weak identity, credential and access management, insecure APIs, system and application vulnerabilities, account hijacking, malicious insiders, advanced persistent threats (APTs), data loss, insufficient due diligence, abuse and nefarious use of cloud services, denial of service and shared technology issues.

Considering the results of analysis of data about security considerations while using cloud, it can be seen that both male and female participants from all the five countries put their confidential data into cloud which is also supported by several literature review findings. Both the male and female participants do not always trust that the service provider will take good care of their data. The participants from Finland trust the service provider more than that from other countries. Very few participants (both male and female) use encryption before uploading data into cloud. More participants from Finland never encrypt data before putting into cloud. This may be because of the participants from Finland having more trust towards the cloud service providers. This may be because of some Finnish cloud service provider offering various cloud services, for instance, F-Secure [Fsecure, 2017]. They may trust those service providers as they may have the server in Finland due to which the consumers may feel that their data is in their own country and also it would be easier for them to communicate with the service provider.

SLR findings show that, although trust building process is challenging and gradual process, there are some ways to establish trust between CSPs and consumers. Use of authentication is one of those ways. Implementing user authentication before providing access to their information ensures users that their information can be accessed only by them which helps to build trust towards those cloud services. There are various authentication methods which can be implemented in cloud such as, username and password authentication, multifactor authentication, mobile trusted module, single sign on, public key infrastructure and biometric authentication [Farooq, 2017].

It is also necessary for CSPs to provide adequate security and ensure the consumers that secured infrastructure is used to store and process their data and they only have the full control over their data. It makes consumers confident that their data are securely stored and processed which establishes their trust over the service providers. It also helps to maintain a certain level of reputation so that existing users will continue using their services and new users will choose their services amongst services offered by other service providers. Accountability and transparency are also the basis for establishing trust with service providers [Huang and Nicol, 2013].

Different methods could be implemented to maintain the secured environment in cloud services. Cryptography is one of the important methods for this purpose. “Cryptography is a generic term used to describe the design and analysis of mechanisms based on mathematical techniques that provide fundamental security services” [Martin 2012]. It converts the plain information into encoded format and uses that encoded format for information exchange so that only the authorized users can have access to that information. It provides security against most of the active and passive security attacks as the encoded information is not in readable and understandable format even if unauthorized users get access to it. However, denial of service may be the exception as cryptography can provide very little protection against this attack. Normally, there need to be security controls in other infrastructure to provide the protection against denial of service attack. Different cryptographic techniques could be used to protect the data in cloud services, such as, encryption, data authentication, hashing and digital signing [Rijmen *et al.*, 2013].

There are several cryptographic algorithms such as, Data Encryption Standard (DES), Advanced Encryption Standard (AES), RSA and Secure Hash Algorithm (SHA) [Martin, 2012]. However, there are some factors which need to be taken into consideration while using those algorithms. One of them is strength which refers to the protection that the algorithm can provide. Not all algorithms provide security against all security issues. Therefore, algorithm that can provide protection against security issues in given situation should be implemented. Second factor to consider is appropriateness. As different cryptographic algorithms have different properties. The algorithm should be chosen in a way that it is appropriate for a particular security purpose. Another consideration should be cost of the algorithm. ‘Cost’ here refers to ease of use, efficiency of operation and the financial worth. [Martin, 2012] Implementing suitable cryptographic algorithms can help to secure the information in storage. However, securing data in motion (network) requires different approaches.

Encrypting data is one of the method to overcome the cloud security issues. However, the service providers encrypt the user’s data in cloud in most of the cases in existing practice. This arises serious trust issues with CSPs as users store and process sensitive information in cloud services and there may be risk of access and misuse of

their confidential information. There may be the risk of malicious insiders. Therefore, allowing users to encrypt their data by themselves before putting into cloud is one of the effective way to build the user's trust towards CSPs. [Berki *et al.*, 2017]

While requesting the personal information to the users, it should be made clear to users what is the purpose of collecting that information and how the information would be stored and processed. If the users don't understand why their personal information is requested and how the information is processed, there arises the suspicion which leads to users' distrust towards the CSP. As trust management is very important in cloud services, various trust management techniques, such as, PocT, RecT, RepT and PrdT can be used to manage the trust relationship between CSPs and service consumers.

Therefore, different measures need to be implemented to build the consumer's trust towards the service provider, for instance, EU countries want to create network of cybersecurity centers for the research of different encryption methods to build consumer's trust towards technology products and the centers could access encryption standards which could result in consumers using more encryption technology if it has been evaluated by EU researchers [Stupp, 2017]. The European Structural and Investment (ESI) Funds predict a contribution of up to €400 million for trust and cyber security. The funds could be used to enhance the interconnection and interoperability of digital infrastructures, trust and privacy services. [European Commission, 2017]

## **6. Conclusion and Recommendations**

This study concludes that trust issues are one of the biggest challenges in cloud based services. Distrust arises when users don't know why their personal information is requested and how the information will be processed. When cloud consumers feel that they don't have the full control over their information, then trust issue arises. It's difficult for the cloud users to trust the service providers not having good reputation. Users may not feel confident whether the infrastructure used to store and process their data is secured or not, which also leads to distrust towards service providers.

There are some measures which should be taken into consideration to build the user's trust towards cloud service provider. Implementing user authentication is one of the way to build user's trust towards cloud services. Security in services is another element in building trust as providing secured services helps to maintain reputation and ultimately establishes users' trust. Various methods such as, cryptography can be implemented to provide security against most of the active and passive attacks. Ensuring the consumers that their sensitive information is stored in secured infrastructure and only they have the full control over their information, is another important way to build user's trust.

Most of the future IT professionals use cloud. However, there is certain percentage of them not using cloud services. In Finland, Greece and UK, this percentage is much

lower compared to that in other countries (China and Nepal). The percentage of male cloud users is higher than that of female cloud users in China and Nepal (Asian countries) while opposite is true for Finland, Greece and UK (European countries).

Lack of knowledge about cloud services may be one of the reasons for not using cloud services. Lack of knowledge about cloud security measures may be another reason for individuals and organizations for not using cloud services as they feel it insecure to use due to security issues. There are also other reasons for not using cloud services by future IT professionals such as, not having need to use cloud services and not having knowledge about how to use them. It shows a need of cloud related courses for higher level IT students so that they can utilize the benefits offered by cloud services along with the knowledge of cloud security measures against different attacks.

Regarding the security considerations while using cloud services, most of the male and female students use cloud services to store their confidential data and trust issue is an issue in cloud services for them. Some students use encryption mechanism before uploading their data into cloud whereas others do not use it. It shows that there is lack of knowledge about encryption (cryptography). Those students should have knowledge about cryptography as it is one of the effective ways to provide security in cloud services.

For the individuals who are not using cloud services due to lack of security mechanisms in cloud should be provided with knowledge about encryption mechanisms and for those who do not use cloud services due to lack of trust, one way would be allowing them to encrypt their data by themselves before putting the data into cloud.

This study has analyzed all the findings from national and gender perspective which shows that national culture and gender plays a significant role in choosing IT studies as well as adopting cloud services and considering security issues while using them. The less number of female IT students shows that more men are interested in technological studies than women. Women should be encouraged to study IT as its scope and usage is increasing every day. Various awareness programs, mentoring and scholarship program should be introduced to achieve the equal gender distribution in technologies studies.

The results about the cloud usage by future IT professional and their security considerations presented by this study could be helpful for the higher educational institutions to redesign the curriculum in a way that students would be aware of cloud services, their advantages and challenges, security measures. It also presents the reasons for not using cloud services which can be useful for the cloud service providers to consider while providing services to consumers. The data presented in this study could be useful for researchers for further study and research. Another factor cloud service provider need to take into consideration is usability as it may be the reason for many individuals and organizations not using cloud services. Therefore, services offered to consumers should be secured and equally usable as well.

Therefore, the future IT professionals and other cloud service users should have Cryptography-based knowledge, which will result in more usage of encryption techniques by cloud services and service consumers. It helps to create the secured cloud environment and on the other hand, it will help to facilitate the trust relationship between the service providers and consumers.

## **7. Further Enhancements**

As this study was based on limited number of data from those five countries, more data could be collected in order to obtain better results. As this study shows that the national culture and gender plays a significant role in adaptation of IT, more studies could be done on national culture - technology adaptation relationship and gender - technology adaptation relationship. This study shows that adequate security in cloud services is one of the way to build trust between CSPs and consumers. However, it does not study different methods for creating secured environment in cloud services. Therefore, the use of various security methods to build trust between cloud users and cloud service provider could be further studied. Usability of cloud services could be examined. In cloud services, security is focused as a main priority while not paying more attention on usability of cloud services. The usability of cloud services could be studied.

## References

- [Alejos *et al.*, 2014] Ana Vazquez Alejos, Manuel Garcia Sanchez, Maria Pilar Milagros, Francisco Falcone, Pablo Sanchís and Antonio López-Martín, The Influence of gender in the adoption of engineering studies, 2014.
- [Alibaba Cloud, 2017] Retrieved September 14, 2017, from, <https://www.alibabacloud.com/product>.
- [Alibaba, 2017] Retrieved September 14, 2017, from, <https://www.alibabacloud.com/why-alibaba-cloud?>.
- [Amazon, 2017] Retrieved July 15, 2017, from, <http://aws.amazon.com/ec2/>
- [Artz and Gil, 2007] Donovan Artz and Yolanda Gil, A survey of trust in computer science and the semantic web, 2007.
- [Avizienis, 2004] Algirdas Avizienis, Jean-Claude Laprie, Brian Randell, Carl Landwehr. Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing* 1(1), 2004.
- [Berki *et al.*,2017] Eleni Berki, Chetan Sharma Kandel, Yan Zhao and Sunil Chaudhary, A comparative study of cyber-security knowledge in higher educational institutions of five countries. In: *Proc. of 9th International Conference on Education and New Learning Technologies*, 2017, 2796-2806.
- [Bose *et al.*,2013] Ranjit Bose, Xin (Robert) Luo and Yuan Liu, The roles of security and trust: comparing cloud computing and banking. In: *2<sup>nd</sup> International Conference on Integrated Information*,2013, 30-34.
- [Bradford, 2017] [Contel Bradford](#), What is an advanced persistent threat? APT definition, Retrieved November 8, 2017, from, <https://www.storagecraft.com/blog/7-infamous-cloud-security-breaches/>
- [Brandenburger *et al.*, 2015] Marcus Brandenburger, Christian Cachin and Nikola Knežević, Don't Trust the Cloud, Verify: Integrity and Consistency for Cloud Object Stores. In: *SYSTOR'15*, 2015.
- [Cachin *et al.*, 2009] Christian Cachin, Idit Keidar and Alexander Shraer, Trusting the cloud. In: *ACM SIGACT News* 40(2), 2009, 81-86.
- [Cappelli *et al.*, 2012] Dawn Cappelli, Andrew Moore, Randall Trzeciak, The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud), The SEI Series in Software Engineering, 2012. Retrieved from <http://ptgmedia.pearsoncmg.com/images/9780321812575/samplepages/9780321812575.pdf>.
- [Chaudhary, 2016] Sunil Chaudhary, The Use of Usable Security and Security Education to Fight Phishing Attacks, 2016. PhD Thesis. School of Information Sciences, University of Tampere.

- [CNET, 2009] Retrieved October 12, 2017, from, <https://www.cnet.com/news/the-biggest-cloud-computing-issue-of-2009-is-trust/>
- [CSA,2017] Retrieved August 30, 2017, from, <https://cloudsecurityalliance.org/about/>
- [CSA, 2016] Cloud Security Alliance, The Treacherous 12 - Cloud Computing Top Threats in 2016, 2016. Retrieved from [https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12\\_Cloud-Computing\\_Top-Threats.pdf](https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf)
- [Cummins, 2015] Dave Cummins, The Top Ten Cloud Computing Countries in the EU, Retrieved August 22, 2017, from, <https://www.comparethecloud.net/articles/the-top-ten-cloud-computing-countries-in-the-eu/>
- [European Commission, 2017] EU cybersecurity initiatives, Retrieved 23 November 2017, from, [http://ec.europa.eu/information\\_society/newsroom/image/document/2017-3/factsheet\\_cybersecurity\\_update\\_january\\_2017\\_41543.pdf](http://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf).
- [Farooq, 2017] Huma Farooq, A Review on Cloud Computing Security Using Authentication Techniques. In: *International Journal of Advanced Research in Computer Science* **8(2)**, 2017 19-22.
- [Ferkoun, 2014] Maamar Ferkoun, Top 7 most common uses of cloud computing, Retrieved July 15, 2017, from, <https://www.ibm.com/blogs/cloud-computing/2014/02/top-7-most-common-uses-of-cloud-computing/>
- [Force, 2017] Retrieved July 15, 2017, from, <https://www.salesforce.com/products/platform/products/force/>
- [Fsecure, 2017] Retrieved October 28,2017 from, [https://www.f-secure.com/en/web/business\\_global/cloud-protection-for-salesforce](https://www.f-secure.com/en/web/business_global/cloud-protection-for-salesforce)
- [Gartner, 2017] Gartner Says Worldwide Public Cloud Services Market to Grow 18 Percent in 2017, Retrieved July 18, 2017, from, <http://www.gartner.com/newsroom/id/3616417>
- [Google Cloud, 2017] Retrieved July 15, 2017, from, <https://cloud.google.com/appengine/>
- [Grandison and Sloman, 2003] Tyrone Grandison and Morris Sloman, Trust Management Tools for Internet Applications. In: *Proc. Of 1st Int.Conference on Trust Management*, 2003, 91-107.
- [Harbajanka and Saxena, 2016] Shimpy Harbajanka and Dr. Preeti Saxena, Survey paper on trust management and security issues in cloud computing. In: *2016 Symposium on Colossal Data Analysis and Networking (CDAN)*, 2016.
- [Harbajanka and Saxena, 2016] Shimpy Harbajanka and Preeti Saxena, Security Issues and Trust Management in Cloud Computing. In: *WIR'16*, 2016.

- [Hofstede Insights, 2017] Compare Countries, Retrieved October 12, 2017, from, <https://www.hofstede-insights.com/product/compare-countries/>.
- [Hofstede *et al.*, 2010] Geert Hofstede, Gert Jan Hofstede and Michael Minkov, Cultures and Organizations: Software of the Mind. Revised and Expanded 3rd Edition. New York: McGraw-Hill USA, 2010.
- [Hofstede, 2001] Geert Hofstede, [Culture's Consequences: Comparing Values, Behaviors, Institutions, and Organizations Across Nations](#). Second Edition, Thousand Oaks CA: Sage Publications, 2001.
- [Huang and Nicol, 2013] Jingwei Huang and David M Nicol. 2013. Trust mechanisms for cloud computing. *Journal of Cloud Computing: Advances, Systems and Applications*.
- [Kandel *et al.*, 2017] Chetan Sharma Kandel, Eleni Berki, Yan Zhao, Sunil Chaudhary, Margaret Ross and Geoff Staples, A Comparative Study of Cloud Services Use by Prospective IT Professionals in Five Countries. In: *Proc. of Software Quality Management International Conference (SQM2017)*, 2017, 175-187.
- [Kessler, 2017] Gary C. Kessler, An Overview of Cryptography, Retrieved July 20, 2017, from, <http://www.garykessler.net/library/crypto.html>
- [Khan, 2016] Minhaj Ahmad Khan, A survey of security issues for cloud computing, *Journal of Network and Computer Applications* **71**, 2016, 13-15.
- [Khorshed *et al.*, 2011] Md Tanzim Khorshed, A B M Shawkat Ali and Saleh A. Wasimi, Trust Issues That Create Threats for Cyber Attacks in Cloud Computing. In: *Proc. of 2011 IEEE 17th International Conference on Parallel and Distributed Systems*, 2011, 900-905.
- [Kirk, 2017] Jeremy Kirk, Australian Government Contractor Exposed 50,000 Records, Retrieved November 8, 2017, from, <https://www.databreachtoday.com/australian-government-contractor-exposed-50000-records-a-10432>
- [Kotha, 2015] Navaneetha Kotha, Evaluation of Secure Access Connectivity to Cloud Service, 2015.
- [Lansing and Sunyaev, 2016] Jens Lansing and Ali Sunyaev, Trust in Cloud Computing: Conceptual Technology and Trust-Building Antecedents, 2016, 58-96.
- [Lord, 2017] Nate Lord, The history of data breaches, Retrieved November 9, 2017, from, <https://digitalguardian.com/blog/history-data-breaches>
- [Lord, 2017] Nate Lord, what is an advanced persistent threat? APT definition, Retrieved September 4, 2017, from, <https://digitalguardian.com/blog/what-advanced-persistent-threat-apt-definition>
- [Lukan 2014] Dejan Lukan, The top cloud computing threats and vulnerabilities in an enterprise environment, Retrieved September 4, 2017, from,

<https://www.cloudcomputing-news.net/news/2014/nov/21/top-cloud-computing-threats-and-vulnerabilities-enterprise-environment/>

- [Marti and Garcia-Molina, 2006] Sergio Marti and Hector Garcia-Molina, Taxonomy of trust: Categorizing P2P reputation systems. In: *Computer Networks* 50, 2006, 472-484.
- [Martin, 2012] Keith M. Martin, *Everyday Cryptography: Fundamental Principles and Applications*. OUP Oxford, 2012.
- [Mell and Grance, 2011] Peter Mell, Timothy Grance, The NIST Definition of Cloud Computing. In: NIST Special Publications 800-145. Tech. Rep., 2011. Retrieved from <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>.
- [Microsoft, 2017] Retrieved July 15, 2017, from, <https://www.office.com/>
- [Microsoft Azure, 2017] Retrieved July 15, 2017, from, <http://azure.microsoft.com/en-us/>
- [Noor *et al.*, 2013] Talal H. Noor, Quan Z. Sheng, Sherali Zeadally and Jian Yu, Trust management of services in cloud environments: Obstacles and solutions. *ACM Comput. Surv.* **46**(1). Retrieved from, <http://dx.doi.org/10.1145/2522968.2522980>.
- [Pardo *et al.*, 2016] Jorge Pardo, Andrew Flavin, Michael Rose, International Trade Administration. 2016 Top Markets Report Cloud Computing, A Market Assessment Tool for U.S. Exporters, 2016. Retrieved from [http://trade.gov/topmarkets/pdf/Cloud\\_Computing\\_Top\\_Markets\\_Report.pdf](http://trade.gov/topmarkets/pdf/Cloud_Computing_Top_Markets_Report.pdf).
- [Pearson and Benameur, 2010] Siani Pearson and Azzedine Benameur, Privacy, security and trust issue arising from cloud computing. In: *Proc. of 2<sup>nd</sup> IEEE Internatioanl Conference on Cloud Computing Technology and Science*, 2010, 693-702.
- [Rad *et al.*, 2017] Babak Bashari Rad, Tinankoria Diaby and Muhammad Ehsan Rana, Cloud Computing Adoption: A Short Review of Issues and Challenges. In: *Proc. of ICEEG*, 2017, 51-55.
- [Rijmen *et al.*, 2013] Vincent Rijmen, Daniel De Cock, Nigel P. Smart and Rodica Tirtea, Recommended cryptographic measures, 2013. Retrieved from, <https://www.enisa.europa.eu/publications/recommended-cryptographic-measures-securing-personal-data>.
- [Rouse, 2017] Margaret Rouse, Cryptography, Retrieved November 23, 2017, from, <http://searchsoftwarequality.techtarget.com/definition/cryptography>
- [Rouse, 2017] Margaret Rouse, Passive attack, Retrieved November 23, 2017, from, <http://whatis.techtarget.com/definition/passive-attack>
- [Sabatar and Sierra, 2005] Jordi Sabatar and Carles Sierra, Review on computational trust and reputation models, 2005.
- [Salesforce, 2017] Retrieved July 15, 2017, from, <http://www.salesforce.com/eu/>

- [Schwartz, 2017] [Mathew J. Schwartz](#), Hacker Steals Joint Strike Fighter Plans in Australia, Retrieved November 9, 2017, from, <https://www.databreachtoday.com/hacker-steals-joint-strike-fighter-plans-in-australia-a-10376>
- [Sherchan *et al.*, 2013] Wanita Sherchan, Surya Nepal and Cecile Paris, A survey of trust in social networks. *ACM Comput. Surv.* **45**(4), 2013. Retrieved from, <http://dx.doi.org/10.1145/2501654.2501661>.
- [Silaghi *et al.*, 2007] Gheorghe Cosmin Silaghi, Alvaro E. Arenas and Luis Moura Silva, Reputation-based trust management systems and their applicability to grids. Tech. rep. Core-GRID (TR-0064), Institute on Knowledge and Data Management Institute on System Architecture, 2007.
- [Stupp, 2017] Catherine Stupp, New EU cybersecurity centers slated to research encryption, 2017. Retrieved from, <https://www.euractiv.com/section/cybersecurity/news/new-eu-cybersecurity-centres-slated-to-research-encryption/>.
- [Sun *et al.*, 2011] Dawei Sun, Guiran Chang, Lina Sun and Xingwei Wang, Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments, 2011.
- [Techopedia, 2017] Retrieved November 23, 2017, from, <https://www.techopedia.com/definition/811/data-integrity-databases>
- [Wikipedia, 2017] Retrieved November 23, 2017, from, [https://en.wikipedia.org/wiki/Application\\_programming\\_interface](https://en.wikipedia.org/wiki/Application_programming_interface)

## **Appendix**

### **Important terminologies and definitions**

#### Account hijacking

In such attacks, attackers can get access to the credentials which can be used to eavesdrop on user's transactions or activities, access confidential data, provide false information or redirect the users to some other sites.

#### Account or service traffic Hijacking

Attacks in which the attackers try to get access to user's credentials and eavesdrops on the transactions and other activities. [Kotha, 2015]

#### Active attacks

Attacks which generally involve modification of data or some process being executed on the data.

#### Advanced Persistent Threats (APTs)

In such kind of attacks, unauthorized user gains access to the system and remains there for long period of time being undetected. Mostly, the goal of APT is data theft. [Lord, 2017]

#### Application Programming Interfaces

An application programming interface (API) is a set of subroutine definitions, protocols, and tools for building application software [Wikipedia, 2017].

#### Cloud Malware Injection Attack

In such attacks, the attacker creates his own malicious program or application and adds it to the cloud system.

#### Cryptography

It is a method to store and transmit the data in a particular format so that only the intended users can access and process that data [Rouse, 2017].

#### Data Access Control

It is a process of controlling the unauthorized access to the data.

#### Data Breaches

In such attacks, sensitive or confidential information is viewed, used, stolen or released by the unauthorized users.

### Data Integrity

Data integrity is the accuracy, completeness and consistency of data [Techopedia, 2017].

### Denial of Service (DoS)

It is an attack in which attacker prevents authorized users from using online service by temporarily or indefinitely disrupting services of a host connected to the internet.

### Encryption

It is process of converting the plain data into encoded format in cryptography.

### Insufficient Due Diligence Issues

Issues such as financial risks, commercial risks, legal risks and technical risks when any enterprise or organization move to cloud technology without performing due diligence.

### Malicious insiders

“A malicious insider threat is a current or former employee, contractor, or business partner who has or had authorized access to an organization’s network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization’s information or information systems” [Cappelli, Moore and Trzeciak, 2012].

### Man-in-the-Middle Attack

In such attacks, the attacker remains in between the client and server and may either redirect the client to wrong websites or modify the data.

### Passive attacks

The attacks in which the attacker monitors the target system, scans for vulnerabilities and get information about it. In such attacks, the attacker does not change any data on the target system. [Rouse, 2017]

### Replay Attack

Attacks in which the attackers steal the packet from the network and sends it to the server repeatedly with the intention to use it maliciously. [Kotha, 2015]

### Session Hijacking

In such attacks, the attacker gets access to the user's session information and make requests to the cloud server as if he is the valid user.

#### Signature Wrapping Attack

Attacks in which invalid or fake element is injected into a message structure as a valid message despite of having the digital signed operation [Kotha, 2015].

#### System and application vulnerabilities

The bugs in cloud system and applications that can be useful for attackers to take control over the system and disrupt the services or steal the information.