Master Thesis
Electrical Engineering

November 2011

Security Techniques for Protecting Data in Cloud Computing

Venkata Sravan Kumar Maddineni
Shivashanker Ragi

School of Computing
Blekinge Institute of Technology
SE - 371 79 Karlskrona
Sweden

This thesis is submitted to the School of Computing at Blekinge Institute of Technology in partial fulfillment of the requirements for the degree of Master of Science in Software Engineering. The thesis is equivalent to 40 weeks of full time studies.

Contact Information:
Author(s):
Venkata Sravan Kumar Maddineni
Karlskrona, Sweden
sravanmusic@gmail.com

Shivashanker Ragi
Karlskrona, Sweden
ragis38@gmail.com

External advisor(s):
Mj Jens Kvarnberg
Swedish Armed Forces
jens.kvarnberg@mil.se

Mr. Ross W Tsagalidis
Swedish Armed Forces
wross@tele2.se

University advisor:
Prof. Lars Lundberg, PhD
School of Computing
lars.lundberg@bth.se

School of Computing
Blekinge Institute of Technology
SE - 371 79 Karlskrona
Sweden

Internet	: www.bth.se/com
Phone	: +46 455 38 50 00
Fax	: +46 455 38 50 57

ABSTRACT

Context: From the past few years, there has been a rapid progress in Cloud Computing. With the increasing number of companies resorting to use resources in the Cloud, there is a necessity for protecting the data of various users using centralized resources. Some major challenges that are being faced by Cloud Computing are to secure, protect and process the data which is the property of the user.

Aims and Objectives: The main aim of this research is to understand the security threats and identify the appropriate security techniques used to mitigate them in Cloud Computing.
The main objectives of this research are:

- To understand the security issues and the techniques used in the current world of Cloud Computing.
- To identify the security challenges, those are expected in the future of Cloud Computing.
- To suggest counter measures for the future challenges to be faced in Cloud Computing.

Research Methodology: In this study, we have used two research methods.

- Systematic Literature Review.
- Survey and interviews with various security experts working on Cloud Computing.

Result: As a result, we have identified the total of 43 security challenges and 43 security techniques. The most measured attribute is confidentiality (31%) followed by integrity (24%) and availability (19%). The impact of identified mitigation techniques is mainly on security (30%), followed by performance (22%) and efficiency (17%). Also we have identified 17 future challenges and 8 mitigation practices.

Conclusion: The identification of security challenges and mitigation techniques in large number of services of Cloud Computing is a very challenging task. In the process of identification from research methods (SLR and Survey), we had identified a satisfactory number of challenges and mitigation techniques which are being used at present and also in future Cloud Computing.

Keywords: Challenges, Cloud Computing, Security, Techniques.

ACKNOWLEDGEMENT

Any attempt at any level can't be satisfactorily completed without the support and guidance of our professor. We would like to express our immense gratitude to our Prof. Lars Lundberg for his constant support and motivation that has encouraged us to come up with this project. We are very thankful to our professor who has rendered their whole hearted support at all times for the successful completion of this thesis "Security Techniques for Protecting Data in Cloud Computing". Furthermore, we are very much thankful to Mr. Jens Kvarnberg and Mr. Ross W Tsagalidis for their support and help throughout the research.

We would also like to thank our survey participants who have contributed towards survey part of this thesis. Finally, we are greatly thankful to our beloved parents and friends for their relentless support that they had given us to reach our goals.

Yours truly,
Venkata Sravan Kumar Maddineni,
Shivashanker Ragi.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

1 INTRODUCTION

From the past few years, there has been a rapid progress in Cloud Computing. Cloud Computing delivers a wide range of resources like computational power, computational platforms, storage and applications to users via internet. The major Cloud providers in the current market segment are Amazon, Google, IBM, Microsoft, Salesforce, etc... With an increasing number of companies resorting to use resources in the Cloud, there is a necessity for protecting the data of various users. Some major challenges that are being faced by Cloud Computing are to secure, protect and process the data which is the property of the user. Below, we have described the two main states that hold your data is out in the Cloud: when the data is in motion (transit) and when the data is at rest, where the data is much expected to be more secure. The below illustrated are the two main scenarios which we have focused to understand the security of the data in the Cloud.

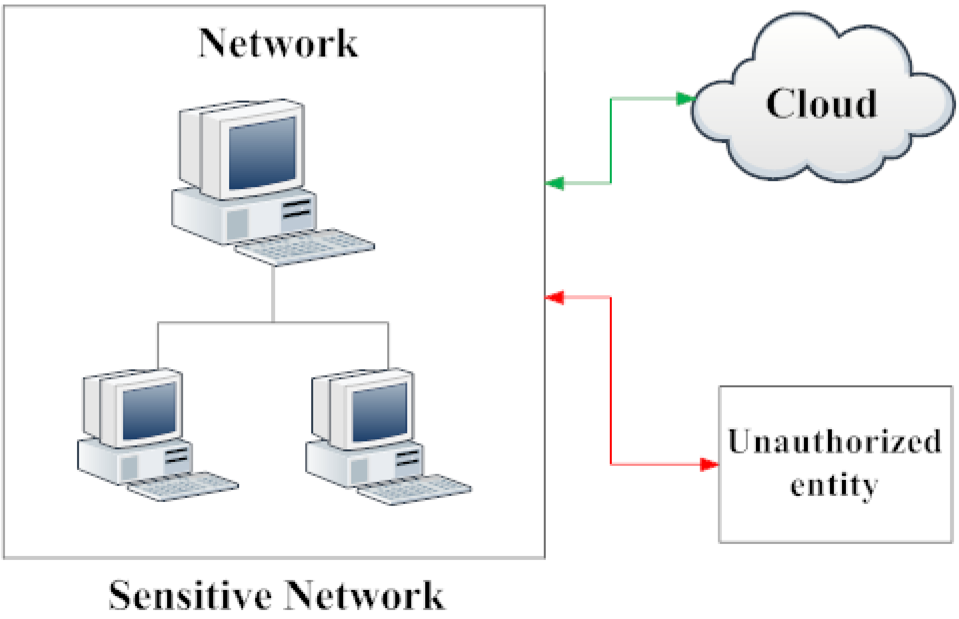


Figure 1.1 Unauthorized access of data between the network and Cloud

The above figure 1.1 describes a scenario where a local network is connected to a Cloud network, in which some part of the network data is broken out from the local network and placed in the Cloud, but the critical data resides in the local network itself. In this case, the Cloud provider does not have any privilege of accessing the data physically which is in the local network. But in some cases, the Cloud needs to access some information which is in the local network, during that access; there exists a possibility of unauthorized access of the local network resources. It describes the typical problem in network security where the information can face active attacks and passive attacks. The active attacks include masquerading, replay attack, modification of messages and denial of service. Passive attacks include traffic analysis. These attacks are likely to happen when the stream of information leaves the client network to the Cloud network.

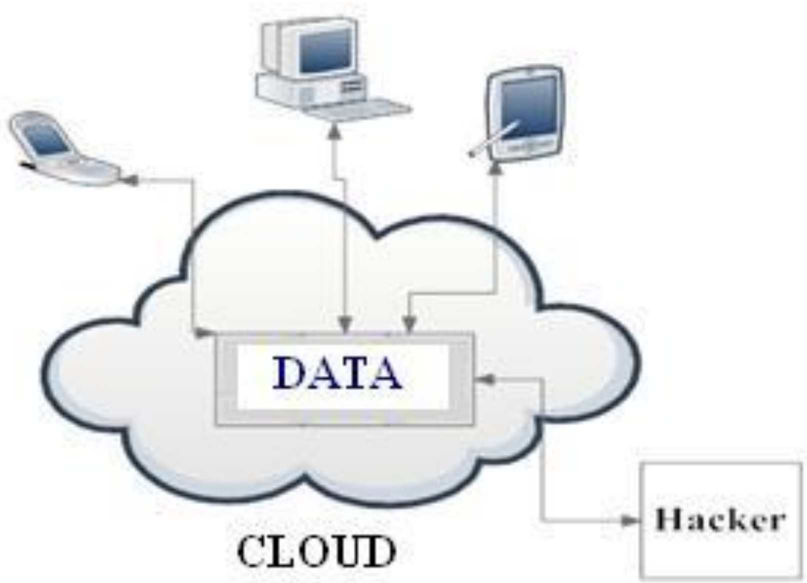


Figure 1.2 Unauthorized access of data within the Cloud

The above figure 1.2 describes the scenario where the total data of the local network resides within the Cloud, where the local network and the authorized users can access their data physically in the Cloud. At that instant of time, there exists a possibility for unauthorized users to enter and access the data in the Cloud. In this situation, the virtual machines are allotted to users of the Cloud. These machines have valid logins. However, these logins can be abused and cracked. The data may also be accessed in other perverted ways.

Regarding this area of study, most of the research papers followed a normal traditional literature survey method. Few papers gave an innovative idea and proposed a security model. However, there are very few works, which considered the opinions of various security experts in Cloud Computing. This study proposes that, reader gets the true reflection of the security practices followed by various Cloud Computing companies in the current era. There are very few papers which focus on the security techniques for specified applications. Our work provides more knowledge in this dimension and also predicts the future threats likely to be faced by Cloud Computing and solutions to these threats.

1.1 Aims and Objectives

The main aim of this research work is to identify and understand the security issues which affect the performance of Cloud Computing. Also, to understand the security techniques which are being used to mitigate these security issues. Thereby providing the standard guidelines for the Cloud service providers and as well as Cloud users.

The main objectives of this research are:

- To understand the security issues and to identify the appropriate security techniques those are being used in the current world of Cloud Computing.
- To identify the security challenges those are expected in the future of Cloud Computing.
- To suggest some counter measures for the future challenges to be faced in Cloud Computing.

1.2 Research Questions

Research Question 1: what are the various security techniques being used by the leading Cloud Computing providers, to prevent active and passive attacks when the data is being transferred between the Cloud and a local network?

Research Question 2: what are the various security techniques being used to prevent unauthorized access to data within the Cloud?

Research Question 3: what are the major security challenges we expect in future Cloud Computing?

Research Question 4: How can we handle security problems that are expected in future Cloud Computing?

1.3 Thesis outline

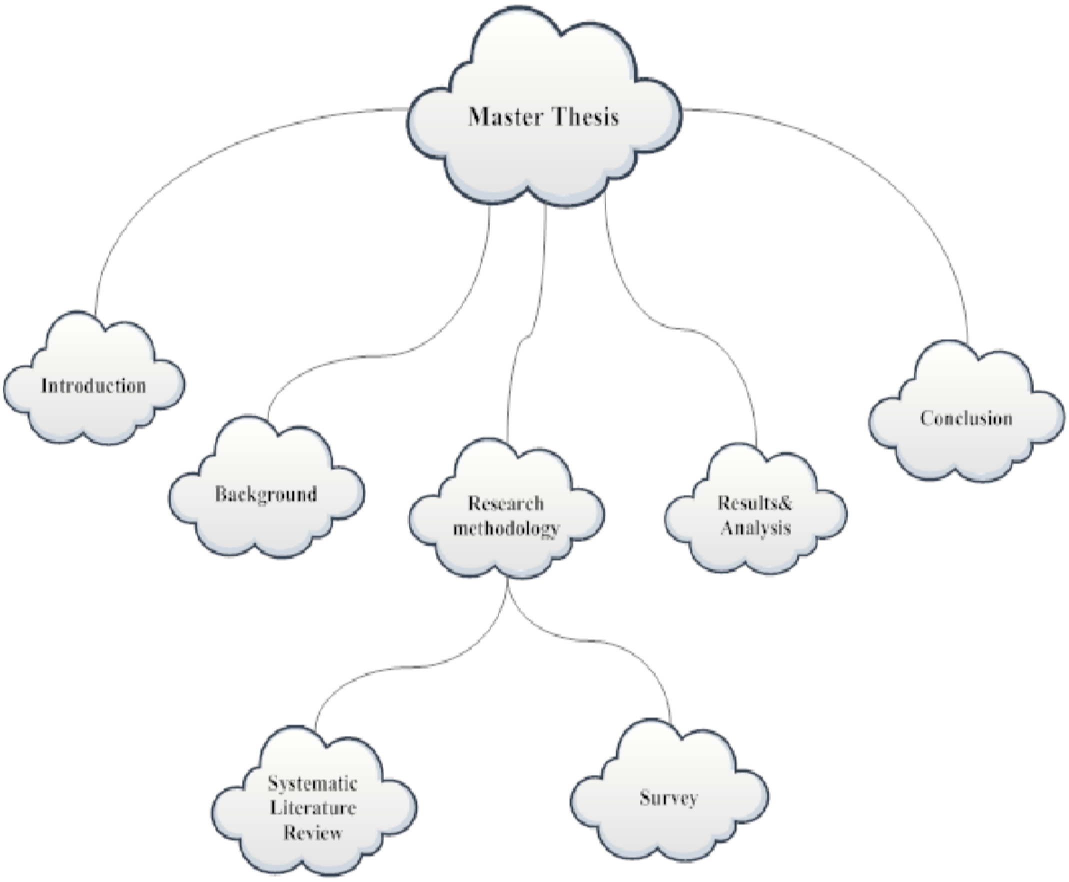


Figure 1.3 Thesis outline

The document is organized as follows: Chapter 1 discusses a brief introduction of the concepts used in this thesis and Chapter 2 discusses the background of Cloud Computing. The research methodologies and the data analysis used are presented in chapter 3. The process of Systematic Literature review is discussed in chapter 4 followed by a brief overview of Survey is discussed in chapter 5. The results from the Systematic Literature Review and Survey are presented in chapter 6. The validity threats of our thesis from various perspectives are discussed in chapter 7. Finally, the conclusion and future directions are discussed in chapter 8. The references used are cited and appendixes are referred at the end of the document.

CHAPTER 2

BACKGROUND

2 BACK GROUND

This chapter provides a brief overview about background of Cloud Computing. Section 2.1 provides the standard definition of Cloud Computing and its essential characteristics, services, deployment models respectively. The section 2.2 gives brief information about the Cloud Computing providers. Section 2.3 deals with the importance of security in the Cloud Computing, whereas section 2.4 provides the major security issues in Cloud.

2.1 What is Cloud Computing?

Cloud is a computing model that refers to both the applications derived as services over the Internet, the hardware and system software in the datacenters that provide those services. Cloud Computing is treated as the high potential paradigm used for deployment of applications on Internet. This concept also explains the applications that are broaden to be accessible through the Internet. Cloud applications use large data centers and effective servers that host web applications and services.

2.1.1 Definition of Cloud Computing

Cloud Computing is rapidly being accepted as a universal access appliance on the Internet. A lot of attention has been given to the Cloud Computing concept in deriving standard definitions. However, the definitions of Cloud Computing remain controversial. But here we have considered the standard definition which was given by the National Institute of Standards and Technology (NIST):

"Cloud Computing is 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", [44].

2.1.2 Essential Characteristics of Cloud Computing

According to NIST, the Cloud model is composed of five essential characteristics:

- ***On-demand self-service****: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider* [44].

- ***Broad network access****: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations)* [44].

- ***Resource pooling****: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth* [44].

- ***Rapid elasticity***: *Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time* [44].

- ***Measured service***: *Cloud systems automatically control and optimize resource use by leveraging a metering capability (pay-per-use basis) at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service* [44].

2.1.3 Service Models of Cloud Computing

According to NIST, the cloud model is composed of three service models:

- ***Software as a Service (SaaS)***: *The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings* [44].

- ***Platform as a Service (PaaS)***: *The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment* [44].

- ***Infrastructure as a Service (IaaS):*** *The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls)* [44].

2.1.4 Deployment Models of Cloud Computing

According to NIST, the cloud model is composed of four deployment models:

- ***Private cloud***: *The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises* [44].

- ***Community cloud****: The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises* [44].

- ***Public cloud:*** *The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider* [44].

- ***Hybrid cloud****: The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)* [44].

2.2 Drivers of Cloud Computing

Cloud Computing is rapidly growing area in the IT security space because Cloud architectures are popping up all over. The major driving thought Cloud providers present in the current market segment are Amazon, Microsoft, Google, IBM, Oracle, Eucalyptus, VMware, Eucalyptus, Citrix, Salesforce, Rackspace and there are many different vendors offering different Cloud services. The cloud providers are having different forms to provide their services [18]:

- Amazon: Amazon Web Services including the Elastic Compute Cloud (EC2), Amazon Simple Storage Service (S3), etc.
    - Provides a highly scalable computing platform to the customer with high flexibility and availability to build a wide range of applications.

- Google: Google App Engine
    - It supports application programming interfaces for the data store, image manipulation, Google accounts and e-mail services.

- Microsoft: Windows Azure Platform
    - Windows Azure platform is a group of Cloud technologies which provides a specific set of services to application developers.

- Eucalyptus
    - Eucalyptus is an open source software infrastructure to create private Cloud architecture on existing enterprise.
- IBM: Lotus Live (Platform as a Service)
- Salesforce: (Software as a Service)
- Rackspace Cloud: (formerly Mosso)
- VMware: Provide Virtualization infrastructure

2.3 Importance of Security in Cloud Computing

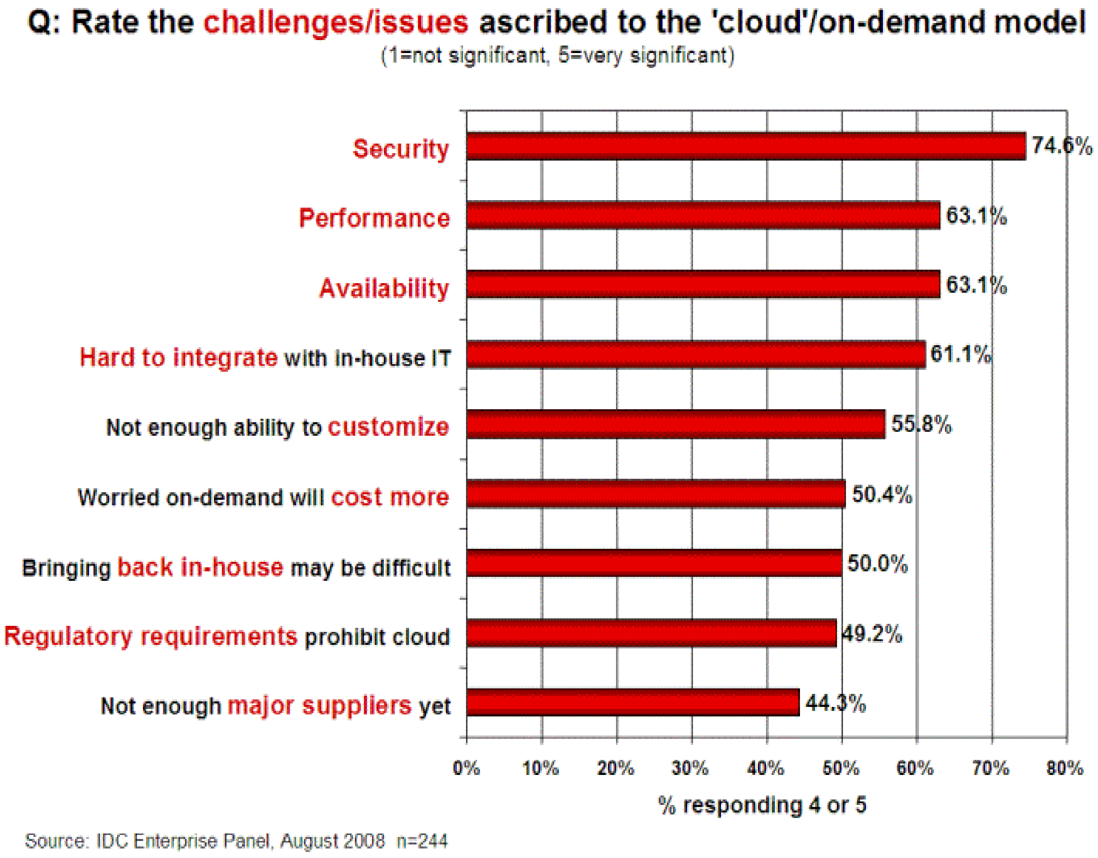


Figure 2.1 Importance of Security in Cloud Computing

(Source: http://www.csrc.nist.gov/groups/SNS/cloud-computing/cloud-computing-v26.ppt at slide 17.)

The above statistical resulted graph represents the results of the survey which was conducted by the IDC (International Data Corporation) in August, 2008 amongst senior business executives and IT professionals regarding the challenges/issues which mainly affect the performance of Cloud Computing. And the survey results show security at the top of the list which declares its importance compared to other parameters of Cloud Computing.

During a keynote speech to the Brookings Institution policy forum, “Cloud Computing for Business and Society”, Microsoft General Counsel Brad Smith also highlighted data from a survey commissioned by Microsoft for measuring attitudes on Cloud Computing among business leaders and the general population in January 2010. The survey found that while 58% of the general population and 86% of the senior business leaders are very much excited about the potential of Cloud Computing and more than 90% of these same people are very much concerned about the security, access and privacy of their own data in the Cloud. (Source: http://www.microsoft.com/ presspass/press/2010/jan10/1-20BrookingsPR.mspx).

The survey results show that the security is the major challenge amongst all the parameters that affect the performance and growth of Cloud Computing.

2.4 Important Security Issues in the Cloud

Even though, the virtualization and Cloud Computing delivers wide range of dynamic resources, the security concern is generally perceived as the huge issue in the Cloud which makes the users to resist themselves in adopting the technology of Cloud Computing. Some of the security issues in the Cloud are discussed below:

Integrity: Integrity makes sure that data held in a system is a proper representation of the data intended and that it has not been modified by an authorized person. When any application is running on a server, backup routine is configured so that it is safe in the event of a data-loss incident. Normally, the data will backup to any portable media on a regular basis which will then be stored in an off-site location [71].

Availability: Availability ensures that data processing resources are not made unavailable by malicious action. It is the simple idea that when a user tries to access something, it is available to be accessed. This is vital for mission critical systems. Availability for these systems is critical that companies have business continuity plans (BCP's) in order for their systems to have redundancy [71].

Confidentiality: Confidentiality ensures that data is not disclosed to unauthorized persons. Confidentiality loss occurs when data can be viewed or read by any individuals who are unauthorized to access it. Loss of confidentiality can occur physically or electronically. Physical confidential loss takes place through social engineering. Electronic confidentiality loss takes place when the clients and servers aren't encrypting their communications [71].

CHAPTER 3

RESEARCH METHEDOLOGY

3 RESEARCH METHODOLOGY

In this research work, we reviewed the previous work in order to acknowledge the current knowledge to answer the research questions 1 and 2. Most of the previous research works were done with traditional literature review which has low scientific value due to non- rigorous and unfair approach. Where the systematic literature review has is of highly defined characteristics with more clear scientific perspective. So we have undertaken the systematic literature review (SLR) as a primary research method, survey and interviews are considered as secondary research method. The outlook of the research methods which are used to answer the research questions is shown in figure 3.1

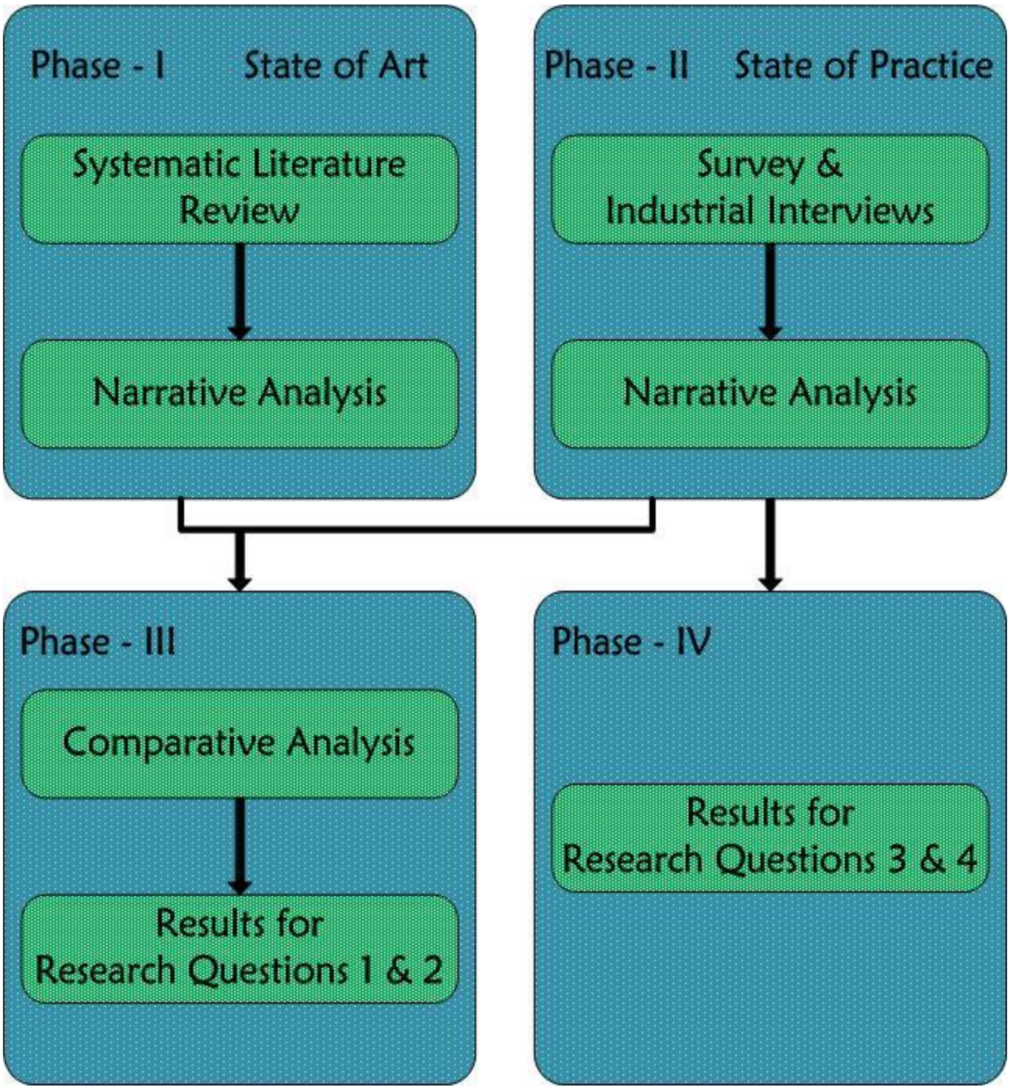

Phase - I State of Art
Systematic Literature Review
Narrative Analysis
Phase - II State of Practice
Survey & Industrial Interviews
Narrative Analysis
Phase - III
Comparative Analysis
Results for Research Questions 1 & 2
Phase - IV
Results for Research Questions 3 & 4

Figure 3.1 Research Design

3.1 Systematic Literature Review (SLR)

The following section provides description about the rationale for SLR and survey.

3.1.1 The rationale for SLR

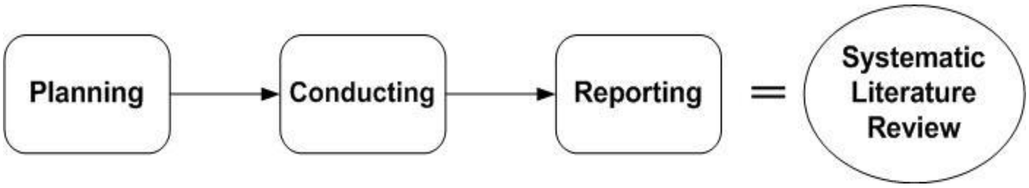
A Systematic literature review is a means of identifying, evaluating and interpreting all available research relevant to a particular research question, topic or phenomenon of interest [34]. Systematic reviews aims to present a fair evaluation of a research topic by using a trustworthy, rigorous and auditable methodology. A systematic literature review synthesizes existing work in a manner that is fair and seen to be fair. Systematic review must be undertaken in accordance with a predefined search strategy. The search strategy must allow the completeness of the research to be assessed. In particular, researchers performing a systematic review must make every effort to identify and report research that does not support their preferred research hypothesis as well as identifying and reporting research that supports it [34]. Systematic reviews are mainly undertaken to summarize the existing evidence, identifying the gaps in current research and providing a framework for new research activities [34].

The main features that differentiate a systematic literature review from a traditional literature review are:

- Systematic Literature Review addresses the specified research questions by defining a review protocol.
- Systematic review defines search strategy that aims to detect as much of the relevant literature as possible.
- Systematic reviews require inclusion and exclusion criteria to assess each potential primary study.

We adopted the guidelines and systematic process by kitchenham [34] in this research work.

Systematic review is conducted mainly in three phases:



- **Planning the review:** Associated with identification of need for a review and developing the review protocol.
- **Conducting the review:** Associated with selection of primary studies, quality assessment, data extraction and data synthesis.
- **Reporting the review:** Associated with reporting the results and documenting the process.

3.2 Survey

Survey is also one of the potential research methods. Survey represents one of the most common types of quantitative scientific research. In survey research, the researcher selects respondents from population and maintains a standardized questionnaire. The questionnaire can be a written document that is completed by the person being surveyed.

The different types of surveys are:

- Written surveys
- Oral surveys
- Electronic surveys

In this research, we have undertaken the electronic survey. In electronic survey questionnaire can be send via electronic mails to a potential respondent.

3.3 Data Analysis Methods

Data analysis or Data synthesis is a means of collecting and summarizing the results of the studies. Data analysis methods are used to structure the data properly based on the findings. In our thesis, initially we have focused on Narrative Analysis for analyzing the results which are obtained from doing Systematic Literature Review and thereafter we have used the Comparative Analysis method for comparing the results of the SLR with the results obtained from the Survey.

3.3.1 Narrative Analysis

Narrative analysis is a method of non-quantitative synthesis which represents the extracted information about studies should be tabulated in a manner consistent with the review questions. Tables should be structured to highlight similarities and differences between study outcomes. It is important to identify whether results from studies are consistent with one another (i.e. homogeneous) or inconsistent (e.g. heterogeneous). Results may be tabulated to display the impact of potential sources of heterogeneity [34].

The Frame work for Narrative analysis is:

- Developing a theory
- Developing a preliminary synthesis
- Exploring relationships in the data
- Assessing the robustness of the synthesis.

3.3.2 Comparative Analysis

Identifying the similarities and differences in the literature with real world context can be yielded through Comparative Analysis. Qualitative Comparative Analysis (QCA) was developed by Charles Ragin [50] [7] [8].

QCA was used to find the relation and dissimilarities between the contexts of study [39]. QCA focuses on recognizing “similarities, differences, and associations between entities” [39]. We have observed QCA fits liable to our study as we are focusing on identifying the challenges and mitigation strategies related to security in Cloud Computing both from literature and surveys.

CHAPTER 4

SYSTEMATIC LITERATURE REVIEW (SLR)

4 SYSTEMATIC LITERATURE REVIEW (SLR)

Systematic Literature Review (SLR) is one of the main research methodologies in this research work. The main reason for undertaking SLR is to summarize the existing information about security threats and to bridge a gap, to get the true reflection of the security techniques used in the current world in Cloud Computing. And to provide a frame work to suggest counter measures for the future challenges to be faced in Cloud Computing. Systematic reviews are based on a defined search strategy that aims to detect as much of the relevant literature as possible. We followed different steps in Systematic Literature Review. The review process phases are illustrated as follows:

4.1 Planning the review

The below section describes the planning of systematic literature review.

4.1.1 The need for a Systematic Literature Review

Prior to identify if any systematic reviews exists or not, we searched the databases IEEE, Science direct, Scopus and Springer link with following search string:

{Cloud Computing} OR {Cloud security techniques} OR {security challenges} AND {systematic review} OR {systematic literature review} OR {research review}.

Fortunately, there were no hits with this search. So the we confirmed that there is a need for systematic review.

4.1.2 Defining the research questions

To achieve the research aims and objectives, research questions are classified and developed as shown in table 1. The main aim of research questions is to identify the threats and security techniques used to mitigate them in Cloud Computing.

Research Questions	Purpose
RQ-1: What are the security techniques being used by leading Cloud Computing companies, to prevent active and passive attacks when the data is being transferred between Cloud and home network?	To identify the security attacks and mitigation techniques that are being used in present Cloud Computing environment when data is at transit state.
RQ-2: What are the security methods being used to prevent unauthorized access to data within the Cloud?	To identify the security techniques those are used when the data resides within the Cloud.
RQ-3: What are major security challenges we expect for the future of Cloud Computing?	To discuss the future security challenges to be faced in Cloud Computing.

RQ-4: how do we handle the security problems that may be expected in future of Cloud Computing?	To suggest the security methods to handle the security problems in future of Cloud Computing.

Table 4.1 Defining Research Questions

4.1.3 Defining Keywords

In this we used PICO criteria [34] to define keywords which have impact on this research.

PICO – Population Intervention Comparison Outcomes

Population: The population might be any of the specific role, application and area.
We had chosen the "*Cloud Computing"* as Population for this research.

Intervention: The intervention is the tool or technology or procedure that addresses a specific issue. "*Security*" is of the Intervention for this research.

Comparison: This is the tool or technology or procedure with which intervention is being compared. In this research, we are not comparing any of the technology or procedure.

Outcomes: Outcomes should relate to factors of importance of specific tool or technology. All relevant outcomes should be specified. We should have different security techniques and challenges as outcomes.

4.1.4 Study Quality Assessment

The main goal of quality assessment is to ensure that appropriate and relevant primary studies were included during the process and should fulfill the overall aim and research objectives. We prepared quality assessment checklist based on guidelines from [34] as shown in table. If a study fulfills assessment criteria then it is filled with value 'Yes' else with 'No'.

No.	**Quality Assessment Criteria**	**Yes/No**
1	Does the Aims and objectives are clearly stated?	-
2	Does the data collection methods fairly described?	-
3	Are the limitations and constraints discussed?	-
4	Are the citations in the paper clearly expressed?	-

Table 4.2 Quality assessment checklist

4.1.5 Review Protocol

A review protocol specifies the methods that will be used to undertake a specific systematic review [34]. In this research the SLR is undertaken to discover published papers related to the security challenges and mitigation techniques in Cloud Computing associated with security attacks. To achieve the research objectives we selected the papers published between 2001 and 2010.

4.1.6 Selection Criteria and Procedures

We followed the selection criteria as mentioned in kitchenham [34]. We ensured that the selected papers are relevant to our research work. The inclusion and exclusion of papers is done, to filter the papers which do not contain the information about security attacks, challenges and mitigation techniques in Cloud Computing. The selection procedure is mentioned in table below.

Relevance	**Criteria**
By search	As search string Publication year (2001 -2011)
Title	Languages used (English) Related to Cloud Security
Abstract/Introduction/ conclusion	Background in industrial or academic in related area
Full text	Empirical study on security challenges and mitigation techniques

Table 4.3 Selection Criteria

4.2 Conducting the Review

The below section describes the conducting of systematic literature review.

4.2.1 Data Extraction Strategy

We developed the data extraction form which is used during the study as shown in table 4.3.

The main aim is to extract the data concerned with Cloud security issues, techniques and future challenges. The data was extracted using inclusion and exclusion selection criteria from the well-known databases. Initially, our search has begun by constructing a suitable search string related to the Cloud security. The search for the papers were further refined from the year 2001-2011. However, our main study was focused on empirical and collaboration studies. Moreover, the investigation was filtered from the case studies, experiments and survey approaches. The methodology extraction was done on by security attacks, challenges and mitigation techniques in Cloud Computing.

4.2.2 Identification of Research

The primary aim of the systematic review is to form a search strategy to find out the primary studies related to research questions [34]. In search strategy we formulated search strings based on the keywords which are discussed in section 4.1.2 and constructed by using Boolean ANDs and ORs.

By the following search strategy, we find required information in Systematic Literature Review (SLR) exploiting the data bases IEEE Xplore, SpringerLink, ScienceDirect and Scopus.

Major keywords that are used to construct the search string are:

- Cloud Computing
- Security attacks
- Security methods
- Cloud security techniques
- Cloud Security challenges

The following search string was constructed and used to find the required information during the SLR.

((Cloud Computing) AND (security) AND (techniques OR method* OR challenge*))*

4.2.3 Study Selection Criteria

Study selection criteria identify the primary studies which provide evidence about research questions [34]. Study selection for this research includes inclusion and exclusion criteria for selection and filtering of papers.

Initially a study selection criterion excludes the searches by title and abstract. The study selection process followed by refining the search according to defined inclusion and exclusion criteria, that reflects the information related to security attacks and challenges in Cloud environment.

Inclusion criteria:

- Studies covering security issues of Cloud Computing when data is at rest and when data is at transit state.
- Studies that formalize the security techniques which are currently being used in Cloud Computing environment.
- Studies that includes the future security challenges and preventions in Cloud Computing.

Exclusion criteria:

- Studies in languages which are not in English.
- Studies which are not replicating security techniques and challenges in Cloud Computing.

We used the search string to explore papers published between 2001 and August 24, 2011. The study selection process has various steps that are shown in figure 4.1.

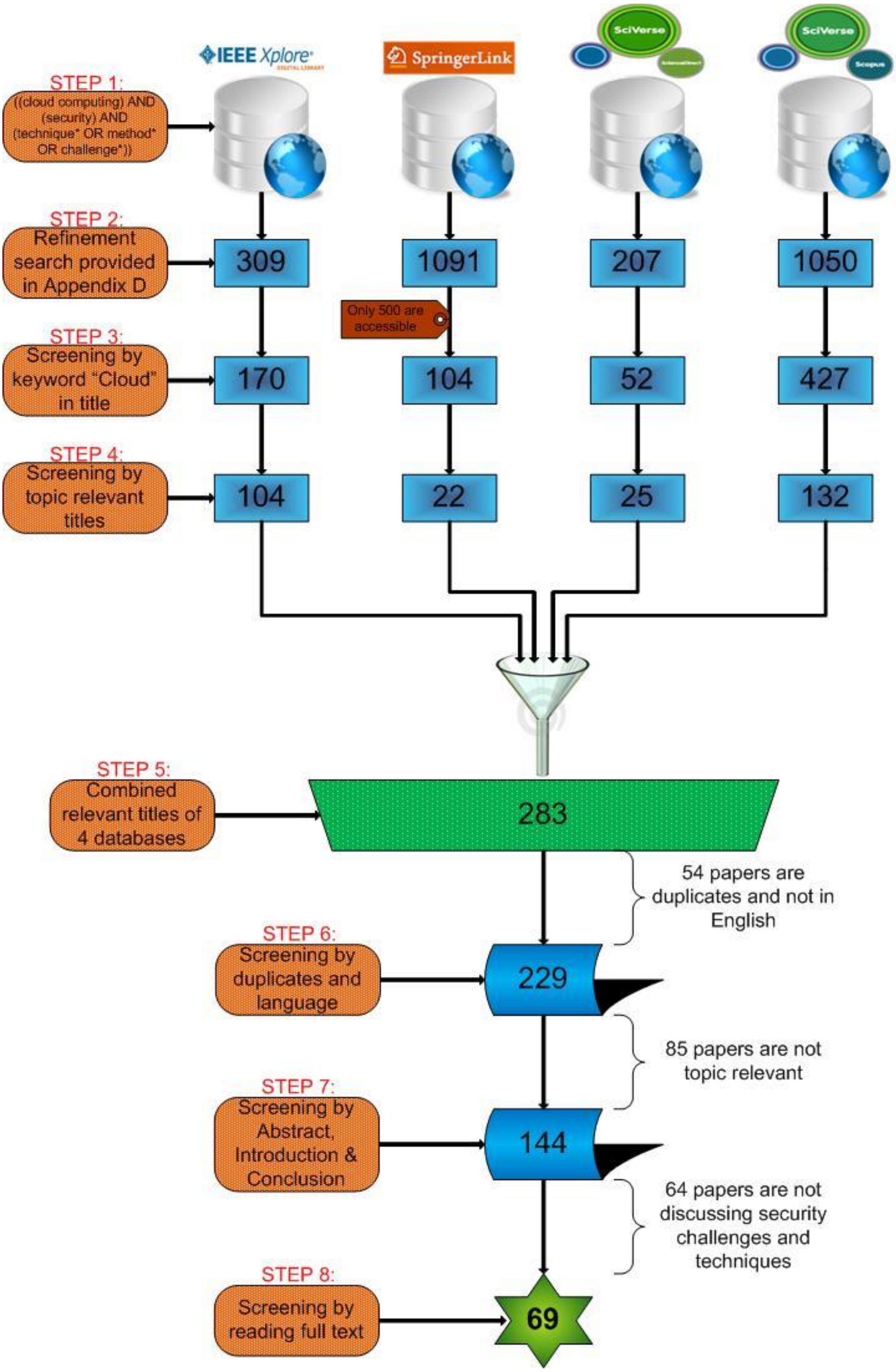

IEEE Xplore
SpringerLink
SciVerse
ScienceDirect
SciVerse
Scopus
STEP 1:
((cloud computing) AND (security) AND (technique* OR method* OR challenge*))
STEP 2:
Refinement search provided in Appendix D
309
1091
207
1050
Only 500 are accessible
STEP 3:
Screening by keyword "Cloud" in title
170
104
52
427
STEP 4:
Screening by topic relevant titles
104
22
25
132
STEP 5:
Combined relevant titles of 4 databases
283
54 papers are duplicates and not in English
STEP 6:
Screening by duplicates and language
229
85 papers are not topic relevant
STEP 7:
Screening by Abstract, Introduction & Conclusion
144
64 papers are not discussing security challenges and techniques
STEP 8:
Screening by reading full text
69

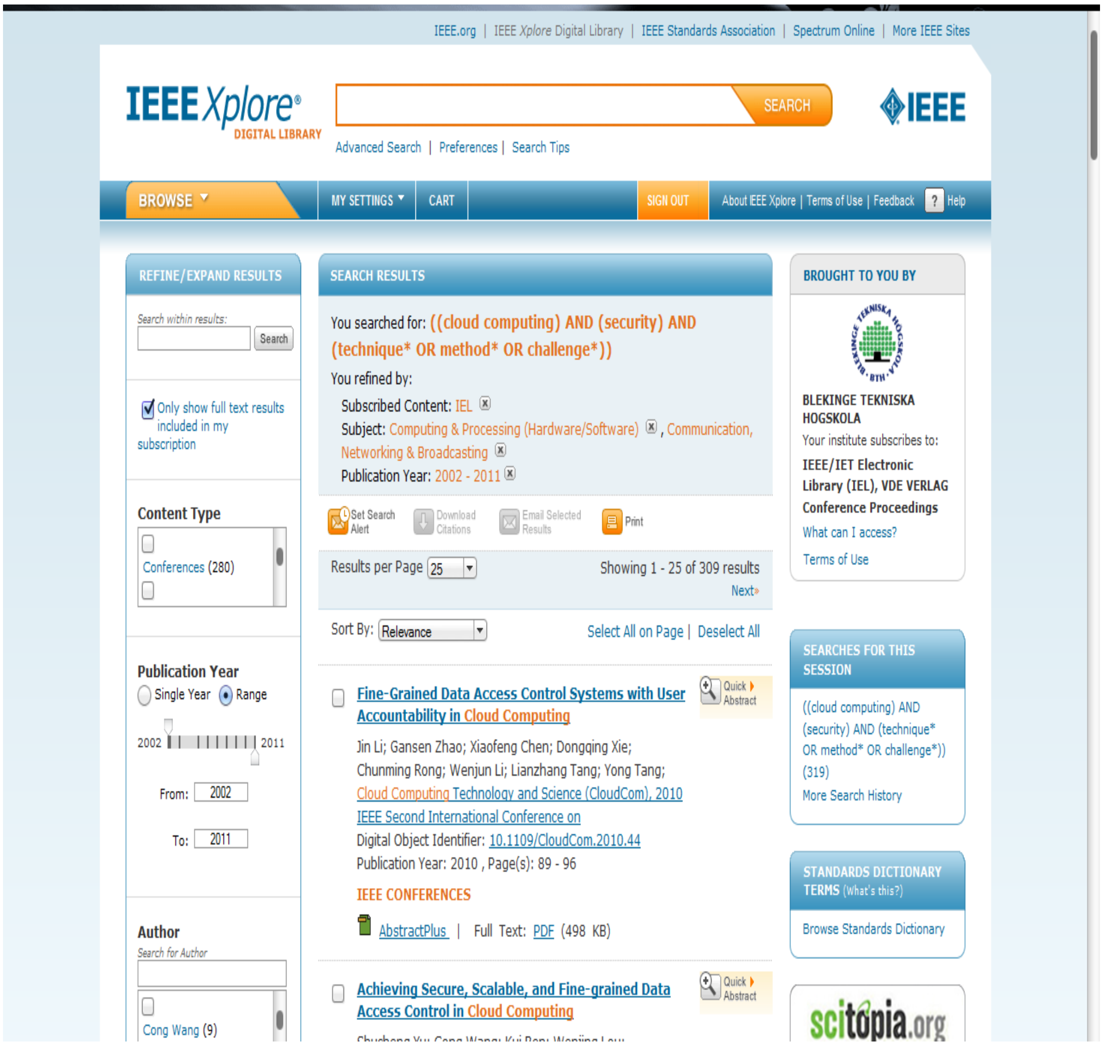
Figure 4.1 Steps of Systematic Literature Review

Step 1:

To identify the papers, the search is followed by four databases which include IEEE Xplore, Springerlink, Science direct and Scopus using search string. The papers which are relevant to research are taken as references and maintained in IEEE referencing standard. Here is a small discussion about four databases subsequently.

IEEE Xplore:

IEEE Xplore is a simple, flexible and user friendly data base. It consists of many advanced search options include logical operators AND/OR/NOT to easily combine the search keywords or phrases. With this, we combined the entire search phrase to use as a single search string as shown in the below figure.


IEEE.org | IEEE Xplore Digital Library | IEEE Standards Association | Spectrum Online | More IEEE Sites
IEEE Xplore® DIGITAL LIBRARY
SEARCH
IEEE
Advanced Search | Preferences | Search Tips
BROWSE
MY SETTINGS
CART
SIGN OUT
About IEEE Xplore | Terms of Use | Feedback | ? Help
REFINE/EXPAND RESULTS
Search within results:
Search
SEARCH RESULTS
BROUGHT TO YOU BY
Set Search Alert
Download Citations
Email Selected Results
Print
Quick Abstract
SEARCHES FOR THIS SESSION
STANDARDS DICTIONARY TERMS (What's this?)
Browse Standards Dictionary
scitopia.org

☑ Only show full text results included in my subscription

Content Type
□ Conferences (280)
□

Publication Year
○ Single Year ● Range
2002 2011
From: 2002
To: 2011

Author
Search for Author
□ Cong Wang (9)

You searched for: ((cloud computing) AND (security) AND (technique* OR method* OR challenge*))

You refined by:
Subscribed Content: IEL ☒
Subject: Computing & Processing (Hardware/Software) ☒ , Communication, Networking & Broadcasting ☒
Publication Year: 2002 - 2011 ☒

Results per Page 25 Showing 1 - 25 of 309 results Next»

Sort By: Relevance Select All on Page | Deselect All

□ Fine-Grained Data Access Control Systems with User Accountability in Cloud Computing
Jin Li; Gansen Zhao; Xiaofeng Chen; Dongqing Xie; Chunming Rong; Wenjun Li; Lianzhang Tang; Yong Tang;
Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on
Digital Object Identifier: 10.1109/CloudCom.2010.44
Publication Year: 2010 , Page(s): 89 - 96
IEEE CONFERENCES
AbstractPlus | Full Text: PDF (498 KB)

□ Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing
Shucheng Yu; Cong Wang; Kui Ren; Wenjing Lou

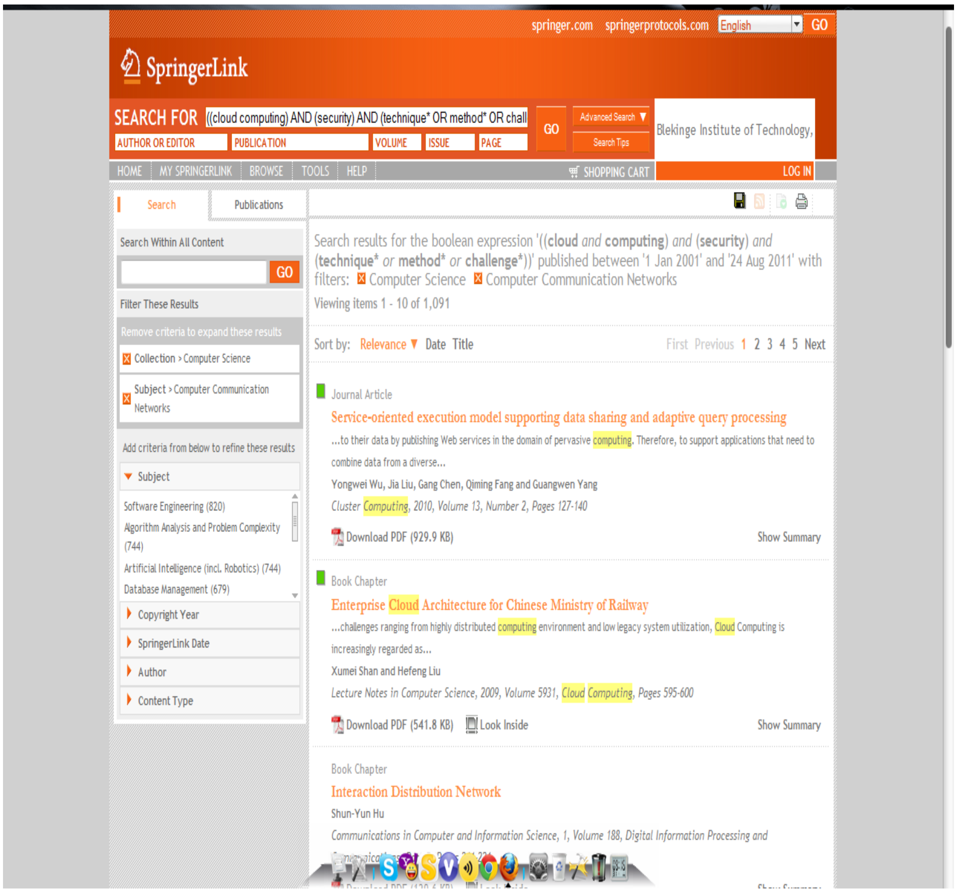
BLEKINGE TEKNISKA HOGSKOLA
Your institute subscribes to:
IEEE/IET Electronic Library (IEL), VDE VERLAG Conference Proceedings
What can I access?
Terms of Use

((cloud computing) AND (security) AND (technique* OR method* OR challenge*)) (319)
More Search History

Figure 4.2 IEEE search interface

Springer link:

Springerlink database hosts in a number of scientific fields. It requires a lot of caution when searching through the springerlink. It is fictional to many topics. The search tool identifies every article matched to even a single word in search string shown in Fig. We searched with specific keyword “Cloud Computing” and so on to avoid the unwanted materials.



SEARCH FOR ((cloud computing) AND (security) AND (technique* OR method* OR chall

Search results for the boolean expression '((cloud *and* computing) *and* (security) *and* (technique* *or* method* *or* challenge*))' published between '1 Jan 2001' and '24 Aug 2011' with filters: ☒ Computer Science ☒ Computer Communication Networks

Viewing items 1 - 10 of 1,091

☒ Collection › Computer Science

☒ Subject › Computer Communication Networks

Subject:
- Software Engineering (820)
- Algorithm Analysis and Problem Complexity (744)
- Artificial Intelligence (incl. Robotics) (744)
- Database Management (679)

Journal Article

Service-oriented execution model supporting data sharing and adaptive query processing

...to their data by publishing Web services in the domain of pervasive computing. Therefore, to support applications that need to combine data from a diverse...

Yongwei Wu, Jia Liu, Gang Chen, Qiming Fang and Guangwen Yang

Cluster Computing, 2010, Volume 13, Number 2, Pages 127-140

Download PDF (929.9 KB)

Book Chapter

Enterprise Cloud Architecture for Chinese Ministry of Railway

...challenges ranging from highly distributed computing environment and low legacy system utilization, Cloud Computing is increasingly regarded as...

Xumei Shan and Hefeng Liu

Lecture Notes in Computer Science, 2009, Volume 5931, Cloud Computing, Pages 595-600

Download PDF (541.8 KB)

Book Chapter

Interaction Distribution Network

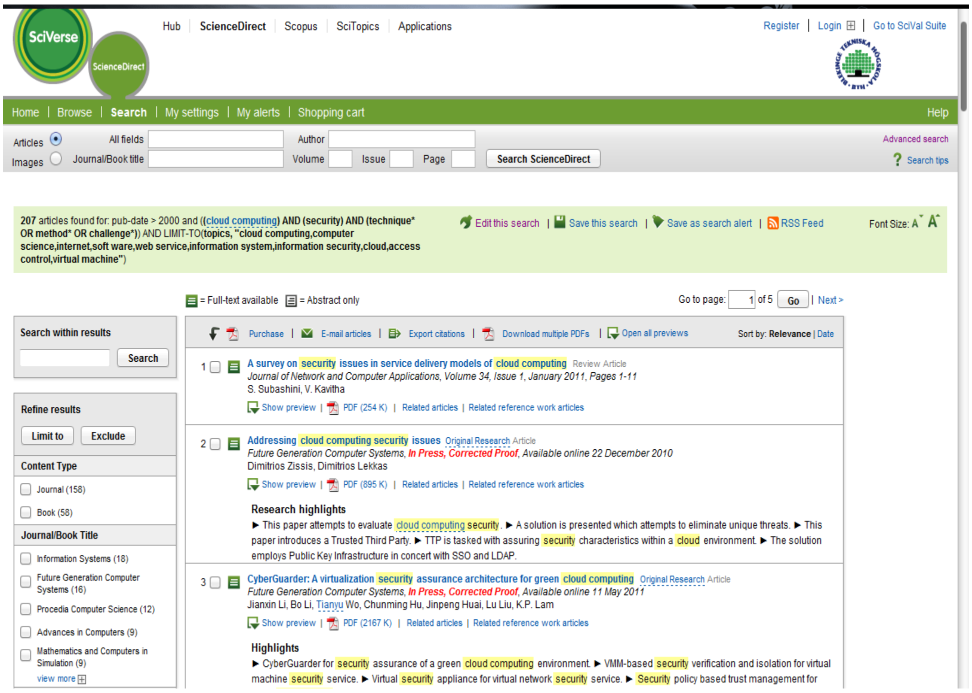
Shun-Yun Hu

Communications in Computer and Information Science, 1, Volume 188, Digital Information Processing and

Figure 4.3 Springer link search interface

ScienceDirect:

ScienceDirect is also one of the most useful databases, which has different search characteristics from the above databases. We have selected advanced search, which enables us to enter the combination of search phrases with the AND/OR/NOT operators as shown in the below figure.



SciVerse
ScienceDirect
Hub | ScienceDirect | Scopus | SciTopics | Applications
Register | Login | Go to SciVal Suite
Home | Browse | Search | My settings | My alerts | Shopping cart
Help
Articles ●
Images ○
All fields
Journal/Book title
Author
Volume
Issue
Page
Search ScienceDirect
Advanced search
Search tips
Edit this search | Save this search | Save as search alert | RSS Feed
Font Size: A A
= Full-text available
= Abstract only
Go to page: 1 of 5 Go | Next >
Search within results
Search
Refine results
Limit to
Exclude
Purchase | E-mail articles | Export citations | Download multiple PDFs | Open all previews
Sort by: Relevance | Date
Show preview | PDF (254 K) | Related articles | Related reference work articles
Show preview | PDF (895 K) | Related articles | Related reference work articles
Show preview | PDF (2167 K) | Related articles | Related reference work articles

207 articles found for: pub-date > 2000 and ((cloud computing) AND (security) AND (technique* OR method* OR challenge*)) AND LIMIT-TO(topics, "cloud computing,computer science,internet,soft ware,web service,information system,information security,cloud,access control,virtual machine")

Content Type
- □ Journal (158)
- □ Book (58)

Journal/Book Title
- □ Information Systems (18)
- □ Future Generation Computer Systems (16)
- □ Procedia Computer Science (12)
- □ Advances in Computers (9)
- □ Mathematics and Computers in Simulation (9)

view more

1 □ A survey on security issues in service delivery models of cloud computing Review Article
Journal of Network and Computer Applications, Volume 34, Issue 1, January 2011, Pages 1-11
S. Subashini, V. Kavitha

2 □ Addressing cloud computing security issues Original Research Article
Future Generation Computer Systems, In Press, Corrected Proof, Available online 22 December 2010
Dimitrios Zissis, Dimitrios Lekkas

Research highlights
► This paper attempts to evaluate cloud computing security. ► A solution is presented which attempts to eliminate unique threats. ► This paper introduces a Trusted Third Party. ► TTP is tasked with assuring security characteristics within a cloud environment. ► The solution employs Public Key Infrastructure in concert with SSO and LDAP.

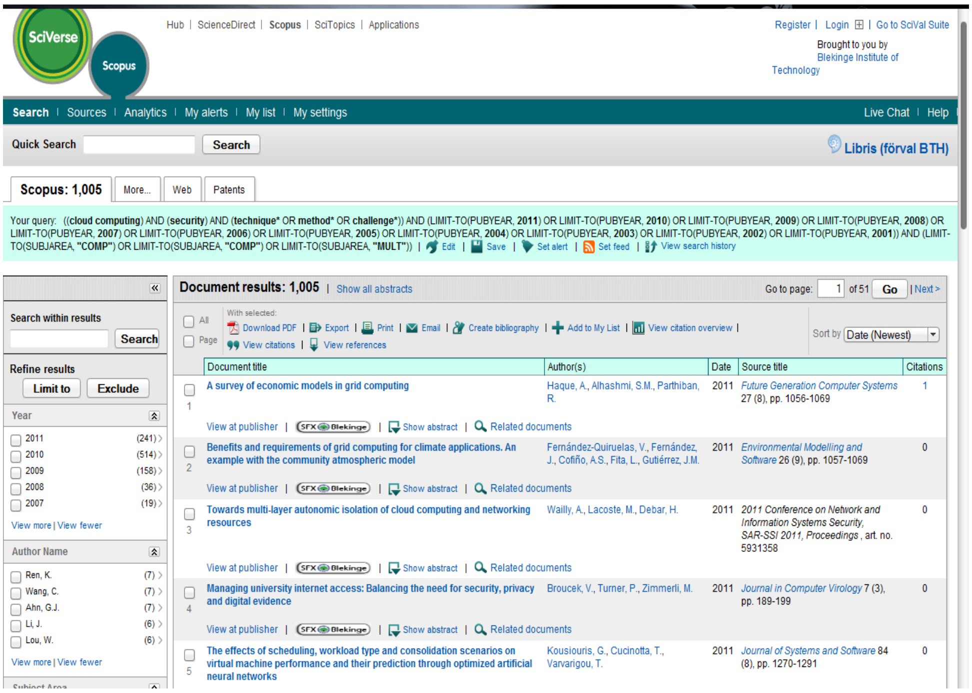
3 □ CyberGuarder: A virtualization security assurance architecture for green cloud computing Original Research Article
Future Generation Computer Systems, In Press, Corrected Proof, Available online 11 May 2011
Jianxin Li, Bo Li, Tianyu Wo, Chunming Hu, Jinpeng Huai, Lu Liu, K.P. Lam

Highlights
► CyberGuarder for security assurance of a green cloud computing environment. ► VMM-based security verification and isolation for virtual machine security service. ► Virtual security appliance for virtual network security service. ► Security policy based trust management for

Figure 4.4 Science Direct search interface

Scopus:

Scopus is another database which is used during the search. Scopus has an option to enter the entire search phrase as shown in figure.



SciVerse
Scopus
Hub | ScienceDirect | Scopus | SciTopics | Applications
Register | Login | Go to SciVal Suite
Brought to you by
Blekinge Institute of Technology
Search | Sources | Analytics | My alerts | My list | My settings
Live Chat | Help
Quick Search
Search
Libris (förval BTH)
Scopus: 1,005
More...
Web
Patents
Edit | Save | Set alert | Set feed | View search history
Search within results
Search
Refine results
Limit to
Exclude
Show all abstracts
Go to page: 1 of 51 Go | Next >
□ All
□ Page
With selected:
Download PDF | Export | Print | Email | Create bibliography | Add to My List | View citation overview |
View citations | View references
Sort by Date (Newest)
View at publisher | SFX Blekinge | Show abstract | Related documents
Subject Area

Your query: ((cloud computing) AND (security) AND (technique* OR method* OR challenge*)) AND (LIMIT-TO(PUBYEAR, 2011) OR LIMIT-TO(PUBYEAR, 2010) OR LIMIT-TO(PUBYEAR, 2009) OR LIMIT-TO(PUBYEAR, 2008) OR LIMIT-TO(PUBYEAR, 2007) OR LIMIT-TO(PUBYEAR, 2006) OR LIMIT-TO(PUBYEAR, 2005) OR LIMIT-TO(PUBYEAR, 2004) OR LIMIT-TO(PUBYEAR, 2003) OR LIMIT-TO(PUBYEAR, 2002) OR LIMIT-TO(PUBYEAR, 2001)) AND (LIMIT-TO(SUBJAREA, "COMP") OR LIMIT-TO(SUBJAREA, "COMP") OR LIMIT-TO(SUBJAREA, "MULT"))

Document results: 1,005

Year
- □ 2011 (241)
- □ 2010 (514)
- □ 2009 (158)
- □ 2008 (36)
- □ 2007 (19)

View more | View fewer

Author Name
- □ Ren, K. (7)
- □ Wang, C. (7)
- □ Ahn, G.J. (7)
- □ Li, J. (6)
- □ Lou, W. (6)

View more | View fewer

	Document title	Author(s)	Date	Source title	Citations
□ 1	A survey of economic models in grid computing	Haque, A., Alhashmi, S.M., Parthiban, R.	2011	*Future Generation Computer Systems* 27 (8), pp. 1056-1069	1
□ 2	Benefits and requirements of grid computing for climate applications. An example with the community atmospheric model	Fernández-Quiruelas, V., Fernández, J., Cofiño, A.S., Fita, L., Gutiérrez, J.M.	2011	*Environmental Modelling and Software* 26 (9), pp. 1057-1069	0
□ 3	Towards multi-layer autonomic isolation of cloud computing and networking resources	Wailly, A., Lacoste, M., Debar, H.	2011	*2011 Conference on Network and Information Systems Security, SAR-SSI 2011, Proceedings* , art. no. 5931358	0
□ 4	Managing university internet access: Balancing the need for security, privacy and digital evidence	Broucek, V., Turner, P., Zimmerli, M.	2011	*Journal in Computer Virology* 7 (3), pp. 189-199	0
□ 5	The effects of scheduling, workload type and consolidation scenarios on virtual machine performance and their prediction through optimized artificial neural networks	Kousiouris, G., Cucinotta, T., Varvarigou, T.	2011	*Journal of Systems and Software* 84 (8), pp. 1270-1291	0

Figure 4.5 Scopus search interface

Step 2:

In this step, we had identified the total number of 2657 papers from all the four databases after refining the search using the configured search string and by year wise from 2001-2011and by subject wise which are related. From those, we have filtered out 753 papers and removed 1904 papers which are not having the keyword “Cloud” in title of the paper. We had also reduced the huge volume of materials after initial search which are described in the further steps.

Step 3:

In this step, we had identified the total number of 753 papers which are having the keyword “Cloud’ in title of the paper. In this step, regarding the papers in SpringerLink database, we got access to only 500 papers out of 1091.

Step 4:

In this step, we had identified the total number of 283 papers which are having the titles that are related to Cloud security and removed the remaining 470 papers which are having the titles that are irrelevant to the topic.

Step 5:

In this step, we had merged all the papers (283 papers) that are obtained by filtering through the titles that are related to Cloud security from all the four databases.

Step 6:

In this step, we had filtered out the total number of 229 papers out of 283 papers by removing the duplicates and the papers which are not in English language. The procedure used in this step is inclusion and exclusion criteria based on duplicated materials and papers that were not published in English. This is because of same search string is used in different databases; we find the same papers which exploit same information.

Step 7:

In this step, we had filtered out the papers by reading through their:

- Abstract
- Introduction and Conclusion

By following the above, we had identified the total number of 144 papers which are containing the relevant content in their abstract, introduction and conclusion. We had removed the remaining 85 papers which are not having related content to the topic.

Step 8:

In this step, we had filtered out the papers by reading through their full text and identified the total number of 69 papers that are most relevant to the topic and which are mostly discussing about the following:

- Cloud Computing concept
- Cloud Security issues and attacks
- Security techniques and methods used to protect data in a Cloud
- Future challenges in the security of Cloud Computing, etc.

From these 69 papers, we finally collected and analyzed the information to identify the security attacks and mitigation techniques which are currently using in Cloud Computing environment.

4.2.4 Reliability of Inclusion

In this thesis, we followed inclusion-exclusion criteria. As a part of it, total search results after screening by title, duplicates and language are studied individually by both of us to exclude the final papers. In this process, the final individually selected papers are approximately equal. This shows the mutual understanding between both of us in selecting the final outcome. Normally, this relation between both of us is calculated with the kappa analysis approach.

CHAPTER 5

SURVEY

5 SURVEY

In research, Survey is a method of gathering information in the real life from individuals who are working in that particular field. Survey comes under non experimental method. It applies to collect the information surrounding a particular topic which helps the researchers.

5.1 Rationale for Survey

To answer the research questions we choose the survey method to collect the information from expert's personnel who involved and experienced their real life in Cloud Computing, and in related areas of security.

The survey was conducted using a questionnaire developed from the knowledge gain after SLR. From the responses of the questionnaire, we experienced knowledge about current industrial practices in Cloud Computing.

5.2 Source of data collection

We have used the direct mailing procedure to send the prepared questionnaire to the experts and few of responses are taken from direct interaction with the experts who is currently having industrial experience in Cloud Computing.

5.3 Survey Questions Formation

In this process, we designed the questionnaire to answer the research questions. The process involves that we designed questionnaire and discussed with Prof. Lars Lundberg and Mr. Jens Kvarnberg and Mr. Ross W Tsagalidis to make the questionnaire error free and correctness that ensures the designed questionnaire truly reflects the aims and objectives of the research. During this process, we designed the questionnaire according to specification and research requirements.

5.4 Survey Administration

In this research, we have adapted the method of electronic survey. This process includes the identification of experts in cloud computing with relevant experience in security, and sent the requesting mail which contains the brief introduction of us, topic area and purpose of conducting the survey and requesting to participate in the survey. After the acknowledgement from the experts, we sent them questionnaire to answer them. This survey is conducted in between May 2011 and October 2011. It has taken a long time to get a more number of responses because of unavailability of experts during summer. The questionnaire starts with the name of the expert, organization name, experience in Cloud Computing and the experience in security. The detailed description about the survey participants is explained in the results.

CHAPTER 6

RESULTS & ANALYSIS

6 RESULTS AND ANALYSIS

The Reporting review consist the results from SLR and Survey. In this we have reported the identified security challenges and mitigation techniques from SLR also given information about survey participants and explained the analyzed results from the survey.

6.1 SLR Results

In recent years, the huge amount of research has been done in the area of Cloud Computing. In the process of SLR, we have extracted 69 papers relevant to meet the goals of the research from the large number of papers published since the year 2001. This section covers the results and analysis of the papers that were extracted in the process of SLR. We have given a detailed description of the list of identified challenges and mitigation techniques in appendix section.

In the past years, research is followed the distributed computing and mainly focused on service like grid computing. From the last decade, there is a rapid increase in research on new paradigm Cloud Computing which is the next generation computing. We mainly focused on security aspects of the Cloud Computing in last 10 years. Totally 69 papers are retrieved during the literature study. Mostly the selected papers are in between the year 2010 and 2011 which revealed 52 papers and 25 papers respectively. Others include 3 papers published in 2009. The figure below shows the empirical evidence of research on security in Cloud Computing in the last 10 years.

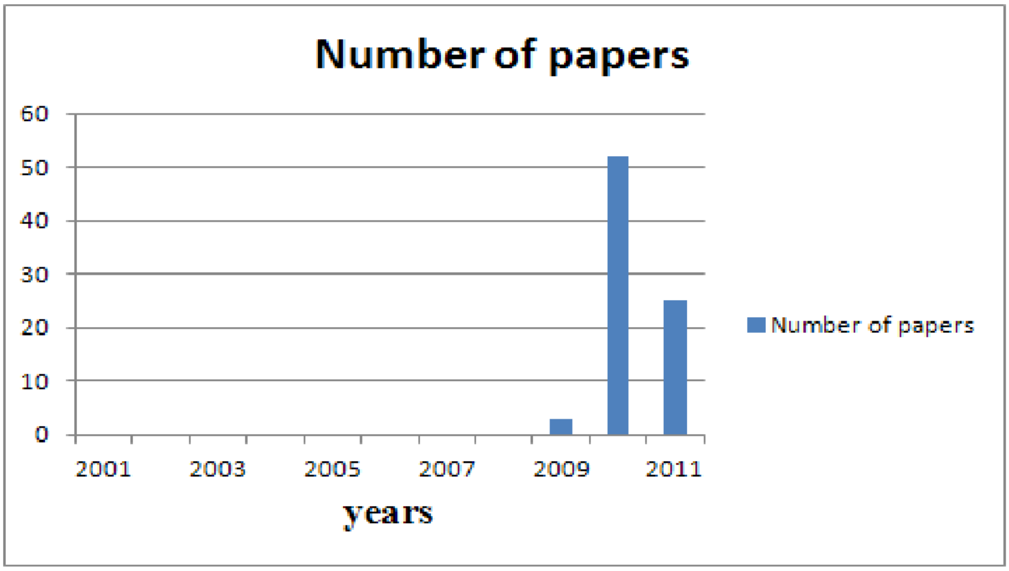


Figure 6.1 Number of papers published in year wise

6.1.1 Identified Challenges

From the analysis, we have identified 43 security challenges during the SLR. The detailed description of these challenges is presented in Appendix A. The list of identified challenges are WS- security, Phishing attack, Wrapping attack, Injection attack, IP spoofing, Tampering, Repudiation, Information Disclosure, Denial of service, Elevation of privilege, Physical security, WLAN's security, Direct attacking method, Replay attack, Man-in-the middle attack, Reflection attack, Interleaving, Timeliness attack, Self adaptive storage resource management, Client monitoring, Lack of trust, Weak SLAs, Perceived lack of reliability, Auditing, Back door, TCP hijacking, Social engineering, Dumpster diving, Password guessing, Trojan horses, Completeness, Roll back attack, Fairness, Data leakage, Computer network attack, Denial of service, Data security, Network security, data locality, Data segregation, Backup, Data integrity, Data manipulation.

In the part of the analysis, we find some of the Cloud Computing attributes which are threats to Cloud Computing. As a part of the result the compromised attributes in Cloud Computing is described in appendix A, they are Confidentiality, Integrity, Availability, Security, Accountability, Usability, Reliability and Auditability. The records of the most threaten attributes are in fig. the fig. shows that Confidentiality 31% and Integrity 24% recorded most threaten, while comparing with usability, reliability, accountability and audit ability which recorded less than the 10%.

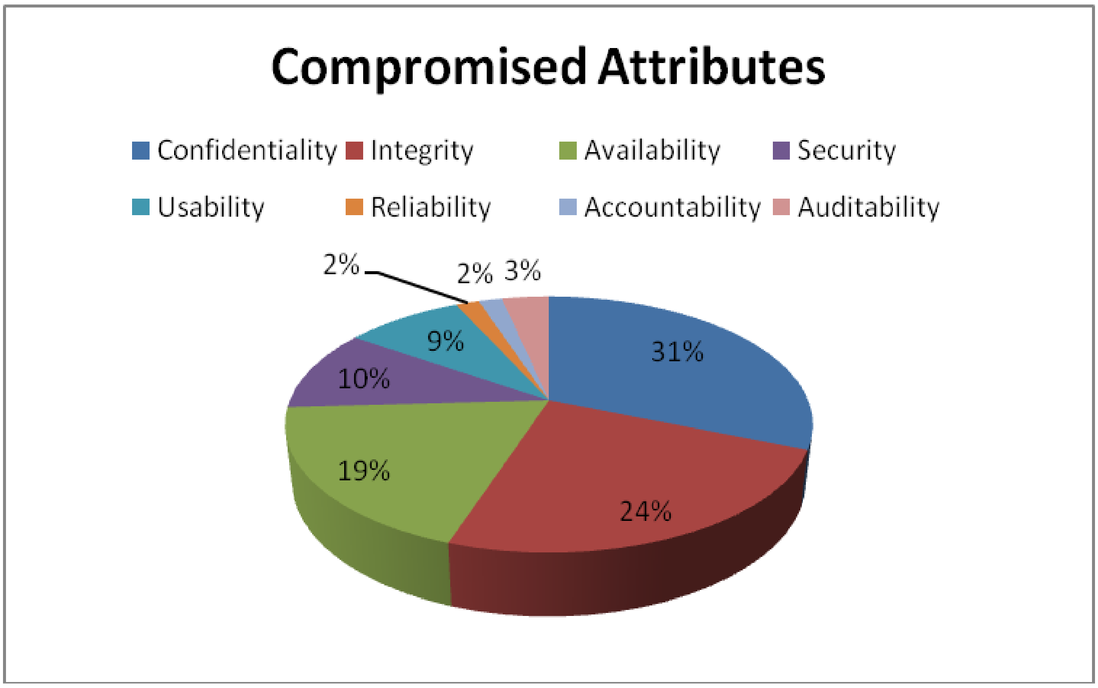


Figure 6.2 List of Compromised attributes

6.1.2 Identified Mitigation Techniques

From the analysis, we have identified 34 security techniques during the SLR. The detailed description of these techniques is presented in Appendix B. The summary include Identity based authentication, RSA algorithm, Dynamic Intrusion detection system, Multi tenancy based access control model, TLS Handshake, Public key homomorphic, Third party auditor, probabilistic sampling technique, Diffle – Hellman key exchange, Private face recognition, MACs, Data coloring and water marking, A novel Cloud dependability model, KP-ABE, RBAC, ARVTM, Security assertion markup language, TPM, Proof of retrievability, Fair MPNR protocol, Sobol sequence, Redundant array of independent Net storages, Handoop distributed file system, self cleansing intrusion tolerance, searchable symmetric encryption, Provable data possession, Privacy manager, Time bound ticket based mutual authentication scheme, Security Access Control Service, The Service Level Agreement, Intrusion detection system.

The above mentioned mitigation techniques have strong impact on the Performance, Security, Efficiency, QoS, Privacy and Access control of Cloud Computing. The defined mitigation techniques somehow improve the overall services in Cloud Computing environment. The result is shown in figure 6.3.

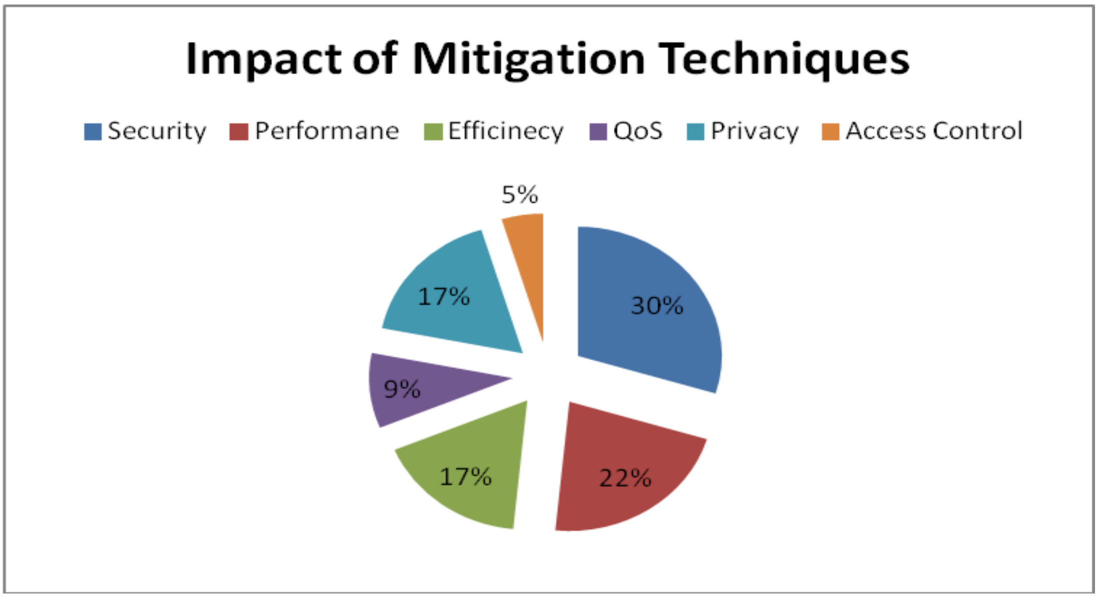


Figure 6.3 Impact of mitigation techniques

6.2 Survey Results

Cloud Computing is a new paradigm. Cloud Computing became popular since decade. To find out the security experts in Cloud Computing is complex. In total, we got 16 number of partially and completed responses from the real time survey. However, many do have relevant experience in Cloud Computing and IT security. The adopted experts have experience from 1 to 31 years.

The Name, country, professional role and experience in relevant field is presented in the table 6.1 below:

Name	Country	Professional Role	Experience in IT Sector (Years)	Experience in Cloud Computing (Years)	Experience in Security domain (Years)
Martin Bergling	Sweden	Information security consultant, IBM	23	1	23
Dan Ahlstrom	Sweden	Former CISO, development	17	2	17

Jan Hendler	Sweden	IT-Security Manger, Swedish Custom	20	4	20
Bengt Ackzell	Sweden	Security Expert	31	0	20 +
Daniel Gustafsson	Sweden	Technical advisor Blackberry, Logica	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A	N/A
Arun Taman	USA	Software Engineer, Oracle	14	4	4
N/A	N/A	N/A	18	0	11
Prajwal Kumar	India	Data base Developer	20	8	10
Johan Trodsson	Sweden	Researcher & Lead Architecture	8	4	0
Pethururaj	India	Enterprise Architect, Sify Software Ltd.	5	3	1
N/A	N/A	N/A	N/A	N/A	N/A
Omar Abduljabbar	India	Infrastructure Architect, MTN.	15	3	10
Sherif	Egypt	Manager Mobinil	10	0	10
Bengt akeclaesson	Sweden	Operational manager	10	3	6
N/A	N/A	N/A	N/A	N/A	N/A

N/A - Not Available

Table 6.1 List of experts interviewed

6.2.1 Reported challenges

In the part of the Survey, we have identified totally 18 Security challenges which are possible to be faced in the future of Cloud Computing. We summarized these future security challenges based on the opinions from experts. The results are included:

- Eaves dropping
- Hypervisor viruses
- Legal Interception point
- Virtual machine security
- Trusted transaction
- Risk of multiple Cloud tenants
- Smart phone data slinging
- Abuse and nefarious use of Cloud Computing
- Insecure application programming interfaces
- Malicious insiders
- Shared technology vulnerabilities
- Service and traffic hijacking
- **Privacy** – Personal information about many people will be handled by IT companies all over the world. No one will know who is accessing user data.
- **Espionage** – National secret information might be handled by IT companies in other countries, but do we really know who is working at these companies?
- **Business intelligence** – Business confidential will be handled by IT companies all over the world. No one knows who is accessing user company's data.
- **Data ownership** – When data is transferred to the Cloud it is important for many organizations to be assured of the continued control of the data, i.e. their ownership should never be challenged.
- **Availability** – The availability must be at least as high as for traditional solutions. Probably higher, since downtime probably will affect many users simultaneously and thus be covered by media. Compare the difference between small accidents (e.g. car) and large accidents (e.g. airplane). Even though many small accidents may be worse than one large, the media coverage (and other things) make the larger ones seem so much worse.
- **Transparency** – Using Cloud services has to be as simple as traditional solutions.

The compromised attributes are confidentiality, security, availability and integrity.

6.2.2 Reported Mitigation Techniques

From analysis of results from survey, we have identified totally 9 security techniques. The major security techniques that are used in the current world are:

- **SSL (Secure Socket Layer) Encryption:** Encryption between browser and web server. It usually provides enough security from the workstation to the browser. The use of SSL does not require Cloud service provider for any functionality. It is all in how you have defined your website. It is easy available as it is very inexpensive. All Cloud customers should require encrypted communication. Optical fiber is another tool, since fibers are harder to manipulate than electrical cables.

- **VPN (Virtual Private Network):** VPNs are most commonly used for home based or mobile applications. When users connect to the internet from home or any public place like airport, hotel etc., then he will be signed into his VPN and get secure communication. Many Cloud providers offer VPNs to cover the area from the work station in user facility to user connection to the internet and across the internet.
- **IPSec (Internet Protocol Security):** IPSec is a prominent appearance of VPN, usually used between facilities where there is a large amount of traffic. In the case of Cloud, Cloud service provider will define and usually facilitate the IPSec device to install user network where it connects to the internet and to facilitate high speed encryption and decryption without keeping workload on servers.
- A proper use of encryption can give good protection against eaves dropping. Traffic analysis is harder, but on the other hand, not only that many need protection against this kind of threat.
- A proper use of encryption can give good protection against active attacks. In order to protect against man-in-the middle attacks, one should observe if there are any delayed response times, in order to detect if there is any "Middle-Man".
- Intrusion Detection system
- Third party auditor
- Message Digesting
- Kerberos, SSH and MD5 for authentication
- Monitoring Agent
- Service management API (SMAPI)

Also, we have summarized suggested practices from experts to mitigate future challenges to be faced in Cloud Computing. The summary includes:

- Increased efforts in risk management – One should have a better risk awareness in order to take proper risks.
- Standardized security methods and solutions.
- Increased efforts to mitigate harmful code; Legal responsibility, and increased security measurements at levels of objects and elements of objects.
- Analyze the security model of Cloud provider interfaces.
- Ensure strong authentication and access controls are implemented in concert with encrypted transmission.
- Enforce strict supply chain management and conduct a comprehensive supplier assessment.
- Implement strong API access control.
- Analyzes data protection at both design and run time.
- Better algorithms, define a security strategy and decouple the security architecture with technical infrastructure, third party compliance, light, but yet effective encryption techniques.

CHAPTER 7

VALIDITY THREATS

7 VALIDITY THREATS

For any research there are mainly four types of threats as discussed by Wohlin et al [14], they are:

- Construct validity
- External Validity
- Internal validity
- Conclusion Validity

7.1 Construct Validity

- *Construct validity involves generalizing from your program or measures to the concept of your program or measures* [68].

In our research, we have data from Systematic Literature Review (SLR), survey and interviews. Comparison of results from SLR, interviews and survey is hard. We have considered this threat due to inconsistency in data. To overcome this we have used Narrative Analysis for Systematic Literature Review and interview data for proper organization of the data. After receiving the survey data we have thoroughly compared the Narrative Analysis results with the survey results, by this we were able to remove redundancy and inconsistencies in our data.

7.2 Internal Validity

- *Internal Validity is the approximate truth about inferences regarding cause-effect or causal relationships* [70].

There are several problems with conducting survey. One of the major challenges is the redundancy in data interpretation by the practitioners. The redundancy occurs when understanding the question and the answers might be interpreted in another sense which might not be relevant for our work. Based on the understanding of the question her/his answers might differ. To overcome this threat we made sure that the questionnaire is clearly understandable,

- We have used terminologies related to Cloud computing which are mostly used in the industrial context.
- We have conducted a pilot test with Cloud Computing professionals.

Based on the feedback of Cloud Computing professionals, survey questionnaire was reformulated. Hence, the chance of internal validity has been reduced.

7.2.1 Data Gathered Through Interview

While conducting interview with Cloud Computing Security Experts, we have prepared notes in order to avoid misunderstanding while data gathering. Data was recorded with the permission of the interviewee which was used as a proof for validation when analyzing the data. As a proof during data validation and not to miss some key points we have asked the interview participant to fill the questionnaire and send it which was used as a validation.

During the interview we faced some problems regarding identifying the information regarding security implementation and practices being followed. Most of the practitioners were not willing to disclose this particular data as it was against to their organization rules. This might pose a threat to some aspects of our study regarding the challenges and mitigation strategies.

7.3 External Validity

- *External validity is the degree to which the conclusions in your study would hold for other persons in other places and at other times* [69].

The external validity threat of this research describes how well our research conclusions are applicable in general to other related technological areas. In relation to that, the security challenges and techniques of Cloud Computing that we have identified are almost similar to the issues faced in normal traditional network Computing. The security policies are different at different times in different places in the world, and because of that it is difficult to standardize the conclusions in an overall perspective, and this may be a valid threat. To overcome this threat, we have conducted a survey and interviews amongst various security experts across the world, considered their answers and opinions and collectively presented as the conclusion in a condensed way. Hence, the chance of external validity has been reduced.

7.4 Conclusion Validity

- Conclusion validity refers to the statistically significant relationships between the treatment and outcome [67].

One possible threat to conclusion validity is the biasness in the selection of papers and the data gathered through interviews. For reducing biasness during SLR we have used a detailed inclusion and exclusion criteria for deleting the articles. For selecting the primary studies a quality assessment criteria was selected based on yes or no.

For the challenges and mitigation strategies identified from SLR we have conducted interviews and survey with practitioners to check whether the same set of challenges and mitigation strategies are being followed or not. In this way we have reduced the conclusion validity.

CHAPTER 8

CONCLUSION

8 CONCLUSION

The identification of security challenges and mitigation techniques in Cloud Computing is challenged by considering the large number of services. Most of the responses from survey, noted that Cloud Computing will place dominant and expandable information transactions. Because it offers many flexible services, provides easy, individualized and instant access control to the services and information where they are for the users. In the process of identification from the research methods SLR and Survey, we have identified satisfactorily number of challenges and mitigation techniques in current and future Cloud Computing.

8.1 For Research Question: 1

In the case of some part of local network data placed in the Cloud the security challenges and mitigation techniques were discussed in a Systematic method. Most of the security challenges and techniques that are being used in current Cloud Computing environment are listed in appendix. Few of the popular security techniques that are identified in SLR are Identity based authentication, Service Level Agreement (SLA), Third party auditor, Message authentication codes, Role based access control mechanism, Proof of retrievability, Time bound ticket based authentication scheme. The impact of these security techniques include on Confidentiality, Integrity, Availability and security described in the section 2.4.

If you need to exchange sensitive or confidential information between a browser and a web server, Encryption is an obvious tool to protect communication. Proper encryption of data and encryption of transmission is necessary.
The mitigation techniques identified from the survey is as follows:

- SSL (Secure Socket layer)
- VPN (Virtual Private Network)
- IPSec (Internet Protocol Security)
- A proper use of encryption can give good protection against active attacks. In order to protect against Man-in-the-middle attacks, one should observe if there are any delayed response times, in order to detect if there is any “Middle-Man”.
- A proper use of encryption can give good protection against eaves dropping. Traffic analysis is harder, but on the other hand, not only that many need protection against this kind of threat.

8.2 For Research Question: 2

We have identified the security techniques that are used in the case of when data resides in the Cloud in Systematic process. The identified challenges, mitigation techniques and compromised attributes are described in Appendix section. The few popular security methods are Secure Socket Layer (SSL) Encryption; Multi Tenancy based Access Control, Intrusion Detection System, Novel Cloud dependability model, Hadoop Distributed File System and Hypervisor.
From the analysis of results from survey we have identified the following security challenges

- Secure identification of users (authentication, e.g. with smart cards or passwords)
- Secure communication (e.g. encryption)
- Secure IT-infrastructure at the vendor site (e.g. secure domains, firewalls, virus control, etc...)
- Secure personnel (e.g. security screening)
- Secure audit (e.g. security logs)
- Separation of users (e.g. different virtualized zones)
- Secure administrative routines for system administration (e.g. separation of duties)
- Security education of all IT personnel.
- Agreements specifying security rules (between vendor and customer)
- Information classification and "Need-to-know".

If you are pertained about storing sensitive or confidential data in the Cloud, you should encrypt the data before keeping it to the Cloud.

8.3 For Research Question: 3

As the security technology has to improve continuously, in order to meet new security threats. People in common have to be more risk aware and security aware, in order to protect their own information and their company's information. The security challenges have to be faced in future are:

- Virtual machine security
- Trusted transaction
- Risk of multiple Cloud tenants
- Smart phone data slinging
- Hypervisor viruses
- Abuse and nefarious use of Cloud Computing
- Insecure application programming interfaces
- Malicious insiders
- Shared technology vulnerabilities
- Service and traffic hijacking
- **Security requirements are complex to specify** – When data and services are moved to the Cloud it becomes even more crucial to be able to specify the security requirements.

Information about the security levels of information systems is necessary for efficacious risk management. Security assessment is difficult since the concept of security is vague and cannot be directly measured. Instead other properties and effects of systems have to be measured and combined in order to illustrate the security levels and create the desired information about security. When data and services are moved to the Cloud, security assessment becomes even more challenging since more parties are involved and the systems become more complex.

8.4 For Research Question: 4

From the analysis of results we have proposed the way to secure the Cloud Computing in future.

- Increased efforts in risk management – One should have a better risk awareness in order to take proper risks.
- Standardized security methods and solutions.
- Increased efforts to mitigate harmful code; Legal responsibility, and increased security measurements at levels of objects and elements of objects.
- Analyze the security model of Cloud provider interfaces.
- Ensure strong authentication and access controls are implemented in concert with encrypted transmission.
- Enforce strict supply chain management and conduct a comprehensive supplier assessment.
- Implement strong API access control.
- Analyzes data protection at both design and run time.
- Better algorithms, define a security strategy and decouple the security architecture with technical infrastructure, third party compliance, light, but yet effective encryption techniques.

8.5 Future Work

In the future, the people will access and share their software applications through online and access information by using the remote server networks instead of depending on primary tools and information hosted in their personal computers because of flexibility in Cloud Computing. The security issues in Cloud Computing are always one of the main research topics for researchers and developers to investigate the appropriate solutions every time. From the perspective of this thesis, we suggest that to find an optimum and appropriate security solutions for the specific services in the Cloud. There is a scope to propose the guidelines to overcome the future challenges like physical security, espionage, transparency, data ownership, hypervisor viruses and malicious insiders in Cloud security. To concentrate on more specific areas like regulatory and compliance issues, jurisdiction laws, etc...

CHAPTER 9

REFERENCES

9 REFERENCES

1. Ahmed S, Raja M. (2010) 'Tackling Cloud security issues and forensics model', *High Capacity Optical Networks and Enabling technologies (HONET)* , 19-21 Dec, pp. 190-195.

2. Ahuja R. (June 2011) 'SLA Based Scheduler for Cloud storage and Computational Services', International Conference on Computatonal Science and Applications (ICCSA), 258-262.

3. Albeshri A, Caelli W. (Sept 2010) 'Mutual Protection in a Cloud Computing Environment', 12th IEEE International Conference on High performance Computing and Communications (HPCC), 641-646.

4. Almulla S, Chon Yeob Yeun. (March 2010) 'Cloud Computing Security management ', 2nd International Conference On Engineering Systems Management and Its Applications , 1-7.

5. B. lagesse. (Mar.2011) 'Challenges in Securing the Interface between the cloud and Pervasive Systems', 2011 IEEE International Conference on Pervasive Computing and Communications Workshops, 106-110.

6. Brenner Michel, Wiebelitz Jan. (may 31, 2011) 'Secret program execution in the Cloud applying homomorphic encryption', Digital Ecosystems and Technologies Conference (DEST), 5th IEEE International Conference 2011, 114-119.

7. C. C Ragin. (1997) 'Turning the tables: How case - oriented research challenges variable oriented research', *Comparative social research*, vol. 16, pp. 27-42.

8. C. C Ragin. (2000) *Fuzzy set science*, Chicago: The university of Chicago.

9. Chang Lung Tsai, Uei –Chin Lin. (Aug 2010) 'Information Security issue of enterprises adopting the application of Cloud Computing', 6th International Conference on Networked Computing and Advanced Information Management (NCM), 645-649.

10. Chenguang Wang, Huaizhi Yan. (Dec 2010) 'Study of Cloud Computing security based on Private Face Recognition', International Conf. on Computational Intelligence and Software Engineering , 1-5.

11. Cong Wang, Kui ren. (2010) 'Toward publicly auditable secure cloud data storage services', *Network ,IEEE*, vol. 24, no. 4, July, pp. 19-24.

12. Cong Wang, Qian Wang. (March 2010) 'Privacy Preserving Public Auditing for Data storage security in Cloud Computing', INFOCOM 2010, IEEE, 1-9.

13. Cong Wang, Qian Wang. (2009) 'Ensuring data storage security in Cloud Computing', International Workshop on Quality of Service, 1-9.

14. C. Wohlin. (2000) *Experimentation in Software engineering: an introduction*, 6th edition, International series in software engineering, Springer.

15. Dawei Sun, Guiran Chang. (Sept.2010) 'A Dependability Model to Enhance Security of Cloud Environment Using System-Level Virtualization Techniques', Pervasive Computing Signal Processing and Applications, 305-310.

16. Dawod W, Takouna I. (March 2010) 'Infrastucture as a service security: challenges and solutions', 7th International Conference on Informatics and Systems (INFOS), 1-8.

17. Doelitzscher F, Reich C. (July 2010) 'Designing Cloud services adhering to Government privacy Laws ', IEEE 10th International Conf. on Computer and Information Technology, 930-935.

18. D.K. Mishra. (Sept.2010) 'Tutorial: Secure Multiparty Computation for Cloud Computing Paradigm by Durgesh Kumar Mishra', Second International Conference on Computational Intelligence, Modelling and Simulation, xxiv-xxv.

19. Ford R.B. (2011) 'Information Security in the Cloud', *Network Security*, vol. 2011, no. 4, April, pp. 15-17.

20. Gul I, Rehman A. (June 2011) 'Cloud Computing Security Auditing', 2nd International Conference on next Generation Information Technology (ICNIT), 143-148.

21. Hao Z, Zhong S. (June,2011) 'A Time-Bound Ticket-Base Mutual Authentication Scheme for Cloud Computing', *International Journal of Computers, Communications and Control*, vol. 6, no. 2, June, pp. 227-235.

22. Huimei Wang, Ming Xian. (May 2011) 'Cloud Evaluation method of Network Attack resitance Ability', Network Computing and Information Security (NCIS), 239-243.

23. Jaatun M.G, Nyre A. A. (March 2011) 'An approach to confidentiality control in the Cloud', Vehicular Technology, Information Theory and Arreospace and Electronic systems Technology, 2nd International Conference on Wireless Communication,1-5.

24. Jensen M, Schwenk J. (Sept.2009) 'On Technical Security Issues in Cloud Computing', IEEE International Conference on Cloud Computing, 109-116.

25. Jia Weiwei Zhu, Haojin Cao. (10-15 April, 2011) 'A Secure data service mechanism in mobile Cloud Computing', Computer Communications Wrokshops (INFOCOMWKSHPS), IEEE Conference 2011, 1060 - 1065.

26. Jin Li, Gansen Zhao. (2010) 'Fine-Grained Data Access Control Systems with User Accountability in Cloud Computing', 2nd International Conference on Cloud Computing Technology and Science, 89-96.

27. Jun Feng, Yu Chen. (Jan 2010) 'Bridging the Missing link of Cloud data storage security in AWS ', 7th IEEE conf. on Consumer Communications and Networking Conference (CCNC), 1-2.

28. Jun Feng, Yu Chen. (Jan 2011) 'Enhancing Cloud storage security against rool- back attacks with a new fais multi party non-repudation protocol', Consumer Communications and Networking Conference (CCNC), IEEE conference 2011, 521-522.

29. Jun Feng, Yu Chen. (Sept 2010) 'Analysis of Integrity Vulnerabillities and a Non repudation Protocol for Cloud Data Storage Platforms', 39th International Conf. on Parallel Processing Workshops (ICPPW), 251-258.

30. Jun-Ho Lee, Min-Woo Park. (feb. 2011) 'Multi level Intrusion Detection System and Log management in Cloud Computing', Advanced Communication Technology (ICACT), 13th International Conference 2011, 552-555.

31. Kai Hwang, Deyi Li. (2010) 'Trusted Cloud Computing with Secure Resources and Data coloring', *Internet Computing*, vol. 15, no. 05, October, pp. 14-22.

32. Kai Zhang, Ying Song. (july,2010) 'Trusted Connection System based on Virtual Machine Architecture', 3rd IEEE International Conference on Computer Science and Information Technology, 192-196.

33. Kandukuri B.R, Paturi V.R. (2009) 'Cloud Security Issues', International Conference on Services Computing, 21-25.

34. Kitchenham B, Charters S. (2007) *Guidelines for performing Systematic Literature Reviews in Software Engineering*, Keele University and Durham University Joint report.

35. Lifei wei, haojin Zhu. (June.2010) 'SecCloud: Bridging Secure Storage and Computation in Cloud', 30th International Conference on Distributed Computing Systems Workshop, 52-61.

36. Lin Weiwei, Chen Liang. (Juy 2011) 'A hadoop Based Efficient Economic Cloud storage system', Communications and Systems (PACCS), 3rd Pacific - Asia Conference on Circuits, 1-4.

37. Lishan Kang, Xuejie Zhang. (Nov.2010) 'Identity-Based Authentication in Cloud Storage Sharing', Multimedia Information networking and Security, 851-855.

38. Liu wei, Zhang Liyan. (may.2010) 'A Computing ModeSuitable for Medium and small sized Enterprises Cloud Computing', 2010 International Conference on Intelligent Computation Technology and Automation.

39. L. M Given. (2008) *The SAGE encyclopedia of Qualitative research methods*, SAGE publications.

40. L. Savu. (May.2011) 'Cloud Computing: Deployment Models, Delivery Models, Risks and Research Challenges', International Conference on Computer and Management, 1-4.

41. Mathisen, Eystein. (may 31, 2011) 'Security challenges and solutions in Cloud Computing', Digital Ecosystems and Technologies Conference (DEST), 5th IEEE International Conference, 208-212.

42. Mukharjee K, S.G. (Mar.2010) 'A secure Cloud Computing ', 2010 International Conference on Recent Trends in Information Telecommunication and Computing, 369-371.

43. Nguyen Q, Sood A. (June 2011) 'Designing SCIT architecture pattern in a Cloud based Environment ', 41st International Conf. on Dependable Systems and Networks workshops, 123-128.

44. Peter Mell. (2011) 'The NIST Definition of Cloud ', *Reports on Computer Systems Technology*, sept., p. 7.

45. Popovic, Kresimir. (May 2010) 'Cloud Computing Security issues and Challenges', MIPRO proceeding of the 33rd International Convention , 344-349.

46. Prasad P, Ojha B. (13 march 2011) '3 Dimensional security in Cloud Computing', Computer Research and Development (ICCRD), 3rd International Conference, 198-201.

47. Qian Wang, Cong Wang. (May 2011) 'Enablic Public Auditability and Data Dynamics for Storage Security in Cloud Computing', IEEE Transactions on Parallel and Distributed Systems, 847-859.

48. Q.L Nguyen. (June 2011) 'Designing SCIT architecture pattren in a Cloud based environment', 41st International Conference on Dependable Systems and Networks workshop (DSN-W), 123-128.

49. Ran Liu, Jian-Ping Li. (2010) 'A Predictive Judgment method for WLAN attacking based on Cloud Computing environment', Apperceiving Computing and Intelligence Analysis (ICACIA), International Conference 2010, 22-25.

50. Rihoux B, R.C. (2004) 'Qualitative Comparative analysis (QCA): state of the art and prospects ', APSA 2004 Annual Meeting Panel 47-9, Chicago.

51. Sanka S, H.C. (Dec.2010) 'Secure data access in Cloud Computing', IEEE 4th International Conference on Internet Multimedia Services Architecture and Application (IMSAA), 1-6.

52. Saripalli P, Walters B. (July 2010) 'A Quantitative Impact and Risk Assessment Framwork for Cloud Security ', 3rd International Conference on Cloud Computing , 280-288.

53. Shucheng Yu, Cong Wang. (March 2010) 'Achieving secure Scalabe and Fine grained data access control in Cloud Computing ', IEEE Conference INFOCOM , 1-9.

54. Sirisha A, Kumari G. (Dec 2010) 'API access control in Cloud using the Role Based Access Control Model', Trendz in Information sciences & Computing (TISC), 135-137.

55. Somani U, Lakhani K. (Oct 2010) 'Implementing Digital signature with RSA Encryption algorithm to enhance the data security of Cloud in Cloud Computing', 1st International Conference on Parallel Distributed and Grid Computing , 211-216.

56. Sravan Kumar R, Saxena A. (jan 2011) 'Data Integrity proofs in Cloud storage', Communication Systems and networks (COMSNETS), Third International Conference 2011, 1-4.

57. Srinivasatava Prashant, Singh Satyam. (June 2011) 'An Architecture based n Proactive model for Securrity in Cloud Computing', International conference on recent Trends in Information Technology (ICRTIT), 661-666.

58. Subashini S, Kavitha V. (2011) 'A Survey in Security issues in service delivery models of Cloud Computing', *Journal of Netwrok and Computer Applications*, vol. 34, no. 1, Jan, pp. 1-11.

59. Syam kumar P, Subramanian R. (Oct 2010) 'Ensuring data storage security in Cloud Computing using Sobol sequence', 1st International Conference on Parallel Distributed and Grid Computing (PDGC), 217-222.

60. Takabi H, Joshi J. (2010) 'Security and Privacy challenges in Cloud Computing Environment', *Security & Privacy, IEEE* , vol. 8, no. 6, December, pp. 24-31.

61. Takabi H. (July.2010) 'Secure Cloud: Towards a Comprehensive Security Framework for Cloud Computing Environments', IEEE 34th Annual Computer Software and Applications Conference Workshops, 393-398.

62. Tie Fang Wang, Baosheng Ye. (July 2010) 'Study on enhancing performance of cloud trust model with famiy gene technology', 3rd IEEE International conf. on Computer Science and Information Technology (ICCSIT), 122-126.

63. Tribhuwan M, Bhuyar V. (OCt 2010) 'Ensuring Data Storage Security in Cloud Computing through Two way Hanshake Based on Token Management', International Conf. on Advances in recent technologies in Communication and Computing , 386-389.

64. Unterkalmsteiner M, Gorschek T. (2011) 'Evaluation and Measurement of Software Process Improvement - A Systematic Literature Review', *IEEE Transactions on Software Engineering*, vol. PP, no. 99, March , p. 10.

65. W.A. Pauley. (2010) 'Cloud Provider Transparency: An Empirical Evaluation', *IEEE Secuirty and Privacy*, vol. 6, no. 6, December, pp. 32-39.

66. Wang Cong, Cao Ning. (June 2010) 'Secure Ranked keyword serch over Encrypted Cloud data ', IEEE 30th International conf. on Distributed Computing Systems (ICDCS), 253-262.

67. W.M, Trochim. (2006) *Conclusion Validity*, 20 Oct, [Online], Available: http://www.socialresearchmethods.net/kb/concval.php .

68. W.M, Trochim. (2006) *Construct validity*, 20 Oct, [Online], Available: http://www.socialresearchmethods.net/kb/constval.php .

69. W.M, Trochim. (2006) *External Validity*, 20 Oct, [Online], Available: http://www.socialresearchmethods.net/kb/external.php .

70. W.M, Trochim. (2006) *Internal Validity*, 20 Oct, [Online], Available: http://www.socialresearchmethods.net/kb/intval.php .

71. Wood K, Pereira E. (Nov.2010) 'An Investigation into CLoud Configuration and Security', 2010 International Conference for Internet Technology and Secured Transactions, 1-6.

72. Xiao Yong Li, Yong shi. (Dec 2010) 'Multi Tenancy Based Access Control in Cloud', International Conf. on Computational Intelligence and Software Engineering (CiSE), 1-4.

73. Xiaofei Zhang, Hui Liu. (Nov 2010) 'Application Oriented Remote Verification Trust Model in Cloud Computing ', 2nd International Conf. on Cloud Computing Technology and Science, 405-408.

74. Xue Jing, Zhang Jian-jin. (Aug. 2010) 'A Brief Survey on the Security Model of Cloud Computing', 9th International Conf. on Distributed Computing and Applications to Business Engineering and Science (DCABES)l, 475 - 478.

75. Dong Xu. (june.2010) 'Cloud Computing: An Emerging Technology', International Conference on Computer Design and Applications, vi-100-104.

76. Yanping Xiao, Chuang Lin. (Dec 2010) 'An Efficient Privacy Preserving Pubish Subscrribe service scheme for Cloud Computing', IEEE Global Telecommunications Conference, 1-5.

77. Youngmin Jung, Mokdong Chung. (Feb 2010) 'Adaptive Security management model in the Cloud Computing environment ', 12th International Conf. on Advanced Communication technology, 1664-1669.

78. Zhang Jianhong, Chen Hua. (Sept 2010) 'Security storage in the Cloud Computing: A RSA based assumption data integrity check without original data', International Conf. on Educational and Information technology (ICEIT), 143-147.

79. Zhidong Shen, Qiang Tong. (July 2010) 'The Security of Cloud Computing System enabled by trusted Computing Technology', 2nd International Conference on Signal Processing Systems (ICSPS), 11-15.

80. Zhidong Shen, Li Li. (May 2010) 'Cloud Computing System Based on Trusted Computing Platform', Intelligent Computation Technology and Automation (ICICTA), 942-945.

CHAPTER 10

APPENDIXES

APPENDIX A

LIST OF IDENTIFIED CHALLENGES

S.No.	Ref. no.	Challenges	Description	Compromised attributes
1	24	WS-Security	The most important specification addressing security for Web Services.	Integrity, confidentiality
2	24	Phishing attack	The risk of the attacker lures the victim to a fake Web page (either using spoofed emails or attacks on the DNS), where the victim enters username and password(s).	Confidentiality
3	24	wrapping attack	The risk of by using XML Signature for authentication or integrity protection.	Integrity
4	24	Injection Attack	To aim at injecting a malicious service implementation or virtual machine into the Cloud system.	Availability
5	52 40	IP Spoofing	The risk of Illegally using another user's authentication information, such as user name and password.	Confidentiality
6	52	Tampering	Unauthorized changes to persistent data or alteration of data over a network.	Integrity
7	52	Repudiation	The risk of user performs an illegal operation in a system that lacks the ability to trace it.	Audit ability
8	52	Information Disclosure	A Cloud user reads a file from a co- tenant's workflow, without permission.	Confidentiality
9	52 16	Denial of Service	An adversary gains control of a tenant's VM, and makes another's web server unavailable.	Availability
10	52	Elevation of Privilege	An attacker penetrates all system defenses to join the trusted system itself.	Confidentiality

11	41	Physical security	The risk of the hardware components may be attacked by people or natural disasters, regardless of the level of internal software and policy security.	Security, availability
12	49	WLAN's security	The risk of the WLAN openness has brought some security issues such as network eavesdropping, identity cheats and message tampering in a greater degree.	Usability, Accountability
13	49	Direct attacking method	It does not attempt to break the Encryption key but deciphers the cipher text directly.	Confidentiality
14	29 40	Replay attack	A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed.	Integrity
15	29 40	Man-in-the-middle attack	It is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them.	Availability, Integrity
16	29	Reflection attack	It is a method of attacking a challenge-response authentication system that uses the same protocol in both directions.	Confidentiality
17	29	Interleaving attack	The interleaving attack is similar to man-in-the-middle attack, but it can attack the protocol in which all parties have authentic copies of all others' public keys.	Integrity, Confidentiality
18	29	Timeliness attack	The risk of without deadline, the protocol does not know when the step is terminated, which can introduce some problems.	Usability, availability

19	15	Self-adaptive storage resource management	The monitored information needs to enable optimized, dynamic control for large-scale data transfers on dedicated circuits, data-transfer scheduling, distributed data scheduling, automated management and performance prediction of remote storage services.	Integrity, Confidentiality
20	15	Client monitoring and security	The storage service has to be aware of the different types of clients and of their access rights.	Security
21	45	Lack of trust	With the growing number of Cloud service providers, the customers are Facing a challenge to select the best and most appropriate providers from numerous offers.	Confidentiality
22	45	Weak Service Level Agreements (SLAs)	Consumers might face problems that occur from vendor lock-in, insufficient security measures, data unavailability, hidden costs, and non-transparent infrastructure.	Availability, confidentiality
23	45	Perceived Lack of Reliability	The risk of not clear information whether the availability is for a single server where the virtual instance of particular customer resides or for all the servers placed in data centers in different locations of the world.	Availability
24	4	Auditing	It is the process of reviewing and examining the authorization and authentication records in	Security, confidentiality

			order to check, whether compliances with predefined security standards and policies.	
25	40	Back-Door	The strategy is to gain access to a network through bypassing of control mechanisms, getting in through a "back door" such as a modem.	Usability
26	40	TCP Hijacking	The attacking computer substitutes its IP address for that of the trusted client, and the server continues the dialog believing it is communicating with the trusted client.	Confidentiality, integrity
27	40	Social Engineering	This attack uses social skills to obtain information such as passwords or PIN numbers to be used against information systems.	Confidentiality
28	40	Dumpster Diving	Dumpster diving involves the acquisition of information that is discarded by an individual or organization.	Availability
29	40	Password Guessing	Passwords are the most commonly used mechanism to authenticate users. obtaining passwords is a common and effective attack approach.	Confidentiality
30	40	Trojan Horses and Malware	Trojan horses hide malicious code inside a host program that seems to do something useful.	Usability
31	40	Completeness	To the fact that a user must be supplied by the data service provider with all the information he/she is authorized to access on the basis of the stated authorizations.	Availability

32	28	Roll back attack	When the data owner updated the data with a new version, the malicious service provider still provide older version to user.	Availability, usability
33	28	Fairness	During the data transmission procedure, in order to gain certain advantages, malicious party may refuse to response after receiving the evidence from other peer.	Confidentiality
34	28 47 57	Data Loss or Leakage	A provider may unethically retain additional copies of the data in order to sell it to interested third parties.	Availability
35	22	Computer Network Attack	CAN is defined as operations to disrupt, deny, degrade, or destroy information Resident in computers and computer networks or the computers and networks themselves.	Integrity. Confidentiality
36	22	Denial of service attack	Destroys the system’s availability	Availability
37	58	Data security	The sensitive data of each enterprise continues to reside within the enterprise boundary and is subject to its physical, logical and personnel security and access control policies.	Security
38	58 19	Network security	All data flow over the network needs to be secured in order to prevent leakage of sensitive information.	Integrity, security
39	58 19	Data locality	The risk of the customer does not know where the data is getting stored.	Reliability
40	58 27	Data integrity	To maintain data integrity in a distributed system, transactions across multiple data sources need to be handled correctly in a fail safe manner.	Integrity

41	58	Data segregation	A malicious user can use application vulnerabilities to hand craft parameters that bypass security checks and access sensitive data of other tenants.	Security, confidentiality
42	58	Backup	The vendor needs to ensure that all sensitive enterprise data is regularly backed up to facilitate quick recovery in case of disasters.	Availability
43	5	Data manipulation	This involves data insertion, modification and data deletion.	Availability, Integrity

APPENDIX B

LIST OF IDENTIFIED TECHNIQUES

S.No:	Ref. No:	Security Techniques	Description	Impact
1	37 4 35	Identity-Based Authentication (IBA)	This scheme divides the sharing users into the very same domain and in this domain relies on the sharing global master key to exercise mutual authentication.	Privacy, Security
2	55	RSA algorithm	This is used to assess Cloud Storage Methodology and Data Security in Cloud by the Implementation of digital signature.	Security, efficiency
3	9 1	dynamic intrusion detection system	This involves for strengthening the security application of Cloud Computing.	Performance
4	72	Multi-tenancy based access control model (MTACM)	This is designed to embed the security duty separation principle in Cloud.	Security, access control
5	24 29	TLS Handshake	It is designed to exchange the evidence in the data transaction, which removes the ambiguities that lead to repudiations or disputations between the user and service provider.	security
6	12 6 11 76 13	Public key based Homomorphic authenticator with random masking	This is used to achieve the privacy-preserving public Cloud data auditing system. It	Privacy, performance

	20 63		solves the problems of encrypted storage access with encrypted addresses and encrypted branching.	
7	12 79 47 21 59	Third party auditor (TPA)	It describes who has expertise and capabilities that Cloud users do not have and is trusted to assess the Cloud storage service security. Merkle Hash Tree: To support efficient handling of multiple auditing tasks	Efficiency, QoS
8	36	Probabilistic sampling technique	This aims to consider secure data storage, computation and privacy preserving together.	Security, privacy
9	78 57	Diffie-Hellman key exchange	It describes protocol between Cloud service provider and the user for secretly sharing a symmetric key for secure data access.	Security, access control
10	10	Private face recognition	It involves face recognition and matching under the encrypted conditions, the result is encrypted again before encrypted transmission to user.	Privacy, performance
12	11 4	Message Authentication Codes (MACs)	This involves verifying the integrity by recalculating the	Efficiency

			MAC of the received data file and comparing it to the locally precomputed value.	
13	31	Data coloring and software water marking techniques	This lets us segregate user access and insulate sensitive information from provider access.	Performance, security
14	15 29 62	A novel Cloud dependability model	This involves enhancing the security of heterogeneous Cloud environments. System-level virtualization techniques are used to enhance the dependability of Cloud environments.	QoS, security
15	53 26	Key Policy Attribute-Based Encryption (KP-ABE)	In this The encryption associates the set of attributes to the message by encrypting it with the corresponding public key Components.	Privacy, efficiency
16	53 25	Proxy Re-Encryption (PRE)	This is a cryptographic primitive in which a semi-trusted proxy is able to convert a cipher text encrypted under user1 public key into another cipher text that can be opened by user2 private key without seeing the Underlying plaintext.	Performance, security
17	77 54	RBAC (Role-Based Access Control)	This describes the central notion of	Privacy, efficiency

	3 61	technique	RBAC is that permissions are associated with roles and the users are assigned to appropriate roles. Thus roles serve as a layer of abstraction between the users and permissions. This greatly simplifies the management of permissions.	
18	73	Application-oriented Remote Verification Trust Model (ARVTM)	This model is capable of adjusting the user’s trust authorization verification contents according to the specific security requirements of different applications, and dynamically adjusting the user’s trust value with the trust feedback mechanism to determine whether or not the requested resource or service should be provided.	Qos, security
19	4	Security assertion Markup Language (SAML)	This is based on XML standards, used as a tool to exchange the authorization and authentication attributes between two entities.	Performance, privacy
20	80 17 32	Trusted Platform Module (TPM).	This involves which Cloud Computing system is combined with Trusted Platform Support Service (TSS) to obtain authentication.	Qos, security

21	9 56	Proof Of Retrievability (POR).	It gives a proof of data integrity in the Cloud which the customer can employ to check the correctness of his data in the Cloud.	Efficiency, performance
22	28	Fair MPNR protocol	This solves the problem of fair non-repudiation and roll back attack. Each message consists of specified data transmission information as evidence.	Security, performance
23	59	Sobol Sequence	This involves The numbers are generated sequentially to fill the larger "gaps" in the Pseudorandom Data to address data storage security in Cloud Computing.	Security, performance, efficiency
24	23	Redundant Array of Independent Net-storages (RAIN)	This involves to splits data into segments and distributes segments onto multiple providers.	Privacy, efficiency
25	36 42	Hadoop Distributed File System	This involves to efficiently organize "Free" computer storage resources existing within enterprises to provide low-cost high-quality storage services.	Performance
26	43	Self-Cleansing Intrusion Tolerance (C-SCIT)	This describes a recovery-based intrusion tolerance scheme leveraging Cloud Services from multiple vendors.	Security, privacy

27	66	searchable symmetric encryption (SSE)	This involves to allow the data owner to outsource his data in an encrypted manner while maintaining the selectively search Capability over the encrypted data.	Security, privacy, performance
28	37	Provable data possession(PDP)	This involves allowing a client that has stored data at a un trusted server to verify that the server possesses the original data without retrieving it.	Security, performance, efficiency
29	21	Time bound ticket based mutual authentication scheme	This involves achieving mutual authentication between the server and the client, this scheme reduces the server's processing overhead efficiently.	Efficiency, security, performance
30	74	Security Access Control Service (SACS)	This includes Access Authorization, Security API and Cloud connection Security.	Access control, Security
31	33 56 2 16 56 65 75	The Service Level Agreement	This involves to identify and define the customer's needs and Provide a framework for understanding, Simplify complex issues, Reduce areas of conflict, Encourage dialog in the event of disputes, Eliminate unrealistic expectations.	Qos, performance
32	30	Intrusion detection	Leads to effective	Efficiency,

		system	resource usage by applying differentiated level of security strength to users based on the degree of anomaly.	Security
33	60	Hypervisor	It helps abstract infrastructure and resources to be made available to the clients as isolated VMs	Access control
34	60 61	Identity Management	It can help to authenticate users and services based on credentials and characteristics	Privacy and Security

APPENDIX C

SURVEY QUESTIONNAIRE
Security techniques for protecting data in Cloud

Base information:

Students Name: Ragi Shivashanker – shra10@student.bth.se
Venkata Sravan Kumar Maddineni – vema10@student.bth.se

We are Master students in Electrical Engineering with emphasis in Telecommunication systems from Blekinge Institute of Technology (BTH), Sweden. Currently we are working on our Master thesis in Cloud Computing security. We are working under Prof. Lars Lundberg as academic supervisor in BTH and Mr. Jens Kvarnberg as external supervisor from Swedish Armed Forces (SAF). Our main aims and objectives are as follows:

Aims and objectives

To understand the threats and security techniques used to mitigate them in Cloud Computing.

- To understand the security techniques used in the current world in Cloud Computing.
- To identify security threats we expect in the future of Cloud Computing.
- To suggest counter measures for the future challenges to be faced in Cloud Computing.

To fulfill above aims we are using survey method in our research methodology. The survey method would employ literature study followed by personal interaction with various security experts working on Cloud Computing.

*(The following fields are optional, in case you feel like sensitive to mention)
Who you are:____
Professional role (Manager, Technical expert, etc):__________________________________
Experience (Number of years):____
Number of years working in the IT sector:____
Number of years working with Cloud Computing:___________________________________
Number of years working with Security issues:_____________________________________

NOTE: Answering all the following questions is not mandatory, answer to the best of your effort and share your ideas and views from your perspective.

Interview Questions:

Research Question 1. What are the various security techniques being used by the leading Cloud Computing companies, to prevent active and passive attacks when the data is being transferred between Cloud and home network?

____
____
____
____
____

a. How can client data be protected from active attacks (masquerading, reply and modification of data) in a public Cloud?

____
____
____

b. How can client data be protected from passive attacks (traffic analysis and release of message contents) in a public Cloud?

____
____
____

c. How can Cloud providers achieve authentication, data confidentiality, access control and integrity of client data in private and public Clouds?

____
____
____

Research Question 2. What are the security techniques being used to prevent unauthorized access to data within the Cloud?

____
____
____

a. What are the main security attacks that exploit Cloud virtualization and what are the security techniques that are implemented?

____
____
____

b. Are cryptographic techniques suitable for protecting data in a Cloud?

____
____
____

c. How can clients trust that a Cloud provider will protect the privacy of their data?

____
____
____

d. Should Cloud provider use standard based or own security solutions?

____
____
____

e. How does the Cloud provider restore client data if any problem occurs (how long does it take and how much data can be lost)?

____
____
____
____

f. How does a Cloud provider secure data on storage devices?

____

____

____

g. How are one customer’s data and applications separated from other customers (who may be a hacker or competitor)?

____

____

____

h. How can Cloud providers avoid data theft from machines in a Cloud?

____

____

____

Research Question 3. What are the major security challenges we expect for the future of Cloud Computing?

____

____

____

a. How are we going to overcome the security challenges in the future of Cloud Computing?

____

____

b. Are present security techniques suitable for future challenges or not?

____

____

____

c. Are the security policies the same for both private and public Clouds?

____

____

____

d. How does the Cloud provider address legal and regulatory issues related to Cloud Computing?

____

____

____

e. How can a client ensure that the Cloud provider fulfils their promises?

____

____

Research Question 4. How do we handle the security problems that may be expected in the future of Cloud Computing?

____

____

____

APPENDIX D

SEARCH QUERIES

Name of the Database	**Search Query**
IEEE Xplore	You searched for: **((Cloud Computing) AND (security) AND (technique* OR method* OR challenge*))** You refined by: Subscribed Content: IEL ☒ Subject: Computing & Processing (Hardware/Software) ☒, Communication, Networking & Broadcasting ☒ Publication Year: 2002 - 2011 ☒
SpringerLink	Search results for the boolean expression '((Cloud and computing) and (security) and (technique* or method* or challenge*))' published between '1 Jan 2001' and '24 Aug 2011' with filters: • Remove Computer Science • Remove Computer Communication Networks
ScienceDirect	((Cloud Computing) AND (security) AND (technique* OR method* OR challenge*)) AND LIMIT-TO(topics, "Cloud Computing,computer science, internet, software, web service,information system,information security,Cloud,access control,virtual machine")
Scopus	((Cloud Computing) AND (security) AND (technique* OR method* OR challenge*)) AND (LIMIT-TO(PUBYEAR, 2011) OR LIMIT-TO(PUBYEAR, 2010) OR LIMIT-TO(PUBYEAR, 2009) OR LIMIT-TO(PUBYEAR, 2008) OR LIMIT-TO(PUBYEAR, 2007) OR LIMIT-TO(PUBYEAR, 2006) OR LIMIT-TO(PUBYEAR, 2005) OR LIMIT-TO(PUBYEAR, 2004) OR LIMIT-TO(PUBYEAR, 2003) OR LIMIT-TO(PUBYEAR, 2002) OR LIMIT-TO(PUBYEAR, 2001)) AND (LIMIT-TO(SUBJAREA, "COMP") OR LIMIT-TO(SUBJAREA, "MULT"))

APPENDIX E

Security Techniques used by leading Cloud providers

S. No.	Company Name	Security Practices
1	Amazon	SSL Encryption, Hypervisor
2	Microsoft	VPN, Identity Management, SSL Encryption.
3	Sales force	Intrusion Detection Systems, TLS encryption, SAML, MD5.
4	IBM	SLA, third party Auditor, SSL Encryption, VPN.