Cloud Computing Risk Assessment: A Systematic Literature Review

Chapter *in* Lecture Notes in Electrical Engineering · January 2014

DOI: 10.1007/978-3-642-40861-8_42

4 authors, including:

Rabia Latif
National University of Sciences and Technology
12 PUBLICATIONS **57** CITATIONS
SEE PROFILE

Haider Abbas
Center of Excellence in Information Assuranc…
62 PUBLICATIONS **193** CITATIONS
SEE PROFILE

Saïd Assar
Telecom Ecole de Management
78 PUBLICATIONS **286** CITATIONS
SEE PROFILE

Cloud Computing Risk Assessment: A Systematic Literature Review

Rabia Latif[1], Haider Abbas[1,2], Saïd Assar[3], and Qasim Ali[1]

[1] National University of Sciences & Technology, Islamabad, Pakistan
rabiya_128@yahoo.com
[2] Centre of Excellence in Information Assurance (COEIA),
King Saud University, Riyadh, Saudi Arabia
hsiddiqui@ksu.edu.sa, haidera@kth.se
[3] Institut Mines-Télécom, Telecom Ecole de Management
Information System Departement, France
said.assar@it-sudparis.eu

Abstract. Cloud computing security is a broad research domain with a large number of concerns, ranging from protecting hardware and platform technologies to protecting clouds data and resource access (through different end- user devices). Although the advantages of cloud computing are tremendous, the security and privacy concerns of cloud computing have always been the focus of numerous cloud customers and impediment to its widespread adaptation by businesses and organizations. The paper presents a systematic literature review in the field of cloud computing with a focus on risk assessment. This would help future research and cloud users/business organizations to have an overview of the risk factors in a cloud environment. And to proactively map their indigenous needs with this technology.

1 Introduction

Cloud computing has gained considerable attention in the scientific community. Cloud computing is 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 [1]. This definition describes cloud computing as having five characteristics i.e., on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. Although there are many benefits to adopting cloud computing, there are also significant barriers to adoption. One of the most significant barrier to adoption is security [2]. As cloud computing represents a relatively new computing paradigm, therefore the most important concern is its security from both the perspective of cloud customer and Cloud Service Provider (CSP). Migrating critical applications and sensitive data to cloud environment is of great concern for organizations that are moving beyond their data centers. To mitigate these concerns, a CSP must ensure that customers will continue to have the same security and privacy controls over their applications and services and provide evidence to customers that their organization are secure and they can meet their service

James J. (Jong Hyuk) Park et al. (eds.), *Future Information Technology*,
Lecture Notes in Electrical Engineering 276,
DOI: 10.1007/978-3-642-40861-8_42,

level agreements [3]. Since the emergence of cloud computing in 2006, a lot of review papers based on cloud computing are available in the current literature but to date no systematic review of cloud computing risks has been published. Therefore, the primary goal of this research is to systematically select and review published research work and provide an overview of risk analysis, risk severity and impact of these risks on cloud users and providers.

The structure of the paper proceeds as follows: Section 2 presents the research methodology. Section 3 presents the overview of data concerning the reviewed studies. Section 4 gives the detailed description of the reviewed papers. Section 5 shows the analysis of the systematic review, and finally the conclusion is presented in section 6.

2 Research Methodology

The proposed research uses a systematic review methodology [4,5] to review existing literature concerning cloud computing security risks, vulnerabilities and threats.

2.1 Research Questions

In this phase, the review process is planned and research questions were identified. The following research questions are addressed in this study: **RQ1.** What are the risks associated with cloud computing from cloud customer's perspective? **RQ2.** What are the risks associated with cloud computing from cloud Provider's perspective?

2.2 Defining the Review Protocol

After the selection of the research question, a set of search terms called keywords was extracted. The keyword and relevant initiatives that make up research question and that were used during review protocol are: risk assessment, risk analysis, systematic literature review, cloud computing security, cloud vulnerabilities and cloud threats. To perform a systematic literature review, the primary research focus is from Springer Link, Elsevier, Science Direct, ACM, DBLP and IEEE digital library. The research was narrowed down through the set of *inclusion and exclusion criteria*. Only full papers in English from peer- reviewed articles, journals and conference proceeding on the specified topic, published from 2009 to 2013 were considered. A *quality assessment checklist* (QAC) is developed to assess the individual studies. The *QAC* is prepared based on kitchenham [4]. The Checklist includes the following questions: a) Does the research paper clearly specify the research methodology? (b) Is the research methodology appropriate for the problem under consideration? (c) Are the analysis of study properly done? If the study fulfills assessment criteria then it is filled with 'yes'.

2.3 Data Extraction and Synthesis

We identified a total of 100 studies. After filtering these studies according to inclusion/ exclusion criteria and QAC, 31 publications were identified as a primary study

for review [6-37]. These included journals (15), conference proceedings (11), white papers (3) and articles (2). The year of publication of the papers is shown in Fig. 1. Fig. 2 shows the distribution of papers in relation to the research questions (RQ).

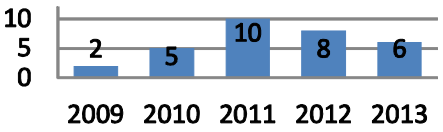

Fig. 1. Paper distribution over publication year

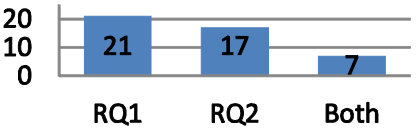

Fig. 2. Paper distribution in relation to RQ

3 Results

The detailed analysis of the selected studies was based on their similarities in terms of the risk analysis in cloud computing. According to the reviewed publication and to answer the research questions we identified five main categories of risks associated with cloud computing both from cloud provider and customer perspective. These categories include: Organizational, Technological, Data Security and Privacy, physical security and Compliance. Fig. 3 shows risk categories along with their sub-categories. We elaborate these categories in the subsequent section from both cloud providers and customer's perspective.

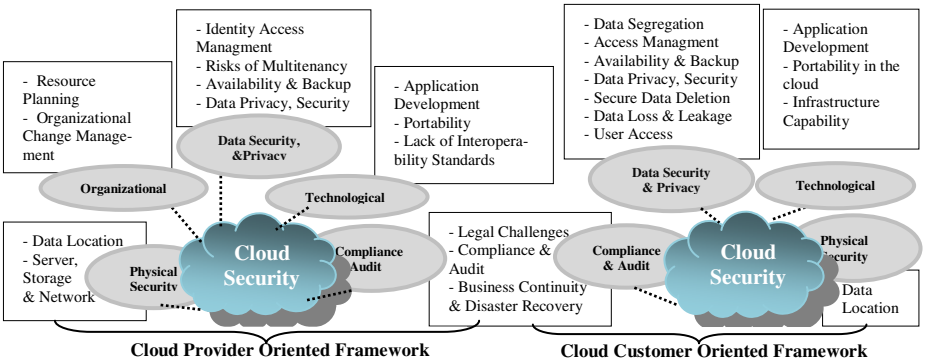

Fig. 3. Cloud Security Risk Categories and sub- Categories

The results of the systematic review are given in Table 1.

Table 1. Summary of the risks considered in each approach

Cloud Provider Risks	List of Studies
Data Security & Privacy	[7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [22]
Technological	[7], [8], [19], [21], [22]
Physical Security	[25], [26]
Organizational	[10], [22], [29]
Compliance and Audit	[20], [23], [24]

Cloud Customer Risks	List of Studies
Data Security & Privacy	[12], [16], [20], [24], [25], [27], [30], [31], [32], [37],
Technological	[10], [22], [33]
Physical Security	[22], [35]
Compliance and Audit	[28], [30], [34], [38]

3.1 RQ1: Risks from Cloud Providers Perspective

1. Data Security, Privacy & Control Risks

Data security and privacy risks are mitigated through data encryption and it is the CSP responsibility to handle these rudimentary risks [6]. To ensure data integrity, confidentiality and availability, the storage provider should offer encryption schema and scheduled data backups [7]. CSP is responsible to adopt added security measures to ensure data security. These security measures involve the use of strong encryption techniques for data security and fine-grained authorization to control user access to data [8]. Providers are more responsible for the privacy and security of data and application services in public than in private clouds [9]. The major problem with data encryption is the responsibility of key management. Ideally, it's the data owners. But due to the lack of user expertise to handle the keys, they usually hand over the key management to CSP. But again it will become more difficult for CSP to maintain keys for a large number of users [10, 11]. CSP is the one responsible for the security of the data while is being processed, transferred and stored [12]. CSP does not have permission for access to the physical security system of data centers rather they must depend on the infrastructure provider to get full data security. The CSP can only specify the security settings remotely, and don't know either they are fully implemented or not. It is major security risks for CSP if the security settings are not fully implemented [13].

— Identity and Access Management (IAM)

IAM improves operational efficiency, regulatory compliance by managing the major security concerns, automated provisioning, authentication and authorization services. Devki solves this issue by using various techniques such as single sign-on, federated identity, access control list, directory based service, access on the basis of attributes [21]. To avoid unauthorized access, the CSP should offer strict access control mechanism. In cloud computing administrative access is done through the internet and this increases the risk of unauthorized access to data and resources. Therefore, it is very important to control and monitor the administrative access to maintain protocols [7]. Data in the cloud is globally distributed which brings the issue of jurisdiction and privacy [11]. According to study only 37% of cloud providers were confident about security to authenticate users before granting access, whereas 50% of cloud users considered IAM as the cloud provider's responsibility. Therefore, achieving compliance requirements could be problematic [15]. According to [14], when the data is outsourced to a cloud, enforcing secure and reliable data access between several users is very critical. The user cannot even trust the server because the user's private data can be exposed in the event of server compromise. The solution is to encrypt data in differentiated manner and disclose the corresponding decryption keys only to authorized users. This approach has a drawback of performance loss and scalability [16]. Gartner list seven security issues from CSP perspective. The data security and privacy risks include privileged user access, which inquires about who has access to data [17].

— Multi-tenancy

Multi-tenancy is an essential attribute of cloud computing as it increases the use of underlying hardware resources and allowing for efficient resource provisioning.

Multi-tenancy security and privacy is one of the critical challenges for the public cloud [16]. It is the responsibility of CSP to ensure an isolated boundary for each user's data at both physical and application levels [8]. It is possible that the customers' personal and financial data are stored by the CSP. Therefore, CSP is responsible to secure the customers' data. Some providers use job scheduling and resource management, but most providers employ Virtualization to maximize the use of hardware [18]. These two methods allow attackers to have full access to the host and cross- VM side channel attacks to extract information from a target VM on the same machine. In multi-tenancy, data from multiple tenants is likely to be stored in the same database, the risk of data leakage between these tenants is high [12]. Data is placed in a shared environment with the data from other clients which poses a great risk of multi-tenancy for CSP. There is a need for some mechanism through which CSP must guarantee data isolation between clients and they also should be liable for ensuring this isolation[19].

— Data Availability and Backup

It is difficult for CSP to guarantee adequate availability and backup of data in the cloud because the data are hosted distantly in the cloud. Therefore it is not only difficult to backup the data but also to recover the data in case of failure [18]. In the cloud environment, there are several areas that will threat the data availability including the availability of cloud computing services, whether the cloud providers would continue to operate in the future? whether the cloud storage services provide backup? [10]

2. Organizational Risks

Organizational risks are categorized are categorized as the risks that may impact the structure of the organization or the business as an entity. These risks include the loss of business reputation and any organizational change that can happen to the CSP and cause the provider's failure, termination of the acquisition [28].

— Organizational Change Management

Resistance to change consequent from organizational politics, changes to people work is a major organizational risk. To mitigate this, use insight from organizational change management and involve key stakeholders in the adoption procedure [21].

— Resource Planning

According to Hosseini et al. [21], the risk to resource planning is the loss of control over resources, which lead to ambiguous roles and responsibilities. To overcome this, it is essential to clarify roles and responsibilities before cloud adoption.

— Organizational Security Management

The existing security management models have considerably changed when enterprises adopt cloud. There is a need to reevaluate the existing security models and develop security standards to ensure the deployment and adoption of secure clouds [9].

3. Technical Risks

Technical risks are defined as the failures associated with the technologies and services provided by the CSP, including resource sharing isolation problems, malicious attacks on the CSP risks related to portability and interoperability [20]. Technical

risks are related to hardware including poor maintenance of hardware, unresponsive system, reduction in the availability and hardware failure [6].

— Portability in the Cloud

Interoperability between clouds are due to incompatibilities between CSP platforms. The solution is to use cloud middleware for the ease of cloud interoperability [21].

— Application Development

Risk of service interruption at providers side results in extensive outages and unavailability of services or loss of data. The solution suggested by the authors is to use multiple cloud providers and monitor applications from outside the cloud [21].

— Lack of Interoperability Standards

Cloud computing lacks interoperability standards. There is no standard of communication and data export format between and within CSP, which makes it difficult to establish appropriate security frameworks [18]. For CSP, adoption of universal standards is also recommended to ensure interoperability among CSP [7].

4. Compliance and Audit

Risks related to lack of jurisdiction information, changes in jurisdiction, illegal clauses in the contract and ongoing legal dispute. It is the responsibility of both CSP and customer to abide by the rules and regulation defined in the contract and audit SLAs regularly [22]. Traditional CSP is subjected to external audits and security certifications. If a CSP does not adhere to these security audits, then it leads to an obvious decrease in customer trust [23]. CSP should have security policies with recovery methods in case of disasters and the ability to restore data completely in a pre-established amount of time [19].

5. Physical Security

— Data Location and Data Center

CSP should guarantee secure operation of the cloud data center in order to provide a secure physical location for customers' data [24]. CSP manages the infrastructure including servers, networks, storage devices. CSP should implement and operate appropriate infrastructure controls including staff training, physical location security, network firewalls. To overcome these risks are of utmost importance because if the physical access control is weak, attackers can steal entire servers, even if they are protected by firewalls and encryption [24]. The cloud provider is not only responsible to store and process data in specific jurisdictions but should also responsible to obey the privacy regulations of those jurisdictions [25].

3.2 RQ2: Risks from Cloud Customer Perspective

1. Data Security, Privacy & Control Risks

— User Access

The customer is fully responsible for the management of all software security controls. These include application access control, IAM, software patching, viruses

protection [24]. One of the risks is how a customer face the privileged status of CSP and security issues such as fault elimination, data damage and data migration [26].

— Data Privacy and Security

It is an essential security concern for the end- users to know about the privacy and protection of their data from CSP in order to ensure that data privacy is not compromised. But eventually the customers are responsible for the security and integrity of their own data even it resides on providers premises [15]. The loss of encryption key or privileged access code will bring serious problem to cloud service users [36]. Accordingly, lack of cryptographic management information will heavily lead sensitive damages of data loss, and unexpected leakage of user data to the outside world. Customer data and commercial secrets should not be leaked while residing on CSP premises [24]. According to CSA group [30], the burden of avoiding data loss does not fall completely on the provider's shoulder. If a customer encrypts data before placing it to the cloud, and lost the encryption key, the data will be lost as well.

— Data Segregation

It is the responsibility of cloud customer to find out the techniques used by the provider to segregate the data and must ensure that the encryption schemes are deployed and are effective enough to provide security [29]. Encryption cannot be assumed as the single solution for data segregation problem. In some cases, customers may not want to encrypt data because encryption accident can destroy the data [23].

— Data Availability

When the client data is uploaded into the cloud, clients no longer possess any data on the cloud. Customers personal data and information on the Cloud in not available either lost or heck, it is difficult to retrieve the original data [31].

— Secure Data Deletion

Appropriate, error free and timely data deletion may be impossible and undesirable. One of the reasons is the extra copies of data reside at different locations and the other is that the disk to be destroyed also contain data from other clients [19]. Data is supposed to be destroyed completely, when it is no longer required. But due to the physical characteristics of storage medium, the data deleted may still exist and can be restored. This may cause a risk of sensitive data disclosure to the customer [11].

6. Technical Risks

— Infrastructure Capabilities

It is difficult to show CSP that their cloud performance is not in accordance with their agreed SLA because of the server's workload and variable nature of the network. This cause disputes and litigation. The solution is to evaluate the cloud performance under appropriate investigation before adopting. Another solution is to use third party monitoring tools for the verification of system performance [21].

— Application Development

The purpose is to allow developers to develop their applications over the provided platform. Therefore, the customers are mainly responsible for protecting their

developed applications and the platform. At the same time, the providers are responsible for isolating the customers applications and development environments [9].

— Portability

According to K. Popovic and Z. Hocenski [32], the risk of compatibility arises if the customer wants to move from one provider to the other because the storage services offered by one CSP may be incompatible with another provider's service.

7. Compliance and Audit

— Disaster Recovery

Cloud Customer should know what will happen to their data if a disaster occurs. Therefore, it is the customers primary security responsibility to ask whether the provider will be able to completely recover your data and how long it will take. [29]

— Legal Challenges

CSP is more susceptible to legal and regulatory concerns and commit to keep and process customers' data in specific jurisdictions that provides security and privacy of data as promised in their SLA's. Even then, the organizations are mainly responsible for the privacy of their data kept at the CSP site [33]. The computer processing power or storage one buys via a Cloud service may be based in another country or may be divided between multiple countries. Despite the advantages of cost and efficiency, it raises legal issues by exporting customer's data abroad [27,37].

8. Physical Security

— Data Location

As the data is stored redundantly in multiple physical locations by the CSP and that location information is not revealed to the customer. On the customer side, it is difficult to determine whether appropriate security measures are in place to secure customers' data [21]. The customer cannot avoid the downtime of a cloud computing environment, which is the time in which the CSP machines are not working properly. This situation brings immense discourage to the confidence of customers [34].

4 Discussion And Analysis

The aim of the proposed research is to thoroughly examine the selected papers and identify the security risks. Customer's thought that once the customer organization relinquish cloud computing responsibility to a CSP, all the security would now be the responsibility of the CSP. But it is equally important that how the customer data is moving outwards from the customer's organization. Before adopting cloud computing, risk management policies and mechanisms need to be developed and properly formulated [35]. In Table 2, we suggest the possible security measures that help in mitigating the identified risks to some extent. The risks related to cloud provider are represented as (CP) and the risks related to cloud customer are represented as (CC).

Table 2. Risks and Suggested Security Measures

	RISKS	SECURITY MEASURES
Data Security & Privacy	Ensure availability of customer's data in cloud (CP)	Specific security measures have been taken by CSP to prevent outages and attacks
	Risks related to data security and privacy (CP), (CC)	• To mitigate these risks is using APIs to implement a robust access control, using encryption to protect data traffic. • Analyze that data is protected during design time, as during run-time. • Provide effective mechanisms for key generation, storage, and destruction of data
	Preventing unauthorized access to customer's data in the cloud (CP), (CC)	Can be resolved by implementing Management, authentication and authorization techniques on both customer and provider's sides
	Risks related to multi- tenancy (CP)	CSP should use effective encryption methods to guarantee data isolation between clients.
	Risks related to data deletion (CP)	The provider should define policies to establish procedures for the destruction of persistent media before throwing it out.
Tech-nology	Lack of standardized technology in the cloud computing system (CC)	The customer should ensure if the provider uses standardized technology and it should be mentioned in its initial contract.
	Compatibility issue between cloud and IT systems in customer's organization (CC)	The solution is to use the hybrid cloud, which is capable of handling much of these compatibility issues
Organi-zational	Risks related to Resource Planning, Change Management (CC)	Involves stakeholders in cloud adoption procedures
	Risks related security management (CC)	Reevaluate existing security standards before cloud adoption.
Physical Security	The physical security of a cloud provider's data centers composed of servers, storage and network devices. (CP)	Cloud providers must have certain policies and procedures in place to prevent physical security breaches these includes physical location security like alarms, CCTV cameras etc.
Compliance	Enforce regulatory obligations in a cloud environment. (CP)	• CSP must abide by all the regulations within a country, regarding cloud security. These regulations include HIPPA, FISMA • CSP has to contend with the Legal Systems under different Jurisdictions with not so much of visibility as to where the Data resides and how it is routed by passing through different Legal Jurisdictions.
	Business Continuity and Disaster Recovery (CP)	Recommends replicating data across multiple infrastructures to avoid vulnerabilities in the event of a major failure

5 Conclusion

The main objective of the SLR presented in this paper is to categorize risks related to cloud computing paradigm. We have followed the SLR methodology depicted in [5] to identify 31 primary studies out of 100 papers. Our analysis is concerned with both service provider and consumer in cloud computing. The review and analysis of the selected studies identify a number of challenges and indicates that there is still enormous opportunities for researchers to contribute in this area. Some topics such as data security and privacy are widely investigated, while others, e.g. physical and organizational security, have received less attention. The framework we have proposed contributes to organize the available knowledge and indicates future research directions.

References

1. Rebollo, O., Mellado, D.: Systematic Review of Information Security Governance Frameworks in the Cloud Computing. Journal of Universal Computer Sc. 18(6), 798–815 (2012)
2. From hype to future: KPMG's 2010 Cloud Computing survey, http://www.techrepublic.com/whitepapers/fromhype-to-futurekpmgs-2010-cloud-computing-survey/2384291

3. Rittinghouse, J., Ransome, J.: Security in the Cloud: Cloud Computing. Implementation, Management, and Security, 1st edn. CRC Press (2009)
4. Hannay, J.E., Sjøberg, D.I.K.: A Systematic Review of Theory Use in Software Engineering Experiments. Journal of IEEE Transaction on Software Engineering 33(2), 87–107 (2007)
5. Kitchenham, B., Brereton, O.P.: Systematic literature reviews in software engineering –A systematic literature review. Journal: Information and Software Technology, 7-15 (2009)
6. Djemame, K., Armstrong, D.: Risk Assessment Framework and Software Toolkit for Cloud Service Ecosystems. In: Int. Conference on Cloud Computing, GRIDs, and Virtualization (2011)
7. Harauz, J., Kauifman, M., Potter, B.: Data Security in the world of cloud computing. IEEE Security & Privacy 7(4), 61–64 (2009)
8. Subashini, S., Kavitha, V.: A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications 34(1), 1–11 (2011)
9. Takabi, H., Joshi, J.B.D.: Security and Privacy Challenges in Cloud Computing Environments. Published. IEEE Security and Privacy 8(6), 24–31 (2010)
10. Chen, D., Zhao, H.: Data Security and Privacy Protection Issues in Cloud Computing. In: Int. Conference on Computer Science and Electronics Engineering, pp. 647–651 (2012)
11. Rahul, S.S., Rai, J.K.: Security & Privacy Issues In Cloud Computing. International Journal of Engineering Research & Technology (IJERT) 2(3) (March 2013)
12. Hashizume, K., Rosado, D.G., Medina, E.F., Fernandez, E.: An analysis of security issues for cloud computing. Journal of Internet Services and Applications 4(5) (2013)
13. Reddy, V.K., Thirumala, R.B., Reddy, L.S.S., Kiran, S.: Research Issues in Cloud Computing. Global Journal of Computer Science and Technology 11(11) (July 2011)
14. Pal, D., Krishna, R., Srivastava, P., Kumar, S.: A Novel Open Security Framework for Cloud Computing. Int. Journal of Cloud Computing and Services Science 1(2) (2012)
15. Argall, K.: Compliance in a Cloud Computing Environment. HIPAA and PCI DSS (2010)
16. Ren, K., Wang, C., Wang, Q.: Security Challenges for the Public Cloud. Journal of Internet Computing IEEE 16(1) (2012)
17. Lovell, R.: White Paper: Introduction to cloud computing (October 2009)
18. Pearson, S., Benameur, A.: Privacy, Security and Trust Issues Arising from Cloud Computing. In: 2nd Int Conference on Cloud Computing Technology and Science (2010)
19. Ayala, L.C., Vega, M., Vargas, L.M.: Emerging Threats, Risk and Attacks in Distributed Systems: Cloud Computing. In: Elleithy, K., Sobh, T. (eds.) Innovations and Advances in Computer, Information, Systems Sciences, and Engineering. LNEE, vol. 152, pp. 37–52. Springer, Heidelberg (2013)
20. Rana, S., Joshi, P.K.: Risk Analysis in Web Applications by Using Cloud Computing. International Journal of Multidisciplinary Research 2 (January 2012)
21. Khajeh- Hosseini, A., Sommerville, I., Bogaerts, J., Teregowda, P.: Decision Support Tools for Cloud Migration in the Enterprise. In: IEEE CLOUD 2011 (November 2011)
22. Chou, Y., Oetting, J.: Risk Assessment for Cloud-Based IT Systems. International Journal of Grid and High Performance Computing, 1–13 (April -June 2011)
23. Kumar, V., Swetha, M.S.: Cloud Computing: Towards Case Study of Data Security Mechanisms. International Journal of Advanced Technology & Engineering Research 2(4) (2012)
24. Julisch, K., Hall, M.: Security and Control in the Cloud. Information Security Journal: A Global Perspective, 299–309 (2010)
25. Kumar, A.: World of Cloud Computing & Security. International Journal of Cloud Computing and Services Science (IJ-CLOSER) 1(2) (June 2012)

26. Che, J., Duan, Y., Zhang, T.: Study on the Security Models and strategies of cloud Computing. In: Proc: Int Conference on Power Electronics and Engineering Application (2011)
27. Prasad, M., Naik, R., Bapuji, V.: Cloud Computing: Research Issues and Implications. International Journal of Cloud Computing and Services Science 2(2), 134–140 (2013)
28. Dahbur, K., Mohammad, B.: A Survey of Risks, Threats and Vulnerabilities in Cloud Computing. In: Int Conference on Intelligent Semantic Web-Services and Applications (2011)
29. Bisong, A., Rahman, S.M.: An Overview of the Security Concerns in Enterprise Cloud Computing. International Journal of Network Security & its Applications 3(1) (January 2011)
30. Cloud Security Alliance CSA: The Notorious Nine Cloud Computing Threats 2013 (2013)
31. Ahmad, T., Amanul, H.M., Al-Nafjan, M., Ansari, A.: Development of Cloud Computing and Security Issues. Information and Knowledge Management 3(1) (2013), http://www.iiste.org
32. Popović, K., Hocenski, Ž.: Cloud computing security issues and challenges. MIPRO (2010)
33. Jansen, W., Grance, T.: Guidelines on Security and Privacy in Cloud Computing. NIST (2011)
34. Peiyu, L., Dong, L.: Risk Assessment Model for Information System in Cloud Computing Environment. Advanced in Control Engineering and Information Science. V. 15 (2011)
35. Rosado, D.R., Gomez, R.D., Mellado, Medina, E.F.: Security Analysis in the Migration to Cloud Environment. Journal: Future Internet, 469–487 (May 2012)
36. Lee, K.: Security Threats in Cloud Computing Environments. International Journal of Security and Applications 6(4) (October 2012)
37. Sharma, M., Bansal, H., Sharma, A.K.: Cloud Computing: Different Approach & Security Challenge. International Journal of Soft Computing and Engineering 2(1) (March 2012)