Security and Privacy in Cloud Computing

Krishnan

Follow this and additional works at: https://scholarworks.wmich.edu/masters_theses

Part of the Information Security Commons

Recommended Citation
https://scholarworks.wmich.edu/masters_theses/919
SECURITY AND PRIVACY IN CLOUD COMPUTING

by

Ramakrishnan Krishnan

A thesis submitted to the Graduate College
in partial fulfillment of the requirements
for the degree of Master of Science
Computer Science
Western Michigan University
April 2017

Thesis Committee:

Dr. Leszek T. Lilien Ph.D., Chair,
Dr. John Kapenga, Ph.D.,
Dr. Ikhlas Abdul Qader, Ph.D.
Cloud computing (CC) gained a widespread acceptance as a paradigm of computing. The main aim of CC is to reduce the need for customers' investment in new hardware or software by offering flexible cloud services, with a user reaping the benefits of the pay per use approach. CC demands addressing many security and privacy issues: both problems (vulnerabilities, threats, and attacks) and solutions (controls). The thesis discusses all these classes of problems and solutions, categorizing them as either security-related issues, privacy-related issues, or intertwined security and privacy issues. The main contributions of the thesis are twofold: first, using the above categorization of the issues; and second, the literature review of the security and privacy issues in CC within the categorization framework. The major lessons learned during this research include confirmation of the decisive role that security and privacy solutions play and will continue to play in adopting CC by customers; understanding numerous vulnerabilities, threats, and attacks; and identifying controls for these problems. In addition, the sheer number of references to trust (in both problems and solutions), demonstrated a significant role of trust in CC.
ACKNOWLEDGMENTS

I would like to express appreciation for several people who have helped and supported my degree and this thesis work. First, I would like to thank my thesis supervisor and committee chair, Dr. Leszek T. Lilien who offered valuable advice, support, and feedback throughout my master’s thesis research. Secondly, I would like to thank Dr. John Kapenga, Dr. Ikhlas Abdul-Qader for their participation on the thesis committee, and for their evaluation and feedback. Finally, I must express my very profound gratitude to my parents Krishnan and Sakunthala for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of researching and writing this thesis. You are always there for me. This accomplishment would not have been possible without them. Thank you.

Ramakrishnan Krishnan
# TABLE OF CONTENTS

ACKNOWLEDGEMENTS ............................................................................................................ ii
LIST OF TABLES ......................................................................................................................... vi
LIST OF FIGURES ...................................................................................................................... vii
INTRODUCTION .......................................................................................................................... 1

1.1. BACKGROUND INFORMATION ON CLOUDS ................................................................. 1
1.2. BACKGROUND INFORMATION ON SECURITY AND PRIVACY IN CLOUDS .......... 3
1.3. RESEARCH METHODOLOGY ............................................................................................... 5
1.4. THESIS CONTRIBUTIONS AND ORGANIZATION ............................................................ 6

CLOUD COMPUTING OVERVIEW ............................................................................................ 8

2.1. CLOUD COMPUTING VS. UTILITY COMPUTING ............................................................. 8
2.2. CLOUD COMPUTING VS. GRID COMPUTING ................................................................. 8
2.3. CLOUD DATA CENTER VS. TRADITIONAL DATA CENTER .............................................. 11
2.4. ESSENTIAL CHARACTERISTICS OF CLOUD COMPUTING ........................................... 12
2.5. DELIVERY MODELS FOR CLOUD COMPUTING ............................................................... 13
    2.5.1. Infrastructure as a Service (IaaS) ................................................................................ 14
    2.5.2. Platform as a Service (PaaS) ....................................................................................... 15
    2.5.3. Software as a Service (SaaS) ...................................................................................... 17
2.6. DEPLOYMENT MODELS OF CLOUD COMPUTING ......................................................... 18
    2.6.1. Public Cloud ............................................................................................................... 18
    2.6.2. Private Cloud .............................................................................................................. 20
    2.6.3. Community Cloud ...................................................................................................... 21
    2.6.4. Hybrid Cloud ............................................................................................................ 21
2.7. OBSTACLES PREVENTING ADOPTION OF CLOUD COMPUTING ............................... 21
2.8. PERFORMANCE AND COST FACTORS ............................................................................ 23
Table of Contents—Continued

SECURITY PROBLEMS IN CLOUD COMPUTING ................................................................. 25

3.1. IMPORTANCE OF SECURITY IN CLOUD COMPUTING .............................................. 25
3.2. CATEGORIES OF CLOUD COMPUTING SECURITY ...................................................... 26
3.3. PROBLEMS: VULNERABILITIES, THREATS AND ATTACKS ...................................... 32
   3.3.1. Buffer Overflow Attacks ...................................................................................... 33
   3.3.2. Cloud Authentication Attacks .......................................................................... 34
   3.3.3. Cloud Malware Injection Attacks .................................................................... 35
   3.3.4. DOS Attacks and Mobile Terminal Security ..................................................... 36
   3.3.5. Insecure API’s .................................................................................................... 37
   3.3.6. Malicious Insiders ............................................................................................ 38
   3.3.7. SQL Injection Attacks ...................................................................................... 40

PRIVACY PROBLEMS IN CLOUD COMPUTING ................................................................. 41

4.1. IMPORTANCE OF PRIVACY AND CONFIDENTIALITY IN CLOUDS ......................... 41
4.2. CLOUD COMPUTING PRIVACY OVERVIEW ............................................................ 42
4.3. PROBLEMS: VULNERABILITIES, THREATS AND ATTACKS ...................................... 45
   4.3.1. Broken Authentication and Compromised Credentials ....................................... 45
   4.3.2. Data Breaches ................................................................................................... 45
   4.3.3. Data Location Problems ................................................................................... 47
   4.3.4. Problems Related to Data Ownership and Content Disclosure ......................... 48
   4.3.5. Virtualization Problems .................................................................................. 48

INTERTWINED SECURITY AND PRIVACY PROBLEMS IN CLOUD COMPUTING ...... 50

5.1. PROBLEMS: VULNERABILITIES, THREATS AND ATTACKS ...................................... 50
   5.1.1. Compromised Shared Platforms ....................................................................... 51
   5.1.2. Natural Disasters ............................................................................................. 51
   5.1.3. Permanent Data Loss ....................................................................................... 51
   5.1.4. Virtual Machine Migration Attack .................................................................... 52
5.2. OTHER INTERTWINED SECURITY AND PRIVACY PROBLEMS ............................. 53
Table of Contents—Continued

5.3. Case Studies of Intertwined Security and Privacy Problems ........................................ 54
   5.3.1. Case Study 2: Account Hijacking ........................................................................ 54
   5.3.2. Case Study 1: Network-based Attack .................................................................. 55

Security Controls for Cloud Computing ........................................................................... 56
6.1. Controls Against Hardware-based Attacks .................................................................. 56
6.2. Controls Against Hypervisor-based Attacks ................................................................. 58
6.3. Controls via Cloud Auditing ....................................................................................... 58
6.4. Controls via Effective Encryption ................................................................................. 60

Privacy Controls for Cloud Computing ............................................................................ 62
7.1. Controls for Authentication and Identity ...................................................................... 63
7.2. Controls for Trust Management ................................................................................... 68

Intertwined Security and Privacy Controls for Cloud Computing .................................... 71
8.1. Controls Against Network-based Attacks ................................................................... 71
8.2. Controls Against Delivery Model Threats .................................................................. 75
8.3. Controls via Computer Forensics ............................................................................... 76
8.4. Risk Assessment Controls ......................................................................................... 80

Concluding Remarks ......................................................................................................... 82
9.1. Contributions ................................................................................................................ 82
9.2. Lessons Learned .......................................................................................................... 82
9.3. Future Work ................................................................................................................... 83

References ........................................................................................................................ 85
LIST OF TABLES

1. Cloud Security Requirements vs. Cloud Service/Mechanisms .........................................................26
2. A Summary of Network Security Problems and Solutions ..................................................................30
3. A Summary of Software Security Problems and Solutions ..................................................................31
4. A Summary of Virtualization Security Problems and Solutions .......................................................49
5. Other Intertwined Security and Privacy Problems with implementation challenges ...53
6. Cloud Specific Auditing Challenges ..................................................................................................59
7. Cloud Problems for Delivery Models and their Solutions .................................................................76
LIST OF FIGURES

1. Forward Search for a Newer Publication from a Given Publication ......................... 6
2. Traditional Data Center vs. Cloud Data Center .................................................................... 11
3. Cloud Computing Delivery Models .............................................................................. 14
4. IaaS vs. PaaS vs. SaaS (Separation of Responsibilities) .................................................. 14
5. Deployment models for Cloud Computing ................................................................... 18
7. Security-only, Privacy-only and Intertwined Security and Privacy problems in CC ... 32
8. Cloud Authentication Threats and Attacks ....................................................................... 34
9. Security-only, Privacy-only and Intertwined Security and Privacy problems in CC ... 44
10. Security-only, Privacy-only and Intertwined Security and Privacy problems in CC ... 50
11. Security-only, Privacy-only and Intertwined Security and Privacy Controls in CC ... 56
12. Security-only, Privacy-only and Intertwined Security and Privacy Controls in CC ... 62
13. Signing in to Amazon Console with User ID ................................................................ 66
14. Getting the Authenticator Code from a device ............................................................... 66
15. Using a code to Sign in to the cloud console ................................................................. 67
16. Security-only, Privacy-only and Intertwined Security and Privacy Controls in CC ... 71
17. Cloud Forensics Process ................................................................................................ 78
CHAPTER 1

INTRODUCTION

This Thesis discusses security and privacy problems in cloud computing, and identifies some of the known solutions for selected problems.

This Section gives an overview of cloud computing technology by describing its basics and the underlying principles. We identify challenges that cloud computing is facing and possible solutions for them.

1.1. Background Information on Clouds

Traditional Computing Models. Data is a valuable resource for organizations and individuals. Their management is an important task and includes assuring integrity of data. For decades, organizations and individuals have been using computer hardware such as hard discs, DVDs, CDs, discs, and floppy discs to store their data. Introduction of database systems enhanced information management and made it more effective [1].

The last decades have made a reality information processing where data can be processed efficiently on large computing and storage platforms accessible via the Internet [2]. Advancements in database systems and networking (including the Internet) enabled the development of new computing models. They include grid computing developed in the early 1990s; as well as utility computing and cloud computing, developed around 2005 [1].

Cloud computing (CC) can be defined as a computing model that enables convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management efforts or service provider interactions [1]. Cloud computing involves the provision and use of IT infrastructure, platforms and applications
of any kind in the form of services that are electronically available on the Internet [22]. Just a few examples of applications using cloud services include: online file storage, social networking sites, webmail, and online business applications [2].

As enterprises strive to identify new methods for driving their businesses forward, surging demand has shifted to solutions that provide lower-cost solutions for use of computing systems (both in terms of access to computing infrastructure and operating costs). This resulted in the exponential growth of cloud computing, which was found to be more effective than the earlier solutions [3].

As technological advances continue, the reach and influence of cloud computing continue to rise. Even so, when organizations outsource data and business applications to CC providers (who are third parties for them), security and privacy issues emerge as crucial concerns.

Virtualization in Cloud Computing. Virtualization is one of the key technologies of cloud computing services, facilities, aggregation of multiple standalone systems into single hardware platform by virtualizing computing resources (e.g.: Network, CPU’s, Memory, Storage).

Virtualization is enabled by hardware abstraction, which hides the complexity of managing the physical computing platform and simplifies scalability of computing resources. It is implemented via hypervisors [11]. A hypervisor is responsible for isolation of Virtual Machines (VMs), so that they are prevented from to directly accessing other VMs' virtual disks, memory, or applications on the same host. Virtualization provides scalability and multi-tenancy (the latter occurs when a single instance of a software application serves multiple customers [4]). These two properties are significant characteristics of CC, and facilitate sharing and pooling of resources in order to improve agility, flexibility, reduce costs and enhance business value.
The practical aspects of virtualization related to configuration, networking, and sizing of cloud systems are faced with challenges [8, 11]. In cloud virtualization, provisioning is a basic mechanism for allocation of a cloud provider's resources to a customer. When a cloud provider accepts a request from a customer, it must create the appropriate number of virtual machines (VMs) and allocate resources to support them. The process is conducted in several different ways: advance provisioning, dynamic provisioning, and user self-provisioning [7]. The dynamic provisioning of cloud resources and services faces a number of challenges such as the optimal configuration for VMs, and the limitations in the number and capabilities of CPUs, memories, disks and network bandwidth to be partitioned among the resident VMs [12]. Cloud service providers undertake a significant effort to make the virtualization mechanisms secure by striving to eliminate or at least reduce vulnerabilities, threats and attacks.

1.2. Background Information on Security and Privacy in Clouds

Security and Privacy Definitions. Security can be defined as follows [14]: “Security is the right not to have one’s activities adversely affected via tampering with one’s objects.”

In an equally succinct way, we can define privacy as follows [14]: “Privacy is the right to have information about oneself left alone.” Similarly, Rocha et al. [8] define privacy as the selective control of access of “self.” Selective control refers to the process where individuals control their interaction and information exchange with others. To assure their privacy, individuals try to control their openness to others. Pearson [9] explains that the level of openness between individuals is determined by their relationship and the value given to the information safeguarded. Privacy can be generally described as the dynamic process whereby individuals regulate the degree of their openness to others.
Classic “CIA” Security Triad. A classic definition of security—in terms of its basic characteristics—specifies it in terms of the CIA triad; the acronym “CIA” stands for confidentiality, integrity and availability--three key requirements for any secure system [16, 17]. They are defined as follows:

1) **Confidentiality**: It is the ability to hide information from those people unauthorized to view it. It is the basis of many security mechanisms protecting not only information but other resources.

2) **Integrity**: It is the ability to ensure that data is an accurate and unchanged representation of the original information [10].

3) **Availability**: It ensures that a resource is readily accessible to the authorized user upon the user’s request.

This model is applicable across the whole subject of security analysis, from access to a user's Internet history to security of encrypted data across the Internet. [11].

Security and Privacy in Clouds. Over the years, numerous researchers have studied and surveyed the issues of security and privacy in cloud environments. To better comprehend those issues and their connections, technology researchers, and experts have taken advantage of different criteria to establish a comprehensive impression. Gruschka et al. [12] recommend a modeling of the security ecosystem in terms of three cloud system participants: service instance, service user, and the cloud provider. Furthermore, they identify attack categories: a) user to service, b) service to user, c) user to cloud, d) cloud to user, e) service to cloud, and f) cloud to service. While cloud computing is associated with numerous security and privacy problems, it
can be made effective by implementing efficacious solutions. In this thesis, we separate cloud computing security issues from its privacy issues.

1.3. Research Methodology

Research methodology is a process of managing and solving research problems systematically. To achieve the goals of research we can use different methods and techniques. For addressing the research questions and objectives, the exploratory approach is used. An exploratory study is a way of gaining new insights and clarifications for specific problems [13].

Systematic Literature Review (SLR): Systematic Literature Review (SLR) is defined as identifying, evaluating and interpreting the available relevant work for a particular topic or phenomenon of interest [14]. The researchers should put a significant amount of work and effort to identify published research results related to his research work. SLR is used mainly to summarize the existing state of the art, and to determine the gaps in it [15].

This Thesis is written based on scientific papers, online sources, journals etc. To find relevant papers, we searched mostly the following databases: IEEEXplore and ACM Digital Library, and ScienceDirect. We looked for the keywords “cloud computing,” “cloud security,” “cloud privacy,” and “cloud security and privacy” in titles, abstracts or keywords of articles. The composition of our search string was the result of a learning process including experimentation with a variety of combinations of keywords in order to test synonyms used in literature and to cover the variety of cloud security and privacy requirements concepts. After a careful review, some of the found references were excluded because they were: (a) irrelevant to CC security; (b) written in a language other than English; or (c) duplicating knowledge from other papers.
To enlarge the pool of references, we also performed backward reference search and forward reference search [16]. A backward search involves identifying articles cited in a given publication. It results in identifying publication that are older than the given publication (it goes backward in time). It requires just looking at the list of references in the given publication. A forward search identifies articles that cite a given publication. It results in identifying publications newer that the given publication (it goes forward in time). As an example, forward search can be performed on the Google Scholar website as follows:

1) Find a certain publication in Google Scholar.

2) Follow the link “Cited by” to see articles referencing the publication from Step 1—as shown in Fig. 1.

![Forward Search for Newer Publication from a Given Publication](image)

Fig. 1. Forward Search for Newer Publication from a Given Publication.

1.4. Thesis Contributions and Organization

The scope of this Thesis includes only technical security and privacy problems and solutions, excluding, among others legal and management aspects.

The main contribution of this thesis are:

1) Proposing *categorization* into security-only issues, privacy-only issues and intertwined security and privacy (in contrast to most surveys lumping security and privacy issues together).
2) Identifying the security-only problems, privacy-only problems, and intertwined security and privacy problems encountered by the cloud users.

3) Presenting selected security-only solutions, privacy-only solutions, and intertwined security and privacy solutions security for cloud computing.

Section 1 briefly describes the cloud and security background with different services, research methodology with systematic literature overview. Section 2 gives a brief overview of cloud computing, describes different services, deployment models present in the clouds. Section 3 describes and provides further insights of security with some of the issues. Section 4 describes and provides further insights of privacy with some of the issues. Section 5 presents some of the intertwined issues which is affecting both security as well as privacy. Section 6 present some control measures for security and privacy issues. Section 7 shows some of the obstacles. Finally, Section 8 concludes the Thesis.
CHAPTER 2
CLOUD COMPUTING OVERVIEW

Cloud computing is an emerging technology driven by the needs for flexible IT infrastructure, the emergence of big data analytics and increased mobile usage.


In utility computing, software and hardware resources are concentrated in large data centers, and users pay per use for storage and communication services.

Similarities: There are many similarities between utility computing and cloud computing. Utility computing often requires a cloud-like infrastructure, but its focus is on the business model for providing computing services. Utility computing involves a straightforward rental of facilities to users (so they are in full control of these facilities).

Differences: In contrast, in cloud computing users still pay for what they use but the service utilization is much more complex in terms of infrastructure and software. The facilities are controlled by the cloud owners and managers.

2.2. Cloud Computing vs. Grid Computing

*Grid computing* is a network with distributed resources, which can divide and farm out pieces hardware and software facilities to a great number of users, and may be owned by diverse organizations (unlike a cloud owned by a single owner). Users are obliged to provide their hardware and software to other users on a schedule managed by the grid managers.
Similarities: Cloud computing has several similarities with grid computing. Theoretically, the concept behind both models is to group up various computing resources together and share their capabilities in a scalable form in order to accomplish one or more complex tasks that are difficult or even impossible to accomplish with one single resource [17]. The computing resources of grid computing may include processing cycles, memory disk spaces, networks, printers, scanners, software licenses, remote devices, etc. Grid computing is commonly used for academic and scientific purposes to process computationally intensive tasks faster and cheaper [17].

In a business model, every client negotiates with the providers for its use of grid resources by providing a detailed proposal for the scope of his research study and anticipated amount of necessary resources [18]. The aim of development of grid computing was to facilitate users to remotely utilize idle computing power within other computing centers when the local one is busy or unable to perform the task alone.

Differences: Grid resources are generally free for using the computing resources but instead must agree to avail their own computing resources to be used by others at any time needed [19].

In contrast, cloud computing is commercially offered by providers for public use at an affordable cost for organizations that are unable or unwilling (possibly due to economic factors) to develop and manage their own computing solutions [20].

From a technical perspective, the purpose of grid computing is to integrate resources from various organizations forming a uniform resource pool which can provide the computing ability that is impossible to be achieved by a single computing center [18]. These organizations are distributed geographically and have their own rights in determining vendors of their resources. The aim of cloud computing is to divide resources into small pieces and deliver them to users according to their preferences.
In contrast, cloud resources are usually possessed or operated by a single organization and physically, they are centralized within the same computing/data center and distributed across multiple computing centers.

Grid computing uses *grid middleware*, a specific software product that provides necessary yet generic services for shielding the inherent underlying heterogeneity and distribution. The core services provided by middleware include information service, security service, data management and executive management [21]. Information service maintains detailed updated knowledge of all resources or services in a grid environment. Security services are deployed to ensure secure cross-organizational resource access, and protect communication and violation of local administrative policies [18]. Data management provides useful mechanisms for data access, data movement, data replication and data integration. Executive management is used to accomplish a task using the resources provided, monitor the progress of the task, and manage the computing result.

In contrast, cloud computing provides its services through *cloudware*. The cloudware provides various factions depending on the types of cloud services supplied. The function of cloudware include maintaining of up-to-date information of the available resources; create and manage virtual machines according to user’s request; application deployment, configuration and execution; and user management, pricing, and accounting [22]. To utilize computing resources effectively, some algorithms or policies are used to determine where to create a virtual machine and when to start and stop a VM based on the user's preferences. User management is important since enables determining of how user’s requests are charged and maintaining the actual usage of resources [18]. In cloud computing, users are shielded from complexity which makes it easy to
use and program. Management of a cloud is easy because most of the time there is only one administrative domain involved in it.

2.3. Cloud Data Center vs. Traditional Data Center

As shown in Fig. 2, traditional and cloud data center security landscapes differ in their characteristics. In both cases the customers submit their jobs for execution. The difference between traditional and cloud data center lies in what the hardware and software components are supposed to do and they are configured to do it.

In the traditional data center, each workload has its own level of security for its own infrastructure, and it is relatively easy to prevent such isolated infrastructures from interacting with each other. The physical infrastructure separates facilitates preventing interactions among networking, computing and storage components of different users [23].

<table>
<thead>
<tr>
<th>Traditional data center</th>
<th>Cloud data center</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiple supported applications and platforms</td>
<td>Few dedicated applications</td>
</tr>
<tr>
<td>Mixed hardware environment to support multiple applications and platforms</td>
<td>Have homogeneous hardware environment</td>
</tr>
<tr>
<td>Multiple supported management tools</td>
<td>Few standard management tools</td>
</tr>
<tr>
<td>Several application updates and patching</td>
<td>Minimal required updates and patching</td>
</tr>
<tr>
<td>High complexity of workloads</td>
<td>Simple workloads</td>
</tr>
<tr>
<td>Multiple supported software and hardware architecture</td>
<td>Single cloud architecture</td>
</tr>
</tbody>
</table>

Fig. 2. Traditional data center vs. cloud data center.

In contrast, cloud infrastructure does not have isolated approach since workloads running in the private cloud share the same infrastructure. All workloads use the same server infrastructure,
same storage infrastructure, and same networking infrastructure. Cloud infrastructure takes advantage of software constructs to create a logical isolation [24].

A cloud data center is considered a better option because it can give all functionality and services that a traditional data center, yet offers it with lower costs due to the economies of scale [24]. The former also provides better flexibility as it does not require building one’s own infrastructure from the ground up, and providing own maintenance and administration. The complexity of traditional data center increases slowly with increase in its storage facilities by purchasing them, while cloud data center is rapidly elastic and scalable as any user’s applications can be served at any time.

2.4. Essential Characteristics of Cloud Computing

Cloud computing is differentiated from other computing paradigms or model by its characteristics. These characteristics are categorized into essential characteristics and common characteristics. Gong et al. [25] enumerate the following five essential characteristics:

1) *On-demand self-service:* it enables the user to unilaterally provision computing capabilities as server time and network storage [26]. This is possible without the need for human interaction with each service provider. Computing resources are instantly available to users as per their requests.

2) *Broad network access:* It refers to the situation where the computing capabilities are available to users over the network. Users can access cloud resources through standard mechanisms that enable them to use heterogeneous platforms i.e. they can access cloud resources through mobile phones, laptops, and PCs [27]. Therefore, users don’t need to be at specific locations in order to access cloud-based services. Cloud-based services can be accessed from any location any time provided that there is adequate IP networking.
3) **Resource pooling:** Service providers pool together computing resources so as to satisfy computing needs of multiple users via different physical and virtual resources. The pooled resources (such as servers, storage devices, etc.) are shared across many users. Providers select which resources from the pool to assign to each cloud consumer’s workload to optimize the quality of service. Sharing facilitates cost reductions because it allows more applications to be served on the computing hardware of the cloud than would be required with dedicated computing resources.

4) **Rapid elasticity:** This refers to the rapid and elastic provision of computing capabilities to quickly scale out, and rapid release to quickly scale in. The capabilities that are provisioned to consumers are (from the user’s point of view) unlimited and can be purchased in any quantity at any time. Elastically increases service capacity during busy periods, and reduces capacity during customers’ off-peak periods, enabling cloud consumers to minimize costs while meeting their service quality expectations.

5) **Measured service:** This service automatically controls and optimizes resource use. It is done – at some level of abstraction appropriate to the type of CC service [26]. This characteristic enables monitoring, controlling and reporting of resource usage and thus enabling fair service purchases.

2.5. Delivery Models for Cloud Computing

Cloud computing delivery models includes three levels [28], as shown in Fig. 3: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software (application)-as-a-Service (SaaS).
2.5.1. Infrastructure as a Service (IaaS)

This CC capability provided to users involves provisioning computing resources and services such as processing, storage, networks, content delivery networks, backup and recovery, etc., on which users can deploy and run their own software [29]. As shown in Fig. 4, IaaS does not give consumers the authority to manage or control the underlying cloud infrastructure or the lower layers of OS but instead allows consumers to have full control over the higher levels of OS, deployed applications; and limited control of networking components, such as host firewalls [30].

Fig. 3. Cloud Computing Delivery Models.

Fig. 4. IaaS vs. PaaS vs. SaaS (Separation of Responsibilities). [31]
IaaS Characteristics: The characteristics of IaaS include [28, 29]

1) Multiple users on a single piece of hardware.

2) Resources available as a service.

3) Dynamic scaling capabilities – the cost varies based on the infrastructure selection.

IaaS Suitability: IaaS suitable for the following: [28, 29]

1) Organizations that need a complete control over their software, e.g., for high performing applications.

2) Startups and small companies that do not wish to spend money and time in procuring hardware and software.

3) Growing organizations not yet sure which applications they will need, or that expect to evolve in an unpredictable way, and hence do not want to commit to specific infrastructure.

4) Services that experience volatile demands – where highly dynamic scaling up or down in sync with traffic spikes or valleys—is critical.

IaaS Examples: Examples of IaaS include Amazon Web Services (AWS), Cisco Metapod, Microsoft Azure, Google Compute Engine (GCE).

2.5.2. Platform as a Service (PaaS)

PaaS gives consumers the ability to deploy onto a cloud infrastructure consumer-created or consumer-acquired applications, which were created using programming languages and tools supported by the CC provider. As shown in Fig. 4, consumers are not given the control or authority to manage their underlying cloud infrastructure, i.e., networks, servers, storage, applications, data etc [32]. However, they are given the authority over their deployed applications in an application hosting environment, which helps in running applications in a
quick transparent manner. PaaS services include a virtual desktop, web service delivery and
development platforms, database service etc., [30].

PaaS Characteristics: The characteristics of PaaS include: [32]

1) A virtualization technology build on top of PaaS enables acquiring resources on demand,
and scaling them up/down as needed.

2) Varying application development and application execution services to facilitate
development, testing, deployment and hosting of software applications in an integrated
development environment.

3) Sharing of the same development environment by multiple users.

4) Integrated web services and databases.

5) Billing and subscription managed by CC tools.

PaaS Suitability: PaaS is suitable for the following: [32]

1) Multiple developers working on the development of same product, or external parties
involved in the development process; PaaS brings in the speed and flexibility to the
development process.

2) Organizations following the Agile Methodology for software development; PaaS cease
the difficulties associated with rapid development and iterations of an application [32].

3) Organizations wishing to spread their capital investment; PaaS reduces the spending on
computing infrastructure as well as application development and execution.

Enterprise PaaS Examples: Examples of PaaS include Apprenda.
2.5.3. Software as a Service (SaaS)

With the SaaS delivery model, CC consumers are given the capability to use the CC provider’s applications running on the cloud infrastructure (in contrast to PaaS, where they run their own applications). In SaaS, the cloud users do not have control or authority to manage the underlying cloud infrastructure or even the individual applications [30]. As shown in Fig. 4, there are possibilities of that user will have limited access to configuring settings in related to applications. SaaS services include email and office productivity applications, customer relations management, enterprise resources planning, social networking, data management, etc. [30, 28].

SaaS Characteristics: The characteristics of SaaS include: [28, 29]

1) Software hosted on a remote server, and always accessible through a web browser over the Internet.

2) Application managed from a central location.

3) Application users do not need to worry about hardware or software (updates, patches, etc.)

4) Any integration with third party applications are done through APIs

SaaS Suitability: SaaS is suitable for the following: [28, 29]

1) Applications where the demands spike or fall significantly. For example, tax software is in a high demand during the tax filing season, hotel reservations see a spike during holiday seasons and so on [32].

2) Applications that require web as well as mobile access. Examples include sales management software, CRM systems.

3) Short term projects that require collaboration. The pay-as-you-go model makes it convenient to quickly set up a collaborative environment, and quickly close it down.
4) Start-up businesses that want to quickly launch e-commerce sites without worrying about server configurations and software updates.

SaaS Examples: Google Apps, Salesforce, Workday, Concur, Citrix GoToMeeting, Cisco WebEx.

2.6. Deployment Models of Cloud Computing

There are four deployment models of cloud computing: public, private, community and hybrid as shown in Fig. 5 [34]. Each of these models has different characteristics and implications for the customers [35].

The choice of the deployment model depends on an organization’s objectives and business needs. Before selecting a deployment model, an organization is encouraged to review the security, reliability and performance issues associated with the model.

![Deployment Models for Cloud Computing](image)

**Fig. 5. Deployment Models for Cloud Computing.**

2.6.1. Public Cloud

A *public cloud* is the most used deployment model, and what most people have in mind as “a cloud.” Cloud services are available to the general public and are managed by CC service providers. The providers own and manage their cloud infrastructures. A public cloud has multi-
tenant capabilities, and is shared by a large number of customers who have nothing or very little in common. Users’ data are not publicly visible [36].

The advantages of a public cloud include:

1) *Low Cost:* The nature of the public cloud is that you only pay for what you use. So as an organization grows or shrinks so do the associated costs. By comparison a private cloud might require an infrastructure designed to cope with growth (thus more expensive); likewise no costs saved if the needs shrinks. Other significant savings are related to costs associated with the size and work of the in-house IT team.

2) *Increased Efficiency:* As public clouds have dedicated teams working on maintaining the infrastructure, downtime is less likely to be an issue. On top of this if applications are hosted by CC provider, updates are usually managed by the provider, saving upgrading expenses.

The disadvantages of a public cloud include:

1) *Wrong Provider:* There are very real hazards of picking a wrong public cloud provider. If a provider does not keep hardware up to date, users may suffer compliance and execution speed issues.

2) *Reduced Control:* As the public cloud is controlled by a CC provider, users do not have as much control as in a private cloud.

3) *Perceived Weaker Security:* Security might be a downside to a public cloud, but, as is proven by the high level of public cloud adoption by some of the world’s biggest organizations, the security concerns are not valid if the public cloud is hosted by a CC provider aware of security issues, and their impact on customers’ perception [40].
2.6.2. Private Cloud

A *private cloud* is a dedication of computing infrastructure to a single specific organization or group without sharing with any other organization. Private cloud can be owned or leased. In a private cloud, there are no additional security regulations, legal requirements or bandwidth limitations [11]. However, the service providers and users have optimized the control of infrastructure and security. An organization may opt for private cloud when they feel they are unable to remotely host their data and hence, they seek the help of cloud to enhance their resource utilization and automation [21].

The advantages of private clouds include the following ones:

1) **Security**: The security is within the organization’s control. Although whilst many are quick to credit private clouds as being more secure [35], the vast array of different deployment types and levels of security within private hosting environments makes this an extremely bold statement [37]. The reality for me is that a private cloud is just as susceptible to security risks as a public cloud. The only difference is that a public cloud may be more attractive to infiltrate than a private cloud as there is a wider amount of data in it.

2) **Performance**: If a private cloud is deployed inside an organization's firewall it increases the performance compared to using the public cloud off premise.

3) **Control and Flexibility**: Organizations have more control in private clouds and as a result deploying new applications and make changes can be done in quick manner.

There are a few disadvantages for private clouds, including the following ones:
1) **Additional Maintenance:** If a private cloud is not maintained by the software vendor, then it is unlikely that the organization will benefit from the regular updates that are often associated with modern SaaS applications.

2) **Higher Costs:** Everything related to a private cloud is more expensive. Whether the organization has to purchase the infrastructure or it is still provided by the vendor, it will be more expensive than for public cloud. Also management costs are higher.

2.6.3. Community Cloud

A *community cloud* should not be confused with a public cloud. In community clouds, resources are available for a number of individuals or groups who have shared interests—in contrast to public cloud in which users do not have shared common interests.

The computing infrastructure can be either on- or off-site. Cloud resources are owned and managed by one or more of the collaborators in the community [38]—in contrast to a public cloud where resources are owned and managed by an individual provider/owner.

2.6.4. Hybrid Cloud

A *hybrid cloud* is a combination of more than one deployment model [39]. There is a management framework that ensures that the environments appear as a single cloud. Adoption of hybrid cloud may be resulted by strong requirements for security, price and performance.

2.7. Obstacles Preventing Adoption of Cloud Computing

Among the obstacles that may prevent or delay adoption of cloud computing [63, 36] by organizations are the following:
1) **Internal Resistance:** Cloud computing has the advantage of reducing the number of administration tasks that are carried out on back-end IT systems. Subsequently, it makes an organization’s staff to work more on the front-end applications. Therefore, it may result in a significant reduction in the size of the IT department staff [41]. Hence, specialists in IT departments in an organization may see cloud computing as a threat. Such individuals may be afraid of losing their jobs or their control of key systems.

2) **Security and Privacy Challenges:** The security and privacy issues associated with cloud computing are serious concerns for many organizations. From a glass-half-empty perspective, some organizations consider the security challenges as hurdles that cannot be removed neither is there an effective solution to address them. Such organizations do not consider the benefits of adopting the technology[3].

3) **Reliability and Trust:** Cloud outages experienced by its providers such as Google and Amazon are well documented and publicized. This has discouraged potential organizations who were thinking of moving into the cloud environment. Cloud computing is a trust-based technology where lack of trust inhibits its adoption [42].

4) **Integration and Interoperability:** The industry lacks standards for APIs and cloud interfaces, interoperability standards, and associated technical standards that allow interoperability of private to private clouds, public to private clouds, and so on [28].

5) **Governance, Service Level Agreement (SLA) and Quality of Service (QoS):** Appropriate end-to-end governance across IT and services lifecycle in cloud computing is absent [41].
2.8. Performance and Cost Factors

The benefits of cloud computing can be limited by the performance and cost factors, including the following:

1) **Security**: Security improves efficiency of any cloud system and provides better performance, which is an auxiliary element in protection of the system [43].

2) **Data Recovery**: Data stored or managed in a cloud may be subject to errors, failures or loss due to various reasons. The ability of and time required for data retrieval affects performance [44].

3) **Service Level Agreement**: Before consumers use cloud resources, they sign a service level agreement (SLA). The agreement describes a user’s request, capabilities of a provider, fines, fees, etc. [45].

4) **Network Bandwidth**: When the bandwidth is too low to provide needed services within the required time, the performance of the cloud will be low.

5) **Number of Users**: When the number of users exceeds the cloud capacity, the performance of cloud services suffers.

6) **Fault Tolerance**: This is the ability of clouds to provide services even when they are experiencing reliability or security problems. A high fault tolerance results in a better cloud performance [46].

7) **Other Factors**: Other factors that can affect cloud performance include problems with scalability, latency, redundancy, workload, and processor power.
Bauer et al. [26] recommend calculation of the total cost of ownership (TCO) for cloud services. TCO includes all costs of cloud services throughout their lifetime, from purchase to disposal. The cost of ownership of cloud services is categorized as either direct or indirect. *Direct costs* include the hardware and software licensing fees, utility costs associated with bandwidth and resources, and costs associated with service management. *Indirect costs* include costs of employing a personal involved in coordinating cloud and local applications, as well as negotiation and management of a cloud service contracts.
CHAPTER 3

SECURITY PROBLEMS IN CLOUD COMPUTING

Clouds can be flexible and cost-efficient. In a cloud infrastructure, sensitive information for a customer is kept on geographically dispersed cloud platforms, under direct control of the cloud—not of the customer. Securing users data in a cloud is one of the most challenging tasks. Cloud resources (such as software, platforms, and infrastructure) are vulnerable to abuse, theft, unlawful distribution, harm, or compromise. Among others, there is a risk that user’s information can be leaked to a competitor. Unauthorized access to data stored in clouds can be minimized through ensuring security.

3.1. Importance of Security in Cloud Computing

Despite the benefits that an organization enjoys after adopting cloud computing, there are security issues that are a notable barrier to adoption of the technology. After adopting CC, the crucial responsibility for data management and protection belongs to the service provider [30]. Waseem et al. [47] argue that loss and manipulation of data from unknown sources is prevented through providing secure computing environment, which is defined as a system implemented to control storage and use of data. Secure computing environment reduces the damage on physical computing device that may result from malware.

Cost of using cloud services is significantly reduced in a secure environment. Security enhances performance and reduces chances of damage to data, software and hardware [48].
### Table 1. Cloud Security Requirements vs. Cloud Services/Mechanisms [52].

<table>
<thead>
<tr>
<th>Cloud Security Requirements</th>
<th>Cloud Services/Mechanisms</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Authentication</td>
</tr>
<tr>
<td>API's</td>
<td>No</td>
</tr>
<tr>
<td>Cloud Software</td>
<td>Yes</td>
</tr>
<tr>
<td>Data Protection</td>
<td>Yes</td>
</tr>
<tr>
<td>Hardware Virtualization</td>
<td>No</td>
</tr>
<tr>
<td>Software Virtualization</td>
<td>No</td>
</tr>
<tr>
<td>Utility Computing</td>
<td>No</td>
</tr>
<tr>
<td>Virtualization</td>
<td>No</td>
</tr>
<tr>
<td>Web Portals</td>
<td>No</td>
</tr>
</tbody>
</table>

#### 3.2. Categories of Cloud Computing Security

A security model is needed in cloud computing to coordinate scalability and multi-tenancy with requirement for trust [49]. Since cloud computing involves pooling of resources so that multiple users can have access to them, data stored or managed in a cloud are likely to face security issues.

When organizations move to cloud environment with their identities, information and infrastructure, they must be willing to give up some level of control. The organization must trust its CC systems and providers, but still be able to verify cloud processes and events [47, 53]. The fundamentals of trust and verification are access control, data security, compliance and event management.

CC services and mechanisms include: authentication, authorization, data encryption, data privacy, and multi-tenancy. Table 1 shows relationships between cloud security requirements...
and cloud services and mechanisms. These requirements are mandatory to achieve integrity and coherence in cloud systems.

Categories of CC security, shown in Fig. 6, include: identity, information, infrastructure, network, and software security [51]. We discuss them in turn.

![Fig. 6. Categories of Cloud Computing Security.](image)

Identity Security: It is defined as the security and business discipline that “enables the right individuals to access the right resources at the right times and for the right reasons” [53]. It ensures the integrity and confidentiality of data and applications while increasing their accessibility to appropriate users. End-to-end identity management, third authentication services and identity are key elements of identity security in cloud. Management in identity security possess capabilities that should be made available to both users and infrastructure components in cloud computing [54].

The identities of users should be managed in a manner that builds and trust. Identity security requires strong authentication and strong authorization.

As identity security in cloud computing requires authentication, it should be more than just username and password. Identity security may require the adoption of standard IT that including
strong authentication, coordination within and between enterprises, and risk-based
authentication, behavior monitoring, current issues and other issues that enables assessment of
risk level of a user request [55]. The authentication capabilities should be constant throughout
the lifecycle of the cloud infrastructure and data. Stronger authorization capabilities are required
in cloud computing especially when handling sensitive data and compliance requirements.

Information Security: It is defined as “a set of strategies for managing the processes, tools and
policies necessary to prevent, detect, document and counter threats to digital and non-digital
information.” Information security responsibilities include establishing a set of business
processes that will protect information assets regardless of how the information is formatted or
whether it is in transit, is being processed or is at rest in storage [56]. The controls on physical
access, access to hardware and software and identity controls are targeted towards protection of
data. The protective barrier in cloud that ensures security of information is diffused.

Data in a cloud needs their own security, including data isolation to protect data in public
cloud. Varying degrees of isolation of data can be achieved through virtualization, encryption
and access control. This ensures protection of data from unauthorized individuals [57]. It is
necessary when it comes to multi-tenancy cloud environment, which can have multiple
customers or users who does not see or share each other's data but can share resource or
application in an execution environment, even if they do not belong to the same organization.

Trusted Computing technologies are used in building trust in multi-tenant infrastructure and
are extended to support virtualization [58]. Virtualization is used in cloud computing to test and
report on the integrity of a particular virtual machine [59]. Various principles used in improving
information security in cloud infrastructure through virtualization and computing include:
reduced trusted computing base; separate management components; separation of policy
enforcement from application space; and separation of policy enforcement from application space. Complex and numerous code components are likely to be subject to having bugs that create vulnerabilities; hence, there is a requirement to reduce the size of the trusted code: with simpler code and fewer lines of code, fewer bugs will appear [60].

Infrastructure Security: Demonstrating that a virtual and physical infrastructure of a cloud can be trusted is a challenge. The attestation of a trusted third party (TTP) is not sufficient for critical business processes. It is absolutely essential for an organization to be able to verify business requirements that the underlying infrastructure is secure.

In trusted infrastructure, software maintaining separation and managing critical system components and policies should be minimized. The minimum set of services needed to support virtual machines management should be determined [61]. The remaining management stack is removed into other virtual machines that are not associated with the trusted computing base [29]. The security of the infrastructure should be assured in such a way that a penetration by an attacker does not enable him to access all systems of the organization.

There also is a need to keep components separate [62]. Separation of management components enables network drivers to prevent easy access to storage drivers or cryptographic keys. Separation of policy enforcement from the application space makes it possible to create containers within which applications can run and control the nature of the container—through setting of policies within the infrastructure. Containers are created with capabilities that are not controlled by running application software [63]. Separation of audit space from the application space protects audit records from tampering. Attestation to communicate trust in a system enables creation of confidence that the system is trustworthy [64].
Network Security: Network Security is a basic requirement for cloud computing. It involves taking physical and software preventative measures “to protect the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure, thereby creating a secure platform for computers, users and programs to perform their permitted critical functions within a secure environment [68].”

Network level issues can directly affect the cloud system basically affecting the bandwidth and increasing the congestion in the system. In mobile platforms many cloud users use smartphones for accessing the SaaS cloud applications and services. The mobile device sometimes not only produce harmful malware but also vulnerabilities [69]. There are many obstacles arise during the design of cloud network security. For example, a TCP connection table hold all TCP connections is handled by the firewall. Suppose that a VM is outside of the firewall and accessed by an external customer. If the VM is migrating to another place in the cloud, it changes the routing path of the firewall security. In this case a malware can spread from one network to another in multi-tenant clouds [69]. Table 2 indicates some studies with network security solutions.

Table 2. A Summary of Network Security Problems and Solutions.

<table>
<thead>
<tr>
<th>Security Topics</th>
<th>Security Problems</th>
<th>Studies/Surveys</th>
<th>Security Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>VMM network sniffing and spoofing</td>
<td>Prolexic (2015)</td>
<td>Authentication based on key exchange in a network, Kumari et al. (2014)</td>
</tr>
<tr>
<td>Mobile Platforms</td>
<td>Generation of mobile malware</td>
<td>Cisco (2015a)</td>
<td>No solutions identified</td>
</tr>
<tr>
<td></td>
<td>Extension of mobile vulnerabilities</td>
<td>HP (2015), Li and Clark (2013)</td>
<td>Intrusion detection system to protect mobile platforms, Yazji et al. (2014)</td>
</tr>
<tr>
<td></td>
<td>Cloud syncing mobile application vulnerabilities</td>
<td>Gripos et al. (2013)</td>
<td>No solutions identified</td>
</tr>
</tbody>
</table>
Table 3. A Summary of Software Security Problems and Solutions.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Uncertain system calls and imperfect memory isolation</td>
<td>Al Morsy et al. (2010)</td>
<td>No solutions Identified</td>
</tr>
<tr>
<td></td>
<td>Bad SDLC mechanism</td>
<td>Martin (2013)</td>
<td>No solutions Identified</td>
</tr>
<tr>
<td>User Front-End</td>
<td>Exposure of front-end interfaces</td>
<td>Ahuji and Komathukattil (2012)</td>
<td>No solutions Identified</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Grobauer et al. (2011)</td>
<td>Lightweight intrusion detection, Amadian et al. (2011)</td>
</tr>
<tr>
<td></td>
<td>Imperfect configurations , Unauthorized access application drawbacks, masked code injection.</td>
<td>Grobauer et al. (2011)</td>
<td>Lightweight intrusion detection, Amadian et al. (2011)</td>
</tr>
<tr>
<td></td>
<td>VMM management console exposure</td>
<td>Wu et al. (2010)</td>
<td>No solutions identified</td>
</tr>
</tbody>
</table>

**Software Security.** While there is a broad range of software development efforts in terms of scope and difficulty, all of them require assurances of security. Since there is no such concept as a *guaranteed* full security, the goals are to create secure software with security carefully designed into it, not an after-thought add-on capability. In this way, it is possible to build software with a high degree of protection against attacks [65].

Security considerations for software should begin with the idea for the software, and carry through the design and implementation phases, to form a cycle of security analysis. Each of these phases depends on the other to provide the highest level of software security [66]. Table 3 indicates some studies with software security solutions.
Developers should follow a procedure for secure software development that includes creation of a secure architecture with proper monitoring and isolation, and the ability to examine design and implementation for relevant security issues [33]. Application development teams must produce record intelligent log streams. Traditionally, these logs are used for troubleshooting and debugging, but an external system might be necessary to combine several log events to produce a security event. A better log stream includes more security-relevant details on traditional events and those produced by embedding security controls [67].

Fig. 7. Security-only, Privacy-only, and Intertwined Security and Privacy Problems in CC.

3.3. Problems: Vulnerabilities, Threats and Attacks

Cloud computing presents various risks to an organization that have adopted it. Cloud security issues are determined greatly by the cloud service delivery model and deployment model. High-
security levels can be more easily achieved in private clouds than in public clouds [40]. Other top security problems in cloud computing include insecure interfaces and APIs, malicious insiders, shared technology issues, account or service hijacking, and unknown risk profiles. The following subsections discuss some of the security problems (VTAs) in cloud computing; they are also shown in Fig. 7.

3.3.1. Buffer Overflow Attacks

A buffer overflow is the condition when the data sent to the buffer is beyond its capacity [80]. When a program runs, the system allocates a section of the adjacent area of memory to store various types of data; this memory space is called a buffer. With a lack of validation of data written into a buffer, buffer overflow can occur: an excess data overflows the buffer and overwrites the adjacent memory. The data that overflows to adjacent memory makes the system more vulnerable to subsequent attacks since it allows attackers to deploy more sophisticated programs that cause bigger damage. Successfully exploited buffer overflow vulnerability can modify the value of a variable in memory, or even hijack the process, execute malicious code, ultimately leading to a full control of the host [81].

The simplest and most common form of the buffer overflow attack combines an injection technique with an activation record corruption. The attacker locates an “overflowable” variable, then feeds the program a large string that simultaneously overflows the buffer (in order to change the activation record) and contains the injected attack code [82].

Attackers use code specifically designed to cause buffer overflows [83]. Buffer overflow is among the worst bug attacks on a cloud since it is difficult to detect and fix. Early detection and
intervention are recommended to ensure that a minimal or no damage is caused by a buffer overflow [84].

3.3.2. Cloud Authentication Attacks

Authentication is a process that ensures and confirms correctness and validity of a user’s credentials (an essential property that is selected for a given authentication process).¹ Authentication begins when a user tries to access information. First, the user must prove his access rights and possessing the required essential property selected for the given authentication process [86]. In a cloud environment a user tries to establish a connection with cloud services using his own credentials that authenticate him in order to allow him access to cloud services [87].

![Cloud Authentication Threats and Attacks](image)

Fig. 8. Cloud Authentication Threats and Attacks.

Threats and attacks on authentication in cloud environment, shown in Fig. 8, include:

1) **Brute Force Attacks**: An attacker guesses the credentials of a user.

¹ Note that authentication must not be confused with identification, which is just one of many user’s properties that can be used in authentication. For example, credit card authentication verifies that a customer has sufficient funds her credit card account (these are the credentials in this case). It does not matter who is the customer, so her identity is totally irrelevant for this authentication.
2) **Cookie Replay Attacks:** An attacker gains access to a user’s system through the reuse of a stolen cookie to a session, which contain important confidential information.

3) **Credential Theft:** An attacker exploits the system and gain access/credentials through data theft, e.g., via phishing.

4) **Dictionary Attacks:** An attacker guesses credentials through trying in turn different terms from the dictionary.

5) **Network Eavesdropping:** An attacker steals credentials by reading network traffic.

As the browser cannot generate cryptographically valid XML tokens to authenticate a user before accessing cloud services, a protocol involving a trusted third party (TTP) is used. A prototype for such protocols is Microsoft’s Passport [88]. The browser may not have the essential credentials, making direct login at the server impossible. A Passport login server receives an HTTP via redirection, allowing users to enter their credentials, such as username or password. Later, the Passport server translates the credentials into a Kerberos token, which is sent to the requesting server via another HTTP redirection. The main security issue with Passport is that the tokens are not bound to the browser. In case of an exploit, the cracker accesses not only the token but also all victim’s services.

MS Cardspace is a Microsoft initiative to replace user IDs and passwords with a digital or virtual identity. It serves as an example of a solution against attacks on cloud authentication services [89].

### 3.3.3. Cloud Malware Injection Attacks

Cloud malware injection attacks aim to inject malicious virtual machine (IaaS) or service implementation (PaaS or SaaS) into the CC system. These attacks can result in eavesdropping
through subtle data modification, full functionality changes, blockings, and so on [50]. To achieve this, crackers create their malicious service implementation modules or virtual machines, and add them into the CC system [90]. Then, the crackers trick the system to treat the malicious services or VMs as valid ones for the victim. When the attack succeeds, the CC system automatically redirects the requests of valid users to the rogue system, allowing the adversary code to be executed [83, 11].

3.3.4. DOS Attacks and Mobile Terminal Security

DOS attacks and mobile terminal security level attacks are quite common.

DOS Attacks: Denial-of-Service (DOS) and distributed denial of service (DDOS) are among the major security threats in cloud computing [162]. A DOS attacks occur when an intruder attempts to deny authorized users access to information and cloud services [73]. A DDOS attack involves the use of multiple corrupted systems to target and corrupt a certain cloud in order to induce DOS attacks [74, 75].

DDoS attacks on an application layer can take advantage of inefficiencies in a web application. They are often difficult or impossible to detect at the network layer, so many upstream protection measures may be unable to help, forcing a website operator to rely on a combination of cloud-based or proxy-based solutions, as well as best practices in application design and management of its supporting architecture (including HTTPD, MySQL server, etc.). This requires making the right choices when deciding which software to use, its configuration, and the design of one’s own software. For instance, an application which makes resource-intensive calls to a MySQL server is easily attacked by DOS creating relatively low volumes of transactions intended to stall the SQL server from operating normally. This is an example of a
case when an attacker can identify a flaw or inefficiency in a web application and use for a DOS attack that is not easily detected at the network layer [76].

DOS and DDOS attacks can be addressed through an efficient DDOS detection and prevention technique based on a Third Party Auditor (TPA) [73].

Mobile Terminal Security and DOS: These problems originated with cell phone users. Waseem et al. [47] identified that these users are usually uninformed about security and confidentiality matters. The authors believe that mobile phone customers often fail to use their devices appropriately, exposing themselves to crackers (malicious hackers).

Attackers may use such lax security to mount DOS attacks preventing users from accessing their cloud services. Meanwhile, the user’s CC provider will be striving to deal with the attack using substantial CC resources, further increasing probability that the cloud services continue being unavailable to customers. Eventually, the crackers can simply erase, manipulate, or misplace private information stored by cloud users [47].

3.3.5. Insecure API’s

Insecure Application Programming Interfaces (APIs) are among the vital security issues in cloud computing. APIs are very likely to be one of the main targets for cyber criminals attempting to breach a company’s network [8], since they act as the public front door to any applications, and by default must be accessed externally. Crackers take advantage of insufficient authentication, authorization, and encryption [45].

APIs are used by cloud providers and software developers to allow their customers to interact, extract, and manage data from cloud services. APIS can be used in at least three ways. First, they can be used to collect logs from an application. Second, they can be used to facilitate integration
with database as well as storage components. Third, they can be used to control particular cloud resources. Furthermore, APIs are the main channels through which mobile applications interact with websites or back end services [85]. Additionally, they facilitate authentication of users.

In a recent incident involving APIs, a system of an online vendor, Moonpig, was breached through a mobile app, using static authentication, and enabled crackers to collect customer information by sequentially trying all customer identities [12].

In addition to APIs, other code-related vulnerabilities (not discussed here) include poor coding methodologies and releasing inadequately hardened code.

3.3.6. Malicious Insiders

A malicious insider can be a current or former employee, contractor or business partner authorized to access network, system or data, who uses his privileges for malicious purposes [70]. In particular, network firewalls and intrusion detection systems can miss activities of an insider, considering them to be authorized. In CC, malicious insiders with access to cloud resources can cause considerably more damage than in a traditional single-organization data, mainly because an insider’s attack in CC can affect a large number of cloud customers (not just the attacker’s own organization). Malicious insiders can significantly affect service offerings, such as access to confidential data, and gain control of cloud services without being detected [49].

Brand damage, monetary impact, and productivity losses are just some of the ways a malicious insider can affect operations of the attacked organizations. According to Khorshed et al. [48], malicious insiders are favored by the absence of transparency in cloud providers’ processes and procedures. As organizations adopt cloud services, the human element takes on an even more profound importance. It is critical therefore that the consumers of cloud services
understand what providers are doing to detect and defend against the malicious insider threat [71]. The threat can be addressed through limiting access of cloud services and data; increasing transparency in security and management processes including compliance reporting and notification in moments of breach [72].

There are two categories of insider threats:

1) *Insider Threats in the Cloud Provider*: In this case, an insider is working for the cloud provider. He/she can cause great deal of damage to both the provider and its customers. There exist controls to reduce impacts of attacks by malicious insiders; they are divided into client-side and provider-side countermeasures. The client-side solutions include confidentiality and availability countermeasures, while the provider-side countermeasures include malicious insider detection models, logging and legal binding.

2) *Insider Threats in the Cloud Outsourcer*: In this case, an insider is an employee of an organization which has outsourced part or whole of its infrastructure on the cloud. Let’s consider an insider who is an administrator. There are few elementary differences between a rogue administrator at the cloud provider and a rogue administrator within the customer organization; both have root access to systems and data, and both may employ similar types of attacks to steal information. Again, there exist controls to reduce impacts of attacks by malicious insiders; they are divided into client-side and provider-side countermeasures. The client-side solutions include Intrusion Detection Systems (IDS), which monitor networks or systems for malicious activity or policy violations. The provider-side controls include multi-factor authentication.
3.3.7. SQL Injection Attacks

An SQL injection attack occurs when a malicious user injects a vulnerable code into a cloud, with the aim of corrupting CC processes [77]. Using SQL code vulnerabilities, attackers can gain unauthorized access to data in the cloud [78], including retrieval or falsification of confidential and sensitive information from the database.

To showcase an example of an SQL injection attack, suppose that we have a web page that receives an integer variable as news id and shows the related news item to that id:

http://www.domain.com/news.php?nid=170. Attacker appends the “OR ‘1’= ‘1’” to the end of the URL: http://www.domain.com/news.php?nid=170 OR ‘1’= ’1’. As a result of opening this address, the PHP web page will return all the news. This is because the “1=1” is a logical tautology and “OR” will make the whole condition a tautology, no matter which statement is true.

In an SQL injection attack, an attacker might also create an entirely new malicious SQL query to perform an unauthorized database operation. It may jeopardize the confidentiality and security of Web sites that depend on databases. An appropriate “code re-engineering” done for a PHP application by its developer can protect the application from SQL injection attacks. Protection of cloud resources from SQL attack may also require having a mechanism for detection and identification of specific SQL injection attack.

Web intrusion detection systems (IDS) can be used to differentiate legitimate events and activities occurring in the cloud from the illegitimate ones. IDS detects harmful codes with low false alarm rate and high detection rate [79].
Privacy is a crucial issue in cloud computing because a customer’s information and business logic must be entrusted to cloud servers owned and maintained not by the customer but by cloud providers [94, 44].

4.1. Importance of Privacy and Confidentiality in Clouds

Apart from the cost effectiveness of cloud computing, another property that, when guaranteed, could increase the use of cloud services is protecting privacy of users’ data. In other words, customers’ conviction that a CC provider assures privacy of their data increases their trust into CC services, and leads to a growth in use of these services.

Confidentiality vs. Privacy: The terms confidentiality and privacy are closely linked; they are too often used inappropriately, also incorrectly considered synonyms [29]. Confidentiality can be defined in terms of protection of personal information or control over personal information. Hence, it involves two parties: one party has the responsibility for protecting access to the information of the other party [92]. In other words, one party trusts that the other party will protect its sensitive or private data, preventing their disclosure against the wishes of the data owner. Therefore, confidentiality entails extrinsic forces that protect information from being accessed by unauthorized individuals while privacy (as defined in Introduction) involves only intrinsic and selective control over openness of an individual’s information [9].

Assuring Confidentiality: The most critical aspect of privacy is assuring their confidentiality, which prevents malicious users from stealing information that may lead to significant problems
in their lives [93]. Reports about breaches of confidentiality discourage users from using clouds services that require storing or managing their sensitive information, or using cloud services [94].

Both cloud providers and users benefit from ensuring confidentiality. Providers benefits through increased revenues resulting from a growth in use of their services when they guarantee non-disclosure of users’ information. Privacy of a user’s information ensures requires specifying which data can be shared with which entities (users, applications, systems, etc.)

That is, protecting privacy ensures that cloud users have the right information disclosed to the right entities. Among many questions that need to be addressed in order to determine the risks to information privacy in clouds are the following ones:

1) Who are the stakeholders involved in a given operation on data?
2) What are their roles and responsibilities?
3) Where are data kept?
4) How are data replicated?

4.2. Cloud Computing Privacy Overview

Since cloud computing involves multi-tenancy and sharing of information, there are higher risks of violation of privacy and confidentiality.

When users put their data into a public cloud, they no longer have control over confidentiality of these data. This demonstrates that cloud computing is not ideal for confidentiality considering that some organizations prefer to develop their own services and keep their data private.

As workloads are migrated to shared infrastructures, users’ private information face elevated risk of unauthorized access and exposure. Organizations have expressed their discomfort to store their data and applications on systems residing outside their on-premises data centers [95]. This
may expose sensitive individual and corporate information, affecting both legal and regulatory requirements of the data being stored or transported [97]. Also privacy-protection organizations voice their doubts. For instance, the World Privacy Forum executive director expressed concerns about the transfer of large city records to a CC service provider [96].

Privacy and Confidentiality in Clouds: Users store, access and manipulate important data in clouds, some of which are sensitive and should not only be accessed by any other person. Users of cloud resources are also expected to have control over the accessibility of their information or activities [98]. Access of individuals’ information or records without their authorization is considered breach of privacy and unethical.

The issues of privacy of individuals’ data in clouds arises when they share it with others are when they are accessed by the provider for unauthorized use [8]. Confidentiality issues result when the provider does not address the loopholes for information leakage or when they share their customers’ information with others without authorization of the user. The risks of privacy and confidentiality are influenced by the terms of service and privacy policies implemented by the service providers [99].
There are some situations when the privacy and confidentiality rights, obligations and states of information and users may change if the user discloses their information to a provider [100]. Remote storage and disclosure of information determines consequences of the legal status and protection of the information stored or accessed through the Internet. Mokbel et al. [93] argue that the location of information in the cloud is also a determinant of privacy and confidentiality issues and the privacy obligations of those who handle the information. However, the privacy and confidentiality of the information in the cloud can be breached if the law demands the cloud provider to provide information regarding a particular user. Subhashini et al. [30] state that a provider has the responsibility of developing and implementing strategies that ensures that their customers’ information is not leaked to other individuals or organization with or without their knowledge. The users also have the responsibility of safeguarding their privacy through
controlling their behaviors and activities in the cloud that are likely to increase the risks of privacy breaches [101].

4.3. Problems: Vulnerabilities, Threats and Attacks

Privacy is certainly one of the issues where the personal information is exploited and the following are some of the vulnerabilities, threats and attacks, also shown in Fig. 9.

4.3.1. Broken Authentication and Compromised Credentials

*Broken authentication* refers to the situation where there is an inadequate mechanism for validation of user certificates (as a special case, a certificate could assure a user’ identity). Breach of privacy for various users of cloud services may result when the providers cannot confirm that access to data in the cloud is performed by legitimate users [117, 118].

Authentication and access control are effective only in uncompromised computing systems. Ineffectiveness or absence of security controls in CC environments is among the causes of compromised credentials [119]. It is the role of providers to ensure that there is an efficient authentication system to ascertain authenticity of customers’ credentials.

4.3.2. Data Breaches

A *data breach* is the situation where sensitive or protected data of cloud users is viewed, stolen or used by an unauthorized individual [102]. Data breaches cause a significant impact on the users, cloud services providers and government agency [103, 104].

Data breaches may lead to permanent data loss. The main security concern in cloud computing relates to data breaches in cloud platforms, which entails both data and computation integrity. Clifton et al. [105] maintain that *data integrity* entails honest storage of user information on cloud servers. In that case, any data breach, such as data loss or compromise,
must be detected. Meanwhile, *computation integrity* entails the execution of programs without any form of distortion. However, user data remains vulnerable to distortions associated with malicious users, cloud providers, and malware, which require instantaneous detection.

In cloud computing, applications offer storage as a service. Apparently, servers store large amounts of information that can be accessed on exceptional occasions. Behl et al. [97] demonstrate that cloud servers are distributed based on security and reliability. That means that user data may be distorted or edited accidentally or maliciously. According to Ateniese et al. [106] administration errors during backup and restore, migration of data, and modification of memberships in P2P systems may also lead to data loss.

Furthermore, adversaries may launch crucial attacks by taking advantage of the loss of control by the data owner over their own systems and data [107]. Meanwhile, with outsourced computation, judging whether the computation is implemented with top-notch integrity may be difficult. Considering that computation details are never transparent enough to the cloud user, cloud servers may act unfaithfully and present misleading computing results; that is, they may fail to adhere to the semi-honest model [108]. For instance, some computations require a large substantial amount of computing resources, which present incentives for the system to be “lazy.” Even when the semi-honest model is followed, issues may arise with outdated cloud servers, vulnerable codes, misconfigured services or policies, or previously breached systems with rootkits [96].

The impacts of data breaches on a victimized organization include loss of revenue, unbudgeted costs incurred during responding to the act, credibility issues, and loss of public and customer confidence. Data breaches may be as a result of intentional theft of data, negligence and accident, improper use of Internet or improper disposal of data [102]. The security and
privacy measures that providers use to protect users’ data may also contribute to breaches of data. Unauthorized individuals may easily access cloud users when the cloud infrastructure lacks effective confidentiality measures that help in monitoring their systems, quickly identifying breaches, and blocking them [109].

4.3.3. Data Location Problems

*Data location* is one of the most common compliance issues that an organization faces after adopting cloud computing. In an in-house computing system, an organization structures its computing environment and therefore, the location of data stored and the measures put in place to protect the data [110]. However, in cloud computing, an organization’s data is stored redundantly in multiple physical locations and no detailed information about the location of the data is given to the organization [111]. Therefore, it is difficult to ascertain whether adequate measures have been put in place to protect the data. Furthermore, the service consumers cannot be sure whether legal or regulatory requirements have been met by the providers [100]. Enterprises should necessitate that the cloud computing provider store and process data in specific jurisdictions and should follow the privacy rules of those Jurisdictions.

Data may be stored across the borders of a country, which raises additional technical and legal concerns. The legal, privacy and regulatory systems vary in different countries. In the US, sensitive data about a service consumer may be availed to the legal authorities without their authorizations in case there are suspected criminal activities [112, 113]. Most of the European countries have placed regulations that ensure relatively more protection of consumers’ data. Trans-border transit of sensitive data as well as the protection measures implemented to safeguard the data is a national and regional security and privacy concern [114]. The laws in the jurisdiction of the location the data was collected may permit or deny the trans-border flow of
data. There have been issues concerning whether the laws where data was collected still applies after data have crossed the border. The destination of the data may present security risks or benefits to the data [115].

4.3.4. Problems Related to Data Ownership and Content Disclosure

Another crucial privacy matter emerging from cloud computing is the problem of data ownership. As users put their data on a cloud service, the privacy of the data could be lost. Besides, the users are at risk of losing ownership authority over their data as well as the right of disclosure by push away ownership to the cloud service providers [116]. Despite the lawful ownership, along with the right of disclosure being at the disposal of the original data owner [34], owner’s right might be violated. For instance, some cloud providers, as data custodians, retain the right of disclosure, while others do not.

When a CC service provider contractually becomes the data owners as well as the data custodian, a privacy issue emerges. Even with outmoded IT services, the best practice is to separate duties, in which a different entity owns the data while another remains the chief custodian of that data [72]. Even so, with cloud computing, that paradigm has shifted, making the service provider the owner and custodian of all information stored or transmitted through their cloud. Such practices violate the core principles of duties separation and job rotation, which are crucial doctrines in best practices for data security [105].

4.3.5. Virtualization Problems

Virtualization was introduced to facilitate sharing of huge expensive resources among different application environments. This enables an organization to interact with their IT
resources in a more efficient way and allows for a much greater utilization. Virtualization technologies rapidly became a standard technology used in IT organizations [5].

Virtualization of resources is achieved with the help of a hypervisor, which allows a dynamic allocation of resources to virtual machines (VMs). Cryptography is used in virtual systems of a cloud to secure data in transit from private premises to the cloud, but data must be decrypted in memory. This creates a loophole through which privacy breaches may occur since virtualization enhances almost transparently the memory pages of an instance, enabling obtaining if data by a malicious provider [34]. Table 4 lists some of the virtualization problems and their solutions.

Table 4. A Summary of Virtualization Security Problems and Solutions.

<table>
<thead>
<tr>
<th>Security Topics</th>
<th>Security Problems</th>
<th>Studies/Survey</th>
<th>Security Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware</td>
<td>Virtual devices software exposure</td>
<td>Pfaff et al. (2009)</td>
<td>No solutions identified</td>
</tr>
<tr>
<td>VM mobility</td>
<td>Tsai et al. (2011)</td>
<td>Improved migration protocol based on trusted channel, Wan et al. (2012)</td>
<td></td>
</tr>
<tr>
<td>VM rollback</td>
<td>Basak et al. (2010)</td>
<td>No solutions identified</td>
<td></td>
</tr>
<tr>
<td>Mobility</td>
<td>Packet sniffing and spoofing</td>
<td>Al Morsy et al. (2010)</td>
<td>No solutions identified</td>
</tr>
<tr>
<td>Network Virtualization</td>
<td>Two fold traffic, limited network access, Inapplicability of standard security mechanisms.</td>
<td>Grobauer et al. (2011)</td>
<td>No solutions identified</td>
</tr>
<tr>
<td>VMs Image Management</td>
<td>VMs theft and malicious code injection overlooked image repository</td>
<td>Wei et al. (2009)</td>
<td>A VM image management system, Wei et al. (2009)</td>
</tr>
<tr>
<td>Virtual Machine Sprawl</td>
<td>Luo et al. (2011)</td>
<td>No solutions identified</td>
<td></td>
</tr>
</tbody>
</table>

49
CHAPTER 5

INTERTWINED SECURITY AND PRIVACY PROBLEMS IN CLOUD COMPUTING

Although there are so many security-only and privacy-only problems, there are also occurrences where security and privacy are intertwined.

5.1 Problems: Vulnerabilities, Threats and Attacks

There are various intertwined security and privacy problems, as shown in Fig. 10. They are discussed in the following sections.
5.1.1. Compromised Shared Platforms

One of the key features of cloud computing is scalability of its infrastructure that enables support for multiple tenants, who share the infrastructure. Hypervisors run many virtual machines (VMs) running applications. Also some applications run directly on the CC hardware.

Hypervisors can be exploited from a virtual machine to gain access all virtual machines on the same server [85, 61]. An attacker may target SaaS to get access to data of another application running in the same VM. Share platform makes CC vulnerable since attacks can be initiated from any layer [124].

5.1.2. Natural Disasters

Natural disasters are predictable or sudden events that leave damages on structures on the landscape and even lives. They are inevitable events but their impact on cloud computing must be reduced. Natural disasters often break electricity lines and thus stop operation of CC devices, denying users their access to CC services [26, 28].

5.1.3. Permanent Data Loss

Data loss is among the serious threats in cloud computing since it has impacts of higher magnitude to both cloud users and providers [120]. Data breaches may result in a permanent data loss when malicious attackers gain access to the data and delete them. They may use sophisticated techniques and programs that prevent restoration of the data.

Cloud users may also delete their data accidentally. This may be enhanced by their uneducated behaviors or inadequate information on how to use cloud services and resources [121]. Cloud service providers may be the cause of data loss when they accidentally delete cloud
data. Finally, damage to cloud infrastructure by natural disasters (discussed next) may lead to permanent data loss [104].

5.1.4. Virtual Machine Migration Attack

VM migration is an administrative tool used for load balancing, disaster recovery, server consolidation, hardware management, etc. [61]. The process of VM migration is characterized by lack of standard access control, manual authentication, confidentiality issues, non-repudiation and integrity of VM data [125]. Managing VM migration adds another level of complexity to the security process especially when the VM is migrated to an insecure environment.

At the start of a VM migration, request for migration is made followed by identification of a target physical host and negotiation with the target host. Their steps are carried out by respective VMs.

VM migration should be secured, among others to ensure that no leakage of information about the process [61]. Lack of authentication and accountability may lead to an adversary easily exploiting the migration to gain control over the VMs and interrupt CC services [70,72]. An attacker may direct a VM to a specific host machine or compromise a VM through broadcasting of false resource information. When attackers have control of the host system where they have directed the VM, they easily gain control over the VM and use it on the Internet to infect other hosts and VMs [91]. Attackers can also cause unplanned migration of VMs leading to interruption of cloud services. VMs can be manipulated by attackers to obtain knowledge about the cloud infrastructure. The attackers can access data, manipulated, delete, steal or used them without authorization [126].

52
Table 5. Other Intertwined Security and Privacy Problems with Implementation Challenges [50].

<table>
<thead>
<tr>
<th>Problems</th>
<th>Implementation Challenges for Resolving Issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account, Service and Traffic</td>
<td>• Rapid development of cloud computing also opens some new loopholes</td>
</tr>
<tr>
<td>Hijacking</td>
<td>• Present way of digital identity management is not good enough for hybrid clouds</td>
</tr>
<tr>
<td>Data Loss/Leakage</td>
<td>• Trust issue with cloud providers that they may become self-interested and store in low-security area than agreed</td>
</tr>
<tr>
<td></td>
<td>• Untested procedures, poor policy and inadequate data retention practices.</td>
</tr>
<tr>
<td></td>
<td>• Lack of knowledge</td>
</tr>
<tr>
<td>Insecure Application</td>
<td>• The inability to audit events associated with API use</td>
</tr>
<tr>
<td>Programming Interfaces</td>
<td>• Incomplete log data to enable reconstruction of management activity</td>
</tr>
<tr>
<td>Malicious Insiders</td>
<td>• Providers try to hide their own company policies for recruiting employees</td>
</tr>
<tr>
<td></td>
<td>• Solution come into effect after the incident occurs, which is too late</td>
</tr>
<tr>
<td></td>
<td>• Cloud provider’s inability of monitoring its employees</td>
</tr>
<tr>
<td>Shared Technology Vulnerabilities</td>
<td>• Shared elements not designed for strong compartmentalization</td>
</tr>
<tr>
<td></td>
<td>• Business competitors using separate virtual machines on the same physical hardware</td>
</tr>
<tr>
<td></td>
<td>• Coexistence of manufacturing and retail sector</td>
</tr>
<tr>
<td></td>
<td>• Uses of vulnerable OS image for cloning can spread to many systems</td>
</tr>
<tr>
<td>Unknown Risk Profile</td>
<td>• Cloud providers unwillingness to provide log and audit data; and security practices</td>
</tr>
<tr>
<td></td>
<td>• Lack of transparency</td>
</tr>
</tbody>
</table>

5.2. Other Intertwined Security and Privacy Problems

Other intertwined security and privacy problems experienced in cloud computing include account or service hijacking, phishing, fraud, and hijacking of user accounts or services [127]. Attackers may manipulate information in user accounts, and direct the cloud users to insecure environment. Insufficient due diligence is another challenge; it is associated with a lack of information for users on the full capacity of cloud. When users lack knowledge of the cloud environment and security mechanisms available in the cloud, they are likely unable to respond effectively to suspicious processes. Table 5 lists some of the other intertwined security and privacy problems in clouds, indicating their implementation challenges [50].
Cloud users need to know the behaviors that increase their vulnerabilities to attackers [128]. Cloud users use various software interfaces and APIs to access services [129]. Some organization and third parties develop interfaces to facilitate value-added services for their users without considering the increased risk of attacks that the additional interfaces bring [41].

5.3. Case Studies of Intertwined Security and Privacy Problems

This subsection discusses a few case studies where security and privacy problems are intertwined.

5.3.1. Case Study 2: Account Hijacking

In July 2012, the CEO of CloudFare suffered account hijacking using stolen credentials after close monitoring of his online activities. UGNazi, a cracker group, performed the account hijacking. The cracker exploited a major flaw in the Google’s Gmail password recovery system and AT&T voicemail system. AT&T system redirected the victim’s cell phone to a fraudulent voicemail box due to malfunctions caused by the cracker. Confusion was created between Google’s account recovery processes making the victim unable to verify that he is the legitimate owner of the account. This gave the attacker the opportunity to gain access into the victim’s Gmail account and add his email address as the recovery email address. On the other hand, the victim was unable to reset his Gmail account password. The victim no longer accessed his account. The hijacking was facilitated by the two-factor authentication setup allowed by the Google account recovery process which denied the victim his administrative privileges. Such account security issue was addressed by removing the two-factor recovery system [43, 125].
5.3.2. Case Study 1: Network-based Attack

A technical writer Mat Honan was a victim of network-based attack in August 2012. In the event, his social life was completely destroyed following the deletion of important information from his computing devices including iPad, MacBook, and iPod. The attack identified a loophole in the authentication systems used by amazon and Apple. The victim’s details were online and even his @me.com address which the attacker used. The attacker compromised the credentials of Honan and used it change the logins. Due to the weak authorization and verification systems of Amazon and Apple, the attacker managed to change the credit card linked to the Amazon account as well as the email address [108]. After changing the @me.com address of the victim, the attacker erased all the information from Honan’s Apple iCloud account from the iPad, MacBook and iPod [130].
There are various measures and controls to secure the cloud in terms of security and privacy, some shown in Fig. 11.

6.1. Controls Against Hardware-based Attacks

The first line of defense against hardware-based attacks ensures high level of physical security of data centers. However, in case of malicious conduct of the provider administrators, they are high chances of violation of customer confidentiality and integrity through bypassing of physical
security mechanisms. To prevent side-channel attacks, changes can be made to the cipher algorithm phases which cause modifications to cache and memory patterns. Side-channel attacks may lead to loss of information.

Cryptography is one of the controls against hardware-based attacks; others include access control and authentication processes [93]. The common cryptography techniques include identity-based cryptography and hierarchical identity-based cryptography (HIDC). Yan et al. [96] describe identity-based cryptography (IBC) is a public key technology that enables the use of a public identifier of a user as the user’s public key. HIDC is an advancement of IDC since it was developed to solve the problem of scalability associated with IDE. In order to achieve effective authentication and access control in the cloud environment through federated identity management and HIDC, each cloud user and server has its own unique identity which is allocated by the system hierarchically [95, 97]. HIDE is composed of five algorithms; root setup, lower-level setup, extraction, encryption and decryption. With the unique identity and hierarchical identity-based cryptography (HIBC), key distribution, authentication and access control is more secure [94].

Some security controls used to address the problem of hardware-based attacks [91] are as follows:

1) Partitioning cache and using partition-locked cache (PLC): Cache partitioning involves allocation of part of cache exclusively to a protected process to avoid leakage of information. PLC enables isolation of cache lines containing critical data only and causes less performance degradation.

2) Cryptography
3) Turning off Cache S-Box access
4) Avoiding lookup tables
5) Inserting dummy operation
6) Performing cache warming.

6.2. Controls against Hypervisor-based Attacks

Some of the mechanisms against hardware-based attacks are also effective in ensuring hypervisor protection. Hardware-assisted Virtualization (HaV) is an efficient technology that offers security of hypervisor [126]. HaV prevents security threats to hypervisor integrity and enhance isolation in system hardware resources. Through HaV, hardware physical memory virtualization is possible; memory addresses are translated from guest virtual to guest physical and then to system physical [28].

The technology also provides secure Input Output Memory Management Unit (IOMMU) that allows virtual machines directly access peripheral devices. Therefore, attacks from malicious devices may compromise the integrity of hypervisor are avoided. Software-based security techniques protect virtual machines where tenants reside on top of virtual machine migration. These techniques protect virtual machines from inside (OS level) or from outside (hypervisor level). The security of VMware’s hypervisor can be achieved through: memory isolation, device isolation and network isolation[5].

6.3. Controls via Cloud Auditing

For security, auditing aims to evaluate the policies, operations, practices, and technical controls of a company and assess compliance, detection, fortification, and security forensics.
Indeed, regular security audits are essential, and thus, should focus both on reactive audits when incidents occur and on proactive audits conducted so as to assess the adequacy and practicality of security controls, processes, procedures, and operations in protecting crucial assets of a client.

Fathy et al. [108] highlight two crucial concern for a security audit in CC a matter of concern. First, cloud service providers ought to make their security audit procedures transparent to their customers [44]. Second, the magnitude of security coverage being used must comply with legal, regulatory, and certification demands while considering a bunch of diverse and wide-ranging information assets, which the cloud service provider oversees. Table 6 categorizes some of the cloud specific auditing challenges.

Table 6. Cloud-specific Auditing Challenges [131].

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Cloud Security Auditing Practice</th>
<th>Cloud-specific Challenge</th>
<th>Potential Cloud Security Auditing Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Colocation</td>
<td>This rarely occurs</td>
<td>CSPs heavily depend on this.</td>
<td>Standardize and increase oversight, Ryoo et al. (2014)</td>
</tr>
<tr>
<td>Encryption</td>
<td>The data owner has control</td>
<td>Cloud service providers might be responsible for encryption.</td>
<td>Use a third party and homomorphic encryption, Ryoo et al. (2014)</td>
</tr>
<tr>
<td>Scale, scope and complexity</td>
<td>These are relatively less</td>
<td>Auditors must be knowledgeable and aware of these differences</td>
<td>Implement continuous education and new certification programs, Ryoo et al. (2014)</td>
</tr>
<tr>
<td>Transparency</td>
<td>Data and information security management systems are more accessible</td>
<td>Data and their security are managed by third parties</td>
<td>Service Level Agreements (SLA) should outline Content Security Policies (CSP) and assurances while CSPs provide client with audit results, Ryoo et al. (2014)</td>
</tr>
</tbody>
</table>

Auditing security requirements within a cloud environment can be a significantly challenging endeavor. In an attempt to resolve this issue, cloud service providers strive to espouse transparency when managing information security [95]. They strive to enhance trust and
relationship with their customers by making those clients, both individual and corporate, abreast with the provider’s audit processes as well as the varying magnitudes of audit coverage.

When it comes to auditing policies, operations, practices, and technical controls, major challenges arise with the cloud providers who ought to make their security audit procedures transparent, while the amount of data they oversee is bountiful. Since cyber crimes and fraudulent activities take place on digital devices, forensic teams might find it difficult to access cloud data that is admissible before the court of law. Table 6 identifies some of the cloud-specific auditing controls.

6.4. Controls via Effective Encryption

To enhance security protection, advanced encryption algorithms can be applied to CC. They include: (1) attribute-based encryption algorithm, (2) fully homomorphic encryption, and (3) symmetric encryption.

Attribute-Based Encryption (ABE) comprises of either cipher text-policy ABE or key policy ABE [120]. In CP-ABE, the encryptor has the responsibility to control the access strategy. As the strategy increases in complexity, the design of the public key system becomes more intricate, proving the security of the system more difficult [57, 132]. In Key Policy Attribute Based Encryption (KP-ABE), the attribute sets are used to explicate the encrypted texts as well as the private keys with the itemized encrypted texts that a user leaves behind to decrypt [116].

Using Fully Homomorphic Encryption (FHE) in cloud computing allows direct computations on encrypted data. Unfortunately, practical use of this method is limited only to very simple processing of data, specifically ones limited to adding and multiplying numbers [47].
Symmetric Encryption (SE) entails a cryptographic primitive facilitating secure search functions over data that is encrypted. To enhance the search efficacy, an SE solution establishes keyword indexes to perform user queries securely [94].

These encryption methods can be enhanced with active bundles [120] to provide better protection for data [132].
Private and sensitive data are vulnerable to hacking by malicious attackers especially in public clouds. Furthermore, when individuals and corporate cloud users put their data in the hands of their cloud providers, it remains unclear who has the authority to own and maintain custody of such information.

The lack of trust into public clouds is exemplified by government entities that resolved to keep their information secret by developing their own clouds. Dangerously, some cloud users, especially mobile users, are barely aware of the matters of privacy of their personal data.
Attackers have taken advantage of that ignorance falsifying users’ data, stealing them, or denying many cloud users access to their personal information.

Various solutions are proposed. First, adopting a user-centric identity management, SSO and two-factor authentication can play a vital role in ensuring the secure and safe data transfer. One way to achieve efficiency for these measures is by adopting zero-knowledge proof-based methods. Some of the various measures and controls taken to protect cloud users’ privacy are discussed below (cf. Fig. 12).

7.1. Controls for Authentication and Identity

Stakeholders within a cloud environment have a significant role to play to mitigate the issues related to security and privacy. While cloud computing offers individuals and corporate entities with an environment in which they can store their information, that data is susceptible to breaches such as manipulation and dishonest computation within the remote servers [63]. This compromises data integrity.

In addition, insecure APIs provide opportunities for crackers due to insufficient authentication, authorization, and encryption. Authentication issues also promote attacks, such as DoS, ID Spoofing, packet dropping, and Man-In-The-Middle (MITM) attack.

User-Centric Identity Management (IdM): Handling private data as well as critical identity attributes received considerable attention [96]. In user-centric identity management identifiers and attributes are used to assist in identifying and defining cloud users. This approach allows both individual and corporate users to control their digital identities. It also eliminates the IdM complexities from the cloud provider, permitting them to concentrate on service delivery [163].

Considering that users have access to cloud services from different locations, it is important that they are able to export and securely transfer their digital identities to various digital devices.
Furthermore, user-centric IdM implies that the cloud system can properly sustain the semantics of the users’ identity information context, occasionally constraining or relaxing them to preeminently respond to the requests presented by the users in particular situations.

Currently, researchers continue to pursue the possibility of developing additional federated IdM solutions that are beneficial to the clouding environment [104]. According to Kumari et al. [94], IdM services in cloud computing must be to be integrated a company’s existing IdM framework. In other instances, the authors’ advice the need to establish privacy-preserving protocols for verifying various identity attributes, for instance, by using zero-knowledge proof-based methods. These techniques use pseudonyms besides accommodating multiple identities to protect the privacy of users, thereby establishing preferred user-centric federated IdM for cloud services [117]. Active data bundles are proposed for protecting sensitive data and IdM in clouds [160, 162, 163].

Accountability: An accountable system is capable of detecting misuse and exposing the responsible entity for a given activity [98]. The cloud system should generate undeniable evidence of the entity’s wrong activity and the innocent part should also be able to defend themselves against any false accusation. In order to achieve an accountable cloud computing system, some proposals have been made in various research studies; identity binding, tamper-evident logs, and execution verification. In identity binding, each action is signed with the private key of action originator. This enables identification of malicious insiders and reduction of the security and privacy issues

SAML: Cloud services (such as Google, Salesforce, Office365, Box, Concur, Jive, etc.) support Security Assertion Markup Language (SAML) which allows various applications to securely pass information about the user's identity. This process of authentication allows a
various cloud vendors to provide services tailored to a particular user without having to ask for their username and password. Also provides a mechanism to integrate with "legacy" cloud services that do not support Federated Identity technologies and require passwords for authentication.

It is a XML-based secure communication mechanism for communicating identities between organizations [134]. The key thing about SAML is that it enables Internet SSO. SAML eliminates the need to maintain multiple authentication credentials such as passwords in multiple locations. It is important for three reasons:

1. It increases the security by eliminating additional credentials which eliminates opportunities for identity theft.

2. It eliminates phishing opportunities by eliminating the number of times a user needs to log in over the Internet using one of those username login forms and in fact recently a major SaaS application was subjected to phishing attack.

3. It increases application access by eliminating barriers to usage so user no longer have to type in a password to basically click on a link there in the application.

4. It eliminates administration time and costs by eliminating those duplicate credentials and also by eliminating all those extra help desk calls to reset those lost passwords.

Single Sign On: A Web access management (WebAM)/Web Single Sign-On (WebSSO) system is middleware used to manage authentication and authorization of users accessing one or more web-enabled applications. A WebSSO system intercepts initial contact by the user's web browser to a web application and either verifies that the user had already been authenticated (typically tracking authentication state in a cookie) or else redirects the user to an authentication page,
where the user may use a password, token, PKI certificate or other method to authenticate himself [135].

Once a user is authenticated, the WebAM component of the system controls the user's access to application functions and data. This is done either by filtering what content the user can access (e.g., URL filtering) and by exposing an API that the application can use to make run-time decisions about whether to display certain forms, fields or data elements to the user [136]. WebSSO/WebAM products typically use an LDAP directory as a back-end repository, to identify all users. They often come tightly integrated with an "identity and access management" application, which enables delegation and in some cases self-service administration of the contents of that single directory.

Examples of SSO include Google account help in logging into multiple applications, such as Gmail, Google Drive, or YouTube [135].

Fig. 13. Signing in to Amazon Console with User ID.
Two Factor Authentication: Two Factor Authentication (TFA or 2FA), shown in Fig. 13, 14, and 15 is a simplest form of multi-factor authentication that requires not only a password and username but also another “token” that only the appropriate user knows or has, e.g., a piece of information that only this user knows or a physical token that only this user has [137]. 2FA makes it harder for potential intruders to bypass or cheat the authentication subsystem. Using a Two Factor Authentication process can help to lower the number of cases of identity theft on the Internet, as well as phishing via email, because the criminal would need more than just the users name and password details.

The downside to this security process is that new hardware tokens (in the form of key fobs or card readers) need to be ordered, then issued and this can cause slowdowns and problems for a company's customers wanting and waiting to gain access to their own private data via this
authentication procedure. The tokens are also usually small and easily lost so causing more problems for everyone when customers call in requesting new ones [137].

A 2FA authentication mechanism (if implemented with one token that is physical in nature) requires a physical attack against the user to in order to steal the security device that is associated with the mechanism. This device could be a mobile phone, one-time password calculator, PKI smart card etc.

This requirement for a physical attack changes the game considerably. For one, phishing attacks from remote countries aimed at trawling for login IDs and passwords are rendered useless. Also, the probability that a user recognizes that he is being attacked approaches 100%.

7.2. Controls for Trust Management

In cloud environments, different service domains determined by services requirements interact. Such interaction can be dynamic, intensive, or transient. As such, a trust framework remains indispensable to facilitate efficient capturing of different parameters required to establish not only establish trust, but also manage changing trust and interaction requirements [42]. What is more, Hassan et al. [50] noted that cloud users’ behavior is changing rapidly, subsequently affecting the already established trust values. This element brings up the need to develop an interoperation that is integrated, trust-based, and secure to create, negotiate, and sustain trust.

Multiple cloud service providers both co-exist in cloud environments and collaborate to deliver different services. However, each entity might have adopted unique security approaches and privacy mechanisms, which triggers the need to address the issue of heterogeneity within their entity [138]. For that reason, deliberated mechanisms can ensure that this dynamic
collaboration is managed in a secure manner so that all security breaches are collectively monitored. Numerous research results demonstrate that while individual domain entities are corroborated, security breaches can still occur during integration. That means cloud service providers have the responsibility to prudently manage access control policies to eliminate the possibility of security breaches.

To promote policy integration between the various domains within the cloud environment, cloud services providers must develop a good reliant trust-based management framework. However, to achieve that, the enterprises must consider several factors. First, they must be able to establish proper credibility among themselves, as well as with their customers, and determine access as that trust evolves. The current mechanisms for trust negotiations focus particularly on the exchange of credentials [50]. What is more, they barely address the highly challenging requirements for integration that drive trust. That means cloud users further, must not be ignorant about and merely trust their service providers simply because they took part in a written-down service offering. Customers must be open-minded and carry out proper due diligence on the enterprise and identify where certain policies are ambiguous. With the assistance of law enforcement agencies and cloud services regulators, cloud users can ensure that omitted policies are included within the service contracts [95]. Both cloud users and providers must understand the various trust boundaries. That way, each cloud computing model will assist the customers and enterprises in decision-making when it comes to selecting the right model to adopt or deploy [74].

For instance, a great trusting relationship can be created when users are able to backup their data and are assured that that information cannot be accessed by unauthorized entities. This is vital especially in the public cloud, which, as open clouds maintained by a vendor for virtually
everyone, thrive the existence of potential crackers [90]. Nevertheless, a trusting relationship is further established when the vendors of public cloud make it possible for the users to create and configure supplementary and customized access controls so as to protect their data. More so, a trusting relationship between users, vendors, and forensic teams, backed up by policy, will ensure security and privacy issues are minimized [62].
CHAPTER 8

INTERTWINED SECURITY AND PRIVACY CONTROLS FOR CLOUD COMPUTING

There are various measures and controls which are taken to secure the cloud in terms of security and privacy and to prevent from various issues. They are shown in Fig. 16 and discussed here.

Fig. 16. Security-only, Privacy-only, and Intertwined Security and Privacy Controls in CC.

8.1. Controls Against Network-based Attacks

In order to enable secure connection of between one virtual machine to another, providers need to protect the traffic inside their cloud infrastructure and the traffic coming from the outside. Coppolino et al. [139] outline techniques such as firewalls, intrusion detection systems, anti-virus gateway, monitoring incoming and outgoing traffic that are commonly used by organizations and providers. They argue that the countermeasures should ensure system
availability, data confidentiality and data integrity at channel and system’s application level. To ensure system availability, cloud providers must defend their cloud environment before, during and after the DOS and DDOS attacks. Defense can be inherent to the system design (always on), or might require activation, which is preceded by DOS attack detection [161].

Flooding attacks occurs when all requests to a particular service need to be individually checked for validity and thus cause service overloading. Overloading may result to direct or indirect DoS attacks and discrepancies associated with accountability. Despite remedying flooding attacks may not be easy, research studies are suggesting a more feasible alternative. The intervention seeks to group different servers into fleets, each of which is designated for a unique type of job. Structuring of the available hardware enables the provider to impose an isolation that prevents an overload of useless requests from affecting the performance of the computational fleet. This intervention a limitation; when servers are overloaded with a large number valid jobs, offloading some of its tasks to other fleets that may have several used nodes available is close to impossible [108].

**Filtration.** Filtration is a common prevention technique against DDOS and can be applied close to the destination, in the routers or close to the source. Filtration techniques include ingress filtering, router based packet filtering and *confidence-based filtering (CBF)* [92]. Dou W. et al. [92] study on CBF shows that the technique has a high scoring speed, a small storage requirement, and higher filtering accuracy. Unlike traditional methods, CBF is easy to implement, and beneficial due to its high efficiency. It meets the real-time filtering requirements in the cloud environment [140]. CBF can be deployed both during non-attack periods and attack period. During the non-attack periods, legitimate packets are collected to extract attribute pairs for generating nominal profile.
Moving Target DDOS Defense Mechanism: A moving target DDOS defense mechanism protects authenticated cloud users from DDOS attacks [141]. The mechanism uses hidden proxies to relay traffic between cloud users and servers. Authenticated cloud users are segregated from malicious insiders and other attackers through a series of proxy shuffles [142]. The mechanism uses a group of dynamic hidden proxies to relay traffic between the authorized cloud users and servers. During the relay of traffic, attack proxies are continuously replaced with backup proxies (shuffling the attacked users onto new proxies). Through this legitimate cloud users are separated from potential attackers, especially malicious insiders [143]. There is a greedy algorithm that increases insider segregation and quarantine capabilities [144]. The algorithm also enables estimates of the resources needed by a CC to prevent DDOS attacks.

There are a few goals satisfied by the Moving Target Defense (MTD) [134, 135]:

1) Defeating targeted attacks using dynamic IP addresses in the huge range of IPv6 addresses.
2) Eliminating packet loss because of address collision.
3) Verification by each node that its new IP is free (avoid address collision); a mechanism is needed to inform correspondent nodes of this verified new IP address (a binding update mechanism).
4) Avoiding adding new requirements like time synchronization.
5) Adding capability of having dynamic address rotation interval.
6) Avoiding sharing IP updates with a correspondent node known as an attacker.
7) Avoiding using permanently accessible home agents because permanent home addresses are only accessible through home agents.
Strategies against Data Breaches and Data Loss: Encryption is one of the common techniques to prevent unauthorized individuals from accessing, using and interfering with data of cloud users. Despite the fact that encrypted network protocol ensures encryption of all traffics from the source to the destination to prevent sniffing and spoofing, this method is not effective [105, 84]. Proxy re-encryption is an improvement of encryption and is more effective in maintaining confidentiality and privacy of data in the cloud. A proxy re-encryption scheme is an asymmetric encryption scheme that allows a proxy to transform ciphertexts under a public key into ciphertexts encrypted under another public key [136, 137]. Cloud users provides a re-encryption key to the proxy that makes the transformation process possible without interacting with the underlying plaintexts and private key [147]. The proxy re-encryption scheme defines the encryption and decryption functions, and the function for executing the transformation. Re-encryption of encrypted data in the cloud facilitates secure sharing within the cloud network. Through the re-encryption proxy scheme, stored ciphertexts can be transformed in such a way that only authorize individuals can decrypt in. even the network servers cannot read the data [142]. This protects the data from data breach and permanent loss.

Re-encryption scheme can be improve through various techniques in order to increase data security and confidentiality. Two of the re-encryption techniques include attribute-based encryption and proxy re-encryption, time-based proxy re-encryption, and conditional proxy re-encryption (CPRE) [148]. According to the study conducted by Liu et al. [132], fine-grained access control on encrypted data and scalable user revocation can be achieved through combining attribute-based encryption (ABE) and proxy re-encryption (PRE). The combination of ABE and PRE requires that the cloud users to be online in order to send PRE keys to providers in a timely manner in order to avoid access future data by revoked users [147]. Time-based proxy
re-encryption technique is more effective since it is characterized by expiry of user’s access rights after the defined period of time. Time-based proxy re-encryption combines three elements; time, Attribute-based Encryption (ABE) and Private Key Encryption (PKE). Data has an attribute-base access structure and access time, and even user is defined by a set of attributes and eligible duration denoting the access rights [149].

Other techniques to ensure confidentiality and integrity of data include:

1) Key management-generation, exchange, storage use and replacement if keys
2) Data tokenization
3) Data backup and replication
4) Monitoring data integrity
5) Authentication and authorization techniques

8.2. Controls against Delivery Model Threats

There are various intertwined security and privacy problems affecting cloud delivery models (IaaS, PaaS, and SaaS). Controls for these problems require, among others, strong end-to-end encryption, and a trust management scheme.

Each delivery model (IaaS, PaaS, and SaaS) requires authorization in a public cloud to prohibit unauthorized accesses. Integrity is also an essential requirement—for checking data correctness. The high availability and integrity of the services requires strong security mechanisms in the underlying network. Table 7 provides further insights for cloud problems for delivery models and their solutions.
Table 7. Cloud Problems for Delivery Models and their Solutions (cf. [69]).

<table>
<thead>
<tr>
<th>Problem</th>
<th>Effects</th>
<th>Affected Cloud Services</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abusive use of cloud computing</td>
<td>Loss of validation, service fraud, stronger attack due to unidentified sign-up</td>
<td>PaaS, IaaS</td>
<td>Observe the network status, provide robust registration and authentication technique, Ashish et al. (2017)</td>
</tr>
<tr>
<td>Data Loss and Leakage</td>
<td>Personal sensitive data can be deleted, destructed, corrupted or modified</td>
<td>PaaS, SaaS, IaaS</td>
<td>Audit configuration and vulnerability, for administrative task use strong authentication and access control mechanisms, Wang et al. (2010) Provide data storage and mechanisms, Ryoo et al. (2014)</td>
</tr>
<tr>
<td>Different service delivery/receiving model</td>
<td>Loss of control over the infrastructure of the cloud</td>
<td>PaaS, SaaS, IaaS</td>
<td>Offered services under the control and monitored, Subhashini et al. (2011)</td>
</tr>
<tr>
<td>Insecure Interface and API</td>
<td>Improper authentication and authorization, wrong transmission of the content</td>
<td>PaaS, SaaS, IaaS</td>
<td>Observe the network status, provide robust registration and authentication technique, Wang et al. (2010)</td>
</tr>
<tr>
<td>Malicious Insiders</td>
<td>Penetrate organizations resources, damage assets, loss of productivity, affect an operation</td>
<td>PaaS, SaaS, IaaS</td>
<td>Data transmission is in encrypted form, strong access control and authentication mechanism, Ashish et al. (2017)</td>
</tr>
<tr>
<td>Service/Account Hijacking</td>
<td>Stolen user account credentials, access the critical data of the cloud, allowing the attacker to compromise the security of the services</td>
<td>PaaS, SaaS, IaaS</td>
<td>Adoption of strong authentication, Banyal et al. (2013)</td>
</tr>
<tr>
<td>Shared Technology Issues</td>
<td>Interfere one user services to other user services by compromising hypervisor</td>
<td>IaaS</td>
<td>Use agreement reporting and breach notifications, security, and management process is transparent, Phua (2009)</td>
</tr>
</tbody>
</table>

8.3. Controls via Computer Forensics

Computer forensics entails identifying, extracting, maintaining, and presenting digital facts piled in digital devices that are legally admissible in court following a cyber crime or fraudulent activity [153]. For one thing, digital information is extremely fragile since it can be manipulated, duplicated, destroyed, and so on. During investigations, it must be guaranteed that such data has not undergone any type of modification whatsoever.
Various forensic challenges exist when it comes to cloud computing environment. First, investigations in cloud computing vary according to the cloud model. For instance, in SaaS and PaaS service models, forensic teams can obtain instant access to the compromised system’s log history; that is not the case in IaaS [153]. The second problem is physical device accessibility. Forensic teams can only access physical devices in private cloud models. In public clouds, access may be limited in accordance with the investigation team’s requirements. The third problem lies with the cloud service provider. According to Sindhu et al. [154], the success of forensic investigation depends on the cooperation the provider, who may legally, contractually, or intentionally decline to provide the investigation team with physical and logical access to trace crime, fraud, or forgery. The fourth issue is that the cloud of the entity under investigation or the provider’s cloud may be compromised. Chen et al.[6], found that client information can be compromised through social engineering techniques such as malicious Java Scripts and other browser extensions. When court admissible data is breached, forensic procedures are subsequently affected. Similarly, when the cloud service provider’s site is disrupted, because of insufficient physical and logical security policies, the work of investigation teams will be futile.

Computer forensics in clouds follows the standard workflow to improve efficiency in investigation standards [155]; its steps are:

1) Determine the purpose of the forensics requirement.

2) Identify the types of cloud services (PaaS, IaaS, and SaaS).

3) Determine the type of background technology used:

   a) Client side: determine the role of user on client side; collect activities performed on client side through live forensics tools.
b) Server side: communicate with Cloud Service Provider for preservation of evidence; collect logs from Cloud Service Provider; collect full evidence from Cloud Service Provider.

c) Developer side: collect full evidence from developer; identify the tools used for upload of data; determine time consistency with Cloud Service Provider.

Forensics in CC follows a number of frameworks and guidelines for better investigation. According to Martini et al. [156], an iterative framework is essential and can be used to identify the existence of cloud storage and to recover data. The cloud framework is shown in Fig. 17 [156].

![Fig. 17. Cloud Forensics Process (cf. [156]).](image)

The computer forensics process can be as described follows:
1) **Evidence Source Identification and Preservation:** This phase is concerned with identifying sources of evidence in a digital forensics investigation. During the first iteration, sources of evidence identified will likely be a physical device (e.g. desktop computers, laptops and mobile devices). During the second iteration, this phase is concerned with identifying cloud services/providers relevant to the case, possible evidence stored with the cloud provider and processes for preservation of this potential evidence. Regardless of the identified source of evidence, forensic investigators need to ensure the proper preservation of the evidence [156].

2) **Collection:** This phase is concerned with the actual capture of the data. Timely preservation of forensic data is critical and due to the complications of cloud computing data collection (e.g. significant potential for the cloud service to be hosted overseas and the potential for technical measures such as data striping to complicate collection), collection is separated from preservation. The collection may first involve the seizure of a client device, with the collection of the server data occurring on the second iteration [157].

3) **Examination and Analysis:** This phase is concerned with the examination and analysis of forensic data. It is during this phase that cloud computing usage would most likely be discovered based upon the examination and analysis of physical devices and this would lead to a second (or more) iteration(s) of the process [157].

4) **Reporting and Presentation:** This phase is concerned with legal presentation of the evidence collected. This phase remains very similar to the frameworks of McKemmish et al. [157] and NIST [104] . In general, the report should include information on all
processes, the tools and applications used and any limitations to prevent false conclusions from being reached.

8.4. Risk Assessment Controls

The possibilities and frequency of occurrence of security and privacy issues can be determined through risk assessment [150]. Risk assessment is important in cloud computing since it facilitates prediction and early intervention to prevent or reduce impact of challenges. The security and privacy for a service is mainly provided by the CC service provider no matter what service type the user selects. Therefore it becomes very important to assess the risk of service provider.

The desktop assessment analyzes only the service plan and reviews the historical incidents, while ignoring the assessment of the platform providing the cloud services. The risk assessment of a cloud provider often includes three dimensions: assets, threats, and vulnerabilities [151]. In the simplest way, risk can be determined as: \( \text{Risk} = \text{NrAssets} \times \text{NrVulnerabilities} \times \text{NrThreats} \) [152].

Risk assessment consists of the following steps [127]:

1) Identification of assets in the cloud environment.

2) Review of the technical, legal and business requirements relevant for the identified assets.

3) Valuation of the identified assets while taking account of the identified technical, legal and business requirement and impacts of loss of confidentiality and trust, integrity, privacy and availability.

4) Determination of potential threats and vulnerabilities for the identified assets.

5) Assessing the likelihood of occurrence of the threats and vulnerabilities.
6) Calculation of the risks and comparison with a predefined risk scale.

After completion of risk assessment, the organization should develop appropriate interventions for the potential security and privacy threats.
CHAPTER 9

CONCLUDING REMARKS

Cloud computing (CC) is a paradigm of computing that offers many valuable services to the end users, including processing, storage, and data management. However, it brings many security and privacy issues that need to be addressed.

9.1. Contributions

In this Thesis, we discuss the major aspects of security and privacy in CC.

We introduce categorization of security and privacy issues into security-only issues, privacy-only issues, and intertwined security and privacy issues. This separation of issues has proven useful, resulting in a better organization of this survey.

Next, we divide security and privacy issues into problems and solutions. In turn, problems include vulnerabilities, threats and attacks (VTAs).

The main contributions of the thesis are twofold: first, using the above categorization of the issues (security-only, privacy-only, and intertwined); and second, the literature review of the security and privacy problems and solutions within this categorization framework.

9.2. Lessons Learned

Cloud computing is emerging as a big and beneficial technology of present day and future. CC provides the benefit of quick deployment, cost efficiency, large storage space and easy access to the system anytime and anywhere. Much of work is being put in it and one can expect more progress in CC technology.
After completing this Thesis, it is even more obvious to us now that security and privacy play a decisive role for customers, as one of the most important factors affecting adoption of cloud computing by them. All users should be well aware of vulnerabilities, threats and attacks possible in the cloud. The awareness of security and privacy problems will help users to properly evaluate pros and cons of relying on cloud services. Until proper (for a given customer) security and privacy solutions become available, some customers will be reluctant to entrust their data and processing to cloud computing systems.

We have significantly deepened our understanding of numerous security and privacy problems (vulnerabilities, threats, and attacks), which we studied after categorizing them as security-only problems, privacy-only problems, and intertwined privacy and security problems. We identified and studied many new controls for these problems, analogously categorized as security-only controls, privacy-only controls, and intertwined privacy and security controls.

In addition, the sheer number of references to trust (in both problems and solutions), demonstrated a significant role of trust in CC, and a need for more security and privacy solutions based on trust in an explicit way [158]. We believe now that—based on the advancement of cloud computing and increasing number of cloud users—the body of knowledge on security, privacy and trust in cloud computing will continue to grow fast.

9.3. Future Work

The CIA triad was mentioned above as the classic definition of security, or, being more precise, the classic definition of security services. However, there are more security services that are essential. Seven of them are provided as the standard set of security services [158, 159] by
International Standards Organization (ISO). Similarly, privacy can be defined via a set of privacy services [159].

In the future, after identifying privacy services (analogously to the ISO’s seven security services), all security and privacy issues (problems and solutions) could be categorized via a two-level classification. At the top level we would still have the presented categorization into three classes: security-only, privacy-only, and intertwined. On the second level, we would further categorize each top-level class into service-oriented subclasses. This means, that the security-only class would be divided into (seven) security-service-based subclasses, the privacy-only class would be divided into privacy-service-based subclasses, and the intertwined-security-and-privacy class would be divided into intertwined-security-and-privacy-service-based subclasses. Prof. Lilien's Research Team at WMU is pursuing this matter.
REFERENCES


2012.


[90] O.L. Barakat *et al.*, “Malware analysis performance enhancement using cloud computing,” *J.*


[122] W. Dawoud, I. Takouna, and C. Meinel, “Infrastructure as a service security: Challenges and


