Cloud Security from Users Point of View: A Pragmatic Study with Thematic Analysis

Saira Syed(✉) and Quazi Mamun

School of Computing and Mathematics, Charles Sturt University, Sydney, Australia
ssyed01@postoffice.csu.edu.au, qmamun@csu.edu.au

Abstract. Despite economic pressure for business to cut costs and fervent assurances from cloud service providers, security remains a top barrier to cloud adoption. Interests in cloud computing are high and many organisations say they are planning to move in that direction. However, the reality is that only 20 % of UK organisations are using infrastructure-as-a-service and only 36 % are using software-as-a-service, according to the National Computing Centre (NCC, UK) research. Lack of trust in cloud computing is slowing broader adoption of cloud services. Therefore, it is important to understand the consumers' perspective on cloud security concerns, especially data security issues. This allows the future research to proceed in the right direction to alleviate users' concerns. In this paper, we present an empirical analysis of IT experts and professionals viewpoint related to security issues in clouds. The study is based on the surveys conducted by three different groups in the time period from 2010 to 2013. Qualitative research analysis is used to collect perception of IT experts and professionals by using interviewing technique. The viewpoints of the experts are then analysed and a qualitative and thematic analysis is presented. The study presents most critical threats, possible causes, and fundamental strategies to avoid them.

Keywords: Cloud computing · Data security · Threats · Cause · Strategies

1 Introduction

The advantages of the cloud computing model of a reduced cost of ownership, no capital investment, scalability, self-service, location independence and rapid deployment are widely extolled. What will it take to get businesses to adopt cloud computing *en masse*? The short answer is that it all boils down to trust.

Cloud computing is the latest IT paradigm which promises to bring many benefits to businesses. However, there are some risks and security concerns that must be addressed correctly [1]. Many research studies [2–4] claim that the most significant reason for deterring cloud computing is the fear of losing control over the data.

Traditional models of data protection such as firewalls and intrusion detection systems are insufficient to protect against complex data security issues of cloud computing. Therefore, this area is currently the focus of attention for the researchers' community. Security is one of the most crucial aspects of this new technology.

J. Tian et al. (Eds.): SecureComm 2014, Part II, LNICST 153, pp. 127–140, 2015.
DOI: 10.1007/978-3-319-23802-9_12

Users, in many cases, are unaware of security threats and may judge security only based on their uninterrupted availability of the respective cloud service. Even if the user understands potential security threats he/she may not be able to restrict the damage in real time or get control of the service.

No matter, how big the company with cloud based services is security incidents are seen in terms of service interruptions to phishing attacks and data leaks. However, it is very important to explore and understand the users' perception in regards to data security and the countermeasures which are currently in place.

This research study presents an empirical analysis of data security issues and their countermeasures from user-centric perspective. The reason for choosing an empirical research method is to discover and interpret facts. Furthermore, this method has been chosen to answer the questions about the topic under investigation. Empirical research can be divided into quantitative method and qualitative method. However this paper is based on qualitative research as this method is appropriate in the early stages of research. In addition qualitative method tends to be applied more easily in real world setting.

The remainder of the paper is organized as follows. Section 2 describes the research themes. In Sect. 3 overview of cloud computing is provided. Section 4 presents synopsis of the literature. In Sect. 5 research methodology is provided. Section 6 presents result followed by discussion in Sect. 7. Finally, in Sect. 8, we conclude the paper and provide the future work.

2 A Basic Overview of Cloud Computing

Cloud computing has been defined by several other researchers, while the most respected one is provided by National Institute of Standards & Technology [5] as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. Some researchers argue that cloud computing is not a new term but only recently it has become a fashionable term [6]. This latest IT paradigm provides large number of benefits to the businesses. Research [7] indicates that the benefits of cloud computing mainly include low-cost, availability, innovation power, high expandability, friendly utilizations and environmental protection. In addition, on-demand self-service, elastic and scalable, consumption-based pricing model are some of the advantages identified by Burton Group, a research and consulting firm [8]. The cloud computing technology is based on three service delivery models and three main deployment models which are as follows:

The deployment models are (1) **Private cloud:** a platform dedicated for specific organization, (2) **Public cloud:** a platform available to public users and (3) **Hybrid cloud:** a private cloud that can extend to use resources in public clouds.

The cloud service deliver models are

(1) **Infrastructure-as-a-service (IaaS):** where computational resources, storage and network as internet-based services are available. For example Amazon EC2

(2) **Platform-as-a-service (PaaS):** where platforms, tools and other business services are available that enable customers to develop, deploy and manage their own application. This model may be hosted on top of IaaS model or on cloud infrastructure directly. MS Windows Azure and Google Apps are the well examples of this model.

(3) **Software-as-a-service (SaaS):** where cloud providers deliver applications hosted on the cloud as a service for end user. SaaS may be hosted on top of PaaS, IaaS or directly on cloud infrastructure. For example: SalesForce CRM.

3 Literature on Cloud Security

Research study conducted by Chow et al. [9] claim that there is a lack of control and transparency [10] when the third-party holds the data. In addition, this study argues that current countermeasure do not adequately address third-party's data storage and processing needs. As a result Chow et al. [9] proposes to extend countermeasures by suggesting the use of trusted computing and cryptographic techniques. However this study is limited to their vision only.

Although the issue of third-party can be addressed by employing trusted third-party (TTP) services [10, 11]. A TTP is an entity which facilitates secure interaction between two parties who both trust this third party. As TTP creates secure zone, its best role is played in cryptography [10]. However Wang et al. [12] argue that cloud storage is not just the third-party data warehouse. The cloud data may not only be accessed but also be frequently updated including insertion, deletion, modification by the users. This makes the data security even more challenging in the cloud environment. Complex data security and privacy issues exist in all stages of data life cycle such as from generation to destruction of data. Many research studies explore and identify [4, 9, 12] complex data security issues in cloud computing however these are limited to derive from existing body of literature. Although, extensive literature survey provides complex data security issues however, there is an urgent need to understand the user's point of view in regard to data security in the cloud.

Clearly, very few research studies have employed different approaches to explore and identify the data security by understanding user's perception. Carroll et al. [13] in 2010 conducted semi-structured interview of 15 participants to explore the issues from user's point of view. On the other hand, Tanimoto et al. [14] analyse risks of utilizing cloud computing extracted from a user's viewpoint. However this study is limited to Japan.

3.1 Strategies and Countermeasures

Any kind of security and privacy violation of data in the cloud is critical and can produce dire consequences [3]. In order to overcome this problem large number of research studies have been conducted which present different strategies and countermeasures to address the data security issues. Moreover, an issue of trusting cloud is a paramount concern for most organizations. However, it is not about trusting the cloud providers' intentions, rather cloud computing's capabilities are questionable. This research study

[16] is based on the fact that the challenges of trusting cloud computing don't lie entirely in the technology alone. This study raises the concern that adoption of cloud computing came before the appropriate technologies appeared to tackle the challenges of trust. Other researches therefore conducted the similar studies in regard to trust issues. Regarding the trust issues, this study recommends to use encryption for identity and data privacy. However research study conducted by Vormetric warns that if encryption keys are not sufficiently protected, they are vulnerable to theft by malicious hackers [15]. Recently Sugumaran [28] suggested that a key is generated for set time duration then get expiry after the time duration. Finally the user updates a private key from the authority in a time intervals.

An encryption is considered as an important technique to retain control over the data in the cloud. However, encryption limits data use. In particular, searching and indexing the data becomes problematic. State-of-the-art cryptography offers new tools to solve these problems [9]. In order to understand the cryptography tools and techniques, more research needs to be done [17]. A recent study conducted by Sood [3] has taken a step forward by proposing a frame work that claims to efficiently protect the data from the beginning to the end by classifying data on three cryptographic parameters, i.e., Confidentiality, Availability and Integrity. Other researchers have attempted to propose security frame work in the past which are based on cryptography.

More recently, new research studies are emerging which are pointing to the fact that, data is not fully secured by applying cryptographic techniques. Surianarayanan and Santhanam [18] therefore, argue that security mechanisms should be applied at each level such as network level, system level, virtual machine level and application level. This study presents different policies, procedures and controls to mitigate the risks associated with each level. However, this research is limited to cloud service provider's end. Securing each level in the cloud computing is of critical importance because cloud services do pose as an attractive target to any cyber-criminal. Research study conducted by Khorshed et al. identify the most common attacks which could lead to top threats for the real world cloud implementation [19]. Moreover, this study [19] proposes a proactive threat detection model by adopting three main goals: (i) detect an attack when it happens, (ii) alert related system (system admin, data owner) about the attack type and take combating action, and (iii) analyse the pattern and generate information about the type of attack.

In order to make the cloud environment more secured, researchers are introducing multi-clouds. These research studies [20, 21] claim that multi-clouds can improve reliability, trust, and security as compared to single clouds by distributing them among multiple cloud providers.

Thus, the above mentioned literature review indicates that past research studies have been conducted in all different directions. However, users are reluctant to move their data to cloud [19]. In addition the past studies have failed to establish user's trust on cloud computing. Therefore, it is important to carry out a study on understanding the user's point of view in regard to data security concerns and issues, causes and fundamental strategies to avoid those issues.

4 A Qualitative Empirical Study on Cloud Security

This research study is conducted by a qualitative empirical study using the datasets from the open sources and in-depth literature review. The qualitative patterns from the sources are then examined to conduct a thematic analysis. This study results in presenting data security concerns, possible causes and strategies to avoid the threats.

4.1 Data Sources

The data related to cloud security is collected from open sources. We chose the sources where survey by interview approach was used.

- AccelOps, the leader in integrated Security Information and Event Management (SIEM) [22].
- Pew Research Centre's internet and American Life Project [23].
- Cloud Security Alliance (CSA) [24].

These surveys used standardized open ended questions to collect qualitative and quantitative data to better understand professionals' view on cloud security issues. The detail of the data sources is provided in Table 1. These data sources are selected due to the following reasons.

- These sources are among the cloud technology experts.
- Based on survey by interview.
- Survey results are qualitatively presented.

Table 1. Data Sources

Source	Sampling	Participants	Year
Pew research centre's	Online survey of 895 participants	Internet experts and users	2010
AccelOps	176 online and conference participants	IT security professional	2013
Cloud security alliance	Unspecified number of participants	Industry experts	2013

The interviewees in these surveys were asked several questions about different aspects of cloud computing, such as benefits, characteristics, adopters, inhibitors and security issues. Majority of question were open ended to gain detailed insight into users' perspective.

4.2 Thematic Analysis

This research study is based on thematic analysis as a data analysis method. Thematic analysis is a common method for qualitative analysis of transcripts for identifying, analysing and reporting themes or patterns within data.

This research article analyzed the survey conducted by three independent groups, resulting in an average of 350–450 participants per group. The survey finding provide some important information of how users view the cloud computing and the security in regard to their data.

Each survey was read carefully and thoroughly in order to develop the following themes (Table 2).

Table 2. Major patterns and Related Themes

Themes	Identified patterns
Major data security threats	Not trusting the cloud for data related services. Dissatisfaction with the data storage on the cloud. Negative real life examples in regard to data breach in the cloud. Reluctant to move data in to the cloud
Causes of the threat	Reasons for not trusting the cloud for data services. Possible root cause of data threats Who is responsible for the threat? Any data breach incident? If yes why? Dissatisfaction with the existing data security tools and measures
Strategies to avoid the threats	Necessary steps before moving data in the cloud. Customers' dissatisfaction with service level agreement. Who is responsible for ensuring cloud data security?

From this point, categorising of data is taken place by labelling passage of data according to what they are about. These categories are then rearranged into different themes by finding relationships between them. The occurrence of themes is seen in the following Tables 3, 4 and 5.

Table 3. Threats and their Occurrences

Major data security threats	Occurrences
Data breach	95 %
Data loss	85 %
Data unavailability	72 %
Third-party data control	69 %
Data privacy	45 %

Table 4. Causes and their occurrences

Possible causes of data security threats	Occurrences
Malicious insiders	100 %
Lack of security tools	89 %
Lack of users knowledge about the cloud environment	75 %
Lack of transparency	69 %
Weak set of interfaces	69 %
Insufficient service level agreement	50 %

Table 5. Strategies and their Occurrences

Strategies to avoid the threats	Occurrences
Risk assessment and mitigation plan	75 %
Disaster recovery and backup plan	72 %
Data encryption	85 %
Service level agreement (SLA)	55 %

Clearly, the above mentioned analysis presents the emerging themes and their occurrence in regard to data security in the cloud. Although, some other themes were emerged after the applying thematic analysis on the collected data. However, this study is focused on the themes which are presented above.

5 Identified Data Security Threats, Causes and Avoidance Strategies

At first, this section presents the key data security threats and issues that are explored and investigated from the empirical data gathered from the surveys. We then discuss the causes and the countermeasure of the identified threats and issues.

5.1 Data Security Threats and Issues

Although cloud computing may seem attractive to all the participants in the survey. According to Research firm Gartner public cloud market is expected to reach $206.6 billion in 2016 from $91.4 billion in 2011. However this much growth is only possible after addressing some security issues and challenges mentioned by the interviewees. Among those issues, this research study identifies the major data security issues and threats in the cloud. As storing, accessing and sharing company's data remotely on the internet poses great risk on the company's profile. One of the major security concerns related to cloud computing is the security of data [26]. Based on the survey reports, the main data security issues are as follows;

i. Data Breach

A data breach is an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by individual unauthorized to do so. Data breach is the most critical concern in the surveys conducted by CSA [24], AccelOps [22] and Pew Research Centre [23]. Organizations are fearful of having their information compromised. One of the respondents predicts that in 2020 the cloud will be barley in use because of data privacy. Data breaches can be embarrassing and costly. Sensitive data stored within cloud environment must be safeguarded to protect its owners and subject alike. According to [25] confidentiality of data must be ensured be the system as the large businesses like banks would not like to do the transactions through clouds which involves the interaction of another system. The identified list of the top threats published in 2010, data breach was ranked at 5th position however, and in 2013 it is ranked at number 1. Clearly, it indicates that industry professionals and experts consider the data breach as the most serious threat of the cloud environment.

ii. Data loss

Data loss is an error condition in information systems in which information is destroyed by failure or neglect in storage, transmission or processing. It is evident from the AccelOp's survey that 63 % respondents claim data loss as top-of-mind issue for security professional. It has been recognised that data is the lifeblood of a enterprise [30]. As per CSA [24] survey report data loss takes on 2nd position as compared to 5th in 2010. Mat Honan, writer for wired magazine loses all his personal data from Apple, Gmail and Twitter accounts after they have been broken by some attackers. However experts in CSA's survey report argue that in addition to malicious attackers, physical catastrophe, accidental deletion by cloud provider can lead to data loss. The risk of data lost becomes higher due to the mobile devices. As one of the respondents point out in Pew's survey that the mobile phone will be the key instrument everywhere from supermarket to school.

iii. Data Unavailability

In simple terms, availability means that resources and data are accessible and usable at all times. Availability can be affected temporarily or permanently due to many factors. A research study [26] claims that organizations are wary of cloud computing and often worry about availability, which could be jeopardized due to technical as well as non-technical reasons. However, the surveys identify the denial of service (DoS) attack as the most common threat to prevent the users to access their data. A DoS attack involves saturating the target with bogus request to prevent it from responding to legitimate request in a timely manner. As per CSA's survey, DoS attack has many forms such as Distributed denial-of-service and asymmetric application-level DoS attacks. A fear of service outages forces the customers to reconsider before moving the company's critical data to the cloud. “How do you retrieve your prized novel or your business records if the cloud fails?” warns one respondent in the survey conducted by Pew. The CSA’s survey reports indicates denial-of-service attack is at 5th position in the latest list of top security threat in cloud computing.

iv. **Third-party Data control**

It is evident from the AccelOps’s survey that over half of the respondents concern over controlling the data that is moved to the third-party in the cloud. As the data is not in the control of the owner when in the cloud, anything can be possible. Entrust your data on to a third party who is providing cloud services is an issue [29]. It is apparent from the survey’s findings that there is a lack of transparency from the provider’s side on how data flows through their services and who has access to the data. Surprisingly, in other surveys the fear of data control by third-party is not reported. It is believed by the participating professionals that cloud providers should manage the data control risks.

v. **Data privacy**

Data or information privacy is way of collecting, storing and disseminating the data legally and ethically. It is clearly evident from the surveys that potential cloud consumers are reluctant to move their valuable asset to the cloud due to privacy reasons. One individual predicts that in 2020, everyone will keep the data at in-home storage and will be available via cloud to the personal devices in order to keep the information private. The majority of respondent felt that to further accelerate the cloud adoption; providers need to ensure the data privacy and control to consumers’ sensitive data. In order to ensure the integrity of user authentication, companies need to be able to view data access logs and audit trails to verify that only authorized users are accessing the data [25].

5.2 Triggers for Data Security Threats and Issues

The second major finding of the thematic analysis is the possible causes of data security threats which are discussed below.

- Malicious insiders, those who have or had access to the sensitive information. Malicious insiders could steal sensitive information, sell the data to other parties or perform any number of other malicious activities. There are large numbers of incidents reported since 2001 about data breaches as a result of malicious insiders.
- Lack of tools and security measures at consumers end. The increased availability and use of social media, personal Webmail, and other sites can impact the security of the browser, its underlying platform, and cloud service accounts. Traditional antiviruses’ solutions and firewalls are not sufficient to protect consumers’ end.
- Lack of understanding about cloud service provider’s environment. Security is at risk if cloud consumers are unaware of cloud providers’ environment such as their hardware, software detail and VMware.
- An Organization rushes to adopt cloud technologies without trusting the providers. Lack of trust is one of the major causes of data security threats. Before selecting a cloud service provider, Organization must assess their capabilities, policies and procedures.

- Lack of transparency between the providers and the consumers. Cloud providers and consumers must maintain strong and transparent relationship between them.
- Reliance on a weak set of interfaces exposes organizations to variety of data security threats. Cloud consumers manage and interact with cloud providers using these sets of interfaces. Thus the security of the cloud services is dependent upon the security of these basic interfaces.
- Privacy rules are designed with the assumption that privacy protections are most reasonable at the ends. Privacy protection mechanisms and procedures are not fully examined before defining the privacy rules. Cloud service providers; therefore assume that both ends are privacy protected.
- Poorly designed service level agreement (SLA). The present SLAs discuss only about the services provided and the waivers given if the services do not meet the agreement. SLA has to discuss the other issues like policies, methods and their implementations.

5.3 Strategies for Avoiding the Data Security Threats

Security administrators need to decide how much time, money, and effort needs to be spent in order to develop the appropriate security policies and controls. Each organization should analyse its specific needs and determine its resource and scheduling requirements and constraints. Computer systems, environments, and organizational policies are different, making each computer security services and strategy unique. However, the principles of good security remain the same, and this document focuses on those principles.

Although a security strategy can save the organization valuable time and provide important reminders of what needs to be done, security is not a one-time activity. It is an integral part of the system lifecycle. The activities described in this document generally require either periodic updating or appropriate revision. These changes are made when configurations and other conditions and circumstances change significantly or when organizational regulations and policies require changes. This is an iterative process. It is never finished and should be revised and tested periodically. Thus, an efficient security technology is cloud computing is required to have proper secured cloud computing and to speedup cloud implementation [28].

Below is the list, in addition to the conventional approaches, of the strategies for avoiding the data security threats that we found during the empirical studies:

- Complete Risk assessment and mitigation strategies at consumers end. Organisations rush to adopt cloud technologies, therefore they avoid making plans for risk assessment and mitigations. This seems to be the first step before moving to the cloud.
- Disaster recovery and backup plan. The cloud providers must include detailed backup and disaster recovery plan. However, cloud consumers take necessary action to ensure all plans are in place.
- An organization should encrypt the data before storing it in the cloud and keep the encryption key secured. This provides confidence to the consumers that they are in control of their sensitive data.

- Consumers should look to prohibit the sharing of account credentials between users and services. Cloud computing is multitenant environment, therefore consumers must ask the providers to keep their credential detail private without sharing with others.
- Security monitoring software should be implemented by the consumers. There are many security monitoring software are available which should be implemented at the consumers end.
- Well prepared service level agreement (SLA). Avoid any jargons in the agreement.

6 Discussion of the Findings

The result presented in this research study indicate that majority of respondents believe that cloud is here to stay. However, most participants pointed that some hurdles must be crossed successfully before this latest IT paradigm gains more adopters as shown in Fig. 1. Among the other factors, the issue of security and controlling the data should be addressed first. To further accelerate adoption, cloud providers need to provide increased clarity, more transparency and better assurance about their security controls. This study is based on three different findings which are as follows;

- Most critical data threats
- Possible causes for the threats
- Fundamental strategies to avoid the threats

The above mentioned findings are analysed from the surveys conducted from 2010 to 2013 from three important groups. In the survey, respondents were asked to highlight their perspective on multiple aspects of cloud computing. However, the current study attempts to discuss three important findings in regard to data in the cloud.

Thus, with the help of the report presented in three different surveys, this study identifies five most critical threats such as data breach, data lost, third-party data control, data unavailability, and data privacy. Although CSA [24] identified nine top threats however these identified concerns and threats seem most critical to the users' community. In addition, six possible causes of these threats are analyzed in this study. Other research studies [5, 6, 10] seem to be consistent with the current findings. In 2012, 9 million records are lost as a consequence of a breach, it appears that data alone is not the only asset; company's reputation is at risk too. Thus, before a business moves its assets into the cloud, it needs to consider all the related issues.

Other major findings in the current study are the possible causes and strategies to avoid the threats. A considerable amount of literature has been published on countermeasures and strategies to protect data in the cloud. However, these research studies do not take in account the users perspectives. This can be seen in the study conducted by Morsy et al. [27] where a detail analysis of cloud security problems is presented. However their findings are from the cloud architecture, stakeholders' and delivery perspective. This study attempts to provide key features that should be covered in a security solution model. On the other hand a study [6] was carried out in Taiwan to understand IT executives and professional perspective on cloud computing. However this analysis is used to underpin the identification of the factors which encourage and prevent the cloud computing adoption.

Clearly, the previous research studies do not take into account the users' perspective about data security in the cloud. Therefore, in our research we did a deep analysis into surveys' participants' responses to identify the most critical data security concerns according to users' perspective. Moreover, this study presents the root causes and key strategies to the identified issues and concerns. As a result, with description and analysis of these data security threats, this study guides the cloud providers, users and researchers' community to take necessary actions to resolve these issues.

This is very important to gain users' trust by addressing their most critical concerns and issues. Therefore, the current research study attempts to fill this gap by analysing users' perspective in regard to dissatisfaction and hesitation for adopting cloud computing. According to [11] understanding and clearly documenting specific users' requirement is imperative in designing a solution targeting at assuring these necessities. The fact is nothing is ever 100 % secured in the real or virtual world. However by avoiding the possible causes, cloud environment can be trusted and secured. According to [10] security is considered a key requirement for cloud computing consolidation as a robust and feasible multipurpose solution.

7 Conclusion and Future Work

The research study is based on qualitative empirical research approach. In this research three different sources are used which are qualitative surveys conducted in the past three years. The current study identifies the major data security threats as per the survey results. A thematic analysis has been applied in order to develop important themes and their occurrences. Security is the crucial aspect in providing trusted environment before moving the data in the cloud. This research study identifies most critical concerns and issues in regard to data in the cloud. The result represents that data breach appears to be the most critical threat to the Organisations. It is then followed by data loss, unavailability, lack of control and privacy at the end. These issues are obstacles for trusting the cloud.

In order to find the users point of view in regard to the above mention threats, possible causes are also identified. This analysis indicates that malicious insiders should be examined and trained thoroughly in order to alleviate the concerns of the users. Furthermore, lack of tools, lack of transparency, weak set of interfaces and insufficient service level agreement contribute in triggering data security threats.

Therefore, this paper presents few fundamental strategies to avoid data security threats and providing trusted cloud adoption. According to the users point of view these strategies include detailed risk assessment, disaster recovery plan, using encryption and securing their keys and final comprehensive service level agreement.

This research study provides a detailed insight in to users' perspective in regards to data security in the cloud. Therefore, research community can increase their focus in this area in order to alleviate the users concerns about cloud computing. This work enhances our current understanding of data security in the cloud from the users' viewpoint however more research is required to understand the threats and their consequences in detail.

In the future, we are planning to conduct the interviews by recruiting selective participants. Current countermeasures will be evaluated and the most concerned areas will be examined and addressed in order to gain users trust on this latest technology of cloud computing.

References

1. Dahbur, K., Mohammad, B., Tarakji, A.B.: A survey of risks, threats and vulnerabilities in cloud computing. In: Proceedings of the 2011 International Conference on Intelligent Semantic Web-Services and Applications - ISWSA 2011, pp. 1–6 (2011)
2. Ii, J.C.R.: Who can you trust in the cloud? A review of security issues within cloud computing. In: Security, pp. 15–19 (2011)
3. Sood, S.K.: A combined approach to ensure data security in cloud computing. J. Netw. Comput. Appl. **35**(6), 1831–1838 (2012)
4. Chen, D., Zhao, H.: Data security and privacy protection issues in cloud computing. In: 2012 International Conference on Computer Science and Electronics Engineering, pp. 647–651 (2012)
5. Mell, P., Grance, T.: The NIST Definition of Cloud Computing (Draft). Recommendations of the National Institute of Standards and Technology, p. 145
6. Lin, A., Chen, N.-C.: Cloud computing as an innovation: percepetion, attitude, and adoption. Int. J. Inf. Manage. **32**, 533–540 (2012)
7. Linthicum, D.S.: Cloud Computing and SOA Convergence in Your Enterprise. A Step-by-Step Guide. Addition Wesley Professional, Boston (2009)
8. Blum, D., Watson, R., Creese, G., Blakley, B., Haddad, C., Howard, C., Manes, A.T., Passmore, D., Lewis, J.: Cloud computing: transforming IT, pp. 1–51 (2009)
9. Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R., Molina, J.: Controlling data in the cloud: outsourcing computation without outsourcing control, pp. 85–90 (2009)
10. Mogre, P.V., Agarwal, G., Patil, P.: Data security and its technique in cloud storage-a review, vol. 1, pp. 1–5 (2012)
11. Zissis, D., Lekkas, D.: Addressing cloud computing security issues. Futur. Gener. Comput. Syst. **28**, 583–592 (2012)
12. Wang, C., Member, S., Wang, Q.: toward secure and dependable storage services in cloud computing. **5**, 220–232 (2012)
13. Carroll, M., Merwe, A., Van Der Kotzé, P.: Secure cloud computing benefits, risks and controls, vol. 12, pp. 12–14 (2012)
14. Tanimoto, S., Hiramoto, M., Iwashita, M., Sato, H., Kanai, A.: Risk management on the security problem in cloud computing. In: 2011 First ACIS/JNU International Conference on Computer Networks, Systems and Industrial Engineers, pp. 147–152 (2011)
15. Khan, K.M., Malluhi, Q.: Establishing trust in cloud computing (2010)
16. Information, P.B., Public, I.N., Environments, H.C.: Data security in the cloud, pp. 1–4 (2012)
17. Ryan, M.D.: Cloud computing security: the scientific challenge, and a survey of solutions. J. Syst. Softw. (2013)
18. Surianarayanan, S., Santhanam, T.: Security issues and control mechanisms in cloud. In: 2012 International Conference on Cloud Computer Technologies, Applications and Management, pp. 74–76 (2012)
19. Khorshed, M.T., Ali, A.S., Wasimi, S.A.: A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. Futur. Gener. Comput. Syst. **28**, 833–851 (2012)

20. AlZain, M., Pardede, E., Soh, B., Thom, J.: Cloud computing security: from single to multi-clouds. In: 2012 45th Hawaii International Conference on System Science, pp. 5490–5499 (2012)
21. Cachin, C., Haas, R., Vukolic, M.: Dependable storage in the Intercloud: Research Report RZ, 37–83 (2010)
22. Manage, E.: AccelOps Cloud SeCurity Survey 2013. www.accelops.com/cloudsurvey2013 (2013)
23. Anderson, J.Q.: The Future of Cloud Computing, pp. 1–26. www.northbridge.com/2010 (2010)
24. Threats, T., Group, W.: The Notorious Nine Cloud Computing Top Threats in 2013. https://downloads.cloudsecurityalliance.org/…/top_threats/ (2013)
25. Kumar, K., Rao, V., Rao, S., Technology, I.: Cloud computing: an analysis of its challenges & security issues, vol. 1 (2012)
26. Sinha, N., Khreisat, L.: Cloud computing security, data, and performance issues, pp. 1–6 (2014)
27. Al Morsy, M., Grundy, J., Müller, I.: An analysis of the cloud computing security problem (2010)
28. Science, C., Lanka, S.: Data security in cloud computing, pp. 810–813 (2013)
29. Sugumaran, M.: An architecture for data security in cloud computing (2014)
30. Technologies, C.: Data security issues in cloud environment and solutions (2014)