Uppsala University
Department of informatics and media

Cloud Computing Security: A Systematic Literature Review

Anton Backe
Hugo Lindén

UPPSALA
UNIVERSITET

Course: Degree project
Level: C
Term: VT-15
Date: 2015-05-25
Supervisors: Franck Tétard, Ross Tsagalidis

ACKNOWLEDGEMENTS

First and foremost we would like to thank our supervisor Franck Tétard for his suggestions and support provided throughout the process of writing this review. We would also like to thank our external supervisor, Ross Tsagalidis, at the Swedish Armed Forces, for his suggestions regarding improvements of the review. Lastly we would like to thank the Swedish Armed Forces for allowing us to collaborate with them in the creation of this review.

Abstract

This literature review seeks to identify the major security issues and their solutions in cloud computing security as well as identifying areas for future research. Utilising a modified version of the approach suggested by Okoli and Schabram (2010) 52 articles were considered for the review, of which 26 were included in the final product. Although many security issues and solutions were identified it has become apparent that much of the research being done only relates to the theoretical side. Thus this review shows that while plenty of issues have been identified future research should focus more on the practical implications of these security risks.

Keywords:

Systematic literature review, Cloud computing, Security, Virtualization, Virtual Machine, Cloud service provider

Sammanfattning

Denna litteraturundersökning identifierar de huvudsakliga säkerhetsbristerna och de lösningar som åtfinns inom litteraturen om datormolnsäkerhet. Undersökningen använder sig av en modifierad version av metoden för litteraturundersökningar som skrivits av Okoli och Schabram (2010). Efter en första litteratursökning identifierades 52 artiklar som relevanta för undersökningen, av dessa 52 användes 26 i slutprodukten. Trots att flera olika säkerhetsbrister och lösningar för dessa identifierades var det uppenbart att mycket av forskningen enbart har teoretiska svar på bristerna. Undersökningen visar således att även om många hot har upptäckts av forskare saknas det forskning av de praktiska konsekvenserna av dessa brister.

Nyckelord:

Systematisk litteraturundersökning, Datormoln, Säkerhet, Virtualisering, Virtuella maskiner, Molntjänstleverantör

Abbreviations

CC	Cloud Computing
CSP	Cloud Service Provider
DoS	Denial of Service
DDoS	Distributed Denial of Service
HaaS	Hardware as a Service
ID	Identification Document
IT	Information Technology
IaaS	Infrastructure as a Service
LAN	Local Area Network
OS	Operating System
PaaS	Platform as a Service
RAID	Redundant Array of Independent Disks
RAM	Random Access Memory
SaaS	Software as a Service
SIO	System Initialisation Operator
SLR	Systematic Literature Review
SSL	Secure Sockets Layer
SwAF	Swedish Armed Forces
TLS	Transport Layer Security
TPA	Third Party Auditing
TTP	Trusted Third Party
VLAN	Virtual Local Area Network
VM	Virtual Machine
VMM	Virtual Machine Monitor

Contents

1. Introduction 1
1.1 Background 1
1.2 Problem area 1
1.3 Motivation 2
1.4 Delimitations 3
1.5 Target group 3
1.6 Outline 4
2 Definitions 5
2.1 Security and information security 5
2.2 Cloud Computing 5
2.2.1 Public cloud 6
2.2.2 Private cloud 6
2.2.3 Hybrid cloud 6
2.2.4 Community cloud 6
2.3 Service models 6
2.3.1 Infrastructure as a Service 6
2.3.2 Software as a Service 7
2.3.3 Platform as a Service 7
2.3.4 Hardware as a Service 7
2.4 Virtualization and multi tenancy 7
3 Methodology 9
3.1 Philosophical paradigm 9
3.2 Literature analysis 9
3.3 Literature search 10
3.3.1 Practical screening 10
3.3.2 Quality appraisal 11
3.3.3 Formulation of the results 12
4 Findings 13
4.1 Security risks 14
4.1.1 Virtualization and multi tenancy 14
4.1.2 Data privacy and integrity 15
4.1.3 Denial of service 16
4.1.4 Deduplication 17
4.1.5 User access control 17
4.1.6 Loss of control, backup issues and availability 18
4.1.7 Trust management 19

4.2 Security solutions 21
4.2.1 Security models 21
4.2.2 Auditing 22
4.2.3 Policies 23
4.2.4 SecCloud 23
4.2.5 RAID 24
4.2.6 Biometrics 25
4.2.7 Self-destructing data 25
4.2.8 Hardware as a Service: Physical and virtual hardware on demand 26
4.3 Security in service models 26
5 Analysis and discussion 28
6. Conclusions and future work 29
6.1 Findings 29
6.2 Limitations of the review 30
6.3 Outcome 30
References 31
Appendix A 35
Appendix B 38

1. Introduction

This section provides a background for the review. Thereafter a research problem is defined and a motivation for the review is presented. The section is concluded with a presentation of the delimitations and the outline of the review.

1.1 Background

Cloud computing (CC) is a network model that makes it possible to achieve on-demand network access and a shared pool of configurable resources, e.g. networks and servers, which can be provided with minimal management or interaction. Simplified, this means that CC represents a model for network access that does not require the same level of maintenance as a standard organisational network would (Mall & Grance, 2011). Clouds are so integrated in our everyday life that most people don't even think about them being used. Examples of everyday CC are platforms such as iCloud, Office 365 and Google Drive.

Since cloud computing is such a quickly expanding field within IT it is not negligent to say that this network model has drastically changed how we perceive networking today. In addition, it has also drastically changed how businesses, organisations and governments act and function. The evolution of CC has brought with it new security challenges which is why individuals and businesses alike act hesitant when confronted with the possibility of implementing a cloud solution (Subashini & Kavitha, 2011).

In a cooperation with the Swedish Armed Forces (SwAF) and Uppsala University, students are offered several research subjects to choose from while contemplating the subject of their essay. The students then write the essay with support and guidance provided by a, from the SwAF, designated expert as an external supervisor. A list of research subjects was published on Uppsala University's service "Careergate". One of these subjects provide the foundation of this essay.

New security challenges means new opportunities for research, however this also means that an overwhelming amount of information becomes available for organisations and individuals searching for information regarding CC security issues. Therefore this essay will present a literature review aiming to summarise the available information and make it more comprehensible.

1.2 Problem area

Initially it is important to mention that the reviewed subject already has a solid foundation in the shape of relevant literature. This review aims to analyse this foundation and summarise it in order to present the reader with a factual, up-to-date depiction of the current security risks and solutions within the CC field. The need for this is simple: since cloud computing continues to grow exponentially it is of utter importance to stay updated on the present risks

and solutions in order to ensure that future clouds are developed based on the latest insights. The problem presents itself in the massive amount of relevant literature you would have to sift through in order to gain these aforementioned insights. It would also be hard to know which literature is trustworthy in comparison to one another. Thus, this review aims to analyse current literature within the CC field demarcated to security risks and solutions in order to form a concrete summarisation which can then be used as an overview by anyone working within the IT sector.

A summary produced in the shape of a Systematic Literature Review (SLR) would be of relevance to individuals and organisations, large and small, with a need for an up to date security overview as well as a tool for future research (Okoli & Schabram, 2010). In addition to this, the literature supports the claim as it is consistently mentioned that businesses, which would benefit greatly from a transition to a cloud-based solution, hesitate when faced with the lack of concrete answers regarding the security of the solution (Subashini & Kavitha, 2011). Thus, a summarisation could provide answers without much effort from either the cloud service providers or the customers. This could potentially lead to an increase in CC usage, which in turn would lead to preferable solutions in the future.

Because of the limited timeframe of the review it is unrealistic to perform a quantitative investigation that would obtain a sufficiently high quality in order to build a solid foundation based on Swedish businesses, organisations and governments. Thus, it has been concluded that this review will strictly analyse literature published since 2011 whereas a majority is either theoretical or case studies performed on corporations worldwide.

The research is built upon the research question:

What security risks and solutions are presented in the literature regarding cloud computing security?

Furthermore the research will also discuss the secondary research question:

What are the differences in security between public, hybrid, community and private clouds as well as the service models; IaaS, PaaS, SaaS and HaaS?

1.3 Motivation

Information security is an important feature in all sorts of systems. Security within cloud computing is no exception. In fact, one quick search on Google Scholar with the search terms “cloud computing security” will warrant roughly 67 000 results even while disregarding results from before 2011. This confirms that the area of CC security is a widely researched subject. While that in itself is an indication that security within CC is a palpable problem, the massive amount of research also contributes to the problem in the sense that finding relevant literature becomes a difficult task. As a result of this increased difficulty there seem to be a lack of summaries regarding the subject. This is proven by the fact that a perspicuous analysis

of the subject cloud computing security, pertaining to both current solutions as well as risks, is nonexistent based upon the authors' own findings.

As such, the purpose of this review is to analyse relevant literature within the CC area. It is essential to clarify that the review does not aim to produce an applicable solution for the aforementioned risks, but instead provide a straightforward, current depiction of security within CC.

1.4 Delimitations

This review is oriented to the area of security within the field of CC. Security is an interesting area to examine as it is quite significant and new research is continuously being produced. At the same time, this brings certain difficulties. A decision was made to only include literature from the year 2011 and onward. The reasoning behind this is that cloud computing grows exponentially and as such new security risks are constantly identified, and solutions constantly developed. In order to ensure up to date information is used literature produced before 2011 was not deemed appropriate for this review.

Due to the study's timeframe another decision was made. As mentioned in section 1.3, this study will not aim to produce a solution for any specific security risks but instead produce a summary of existing solutions and risks.

1.5 Target group

The products generated by this review targets those who wants to gain insight in the field of CC security. This could be of use for several different groups.

An organisation or a business, including the SwAF, could make use of the review in order to achieve a more secure cloud based service by including the summary in the early stages of development or when redesigning an already existing service. The objective of the summary is to provide the reader with a depiction of the security area within the CC field. This depiction can then be used to identify which areas should be focused on as well as which areas might need further investigation.

A student or a researcher within the field of information systems, or similar fields, might use the review as a foundation for future research. They may also take advantage of the extensive bibliography to gain a further advantage.

Lastly, an individual interested in IT might use the review in order to obtain a picture of how CC is described within the scientific community and can then be used to help the individual identify further reading.

1.6 Outline

The review is divided into six sections: introduction (1), definitions (2), methodology (3), findings (4), discussion (5) and conclusion (6).

The definition section defines the central terms of the review. In the methodology section the methods used to conduct the research are presented, afterwards details about the literature is given. In the findings section the result of the literature review is presented. Afterwards the discussion section presents relevant groupings of the findings as well as a motivation for these groups. In the concluding section the research questions are answered and the authors' recommendations for future research presented. Finally limitations of the review are also discussed in the concluding section.

2 Definitions

This section covers the central terms used throughout the review.

2.1 Security and information security

Ensuring the confidentiality, integrity and availability, also known as the CIA triangle, has been considered the industry standard for quite some time now (Whitman and Mattord, 2009, p. 8). While these characteristics remain of utmost importance, the rapid development surrounding the IT sector means this definition must be expanded in order to encapsulate the new security situation.

Information and communication technology (ICT) can arguably be considered a sub-component of information security since information security includes the protection of underlying resources. ISO/IEC 13335-1 (2004) defines ICT security as all aspects relating to defining, achieving and maintaining the confidentiality, integrity, availability, non-repudiation, accountability, authenticity and reliability of information resources. Thus, von Solms & van Niekerk (2011) argues that a clear understanding of these additional characteristics is essential as without them, information cannot be considered secure.

As such, whenever this review utilises the terms “security” or “information security”, this is the definition being referred to.

2.2 Cloud Computing

Various cloud computing solutions exist, all with different types of characteristics. The different types of clouds are defined in this section, as well as the service models discussed in this review. A short definition of CC itself was introduced in section 1.1 however this definition can be extended. Some key characteristics of CC is that it is capable of on-demand self-service as well as capable of rapid elasticity. This means that not only should a user be able to access the cloud without human interaction, in addition the cloud environment capabilities should be automatically scalable (Mall & Grance, 2011). Aside from this a cloud environment must also be available over the network, capable of resource pooling and capable of being measured. This means that a cloud environment must contain mechanics for monitoring, reporting and controlling the above mentioned characteristics (Mall & Grance, 2011).

Furthermore, clouds are deployed using different deployment methods, or types of clouds. It is important to know the difference between the different deployment methods as they can impact which security risks and solutions that are applicable to a cloud. The common ones are public, private, hybrid and community clouds.

2.2.1 Public cloud

The simplest way to describe a public cloud is an infrastructure that is used by the public and provided by a government, organisation or other companies (Mall & Grance, 2011).

2.2.2 Private cloud

A private cloud is used exclusively by an organisation and the cloud provider is either the organisation themselves or a third party (Mall & Grance, 2011).

2.2.3 Hybrid cloud

A hybrid cloud is an infrastructure that combines public and private clouds. It consists of a composition of two or more clouds that all remain unique entities but are bound together by standardised or proprietary technology (Mall & Grance, 2011).

2.2.4 Community cloud

A community cloud is used by a community of consumers from various organisations that share common views. This particular setup may be controlled and maintained by a third party or by the organisations themselves. In addition, a community cloud setup may reside inside or outside the CSP premises (Srinivasan, Sarukesi, Rodrigues, Manoj, & Revathy, 2012). Community cloud consumers therefore seek to exploit economies of scale while at the same time minimising the costs associated with private clouds or hybrid clouds as well as the risks associated with public clouds (Boampong & Wahsheh, 2012).

2.3 Service models

Clouds use architectural models in order to provide different services to the users. Service models are not tied to a specific deployment type, public, private, hybrid and community, rather each deployment type can use each service model (Cloud Security Alliance, 2011). Just as with the different deployment methods the service models can have implications for a clouds security state, it is therefore important to have knowledge of these service models. The common service models are explained below.

2.3.1 Infrastructure as a Service

Infrastructure as a Service, often abbreviated to ‘IaaS’, consists of offering infrastructure solutions as a service. The major benefit of this is the ability to only pay for what you actually use. An example of this is Dropbox where the user can pay more or less depending on how much storage they need (Srinivasan, Sarukesi, Rodrigues, Manoj, & Revathy, 2012).

2.3.2 Software as a Service

Software as a Service, often abbreviated to 'SaaS', utilises an instance of an application and the underlying database to offer the software to multiple customers simultaneously (Srinivasan, Sarukesi, Rodrigues, Manoj, & Revathy, 2012).

2.3.3 Platform as a Service

Platform as a Service, often abbreviated to 'PaaS', provides a platform that can be used during the development of an information system, e.g. for testing and distribution. Examples of these kind of services are GAE and Microsoft Azure (Srinivasan, Sarukesi, Rodrigues, Manoj, & Revathy, 2012).

2.3.4 Hardware as a Service

Hardware as a Service, often abbreviated to 'HaaS'. It brought forth a significant improvement because it allows for easy access to physical hardware devices, distributed among several geographical locations. If the cloud consumers subscribe to this service, it will appear as if they are connected to the local machine. The HaaS cloud middleware will ensure transparency between data exchanges while the local system considers all connected hardware to be locally connected, even though this is not always the case (Stanik, Hovestadt, & Kao, 2012).

2.4 Virtualization and multi tenancy

Virtualization and multi tenancy are two of the core technologies that enables CC to be used as we know it today. A traditional way of hosting applications and data storage involves running one operating system (OS) on one physical server. This traditional hosting method can also be used to create a functioning but inefficient cloud. This is achieved by linking multiple servers using a Virtual LAN (VLAN). This is secure but inefficient in the long term as a large part of the physical hardware available end up being unused. Virtualization was created in order to solve this efficiency problem. By using a Virtual Machine Monitor (VMM) a single physical server can host multiple instances of an OS. This means that a single server can utilise the available hardware power in a more efficient manner (Srinivasan, Sarukesi, Rodrigues, Manoj, & Revathy, 2012).

The figure below is a basic illustration of a VMM running multiple instances of an OS using a virtualization layer. The virtualization layer is often known as hypervisor. There are two main ways of utilising this hypervisor to run virtual machines (VM). These are known as full virtualization and paravirtualization. The difference between them lies in how much of the OS needs to be emulated. A VM deployed using full virtualization has to emulate the BIOS and drives of the OS, in addition to the other functions. A VM using paravirtualization runs a version of the OS that has been modified to work without needing a BIOS or similar components (Mishra et al., 2013).

There are also two major architectures used to deploy virtual machines, hosted architecture and hypervisor architecture. The difference here stems from the way the hypervisor is handled by the server. In a hosted architecture the hypervisor is a platform that the host OS runs as a normal application. The application is then charged with the upkeep of the virtual machines. On the other hand a hypervisor architecture skips the OS and is instead run directly on the hardware. Depending on which deployment method and architecture used different security aspects apply (Mishra, Mathur, Jain & Singh, 2013).

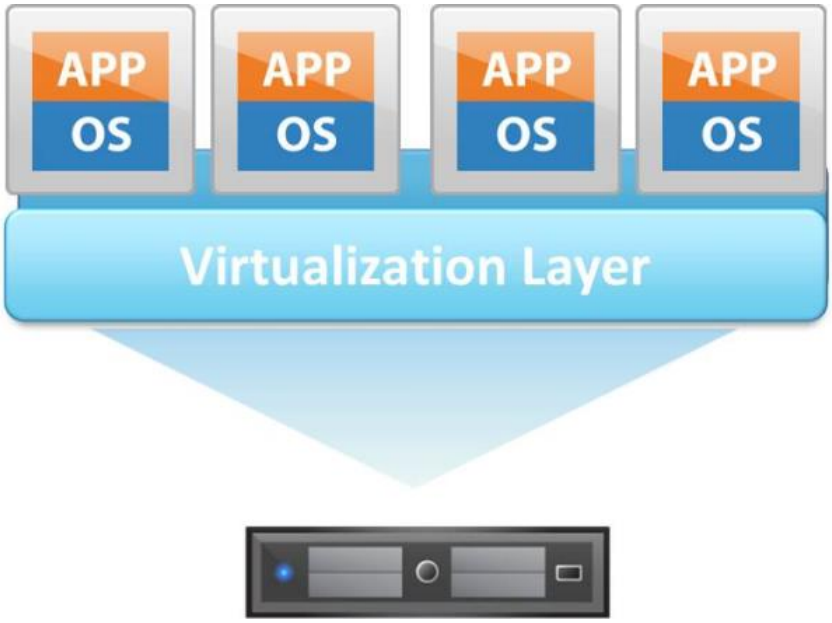

Figure 1. Descriptive image of Virtualization (Source: Burkley, 2015).

Multi tenancy is closely tied to virtualization. In short, multi tenancy allows several users to share computing resources with logical separation of the different users, a user in this case is a tenant of the system (Mishra et al., 2013). In the context of cloud computing, each VM can be considered a tenant. However multi tenancy is not limited to multiple VMs running on the same hardware. Applications can also be utilised in a way that allows multiple tenants to use them, while at the same time separating the different users from each other (Mishra et al., 2013). While virtualization and multi tenancy are core technologies needed for cloud computing to remain efficient and viable they introduce new security risks. These are discussed in section 4.1.1.

3 Methodology

In this section the methodology used in the review will be explained. It includes the philosophical paradigm this essay is based on as well as the overarching research strategy including the methodology that will be used to analyse the literature used in this review.

3.1 Philosophical paradigm

This review is based on the interpretivistic paradigm. Interpretivism is based on the idea that phenomenon need to be understood in a social context (Oates 2006, p. 292). This paradigm is well suited for this literature review. Initially security can have different meanings in different social contexts. This is something that is important to understand when discussing security as the various authors of the literature reviewed might have different views on what is considered secure. Interpretivism acknowledges that there are multiple subjective realities (Oates 2006, p. 292), making it well suited to discuss security. Secondly interpretivism is often used in conjunction with qualitative data analysis (Oates 2006, p. 292), something this review will be based on. Lastly the interprevistic paradigm acknowledges that there are multiple interpretations of a given phenomenon (Oates 2006, p. 292), something which is often true when discussing security. All of this makes it a well suited paradigm for this review.

3.2 Literature analysis

This analysis is based upon a qualitative approach and the methodology is loosely grounded in the eight-step design of how to conduct a systematic literature analysis as suggested by Okoli and Schabram (2010).

Step 1. Define the purpose of the analysis
The purpose of this analysis is to collect relevant literature regarding CC security from a myriad of non-relevant literature. Through identifying security risks and solutions from this literature a summary depicting the current security situation may be constructed for future use.

Step 2. Practical screening
For this step, the authors' aims to accumulate information from various sources such as scientifically reviewed journals, conference papers and books. It is the authors' perception that the majority of this information will be obtained from the Internet.

Step 3. Quality appraisal
A set of criteria will be formulated in order to facilitate sifting of the literature based upon its quality and relevance to this review.

Step 4. Formulation of the results
After the appraisal, the literature will be further scrutinised in order to identify the risks and solutions found in the literature.

3.3 Literature search

3.3.1 Practical screening

This step is implemented in order to identify relevant literature. The search for this was mainly performed with the help of provided databases from Uppsala University and Google Scholar. Its focus was to find existing, relevant literature regarding security within the CC field. Thus, literature such as newspaper articles and blogs were quickly eliminated. In addition, a conclusion was made that since the review aims to be a current view on CC, literature published before 2011 should be excluded. The motivation behind the chosen databases were that a quick search of the subject showed that AMC DL and IEEE Xplore yielded the most relevant results. Google Scholar was chosen since it returns result from a large number of sources. It is important to note that it is impossible from a practical standpoint to go through all the results found in these databases. Since literature published before 2011 were to be excluded the search was refined to only include publications between 2011 and 2015. The results were sorted by relevance using the tools provided by the search engine. It is important to mention that due to the way search engines operate the results and their order might shift depending on the computer used for the search and other similar factors. After sorting the results the first 100 results from each database were selected for appraisal.

Search term	IEEE Xplore	AMC DL	Google Scholar
Cloud computing security	4492 results	4335 results	67 400 results

Table 1: The number of search results from the different databases

These 300 results were appraised using the following three questions:

- *When was the literature published?*

This question was included in order to ensure that no results published before 2011 had been selected.

- *At first glance, does the title and abstract seem relevant for the review's research questions?*

This question was included in order to filter the results further. While reading through all the literature would have been preferable this is not realistic due to the amount of time required to

do this. Thus it was determined that a more realistic approach was to only read the abstract in order to ensure that it was related to this review's research questions. This means that the abstract should at least mention cloud computing security and/or specific risks associated with this field.

- *Is the source published in a trustworthy and credible medium?*

This question was included in order to ensure that none of the results were from sources such as blog posts or news article. A trustworthy and credible medium refers to a peer-reviewed publication such as conference papers, journal articles and books.

This practical screening generated 52 sources which were considered relevant to the review's research questions. It is clear that the majority was either of the type journal or conference paper, a reasonably expected result considering the research field.

Type of literature	Amount of literature
Conference papers	20
Journals	29
Books	3

Table 2: Type of literature

3.3.2 Quality appraisal

The 52 sources were evaluated thoroughly to determine their quality. Quality in this case refers to whether a potential source was relevant to the essays research questions, and written by what appears to be a credible author. In order to do this efficiently, the sources were divided in two and the authors' of this review reviewed them based on their abstract, results and conclusions. Solely those whom fulfilled the specific criteria were included in the analysis. Beside the publication year, two other criteria were contextualised to determine whether or not the source was relevant for this review. These are as follows:

- *Does the literature relate to the review's research questions?*

In order to fulfil this criterion the reviewed literature would have to focus on specific security risks and solutions related to cloud computing or the security aspects of the different deployment methods and service models. This means that literature that only briefly mentioned a security risk or solution, for example just naming a risk/solution without further discussion, would not be classified as relevant to this review. Literature that focused on problems that fell outside the scope of the research questions, such as complex mathematical models of security or similar, were also excluded.

- *Does the authors appear to be credible?*

A credible author in this context is an author who has previous publications within the IT field, preferable related to security or cloud computing.
After the above mentioned appraisal process was completed 26 articles remained and 26 had been eliminated. 26 of the articles were eliminated due to not being deemed relevant to the research questions, this means that all of the authors were deemed credible based on our credibility check of the author. Of the 26 articles remaining 14 were journal articles and 12 were conference papers, meaning this review will be based on a good mixture of these two mediums. A complete summary of the appraisal process can be found in Appendix A.

3.3.3 Formulation of the results

After the quality appraisal, the remaining literature was once again reviewed thoroughly in order to identify the various security risks and solutions. This was achieved by scrutinising the abstract, results and the conclusion of each article. In the majority of the literature, a security solution was presented and discussed in conjunction to a specific security risks. This type of structure will be used in the process of presenting this review's findings. Alas, not all of the literature maintained this structure as some presented either a specific solution or a model for said solution. In conjunction to this, the results were grouped into security risks and the solutions to the identified risks, as well as security solutions which are not connected to any specific risks. These will be presented in section 4.

4 Findings

In this section the security risks found in the literature as well as various solutions are presented. Solutions are discussed in the same section as their risks, however if the solution is not specifically connected to a specific risk it is discussed towards the end of this section. Below two tables are presented that provides a summary of how many articles that discussed each different risk and solution. The number outside the parenthesis represents the number of articles discussing the security risk/solution in question. The numbers inside the parenthesis is a reference to the matching source in Appendix A and B.

Security risks	Number of sources and references to Appendix B
Virtualization and multi tenancy	4 (5, 8, 11, 15)
Data privacy and integrity	5 (1, 8, 15, 17, 28)
Denial of service	3 (24, 48, 49)
Deduplication	1 (32)
User access control	2 (2, 19)
Loss of control, backup issues and availability	6 (13, 15, 17, 22, 28, 35)
Trust management	1 (40)
Security in service models	2 (27, 51)

Table 3: Number of articles related to security risks

Security solutions	Number of sources and references to Appendix B
Security models	1 (33)
Auditing	2 (28, 46)
Policies	2 (2, 8)
SecCloud	2 (31, 32)
RAID	1 (35)
Biometrics	2 (49, 52)
Self-destructing data	1 (25)
Hardware as a Service	1 (50)

Table 4: Number of articles related to security solutions

4.1 Security risks

4.1.1 Virtualization and multi tenancy

While virtualization and multi tenancy are two staple technologies of CC they are still part of many security issues. As discussed in 2.4 the different types and different architectures for virtualization affect the security concerns related to these areas. However the difference between the different types of virtualization is less important than the overall cloud service type. It is also important to note that an emulated OS is still at risk from attacks that targets the traditional version of the OS. For instance a virtual machine running Windows is still at risk from attacks that target normal Windows machines. It is also important to note that hypervisors are additive to the overall security risk (Mishra et al., 2013)

As was just stated, normal security risks associated with operative systems still apply to virtual instances, however securing multiple virtual machines is more difficult. This stems from the fact that if one VM gets infected it can infect other VM since there is no need to bypass things such as network protocols, the infected VM is already inside the network. The infected VM can then perform VM to VM attacks or attacks against the hypervisor software (Mishra et al., 2013). Running an antivirus software on the hosted VMs is all well and good but ensuring they are all up to date simultaneously is not so easy. If just one instance of the antivirus software is forgotten all VMs hosted on that platform are at risk. One solution to this is to run an antivirus software on the underlying platform hosting the VMs. This antivirus would not be used to secure the platform itself, rather it would be used to monitor and secure all the data processed by the VMs. This means you only need to update one central antivirus in order to secure all the tenants on that physical server. Aside from this it also means that a virus attacking a VM will have a harder time affecting the overall antivirus system, since it resides outside the infected VM (Tari, 2014).

Another issue that might have a very severe negative impact on the organisation using a cloud computing solution is data leakage. Data leakage occurs due to the shared resources used by the VMs. These can have the form of cache based attacks or RAM based attacks (Tari, 2014). These attacks occurs since both the shared cache and RAM does not automatically flush upon completion of a computing task. This means a infected VM can recreate data based on the information left in the shared resources. In order to combat this the hosting platform can inject ‘noise’ into the cache in order to flush if from any remaining information left behind by a VM (Tari, 2014). To combat the RAM based attacks it is necessary to restrict a VMs ability to lock the memory bus. Both of these solution requires no expensive hardware modifications but can simply be introduced by adding software.
The risks associated with multi tenancy described above have slightly different implications depending on which service model is being used.

While the above mentioned solution with flushing the cache and preventing RAM bus locking works on all service models it is often better to prevent the issue from occurring in the first place. This is done by isolating the tenants from each other. In an IaaS environment this would mean isolating the data storage and processing resources. In a PaaS environment the isolation focus should be on isolating API calls as well as running services. In a SaaS environment the focus should instead be on isolating the transactions carried out on the same instance by different tenants. (Behl & Behl, 2012)

Regardless of the isolation degree chosen a user should never be fully aware of the exact server location for their data. While general information such as the country or region level is fine preventing the user from knowing the exact location decreases the risk of other malicious users learning the location. This means that multi tenancy attacks that rely on gaining access to a VM on the same physical server as the target will be much harder to achieve (Bouayad, Blilat, El Houda Mejhed, & El Ghazi, 2012). For instance, a cache based attack cannot be used if the target VM is in another geographical location.

While isolation is a good solution it is important to note that it might mean less efficient resource sharing, this increases the cost and reduces the flexibility of cloud computing. An organisation must therefore carefully consider the cost and benefit of increased isolation. While some data might be considered sensitive enough to warrant full isolation that is not necessarily the case for all the data used by the organisation.

4.1.2 Data privacy and integrity

Ensuring that your data is kept private and secure from unauthorised users as well as free from malicious or unintentional modifications is no easy task. When managing these aspects of security one main issue is the lack of control a cloud user has over the actual server the data is stored on (Chen & Zhao, 2012).

Data stored in the cloud can be divided into two groups, IaaS environment data and data in PaaS or SaaS environments. IaaS data is data that is stored in the cloud instead of on a local hard drive, examples of this include services such as Amazon Simple Storage Service. PaaS and SaaS data differs from this since this data is primarily used in applications processing the data, not necessarily storing it long term (Chen & Zhao, 2012).

Data stored in an IaaS environment can simply be encrypted in order to decrease the risk of private data becoming public. However this is not always as easy as it sounds as the encryption will only be as secure as the encryption method chosen. Aside from this key management is a crucial issue (Behl & Behl, 2012). Often the users owning the data do not have the expertise needed to manage their encryption keys. Allowing the cloud service provider to manage the keys solves this problem but managing a large number of keys is a difficult task and the cloud service provider must have a secure way of doing this. Aside from this the entity responsible for key management must be a trusted entity. If the key management entity is not trusted by all parties the encryption might be rendered null and void seeing as there is no guarantee the keys will be kept out of reach from malicious interests. (Chen & Zhao, 2012)

For data used in PaaS or SaaS environments encryption is not a suitable solution. Seeing as the data has to be processed in an application it is not feasible to decrypt and encrypt the data for each computing task (Chen & Zhao, 2012). This means that data is left vulnerable to snooping co-tenants as discussed in section 4.1.1. While it has been shown that it is possible to perform some computing tasks on encrypted data it is not suitable for all types of computing (Tari, 2014).

Data integrity is a core part of managing data. Doing this in the cloud introduces new major challenges that must be solved if CC is to be considered secure. This is due to the fact that cloud servers are distrusted in terms of both security and reliability. The data stored in the

cloud may be corrupted by both administrative errors as well as malicious attacks (Xiao & Xiao, 2014). Many cloud providers charge a fee for the uploading and downloading of data. This means that downloading large sections of data to verify the integrity of the data is not a viable solution. Some solutions have been proposed, including letting a trusted third party appointed by the cloud provider periodically check for data integrity. Despite this more research is needed to fully solve the data integrity issue. (Chen & Zhao, 2012)

Integrity is not only concerned with data. Software integrity also needs to be taken into account. Software integrity becomes a problem since the CSP provides the applications the user utilises. Thus it is important that the software providers have a clear security policy on how to ensure that any software used will not do unexpected things to the users' data. (Zissis & Lekkas, 2012)

4.1.3 Denial of service

Denial of Service (DoS) or Distributed Denial of Service (DDoS) is one of the biggest security risks in cloud computing as well as any other internet based service. DoS or DDoS generally functions by the attacker sending large amounts of data packets, such as simple TCP/UDP or really any other type of data. The goal of a DoS attack is to negatively affect the availability of service for legitimate users by overloading the server's capacity and bandwidth (Rahman & Cheung, 2014 b). This is achieved when the host computer is unable to compute anymore data causing its many VM's to disrupt in their service, effectively making them unreachable by users (Rahman & Cheung, 2014 a).

DDoS is even more dangerous to cloud computing in comparison to other internet based services due to the nature of the attack. This is because DDoS takes advantage of hundreds of different computers, known as "bots", to attack a server using different types of data packets which makes it undeniably hard for a cloud service to defend itself. In addition to this, the VM configuration data is stored in the host computer. Thus, if an attacker gains access to the host he can simultaneously take control of all the VM's. (Rahman & Cheung, 2014 a). DoS or DDoS attacks can take place against any type of cloud service such as IaaS, PaaS and SaaS as well as private, public, hybrid and community clouds (Rahman & Cheung, 2014 b).

A common solution to DDoS attacks is the use of a firewall (Liu, Dou, Yu, & Zhang, 2015). However using a firewall in a cloud computing environment comes with unique challenges. A centralised firewall has been proposed as a way to secure a cloud environment against a number of attacks. However such a centralised firewall comes with a number of disadvantages. Since a cloud environment runs many different services the number of rules the firewall will operate on as well as the package arrival rate allowed will be different for each service. In order to use a centralised firewall the ruleset will grow to be far too large, and individual customers cannot specify separate rules for their cloud environment (Liu, Dou, Yu, & Zhang, 2015).

To solve this issue a decentralised firewall framework has been proposed. Such a framework has been shown to be cost effective (Liu, Dou, Yu, & Zhang, 2015). The framework operates by grouping multiple hosting servers into clusters, each cluster is then given dynamical resources to launch a VM instance that hosts the firewall for that specific

cluster. This means that a customer can then rent a firewall for their specific application environment, allowing them to specify their own ruleset and package arrival rate, thus solving the problem with a centralised firewall (Liu, Dou, Yu, & Zhang, 2015).

4.1.4 Deduplication

Deduplication is a technique where the server stores only a single copy of each file, regardless of how many clients requested the storage of the same file. By doing this the cloud servers as well as the network bandwidth are saved. However, deduplication may lead to leakage of sensitive side channel information. For instance a server utilising this technology might get a request to store a file, however this file is already stored on the server. The server then tells the client making the request that the file already exists in the storage, and as such need not be transferred again. This would reveal to the client that another cloud user has the exact same file, which could be sensitive information in some cases. (Li, Li, Xie & Cai, 2015)

4.1.5 User access control

User access control is an important part of any information system. Access control is the way a service provider can ensure that only authorised users have access to applications and data storage. It is important to have formal procedures in place when allocating access rights to users. Policies that dictate how and when a user can gain access privileges as well as deciding on what application level their access should be viable is an important step towards keeping access control secure (Sabahi, 2011).

Depending on the type of cloud service model used different user access responsibilities applies. In the SaaS model the cloud provider is the one responsible for all things network, server and application related and the responsibility of user control falls to the customer. The customer must ensure only the intended users gain access rights by managing passwords and similar internally (Sabahi, 2011).

In the PaaS model the service provider is responsible for managing access to things such as the network and server platforms. Customers are the ones responsible for managing access to the specific application provided by the service (Sabahi, 2011).

In the IaaS model the customer is the one responsible for managing all aspects of access control, including resources such as host platform, network and so on. They are also responsible for managing access to their virtual machines and storage (Sabahi, 2011).

It is important for cloud users to adapt their access controls depending on which service model being used. Access control is a problem that is not solved with fancy technologies, rather it requires good policy management from the organisation using the cloud. Despite this there are still risks associated with access control that are more technical in nature.

One of these technical issues is launching a denial of service attack using account lockouts. Some authenticating services locks an account if a certain number of failed login attempts occur. An attacker could therefore deny service to a large number of users if they manage to get hold of their account names. They would do this by repeatedly try to log in

using the username and an arbitrary password to lock the account (Grobauer, Walloschek, & Stocker, 2011).

Another issue related to the one mentioned above is weak password reset mechanisms. It is important that a user locked out of their account can regain access to the account by resetting the password. However this must be done in a secure manner or a potential attacker could gain control of the account instead (Grobauer, Walloschek, & Stocker, 2011).

While the above mentioned issues can partially be solved using better technical solutions such as more secure password reset mechanisms it is still important to note that a large part of avoiding these exploits is to have a clear and effective policy in place detailing how a legitimate user can get their account back in the event of a lock out. The policy should specify how a user must identify themselves in order to reset their password. It should also specify who can use the password reset function. For instance not all users need to have password reset privilege, rather a trusted entity at the organisation utilising the cloud could be in charge of identifying a user requesting the password reset as well as being the one to approve it.

4.1.6 Loss of control, backup issues and availability

Loss of control risks are all associated with the fact that a user of cloud computing generally does not have access to the physical hardware being used. This has several implications for the users. One of the first and most important steps is evaluating if storing sensitive data in the cloud violates previous agreements with data owners (Zissis & Lekkas, 2012) (Al-Anzi, Salman, Jacob & Soni, 2014). If storing sensitive data in the cloud can be seen as a violation of the data privacy due to loss of control an organisation should not progress with their plans to move data storage and processing to the cloud. Aside from this choosing a trustworthy cloud service provider is equally important. The organisation looking to migrate to the cloud must make a careful and thorough evaluation of the cloud service providers' security measures (Xiao & Xiao, 2013).

When an organisation stores information in the cloud the service provider could gain access to this information. This is a major threat to the organisation using the cloud. Seeing as the administrators of a cloud already have inside access preventing a malicious administrator from reading and manipulating data is no easy task. There are many solutions to this problem but no single solution can fully protect against this possibility. One solution is to never give the cloud service administrators more privilege than they absolutely need (Varadharajan & Tupakula, 2014). This would prevent them from accessing all data and functions of a cloud. Another solution is to encrypt all the data stored in the cloud. However encrypting large quantities of data might not be feasible from a performance standpoint. Therefore research has been done that suggest it might be possible to perform some computing tasks without decrypting the data. This would mitigate the performance issues as well as giving the data owner increased control of their data (Tari, 2014).

Availability is another large part of loss of control. Availability refers to the property of a system being accessible and usable upon demand by an authorised entity. The user of a cloud cannot guarantee the availability of the servers hosting the cloud. This must be done by the cloud service provider. In order to ensure data is always available the service provider and

user must agree to specific specification regarding system availability (Zissis & Lekkas, 2012). Such an agreement should also detail who is responsible in the event of down time. This agreement should also specify any monetary compensation or similar if the target availability is not met.

Lastly ensuring data is properly secured against data loss through the use of backups also need to be specified. Keeping a local backup of everything a user stores in the cloud would be the most secure option. However this is not very economical and defeats part of the purpose of cloud computing. Just as with availability it is important to specify what is backed up, how this is done and who is the responsible party if a backup fails. It has been noted that there is a risk that the user and data owner will suffer the full responsibility if data loss occurs, with no liability for the cloud service provider (Khalil, Khreishah, Bouktif, & Ahmad, 2013).

While technology can make backups more secure the best way to establish reliable backups is to ensure that there is a clear agreement between the user and the service provider. The agreement should specify how the service provider will ensure that backups are being created and stored in a secure manner, as well liability in case of faulty backups.

4.1.7 Trust management

Trust Management is one of the most challenging issues in the emerging CC field. Noor, Sheng, Zeadally & Yu (2013) mentions that there have been several studies performed in order to address these issues but unfortunately several trust management issues such as; identification, privacy, personalisation, integration, security and scalability have been mostly neglected.

Trust Management was initially developed to overcome the issues of centralised security systems such as the heterogeneity of policy languages. These policies are responsible for setting authorisation roles and implementing security policies. Noor, Sheng, Zeadally & Yu (2013) say that trust management techniques can be classified into four categories: Policy, Recommendation, Reputation and Prediction. Policy as a Trust Management Technique (PocT), in short, uses a set of policies each of which assumes several roles to authorise access. Recommendation as a Trust Management Technique (RecT) takes advantage of participant's knowledge about the trusted parties. Reputation as a Trust Management Technique (RepT) is an important one since feedback provided by cloud service consumers can dramatically affect the reputation of a specific CSP and its service. Prediction as a Trust Management Technique (PrdT) is useful when there is no prior information regarding the cloud service's interactions. The basic idea behind it is that similar minded entities, e.g. cloud service consumers, are more likely to trust each other than the CSP.

There are several trust characteristics within cloud services which can be compared in relation to the different service models (i.e. IaaS, PaaS and SaaS) including authentication, security, privacy responsibility, virtualization and cloud service consumer accessibility.

- Authentication specifies the techniques and mechanisms that are used for authentication in a specific cloud. Since cloud consumers have to establish their identities each time they attempt to use a new cloud service there is a risk of privacy breaches if no proper identity scheme is applied.

- Security refers to three separate security levels: Communication security Level (CSL), Data Security Level (DSL) and Physical Security Level (PSL). CSL includes the communication techniques such as SSL, DSL refers to data replication techniques for data recovery and PSL refers to the physical security techniques (i.e. hardware security).

- Privacy responsibility can be categorised into two different categories: the CSP privacy responsibility and the cloud consumer responsibility.

- Virtualization covers the techniques that are used to achieve virtualization within a cloud. There are two separate levels of virtualization: The OS level and the application container level.

- Cloud Consumer Accessibility are the techniques and mechanisms used for cloud consumers to access cloud services, e.g. Graphical User Interfaces (GUIs) and Application Programming Interfaces (APIs).

To conclude this research, the authors encourage more insight and development of innovative solutions to address the open research issues that have been identified (Noor, Sheng, Zeadally, & Yu, 2013).

4.2 Security solutions

4.2.1 Security models

Al-Anzi, Yadav & Soni (2014) suggest a security model for CC comprising governance, risk management and compliance. CC security requirements vary quite significantly from traditional environments because of its dynamic nature and customer ownership. It is pertinent to mention that this model can be applied to each type of cloud, e.g. private, public, hybrid and community as well as the different type of services; IaaS, PaaS and SaaS. Fig. 2 presents an overview of the security model and below it follows an elucidation.

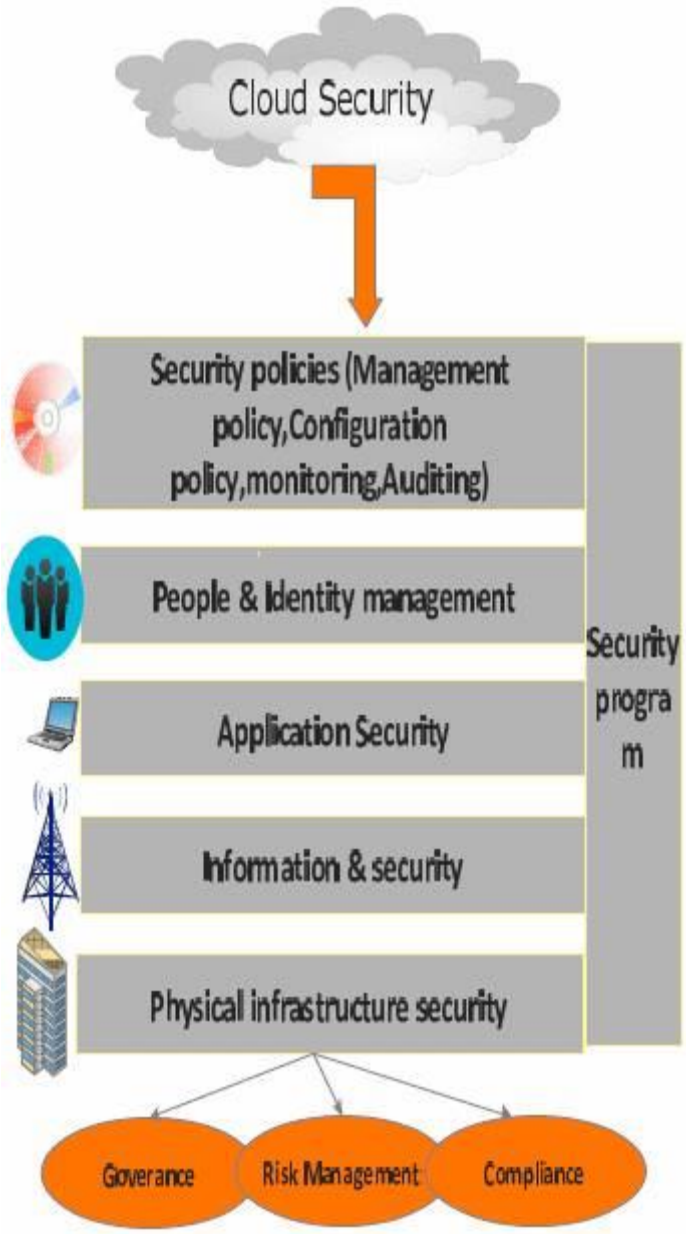

Figure 2. The suggested security model (Source: Al-Anzi, Yadav & Soni, 2014).

- Security governance, risk management and compliance: The fundamental responsibility of the organisation is to identify and implement process, control and organisational structure so that effective security could be achieved. Governance is any set of policies, laws and technologies that work within an organisation and provide direction in order to achieve security objectives. Al-Anzi, Yadav & Soni (2014) suggest that an organisation should implement a framework for effective risk management and measure the performance of the risk management by metrics.

- People and identity management: Only authorised users should be able to access assets, an identity federation approach is applied in order to achieve secure authentication and authorisation.

- Application security: An XML signature as well as an XML encryption is implemented in order to protect applications from XML attacks and other web service attacks.

- Information security: Data and information security is a top concern for any CSP as well as the customers using the service. As such, Al-Anzi, Yadav & Soni (2014) suggest that CSPs need to focus on how data is stored, processed and audited. In addition, they recommend an implemented intrusion detection and prevention system.

- Physical infrastructure: For physical measures they suggest the implementation of biometric access controls and a computer based access control system (CAS) which, in short, restricts access to users who can provide authorisation.

4.2.2 Auditing

Auditing within a CC environment basically refers to the process of ensuring data integrity of outsourced data and save the user's computation time and online burden of additional processing. Rewadkar & Ghatage (2014) propose a privacy-preserving third party auditing (TPA). TPA will verify the storage correctness of the outsourced data periodically when the users initiate a request for verification. The goal of the TPA is to reduce the burden of users by saving their computation resources while ensuring the correctness of their data stored in the cloud.

The problem that could arise by choosing not to use TPA is that CSP's, for monetary reasons, may delete data that is not being used or they may hide the data loss incidents to maintain reputation. Of course the users have the option of verifying this data themselves, albeit these options are impractical or risks the confidentiality of the data (Rewadkar & Ghatage, 2014).

The proposed solution will perform the auditing on the user's request. This will be done by sending the verification metadata from the user to the server and the response will then be verified by the TPA. It also includes a so called 'batch auditing' which will decrease the response time for audit requests when sent by multiple users. Rewadkar & Ghatage (2014)

own test-environment showed that this batch auditing decreased the request time from 1210 ms to 80 ms.

Another form of auditing is achieved by implementing a so called Trusted Third Party (TTP) which, in cryptography is an entity which facilitates secure interactions between two parties, e.g. a user and a CSP (Zissis & Lekkas, 2012). The TTP reviews all critical transactional communications between the parties. Implementing a TTP in a cloud solution can address the loss of the traditional security boundary by producing trusted security domains. In short, a TTP will take advantage of Public Key Infrastructure (PKI) to ensure strong authentication, authorisation, data confidentiality, data integrity and non-repudiation (ensuring that no entity in an electronic transaction can deny its participation) (Zissis & Lekkas, 2012).

4.2.3 Policies

Policies are often used as a way to ensure that organisation wide security targets are being handled the same way across the organisation. While policies on their own cannot solve security issues they are an important management tool. Cloud computing is no exception to this. When creating a policy regarding cloud computing it is important to remember that the cloud service provider must be aware of the policy. Indeed it might be wiser to develop a mutual understanding of the policy together with the service provider (Behl & Behl, 2012). This is also important due to the fact that the CSP might have several customers with different security needs and therefore it might be impossible for the CSP to create a policy that covers all the security needs of all the customers. Instead it is wiser to create policies that deal with individual customers and their specific needs (Sabahi, 2011). Ultimately a policy is only effective if the organisation owning it continuously develops secure practices using the policy as a base. Whether it is porting an existing policy or creating a new one policies alone cannot not solve the security issues all cloud users face.

4.2.4 SecCloud

SecCloud is a basic protocol which uses identity based cryptography. An overview of what this actually means and how it works is followed by the steps presented below, as described by Wei et al. (2014):

- The System Initialisation Operator (SIO) generates system parameters as well as master secret keys. After the system parameters are set the SIO selects a random number as its master key and another one for its public key. Once a user connects to the cloud it must first be registered with the SIO. The user can do this by using its unique ID, e.g. a user ID, and is then provided a secret key by the SIO through a TLS or SSL connection.

- Before the user can upload data to the cloud, the necessary storage for it is requested and is then allocated by the CSP. In an attempt to ensure data storage auditing, the user has to sign every single transmission block in order to generate authenticated

data. SecCloud has a function that allows an organisation to be set as 'trusted' which means the above mentioned process can be completed automatically.

The data is then encapsulated and a session key is created before it is sent to the CSP. Once it's been received, it is decrypted by using the session key and the user's signature is verified.

- After the steps mentioned above, the result is verified in order to confirm that everything has been completed in a correct manner, e.g. that the data has been stored at the correct positions.

What separates SecCloud from other cryptographic protocols is the effectiveness, the usage of auditing at the time of uploading and that several users can be handled simultaneously through batch verification.

In addition to this basic protocol, there are also other forms of the SecCloud protocol such as SecCloud+ and SecCloudHDFS. These are more advanced and as such, require further computing power but offer new forms of security. One of these additional types of security is deduplication of data. SecCloud+ also offers the possibility to encrypt the data before uploading (Wei et al., 2014).

As of today, clouds don't generally store massive amounts of data. But from an analysis report performed by Li, Li, Xie and Cai (2015) this will not be the case in just 5 years' time. They estimate the volume of data by 2020 to be 40 trillion gigabytes. Thus, a user should demand improved security and integrity surrounding their data from the CSP.

4.2.5 RAID

In the system architecture "Robust, Scalable and Secure Network Storage (RSSNS)" presented by Al-Anzi, Salman, Jacob & Soni (2014) an encryption mechanism is first applied to the data which in turn is split into cipher blocks. These blocks of cipher data are then placed among several different CSPs. E.g. if a customer stores a file, A, on the cloud. A is then encrypted before uploading and is split into different blocks of data; A1, A2 and A3. These are then distributed on different servers within the cloud.

RSSNS achieves this by applying a Redundant Array of Independent Disks (RAID) implementation at each server within the cloud. They compare different versions of RAID and reach the conclusion that RAID 10 (1 + 0) is most efficient. RAID 10 provides several unique features such as data redundancy, availability and fault tolerance by mixing the features of striping and mirroring. Availability is achieved by the usage of parity. Parity, in short, is information pertaining to a specific cipher block and can be used to reconstruct a file that's been damaged or is unavailable for various purposes. E.g. if A1 is stored in S1, A2 is stored in S2 and A3 is stored in S3, the parity information from A1 and A2 is stored in S3. Thus, if A1 is damaged, the complete file can still be reconstructed using the information stored in S2 and S3 (Al-Anzi, Salman, Jacob & Soni, 2014).

4.2.6 Biometrics

In many cryptographic systems the key to success lies on the client side, where cryptography and decrypting is stored. If this client in turn is attacked and hijacked by an aggressor, the whole cryptographic system is in critical condition. Rahman & Cheung (2014 b) have described ICMetrics technology as the possibility to produce unique identifiers based on the electric system's behaviour which can then be used as a key. However, Tahir et al. (2013) argue that low entropy and a short key length for the ICMetrics key might make it sensitive to attacks. Thus, the authors suggest that this key has to be reinforced before it can be implemented as a security solution. This would be done using the cryptographic algorithm SHA-2. If SHA-2 is applied to the ICMetrics key it would provide the key with sufficient length and high entropy. Biometrics can also be used in order to create and store various cryptographic keys.

By implementing ICMetrics/Biometrics as a security solution, each individual VM running on a host computer can be encrypted in a unique manner which in turn would solve the virtualization risks VM-hoping and VM-escape. VM-hoping and VM-Escape are two newly derived virtualization threats. VM-hoping basically means that an attacker may use one VM to spy on another VM within the same physical host whereas VM-escape is the process in which the attacker takes control of one VM and in turn also takes control of the host-computer as well as every other VM stored on the host-computer (Rahman & Cheung, 2014 b).

4.2.7 Self-destructing data

In order to combat the loss of control commonly associated with storing sensitive data in the cloud some researchers suggest implementing a self-destructing data scheme. At first glance this might seem like an odd solution. The idea is that self-destructing data gives the data owner control over their data even if they do not control the servers the data is stored on. By encrypting the data using a secure encryption method as well as a time span specified by the user the data owner can control how long the data will be available. The key used to decrypt the data is associated with the same time span as the encrypted data, and the key will only function as long as it is used within the given time span. After the times pan has expired the data can no longer be decrypted, and thus can be safely destroyed (Xiong et al., 2014).

While this solution can be used for any type of data it is especially useful for sensitive data that is only needed temporarily. For instance personal data used temporarily within the cloud but normally stored locally would be well suited for this approach. The same can be said about data needed only to compute a result using some kind of data processing. Seeing as that kind of data is only needed temporarily anyway this gives the user the freedom to specify how long their sensitive data will be available in the cloud, even if they cannot physically control the server (Xiong et al., 2014).

4.2.8 Hardware as a Service: Physical and virtual hardware on demand

Cloud computing has already been adopted in a broad range of application domains. At the same time, domains such as the distributed development of embedded systems are still unable to benefit from the advancements of CC. A common obstacle is often the incompatibility between such applications and the cloud (Stanik, Hovestadt & Kao, 2012). Stanik, Hovestadt & Kao (2012) describes a solution to this problem in form of a novel cloud layer, HaaS. This additional layer allows for usage of distinct hardware components through the Internet analogously to the cloud services. This way, HaaS will not only enable interconnection of physical systems but also virtual hardware emulation. By making emulators accessible as HaaS services, the emulated hardware components will appear to be connected to the local computer just like physical hardware normally would. For software developers this means that developed software can be tested against hardware long before the first hardware prototype has been developed, resulting in saving both time and money. As such, it would benefit the cloud service, PaaS, enormously.

Since these devices will appear to be attached to a local system, arbitrary hardware devices can be virtualized using HaaS as well as specific software can access such virtualized hardware devices even though they have not been designed for being used in a cloud specific context.

By using a virtual bus, multiple hardware devices can be connected even if these devices are distributed over multiple geographical locations or multiple organisations (Stanik, Hovestadt & Kao (2012). It is therefore also a viable option to implement in a community based cloud environment as well as the other type of environments, i.e. public, private and hybrid.

4.3 Security in service models

As previously mentioned, CC utilises three delivery models (community is more of a special solution configured to adapt to certain conditions) by which different types of services are delivered to the cloud consumer. The three service models are SaaS, PaaS and IaaS which provide infrastructure resources, an application platform and a software as services to the consumer. These service models also place a different level of security requirements in the cloud environment.

IaaS is the foundation of all cloud services where PaaS is built upon it and SaaS in turn is built upon PaaS. Just as capabilities are inherited, so are the information security issues and risks. Subashini & Kavitha (2011) claim that there are significant trade-offs to each model in the terms of integrated features, complexity versus extensibility and security. As such, if the CSP only takes care of the security at a lower part of the security architecture, the consumers become more responsible for implementing and managing the various security capabilities.

SaaS is the software deployment model where applications are remotely hosted by the application or service provider and made available to consumers on demand. This offers the consumers significant benefits and is, as a result of that, rapidly emerging as the dominant

delivery model. However, most enterprises are still uncomfortable with SaaS due to the lack of visibility about the way their data is stored and secured (Subashini & Kavitha, 2011).

IaaS on the other hand completely changed the way developers deploy their applications. Instead of spending a lot of money on their own data centres they can simply apply a service such as Amazon Web Services, get a virtual server running and only pay for used resources. In addition, IaaS provides basic security (perimeter firewall, load balancing etc.) which makes it a compelling alternative to the other service models. However, applications moving into the cloud will need higher levels of security then what can be provided by the host (Subashini & Kavitha, 2011).

PaaS abstracts everything up to OS, middleware etc. This means that developers are offered an environment where they can build applications without having to worry about the underlying service. In short, it's a service that provides a complete software development lifecycle where everything not pertinent to the development is abstracted away from the developers. The dark side of PaaS is that these advantages can be helpful for hackers to leverage the PaaS infrastructure for malware command and control in order to go behind the IaaS applications (Subashini & Kavitha, 2011).

Subashini & Kavitha (2011) continue by explaining various exploits a malicious user may attempt in order to gain access to unauthorised data such as Cross-site scripting (XSS), insecure configuration and cookie manipulation. In addition to these threats they also state that the choice of deployment model may impact security, e.g. by using a public cloud instead of a private/community cloud, the service is susceptible to more risks. This is due to the fact that you want to know who is accessing the information and from where it is being accessed. In a public cloud juxtaposed a private cloud, whose consumer base is usually located within an organisation, this could prove a difficult task (Chavan, Patil, Kulkarni, Sutar & Belsare, 2013).

5 Analysis and discussion

During the process of analysing the literature, the authors' of this review made a discovery. It appears as if literature that discussed a certain security topic often chose to focus on only one of the affected security areas. In the area of integrity the majority of the literature focused on data integrity whereas sub-areas such as software integrity and hardware integrity were basically non-existent.

This observation that the majority of the literature neglected sub-areas of their respective research could be considered a serious threat to the future of cloud computing. Another example is physical security. Physical is often mentioned in the literature, however it is seldom seen as a major security risk. Malicious or ignorant users are also often overlooked. While it is mentioned in a small part of the literature it is possible this particular risk is often overlooked due to how broad it is. Seeing as a malicious or ignorant user can be considered a threat in all areas of an organisation it makes sense that it is not seen as a key threat in literature focused on a specific risk. The final example of this is the different service models and deployment models. Almost all of the literature included a definition for the different service models. Despite this only a small part of the analysed literature attempted to distinguish unique security issues and solutions for each of the different service models. As the service models are a core part of cloud computing the authors' of this review consider this a major weakness in the available literature. The same can be said for the different deployment types, however the lack of discussion surrounding the different deployment types is not as severe of a flaw as it is in regards to the service models. This is due to the differences between the types of deployment being more obvious. For instance a public cloud is obviously more vulnerable to malicious users since the organisation providing the cloud cannot maintain control over who use the cloud. Compare this to a private cloud where the cloud provider has a greater control over who gets access rights.

The lack of literature on these sub-areas can be explained in a few different ways. First, there is research conducted in these areas but it might not be published as a topic related to cloud computing security. For example the article related to HaaS written by Stanik, Hovestadt & Kao (2012) is published under cloud computing but not security nor cloud computing security. Second it might be possible that the sub-areas omitted from the majority of the research are not deemed important enough to warrant an entire paper. However it is most likely a combination of these reasons.

6. Conclusions and future work

In this literature review we systematically examined research regarding cloud computing security in order to identify the major security issues this technology faces today. By using criteria to determine what literature to include in the review 52 different articles were initially selected. These 52 were then further evaluated and 26 articles were deemed relevant to the research questions. Using these 26 articles the authors of this review were able to identify major issues and solutions regarding cloud computing security as well as areas where further research must be done.

6.1 Findings

What security risks and solutions are presented in the literature regarding cloud computing security?

It is clear that there is plenty of available research regarding cloud computing security. Even so, this review proves that it is still one of the predominant issues with the technology in its entirety. This review has managed to identified several significant security threats related to virtualization and multi tenancy, data privacy and integrity, denial of service, deduplication, user access control, loss of control, backup issues, availability, trust management and security in the different service models. The review also identified several different solutions to some security risks in the reviewed literature. The identified solutions were security models, auditing, policies, SecCloud, RAID, biometrics, self-destructing data and hardware as a service.

What are the differences in security between public, hybrid, community and private clouds as well as the service models; IaaS, PaaS, SaaS and HaaS?

One important trend in the reviewed literature is the absence of research related to the differences in security between public, private, hybrid and community cloud deployment models. While a lot of the reviewed research included definitions for the different types of clouds merely a few of the twenty six journals and conference papers that passed the evaluation actually mentioned the security differences between a public, private, hybrid and community cloud. This is partially due to the fact that it seems many issues and solutions affect all four types. It is pertinent to mention that what was mentioned in this literature regarding security differences was miniscule at best. Thus, the conclusion was drawn to not present these differences in their own respective sections.

In addition, the different service models associated with the various deployment models proved to be more common in the literature. IaaS, PaaS and SaaS all have their unique challenges when it comes to security, and it is clear that some research has been done in order to identify the unique threats and solutions applicable to the different service model. Alas, there was not enough information to draw factual conclusions. However, it would appear as if the IaaS layer greatly affects the security of the built upon layers, e.g. PaaS and SaaS.

6.2 Limitations of the review

While the goal of the review was to include a large and diverse amount of sources it is impossible to review all the literature available. As such several criteria were established in order to select the appropriate literature. It is possible that these criteria incorrectly excluded some relevant literature. Aside from this only three databases were used, while the authors' consider this sufficient, the possibility that relevant literature was overlooked cannot be completely excluded. In the end a meaningful summary of current security issues and solutions was produced and while more sources could have ensured an even better result practical limitations such as time meant that this was not possible.

6.3 Outcome

This review could serve as a theoretical basis for future research, showcasing the current major security issues as well as theoretical solutions. Future research should focus on practical case studies in order to validate the theoretical solutions discussed and presented in this review. Aside from this more research should be done in order to better understand the attitudes of cloud computing consumers as well as cloud service providers when it comes to security. Finally future research should strive to better understand the way the different deployment methods and service models affect the overall security of a system.

References

Al-Anzi, F. S., Salman, A. A., Jacob, N. K., & Soni, J. (2014). *Towards robust, scalable and secure network storage in Cloud Computing.* In 2014 Fourth International Conference on Digital Information and Communication Technology and it's Applications (DICTAP) (pp. 51–55). http://doi.org/10.1109/DICTAP.2014.6821656

Al-Anzi, F. S., Yadav, S. K., & Soni, J. (2014). *Cloud computing: Security model comprising governance, risk management and compliance.* In 2014 International Conference on Data Mining and Intelligent Computing (ICDMIC) (pp. 1–6). http://doi.org/10.1109/ICDMIC.2014.6954232

Behl, A., & Behl, K. (2012). *An analysis of cloud computing security issues.* In 2012 World Congress on Information and Communication Technologies (WICT) (pp. 109–114). http://doi.org/10.1109/WICT.2012.6409059

Boampong, P. A., & Wahsheh, L. A. (2012). *Different Facets of Security in the Cloud*. In Proceedings of the 15th Communications and Networking Simulation Symposium (pp. 5:1–5:7). San Diego, CA, USA: Society for Computer Simulation International. Retrieved from http://dl.acm.org/citation.cfm?id=2331762.2331767

Bouayad, A., Blilat, A., El Houda Mejhed, N., & El Ghazi, M. (2012). *Cloud computing: Security challenges.* In Information Science and Technology (CIST), 2012 Colloquium in (pp. 26–31). http://doi.org/10.1109/CIST.2012.6388058

Burkley, R. Virtualization Explained on a "Napkin." (2015). Retrieved June 9, 2015, from https://www.linkedin.com/pulse/virtualization-explained-napkin-rodger-burkley

Chavan, P., Patil, P., Kulkarni, G., Sutar, R., & Belsare, S. (2013). *IaaS Cloud Security*. In 2013 International Conference on Machine Intelligence and Research Advancement (ICMIRA) (pp. 549–553). http://doi.org/10.1109/ICMIRA.2013.115

Chen, D., & Zhao, H. (2012). *Data Security and Privacy Protection Issues in Cloud Computing*. In 2012 International Conference on Computer Science and Electronics Engineering (ICCSEE) (Vol. 1, pp. 647–651). http://doi.org/10.1109/ICCSEE.2012.193

Cloud Security Alliance. (2011). *Security Guidance for Critical Areas of Focus in Cloud Computing V3.0.* Retrieved 14 May, 2015, from https://downloads.cloudsecurityalliance.org/initiatives/guidance/csaguide.v3.0.pdf

Grobauer, B., Walloschek, T., & Stocker, E. (2011). *Understanding Cloud Computing Vulnerabilities.* IEEE Security Privacy, 9(2), 50–57. http://doi.org/10.1109/MSP.2010.115

ISO/IEC TR 13335-1:2004 (2004) *Information technology security techniques management of information and communications technology security part 1: concepts and models for information and communications technology security management*. ISO/IEC, JTC 1, SC27, WG 1. Retrieved from http://www.iso.org/iso/catalogue_detail.htm?csnumber=39066

Khalil, I. M., Khreishah, A., Bouktif, S., & Ahmad, A. (2013). *Security Concerns in Cloud Computing*. In 2013 Tenth International Conference on Information Technology: New Generations (ITNG) (pp. 411–416). http://doi.org/10.1109/ITNG.2013.127

Li, J., Li, J., Xie, D., & Cai, Z. (2015). *Secure Auditing and Deduplicating Data in Cloud* IEEE Transactions on Computers, PP(99), 1–1. http://doi.org/10.1109/TC.2015.2389960

Liu, M., Dou, W., Yu, S., & Zhang, Z. (2015). *A Decentralized Cloud Firewall Framework with Resources Provisioning Cost Optimization*. IEEE Transactions on Parallel and Distributed Systems, 26(3), 621–631. http://doi.org/10.1109/TPDS.2014.2314672

Mell, P., Grance, T. (2011). *The NIST definition of Cloud Computing*. (Artikelnr 800-145). National Institute of Standards and Technology. Retrieved 10 february, 2015, from http://www.nist.gov/itl/cloud/

M.E. Whitman, H.J. Mattord. (2009) *Principles of information security* (3rd ed.)Thompson Course Technology

Mishra, A., Mathur, R., Jain, S. & Singh Rathore, J. (2013). *Cloud Computing Security*. In International Journal on Recent and Innovation Trends in Computing and Communication (IJRITCC) (pp. 36-39). Retrieved from http://www.ijritcc.org/download/IJRITCC_1309.pdf

Noor, T. H., Sheng, Q. Z., Zeadally, S., & Yu, J. (2013). *Trust Management of Services in Cloud Environments: Obstacles and Solutions*. ACM Comput. Surv., 46(1), 12:1–12:30. http://doi.org/10.1145/2522968.2522980

Oates, B. J. (2006). *Researching Information Systems and Computing* (4th issue). London: Business & Economics

Okoli, C., & Schabram, K. (2010). *A Guide to Conducting a Systematic Literature Review of Information Systems Research* (SSRN Scholarly Paper No. ID 1954824). Rochester, NY: Social Science Research Network. Retrieved from http://papers.ssrn.com/abstract=1954824

Rahman, M., & Cheung, W. M. (2014) a. *Analysis of Cloud Computing Vulnerabilities.* International Journal of Innovation and Scientific Research, 2(2), 308–312.

Rahman, M., & Cheung, W. M. (2014) b. *Cloud Computing, Security Issues and Potential Solution by Using ICMetrics or Biometrics Based Encryption*. Intertional Journal of Advances in Computer Science and its Applications (IJCSIA) (Vol. 4: Issue 1. pp. 36-41).

Rewadkar, D. N., & Ghatage, S. Y. (2014). *Cloud storage system enabling secure privacy preserving third party audit.* In 2014 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT) (pp. 695–699). http://doi.org/10.1109/ICCICCT.2014.6993049

Sabahi, F. (2011). *Cloud computing security threats and responses*. In 2011 IEEE 3rd International Conference on Communication Software and Networks (ICCSN) (pp. 245–249). http://doi.org/10.1109/ICCSN.2011.6014715

Srinivasan, M. K., Sarukesi, K., Rodrigues, P., Manoj, M. S., & Revathy, P. (2012). *State-of-the-art Cloud Computing Security Taxonomies: A Classification of Security Challenges in the Present Cloud Computing Environment.* In Proceedings of the International Conference on Advances in Computing, Communications and Informatics (pp. 470–476). New York, NY, USA: ACM. http://doi.org/10.1145/2345396.2345474

Stanik, A., Hovestadt, M., & Kao, O. (2012). *Hardware as a Service (HaaS): Physical and virtual hardware on demand.* In 2012 IEEE 4th International Conference on Cloud Computing Technology and Science (CloudCom) (pp. 149–154). http://doi.org/10.1109/CloudCom.2012.6427579

Subashini, S., & Kavitha, V. (2011). *A survey on security issues in service delivery models of cloud computing.* Journal of Network and Computer Applications, 34(1), 1–11. http://doi.org/10.1016/j.jnca.2010.07.006

Tahir, R., Hu, H., Gu, D., McDonald-Maier, K., & Howells, G. (2013). *Resilience against brute force and rainbow table attacks using strong ICMetrics session key pairs*. In 2013 1st International Conference on Communications, Signal Processing, and their Applications (ICCSPA) (pp. 1–6). http://doi.org/10.1109/ICCSPA.2013.6487307

Tari, Z. (2014). *Security and Privacy in Cloud Computing.* IEEE Cloud Computing, 1(1), 54–57. http://doi.org/10.1109/MCC.2014.20

Varadharajan, V., & Tupakula, U. (2014). *Security as a Service Model for Cloud Environment.* IEEE Transactions on Network and Service Management, 11(1), 60–75. http://doi.org/10.1109/TNSM.2014.041614.120394

Von Solms, R., & van Niekerk, J. (2013). *From information security to cyber security.* Computers & Security, 38, 97–102. http://doi.org/10.1016/j.cose.2013.04.004

Wei, L., Zhu, H., Cao, Z., Dong, X., Jia, W., Chen, Y., & Vasilakos, A. V. (2014). *Security and privacy for storage and computation in cloud computing.* Information Sciences, 258, 371–386. http://doi.org/10.1016/j.ins.2013.04.028

Xiao, Z., & Xiao, Y. (2013). *Security and Privacy in Cloud Computing*. IEEE Communications Surveys Tutorials, 15(2), 843–859. http://doi.org/10.1109/SURV.2012.060912.00182

Xiong, J., Liu, X., Yao, Z., Ma, J., Li, Q., Geng, K., & Chen, P. S. (2014). *A Secure Data Self-Destructing Scheme in Cloud Computing.* IEEE Transactions on Cloud Computing, 2(4), 448–458. http://doi.org/10.1109/TCC.2014.2372758

Zissis, D., & Lekkas, D. (2012). *Addressing cloud computing security issues.* Future Generation Computer Systems, 28(3), 583–592. http://doi.org/10.1016/j.future.2010.12.006

Appendix A

This appendix contains the 52 sources selected in the first literature search, as well as the outcome of applying the different selection criteria to these sources. In order to make the table easier to read the letters in the first row correspond to the following:

A: Number
B: Title
C: Year of publication
D: Type of publication
E: Trustworthy author?
F: Relevant to research questions?
G: Include in review?
- : Could not access a full version of the literature.

A	B	C	D	E	F	G
1	Data Security and Privacy Protection Issues in Cloud Computing	2012	Conference	Yes	Yes	Yes
2	Cloud Computing Security Threats and Responses	2011	Conference	Yes	Yes	Yes
3	Cloud Computing Security	2012	Book	Yes	No	No
4	Pervasive and Ubiquitous Technology Innovations for Ambient Intelligence Environments	2012	Book	Yes	No	No
5	Cloud Computing Security	2013	Journal	Yes	Yes	Yes
6	Cloud Computing Security: From Single to Multi-clouds	2012	Conference	Yes	No	No
7	Research on Cloud Computing Security Problem and Strategy	2012	Conference	Yes	Yes	No
8	An Analysis of Cloud Computing Security Issues	2012	Conference	Yes	Yes	Yes
9	A Cloud Computing Security Solution Based on Fully Homomorphic Encryption	2014	Conference	Yes	Yes	No
10	A Security Aspects in Cloud Computing	2012	Conference	Yes	No	No
11	Cloud Computing: Security Challenges	2012	Conference	Yes	Yes	Yes
12	A Novel Based Security Architecture of Cloud Computing	2014	Conference	Yes	No	Yes
13	Security Concerns in Cloud Computing	2013	Conference	Yes	Yes	Yes
14	Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing	2011	Journal	Yes	No	No

15	Security and Privacy in Cloud Computing	2013	Journal	Yes	Yes	Yes
16	On-Demand Security Architecture for Cloud Computing	2012	Journal	Yes	No	No
17	Security and Privacy in Cloud Computing	2014	Journal	Yes	Yes	Yes
18	Using Cloud Computing to Implement a Security Overlay Network	2014	Journal	Yes	No	No
19	Understanding Cloud Computing Vulnerabilities	2011	Journal	Yes	Yes	Yes
20	The Threat in the Cloud	2013	Journal	Yes	No	No
21	Anonymous Multi-Receiver Remote Data Retrieval for Pay-TV in Public Clouds	2015	Journal	Yes	No	No
22	Security as a Service Model for Cloud Environment	2014	Journal	Yes	Yes	Yes
23	CloudAC: A Cloud Oriented Multilayer Access Control System for Logic Virtual Domains	2013	Journal	Yes	No	Yes
24	A Decentralized Cloud Firewall Framework with Resource Provisioning Cost Optimization	2015	Journal	Yes	Yes	Yes
25	A Secure Data Self Destructing Scheme	2015	Journal	Yes	Yes	Yes
26	Cloud Computing Security: The Scientific Challenge, and a Survey of Solutions	2015	Journal	Yes	No	No
27	A Survey on Security Issues in Service Delivery Models of Cloud Computing	2011	Journal	Yes	Yes	Yes
28	Addressing Cloud Computing Security Issues	2012	Journal	Yes	Yes	Yes
29	A Compendium Over Cloud Computing Cryptographic Algorithms and Security Issues	2014	Journal	Yes	No	No
30	Different Facets of Security in the Cloud	2012	Conference	Yes	Yes	Yes
31	Security and Privacy for Storage and Computation in Cloud Computing	2013	Journal	Yes	Yes	Yes
32	Secure Auditing and Deduplicating Data in Cloud	2015	Journal	Yes	Yes	Yes
33	Cloud Computing: Security Model Compromising Governance, Risk Management and Compliance	2014	Conference	Yes	Yes	Yes
34	Common Cloud Architecture for Cloud Interoperability	2014	Conference	Yes	No	No

35	Towards Robust, Scalable and Secure Network Storage in Cloud Computing	2014	Conference	Yes	Yes	Yes
36	Key Challenges in Cloud Computing: Enabling the Future Internet of Services	2013	Journal	Yes	No	No
37	State-of-the-art Cloud Computing Security Taxonomies: A Classification of Security Challenges in the Present Cloud Computing Environment	2012	Conference	Yes	Yes	Yes
38	CloudVisor: Retrofitting Protection of Virtual Machines in Multi-Tenant Cloud with Nested Virtualization	2011	Conference	Yes	No	No
39	Secure the Cloud: From the Perspective of a Service-Oriented Organization	2015	Journal	Yes	No	No
40	Trust Management of Services in Cloud Environments: Obstacles and Solutions	2013	Journal	Yes	Yes	Yes
41	Virtualization: Issues, Security Threats and Solutions	2013	Journal	Yes	No	No
42	Interconnected Cloud Computing Environments: Challenges, Taxonomy, and Survey	2014	Journal	Yes	No	No
43	A Survey of Security Issues in Hardware Virtualization	2013	Journal	Yes	No	No
44	Secure Cloud Data Computing with Third Party Auditor Control	2014	Book	----	----	No
45	Security Issues and Countermeasures in Cloud Computing	2011	Conference	Yes	No	No
46	Cloud Storage System Enabling Secure Privacy Preserving Third Party Audit	2014	Conference	Yes	Yes	Yes
47	Improvements of Cloud Computing: Scenario of MDC's and LDC's	2014	Journal	Yes	No	No
48	Analysis of Cloud Computing Vulnerabilities	2014	Journal	Yes	Yes	Yes
49	Cloud Computing Security Issues and Potential Solution by Using IMCMetrics or Biometrics Based Encryption	2014	Journal	Yes	Yes	Yes
50	Hardware as a Service (HaaS): Physical and Virtual Hardware On Demand.	2012	Conference	Yes	Yes	Yes
51	IaaS Cloud Security	2013	Conference	Yes	Yes	Yes
52	Resilience Against Brute Force and Rainbow Table Attacks Using Strong ICMetrics Session Key Pairs	2013	Conference	Yes	Yes	Yes

Appendix B

This appendix contains the complete bibliographic information from the sources in appendix A. Note that sources outside of the 52 sources presented in appendix A are not found in this section, but can instead be found in the references section. The sources appear in the same order as they did in appendix A.

1. Chen, D., & Zhao, H. (2012). *Data Security and Privacy Protection Issues in Cloud Computing*. In 2012 International Conference on Computer Science and Electronics Engineering (ICCSEE) (Vol. 1, pp. 647–651). http://doi.org/10.1109/ICCSEE.2012.193

2. Sabahi, F. (2011). *Cloud computing security threats and responses*. In 2011 IEEE 3rd International Conference on Communication Software and Networks (ICCSN) (pp. 245–249). http://doi.org/10.1109/ICCSN.2011.6014715

3. Trivedi, K., & Pasley, K. (2012). *Cloud Computing Security* (1st ed.). WebEx Communications.

4. Kevin, C. (2012). *Pervasive and Ubiquitous Technology Innovations for Ambient Intelligence Environments.* IGI Global.

5. Mishra, A., Mathur, R., Jain, S. & Singh Rathore, J. (2013). *Cloud Computing Security*. In International Journal on Recent and Innovation Trends in Computing and Communication (IJRITCC) (pp. 36-39). Retrieved from http://www.ijritcc.org/download/IJRITCC_1309.pdf

6. AlZain, M. A., Pardede, E., Soh, B., & Thom, J. A. (2012). *Cloud Computing Security: From Single to Multi-clouds*. In 2012 45th Hawaii International Conference on System Science (HICSS) (pp. 5490–5499). http://doi.org/10.1109/HICSS.2012.153

7. Liu, W. (2012*). Research on cloud computing security problem and strategy*. In 2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet) (pp. 1216–1219). http://doi.org/10.1109/CECNet.2012.6202020

8. Behl, A., & Behl, K. (2012). *An analysis of cloud computing security issues.* In 2012 World Congress on Information and Communication Technologies (WICT) (pp. 109–114). http://doi.org/10.1109/WICT.2012.6409059

9. Zhao, F., Li, C., & Liu, C. F. (2014). *A cloud computing security solution based on fully homomorphic encryption.* In 2014 16th International Conference on Advanced Communication Technology (ICACT) (pp. 485–488). http://doi.org/10.1109/ICACT.2014.6779008

10. Kulkarni, G., Gambhir, J., Patil, T., & Dongare, A. (2012). *A security aspects in cloud computing*. In 2012 IEEE 3rd International Conference on Software Engineering and Service Science (ICSESS) (pp. 547–550). http://doi.org/10.1109/ICSESS.2012.6269525

11. Bouayad, A., Blilat, A., El Houda Mejhed, N., & El Ghazi, M. (2012). *Cloud computing: Security challenges*. In Information Science and Technology (CIST), 2012 Colloquium in (pp. 26–31). http://doi.org/10.1109/CIST.2012.6388058

12. Gupta, S. K., Rawat, S., & Kumar, P. (2014). *A novel based security architecture of cloud computing.* In 2014 3rd International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions) (pp. 1–6). http://doi.org/10.1109/ICRITO.2014.7014676

13. Khalil, I. M., Khreishah, A., Bouktif, S., & Ahmad, A. (2013). *Security Concerns in Cloud Computing*. In 2013 Tenth International Conference on Information Technology: New Generations (ITNG) (pp. 411–416). http://doi.org/10.1109/ITNG.2013.127

14. Wang, Q., Wang, C., Ren, K., Lou, W., & Li, J. (2011). *Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing*. IEEE Transactions on Parallel and Distributed Systems, 22(5), 847–859. http://doi.org/10.1109/TPDS.2010.183

15. Xiao, Z., & Xiao, Y. (2013). *Security and Privacy in Cloud Computing*. IEEE Communications Surveys Tutorials, 15(2), 843–859. http://doi.org/10.1109/SURV.2012.060912.00182

16. Chen, J., Wang, Y., & Wang, X. (2012). *On-Demand Security Architecture for Cloud Computing*. Computer, 45(7), 73–78. http://doi.org/10.1109/MC.2012.120

17. Tari, Z. (2014). *Security and Privacy in Cloud Computing*. IEEE Cloud Computing, 1(1), 54–57. http://doi.org/10.1109/MCC.2014.20

18. Salah, K., Alcaraz Calero, J. M., Zeadally, S., Al-Mulla, S., & Alzaabi, M. (2013). *Using Cloud Computing to Implement a Security Overlay Network*. IEEE Security Privacy, 11(1), 44–53. http://doi.org/10.1109/MSP.2012.88

19. Grobauer, B., Walloschek, T., & Stocker, E. (2011). *Understanding Cloud Computing Vulnerabilities.* IEEE Security Privacy, 9(2), 50–57. http://doi.org/10.1109/MSP.2010.115

20. Green, M. (2013). *The Threat in the Cloud. IEEE Security Privacy*, 11(1), 86–89. http://doi.org/10.1109/MSP.2013.20

21. Wang, H. (2015). *Anonymous multi-receiver remote data retrieval for pay-TV in public clouds*. IET Information Security, 9(2), 108–118. http://doi.org/10.1049/iet-ifs.2013.0376

22. Varadharajan, V., & Tupakula, U. (2014). *Security as a Service Model for Cloud Environment*. IEEE Transactions on Network and Service Management, 11(1), 60–75. http://doi.org/10.1109/TNSM.2014.041614.120394

23. Qiang, W., Zou, D., Wang, S., Yang, L. T., Jin, H., & Shi, L. (2013). *CloudAC: a cloud-oriented multilayer access control system for logic virtual domain*. IET Information Security, 7(1), 51–59. http://doi.org/10.1049/iet-ifs.2012.0094

24. Liu, M., Dou, W., Yu, S., & Zhang, Z. (2015). *A Decentralized Cloud Firewall Framework with Resources Provisioning Cost Optimization*. IEEE Transactions on Parallel and Distributed Systems, 26(3), 621–631. http://doi.org/10.1109/TPDS.2014.2314672

25. Xiong, J., Liu, X., Yao, Z., Ma, J., Li, Q., Geng, K., & Chen, P. S. (2014). *A Secure Data Self-Destructing Scheme in Cloud Computing*. IEEE Transactions on Cloud Computing, 2(4), 448–458. http://doi.org/10.1109/TCC.2014.2372758

26. Ryan, M. D. (2013). *Cloud computing security: The scientific challenge, and a survey of solutions.* Journal of Systems and Software, 86(9), 2263–2268. http://doi.org/10.1016/j.jss.2012.12.025

27. Subashini, S., & Kavitha, V. (2011*). A survey on security issues in service delivery models of cloud computing*. Journal of Network and Computer Applications, 34(1), 1–11. http://doi.org/10.1016/j.jnca.2010.07.006

28. Zissis, D., & Lekkas, D. (2012). *Addressing cloud computing security issues*. Future Generation Computer Systems, 28(3), 583–592. http://doi.org/10.1016/j.future.2010.12.006

29. Mishra, N. (2015). *A Compendium over Cloud Computing Cryptographic Algorithms and Security Issues.* RIET-IJSET: International Journal of Science, Engineering and Technology, 2(1), 59. http://doi.org/10.5958/2395-3381.2015.00008.8

30. Boampong, P. A., & Wahsheh, L. A. (2012). *Different Facets of Security in the Cloud. In Proceedings of the 15th Communications and Networking Simulation Symposium* (pp. 5:1–5:7). San Diego, CA, USA: Society for Computer Simulation International. Retrieved from http://dl.acm.org/citation.cfm?id=2331762.2331767

31. Wei, L., Zhu, H., Cao, Z., Dong, X., Jia, W., Chen, Y., & Vasilakos, A. V. (2014). *Security and privacy for storage and computation in cloud computing*. Information Sciences, 258, 371–386. http://doi.org/10.1016/j.ins.2013.04.028

32. Li, J., Li, J., Xie, D., & Cai, Z. (2015). *Secure Auditing and Deduplicating Data in Cloud.* IEEE Transactions on Computers, PP(99), 1–1. http://doi.org/10.1109/TC.2015.2389960

33. Al-Anzi, F. S., Yadav, S. K., & Soni, J. (2014). *Cloud computing: Security model comprising governance, risk management and compliance*. In 2014 International Conference on Data Mining and Intelligent Computing (ICDMIC) (pp. 1–6). http://doi.org/10.1109/ICDMIC.2014.6954232

34. Balamurugan, B., Kumar, N. S., Lakshmi, G. V. R., & Shanmuga, R. N. S. (2014). *Common Cloud Architecture for Cloud Interoperability*. In Proceedings of the 2014 International Conference on Information and Communication Technology for Competitive Strategies (pp. 10:1–10:6). New York, NY, USA: ACM. http://doi.org/10.1145/2677855.2677865

35. Al-Anzi, F. S., Salman, A. A., Jacob, N. K., & Soni, J. (2014). *Towards robust, scalable and secure network storage in Cloud Computing.* In 2014 Fourth International Conference on Digital Information and Communication Technology and it's Applications (DICTAP) (pp. 51–55). http://doi.org/10.1109/DICTAP.2014.6821656

36. Moreno-Vozmediano, R., Montero, R. S., & Llorente, I. M. (2013). *Key Challenges in Cloud Computing: Enabling the Future Internet of Services*. IEEE Internet Computing, 17(4), 18–25. http://doi.org/10.1109/MIC.2012.69

37. Srinivasan, M. K., Sarukesi, K., Rodrigues, P., Manoj, M. S., & Revathy, P. (2012). *State-of-the-art Cloud Computing Security Taxonomies: A Classification of Security Challenges in the Present Cloud Computing Environment*. In Proceedings of the International Conference on Advances in Computing, Communications and Informatics (pp. 470–476). New York, NY, USA: ACM. http://doi.org/10.1145/2345396.2345474

38. Zhang, F., Chen, J., Chen, H., & Zang, B. (2011). *CloudVisor: Retrofitting Protection of Virtual Machines in Multi-tenant Cloud with Nested Virtualization*. In Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles (pp. 203–216). New York, NY, USA: ACM. http://doi.org/10.1145/2043556.2043576

39. Roy, A., Sarkar, S., Ganesan, R., & Goel, G. (2015). *Secure the Cloud: From the Perspective of a Service-Oriented Organization.* ACM Comput. Surv., 47(3), 41:1–41:30. http://doi.org/10.1145/2693841

40. Noor, T. H., Sheng, Q. Z., Zeadally, S., & Yu, J. (2013). *Trust Management of Services in Cloud Environments: Obstacles and Solutions*. ACM Comput. Surv., 46(1), 12:1–12:30. http://doi.org/10.1145/2522968.2522980

41. Pearce, M., Zeadally, S., & Hunt, R. (2013). *Virtualization: Issues, Security Threats, and Solutions.* ACM Comput. Surv., 45(2), 17:1–17:39. http://doi.org/10.1145/2431211.2431216

42. Toosi, A. N., Calheiros, R. N., & Buyya, R. (2014). *Interconnected Cloud Computing Environments: Challenges, Taxonomy, and Survey.* ACM Comput. Surv., 47(1), 7:1–7:47. http://doi.org/10.1145/2593512

43. Pék, G., Buttyán, L., & Bencsáth, B. (2013). *A Survey of Security Issues in Hardware Virtualization*. ACM Comput. Surv., 45(3), 40:1–40:34. http://doi.org/10.1145/2480741.2480757

44. Rathi, A., & Parmar, N. (2015). *Secure Cloud Data Computing with Third Party Auditor Control.* In S. C. Satapathy, B. N. Biswal, S. K. Udgata, & J. K. Mandal (Eds.), Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014 (pp. 145–152). Springer International Publishing. Retrieved from http://link.springer.com/chapter/10.1007/978-3-319-12012-6_17

45. Wang, J.-J., & Mu, S. (2011). *Security issues and countermeasures in cloud computing*. In 2011 IEEE International Conference on Grey Systems and Intelligent Services (GSIS) (pp. 843–846). http://doi.org/10.1109/GSIS.2011.6043978

46. Rewadkar, D. N., & Ghatage, S. Y. (2014). *Cloud storage system enabling secure privacy preserving third party audit*. In 2014 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT) (pp. 695–699). http://doi.org/10.1109/ICCICCT.2014.6993049

47. Rahman, M. A., & Rahman, M. M. (2014). *Improvements of Cloud Computing: Scenario of MDCs and LDCs*. International Journal of Scientific & Engineering Research, Volume 5, Issue 2. Retrieved from http://www.ijser.org/researchpaper%5CImprovements-of-Cloud-Computing-Scenario-of-MDCs-and-LDCs.pdf

48. Rahman, M., & Cheung, W. M. (2014) a. *Analysis of Cloud Computing Vulnerabilities.* International Journal of Innovation and Scientific Research, 2(2), 308–312. Retrieved from http://www.issr-journals.org/links/papers.php?journal=ijisr&application=pdf&article=IJISR-14-120-07

49. Rahman, M., & Cheung, W. M. (2014) b. *Cloud Computing, Security Issues and Potential Solution by Using ICMetrics or Biometrics Based Encryption*. Intertional Journal of Advances in Computer Science and its Applications (IJCSIA) (Vol. 4: Issue 1. pp. 36-41). Retrieved from http://seekdl.org/conferences_page_papers.php?confid=111

50. Stanik, A., Hovestadt, M., & Kao, O. (2012). *Hardware as a Service (HaaS): Physical and virtual hardware on demand.* In 2012 IEEE 4th International Conference on Cloud Computing Technology and Science (CloudCom) (pp. 149–154). http://doi.org/10.1109/CloudCom.2012.6427579

51. Chavan, P., Patil, P., Kulkarni, G., Sutar, R., & Belsare, S. (2013). *IaaS Cloud Security*. In 2013 International Conference on Machine Intelligence and Research Advancement (ICMIRA) (pp. 549–553). http://doi.org/10.1109/ICMIRA.2013.115

52. Tahir, R., Hu, H., Gu, D., McDonald-Maier, K., & Howells, G. (2013). *Resilience against brute force and rainbow table attacks using strong ICMetrics session key pairs*. In 2013 1st International Conference on Communications, Signal Processing, and their Applications (ICCSPA) (pp. 1–6). http://doi.org/10.1109/ICCSPA.2013.6487307