International Journal of Management, IT & Engineering
Vol. 9 Issue 9, September 2019,
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Cloud computing and its Security issues: An instance-based study and it's solution.

Fakhruddin Khan

Abstract

Cloud computing is an Internet-based computing, where shared resources, software and information, are provided to computers and devices on-demand. Since cloud computing uses distributed resources in open environment, thus it is important to provide the security and trust to share the data for developing cloud computing applications. Despite all kinds of risk, cloud computing users increasing rapidly. In this article, two points is of our concern. In the very first part we discussed about cloud computing and their issues providing multi-cloud security and its benefits and highlight their challenges and future research directions. This aims to understand the current trend in terms of complexity and strength of a secured solution and provide some insights of what is still left in such area of research. Second part of my work aims to provide some of the solutions for cloud security and reduce risks that affect the cloud computing users.

Keywords:

Multi-clouds,
single clouds,
data privacy,
data integrity,
cloud security,
malicious insider,
Iaas, PaaS, SaaS,
RaaS, cloud architectures

Author correspondence:

Assistant Professor,
Department of IT &Management,
Amity University Patna
E-mail: fkhan@ptn.amity.edu

Introduction:

1950, the era when new concepts of computing come into existence with the implementation of mainframe computers. Since then, cloud computing has been evolved from static clients to dynamic ones from software to services. Cloud computing is quickly becoming the standard way for technology companies to access IT infrastructure, software and hardware resources. This technology helps companies and organizations to be able to use applications and other resources managed by third party companies that are stored in high-end server computers and networks. Cloud computing methods are mainly set up for business or research purposes. Companies uses cloud computing to increase their IT functionality or capacity without investing in additional training or set up new infrastructure. In 21st century, cloud is the main source of storage of data in all aspects, it includes the private data or organizational data, or the different kind of software provided by developer companies. The evolution of cloud computing varies between 1950's to 2000's and after it blasts and became known to everyone, whether he belongs to the same domain or not.

Mainframe computers	Rise of the PC (Personal computers)	Client- server architecture	Hosted Environment	Cloud computing
• Automation phase • Localized Infrastructure	• Demand of PC increases • Decentralized computing starts • Birth of IT service industry	• VPN offered • Demand of high bandwidth • Dot com revolution	• IT infrastructure management outsourcing • Virtualization increases	• Emergence of as a service • Delivery of IaaS, PaaS, SaaS, NaaS • Collaborative computing • Utility computing model
1950's	1960's	1990's	2000's	Beyond 2000

The following table explains the evolution of cloud computing:

Cloud computing consists of three distinct types of computing services delivered remotely to clients via the internet. Clients typically pay a monthly or yearly service charges to the service providers, to gain access to systems that deliver software as a service [SaaS], platforms as a service [PaaS] and infrastructure as a service [IaaS] to subscribers. Clients who subscribe to cloud computing services can gain a variety of benefits, depending on their business needs at a given point in time. The days of large capital investments in software and IT infrastructure are now a thing of the past for any enterprise that chooses to adopt the cloud computing model for procurement of IT services. The companies subscribed to gain IT services reap best service at low cost without any software or hardware installed for the purpose.

Cloud services are mainly classified into three categories which are defined for security purpose and it is called cloud deployment model. These are private cloud, public cloud and hybrid cloud. Hybrid cloud is a cloud computing environment that uses a mix of on-premises, private cloud and third-party, public cloud services with orchestration between the two platforms. By allowing workloads to move between private and public clouds as computing needs and costs change, hybrid cloud gives businesses greater flexibility and more data deployment options. Its expansion is up to large extent.

Cloud service deployment approaches:

Basic models of the service adopted by cloud computing service providers are: SaaS, PaaS and IaaS. Basic segments of the cloud Formation modelling are backend stages and front-end stages. Back end stage contained the servers and information stockpiling while front end stage typically contains thin client, fat client, zero client and portable per Subcomponent includes the presence of intranet, web and intra cloud. So, the cloud information stockpiling and collaboration gets to be conceivable through virtual interactive sessions and applications. For example, middleware and programming and software component, administration and services, cloud resources, and geographical locations.

1. Infrastructure as a Service [IaaS]

IaaS is the lowest level of cloud solution and refers to cloud-based computing infrastructure as a fully-outsourced service. An IaaS provider will deliver pre-installed and configured hardware or software through a virtualized interface. What types of services used by customer depends upon their service provider and customer use. Some of the web hosting company is an IaaS provider. Some of the major players offering IaaS are Google, IBM, Rackspace Cloud Servers, Amazon EC2 and Verizon. Various benefits associated with IaaS like it reduces total cost of ownership and capital expenditure.

2. Platform as a Service [PaaS]

PaaS cloud computing is like IaaS but is more advanced. PaaS providers offer a fully configured sandbox and deployment environment for customers to develop, test and deploy their cloud applications. Examples of PaaS, the leading PaaS vendors include Amazon Web Services, Microsoft Azure, IBM and Google Cloud Platform.

3. Software as a Service [SaaS]

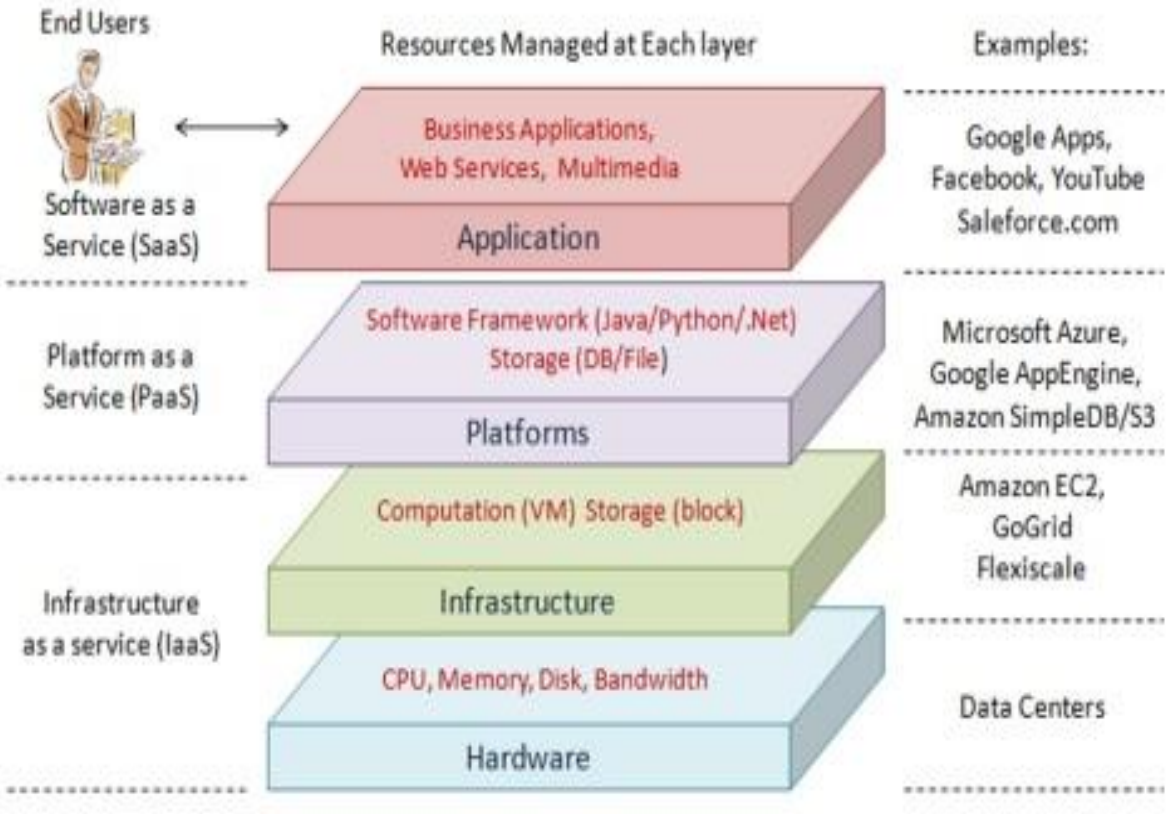
SaaS providers provide fully functionally web-based applications on demand to customers. These applications are used at business users and can include web conferencing, ERP, CRM, Email, time management, project tracking among others. Well known examples of SaaS includes Salesforce.com, Microsoft Office 365, Google G Suite, Dropbox, Adobe Creative Cloud and others

4. Recovery as a Service [RaaS]

Recovery is the process of getting back data if deleted or misplaced as a Service. RaaS solutions helps companies to replace their backup, archiving, disaster recovery and business continuity solutions in a single, integrated platform. RaaS is also referred to as

DRaaS means Disaster Recovery as a Service, Example of companies doing RaaS is Geminare, WindStream Business.

The models of different services can be understood by the following graphical architectural layers of cloud computing representation. Different layers show end users and their resource models at each layers and related examples.



*

Advantages of Cloud Services:

Cloud service is very easy to install and use for your required purpose. It only takes you a very small time to set up a cloud service application with its robust features. It costs a very few amounts per seat per month. You can access the cloud service from any computing device attached to the internet including Desktop, smartphones, tablets and laptops. It can be accessed from anywhere; home, at the airport, at the office, etc. As the company grows, one can increase his subscription and resource requirements. Companies that adopt cloud services usually benefit from improved efficiency and lower costs.

Adaptation of organizations to store their large amount of data in an efficient way without worrying about acceding their storage limits, Cloud computing storing and accessing data

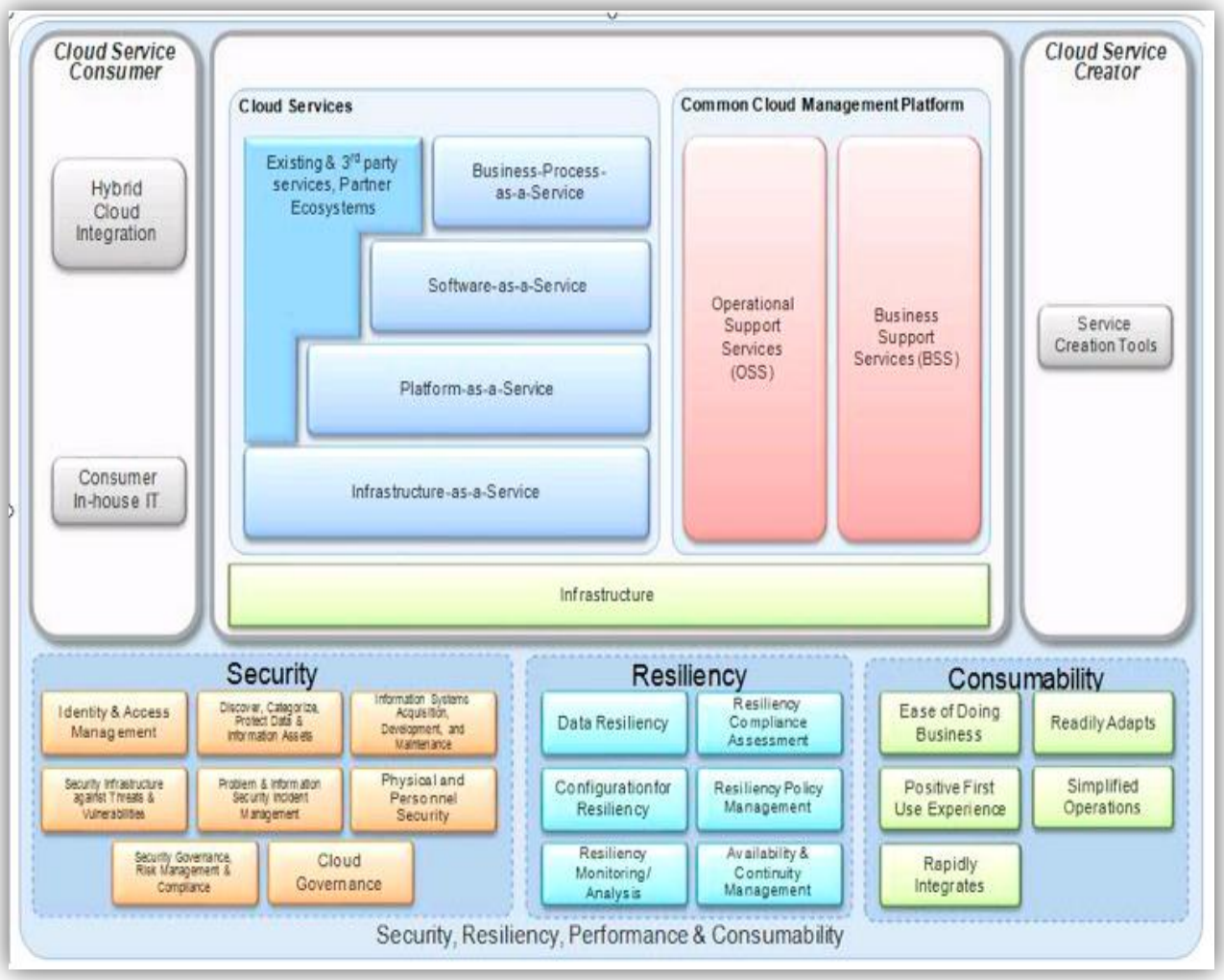
* This figure was uploaded by Anurag Jain. https://www.researchgate.net/publication/264435521_Survey_Paper_on_Cloud_Computing/figures?lo=1, Downloaded on 10th July, 2019.

in multi-cloud infrastructure is being a common solution adopted by large organizations. It is flexible and dynamic storage that can grow and shrink based on the current need for data storage. Besides, it provides them with the gain of multiple services from different clouds. Therefore, it is now a common and less cost solution to store data in this era where needs changes dynamically.

Working actors of cloud computing:

Factors	Details
Cloud provider	A person, organization or entity responsible for providing cloud services to interested parties
Cloud consumer	A person or organization uses cloud services for its own or organizational interest
Cloud Auditor	A person doing independent assessment of cloud services, performance and security of the cloud implementation.
Cloud Broker	An entity responsible for the performance and delivery of cloud services and negotiates relationships between Cloud providers and Cloud Consumers.
Cloud Carrier	An intermediary that provides connectivity and transport of cloud services from Cloud Providers to Cloud Consumers.

Cloud Architecture: A Conceptual reference model



†

Cloud Security Requirements:

Security requirements in single to multi-cloud systems can be divided into following categories:

- Access control and its management: Access management is set of rules that are defined by providers for their costumer access which guarantee their security. A provider, like a company or system owner, should have the ability to enforce their access policies and manage them so that they can differentiate between different user levels and privileges.
- Data privacy: providers need to guarantee their data privacy in which unauthorized user don't get access to confidential data.
- Data integrity: providers need to have some data integrity in which data can be retrieved and understood even if some portion of data is damaged.

† https://www.ibm.com/blogs/cloud-computing/2014/06/11/cloud-computing-reference-architecture-ccra-a-blueprint-for-your-cloud/ downloaded on 11th July 2019

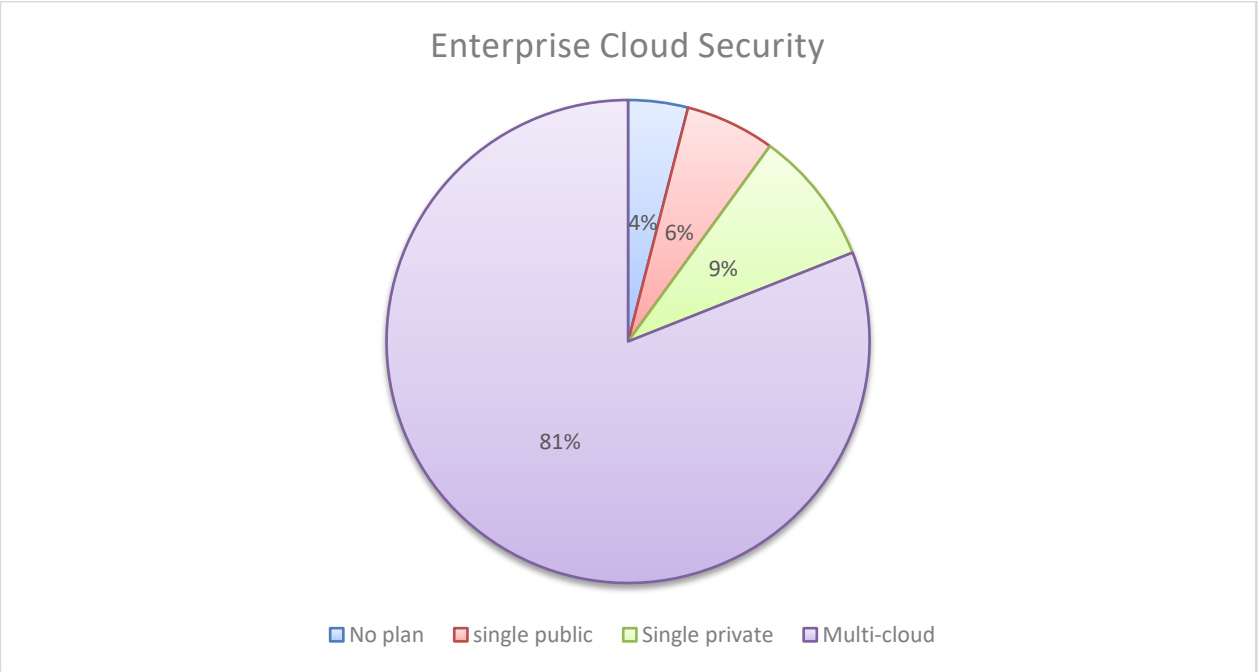
- Data intrusion: Another security requirement by providers is data intrusion in which una
- Data availability: Providers need to guarantee availability in which users can access data at any time within their provider rules and policies, i.e. data cannot be accessed if the user violates any of the provider rules.

Single Clouds Famous Breaching Examples:

Some examples of breaching schemes that occurred in last decade did happen to famous cloud providers such as Facebook, Amazon and Google. In this part, we share some of the known attacks and point the reader to [16] for some more. For example:

- Signature wrapping attacks, [14], have proven their feasibility in [15] when implemented on EC2 frameworks. In such attacks, the eavesdropper, or communication listener, add a secondary random operation to the message while keeping the signature fixed. Such change will not be detected by EC2 framework and the operation will be executed on behalf of the victim account.
- In [17], the author attacked EC2 system by virtualization of the IaaS systems in which the attacker replaces the physical machine by a virtualized one and use VM side channel attacks.
- [17] has reported an attack to Google Docs happened in 2009 which can be characterized as SaaS attacks example. Google Docs allow used to share documents and edit them with others by accessing online websites. Once a document is shared with anyone, it can be accessed by everyone who shared a document with the owner in previous. As such, unauthorized people can have the access to private data which defeat the privacy constrain to achieve security.

Single cloud is more prone to get malicious attack by hackers than multi-clouds. Multi-cloud is also called clouds of cloud or inter-cloud is the extension of single cloud. It includes high level security and privacy. Enterprise or business industry prefer to use multi-cloud for security and privacy reason and since it is available by vendors at low cost. The term “multi-clouds” is like the terms “interclouds” or “cloud-of-clouds” that were introduced by Vukolic [7]. Cachin et al. [5] identify two layers in the multi-cloud environment: the bottom layer is the inner-cloud, while the second layer is the inter-cloud. In the inter-cloud, the Byzantine fault tolerance finds its place. The following pie- chart shows the comparison of uses of cloud computing by business enterprise following the security reasons.



Enterprise using single and multi-clouds

The above graph shows more than 80% people using multi-clouds where the data is safe and can be out of prone to malicious attack by hackers. Since Multi-cloud is more secure against proxies and privacy attacks.

For example, that is IBM mashup centre, which a platform for sharing and reusing applications by web application tools. Appirio is an IaaS system that allow users to store their data in multiple Amazon C3 clouds using Salesforce.com clouds.

Current Security Risks:

The security risks in cloud computing is the trust problem, policy conflicts and privacy.

i) Trust problem: how can one trust on proxies and provide his important information.

ii) Policy conflicts: Conflicts between multiple clouds and how can proxies assure meeting the requirement for each cloud.

iii) Privacy: How client can keep their privacy while providing enough information to proxies.

Methods of security solutions:

A) Cryptography based: To reduce the risk related to security in cloud storage, one method that clients need to use cryptographic methods to protect the stored data in the cloud [9]. Using a hash function [35] is a good solution for data integrity by keeping a short hash in local memory. In this way, authentication of the server responses is done by recalculating the hash of the received data which is compared with the local stored data [9]. If the amount of data is large, then a hash tree is the solution [35].

B) DepSky based: Due to loss of data by single cloud in 2009 causes a lot of problems and hence multicloud introduced. DepSky is the method of storing data in different clouds to avoid loss in one one cloud. System data is replicated in four commercial storage clouds (Amazon S3, Windows Azure, Nirvanix and Rackspace).

It is not relayed on a single cloud; therefore, this avoids the problem of the dominant cloud causing the so-called vendor lock-in issue [3]. This type of cloud method is called multicloud storage of data. In addition, storing half the amount of data in each cloud in the DepSky system is achieved using erasure codes. Consequently, exchanging data between one provider to another will result in a smaller cost. The DepSky system aims to reduce the cost of storage of data in different clouds.

C) Distribution Based:

Secure Cost-Effective Multi-Cloud Storage: As proposed in [9], secure cost-effective multi-cloud storage technique is based on optimization technique uses minimizing a cost function based on LP problem. The cost function is subject to a given maximized quality of services (Z) achieved at the time of retrieval. Having, x cloud providers, each with a cost y per data unit and xoy level for storage services, and n chunks of data divided by the users, where at least k number of chunks is needed to understand the data.

Minimize $w1 \sum_{i=1}^{n} ri * xiyi \ - w2 \sum_{1}^{p} si * Ci$

where w1 + w2 = 1

subject to $\sum ri = q, \sum si = n$

$k \leq n \ \leq p$

D) Hybrid Based: A Hybrid Cloud Approach for Secure Authorized Deduplication: This scheme, as proposed in [10], explores the use of both private and public cloud to solve the problem of duplicates with different privileges access. The private cloud is used to store the keys for the files with specific privileges. In order to access a file, the user will need to have the key of that file and he need to be in a specific privilege. Hence, the private cloud is acting as an interface between the user and the public cloud. Fig. 9 highlights the protocol procedure in a simplified way while the rest of this subsection would explain it in detail.

Uploading a file passes through a procedure which can be highlighted in the following:

- First, when a client wants to store the data, he interacts with the private cloud to prove his identification with his privilege and private key. If the identification is passed, private cloud should find the corresponding privileges in its stored table.
- The user calculates and sends the file tag to the private cloud which return back the token to allow it to communicate with the public cloud. store its data in public cloud.

Conclusion:

After all we ca say that use of multi-cloud systems has been widely used over the last decade in industry, research work or different enterprises. The reason the need of multiple clouds to support big data, multiple services and some level of security guarantees. Customers do not want to lose their private information because of malicious insiders in the cloud. In addition, the loss of service availability has caused many problems for many customers recently.
The purpose of this work is to survey the recent research on single clouds and multi-clouds to address the security risks and solutions. It is found that several researches conducted on single cloud for its security reason and less research on multicloud. Since, multicloud has good security of enterprise and all data. My suggestion is to move towards multicloud for secured storage of data.

Bibliography:

1. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson and D. Song, "Provable data possession at untrusted stores", Proc. 14th ACM Conf. on Computer and communications security, 2007, pp. 598-609.
2. A. Bessani, M. Correia, B. Quaresma, F. André and P. Sousa, "DepSky: dependable and secure storage in a cloud-of-clouds", EuroSys'11: Proc. 6thConf. On Computer systems, 2011, pp. 31-46.
3. K. Birman, G. Chockler and R. van Renesse,"Toward a cloud computing research agenda", SIGACT News, 40, 2009, pp. 68-8
4. C. Cachin, I. Keidar and A. Shraer, "Trusting the cloud", ACM SIGACT News, 40, 2009, pp. 81-86.
5. C. Cachin and S. Tessaro, "Optimal resilience for erasure-coded Byzantine distributed storage", DISC:Proc. 19thIntl.Conf. on Distributed Computing, 2005, pp. 497-498.
6. M. Castro and B. Liskov, "Practical Byzantine fault tolerance", Operating Systems Review, 33, 1998, pp. 173-186.
7. G. Chockler, R. Guerraoui, I. Keidar and M. Vukolic, "Reliable distributed storage", Computer, 42, 2009, pp. 60-67.
8. Clavister, "Security in the cloud", Clavister White Paper, 2008.R.C. Merkle, "Protocols for public key cryptosystems", IEEE Symposium on Security and Privacy,1980, pp. 122-134.
9. E. Grosse, J. Howie, J. Ransome, J. Reavis and S. Schmidt, "Cloud computing roundtable", IEEE, Security & Privacy, 8(6), 2010, pp. 17-23.
10. C. Cachin, I. Keidar and A. Shraer, "Trusting the cloud", ACM SIGACT News, 40, 2009, pp. 81-86.
11. Clavister, "Security in the cloud", Clavister White Paper, 2008.
12. H. Takabi, J. Joshi, and G.-J. Ahn, “Security and privacy challenges in cloud computing environments,” Security Privacy, IEEE, vol. 8, no. 6, pp. 24–31, Nov 2010.

13. S. L. Garfinkel, “An evaluation of amazon’s grid computing services: Ec2, S3 and SGS,” Tech. Rep.
14. Amazon, “Aws customer agreement,” https://aws.amazon.com/agreement/, June 2015.
15. Armding, “The 15 worst data security breaches of the 21st century — cso online,” http://www.csoonline.com/article/2130877/dataprotection/data-protection-the-15-worst-data-security-breaches-of-the-21st-century.html, Feb 2015.
16. P. Mahajan, S. Setty, S. Lee, A. Clement, L. Alvisi, M. Dahlin and M. Walfish, "Depot: Cloud storage with minimal trust", OSDI'10: Proc. of the 9th USENIX Conf. on Operating systems design and implementation, 2010, pp. 1-16.
17. Krutz, Ronald L., and Russell Dean Vines. "Cloud Computing Security Architecture."
18. Cloud Security: A Comprehensive Guide to Secure Cloud Computing. Indianapolis, InN:Wiley, 2010. 179-80.
19. M.A. Morsy, J. Grundy and Müller I. “An Analysis of the Cloud Computing Security
20. "Gartner: Seven cloud-computing security risks". InfoWorld. 2008-07-02.
21. Cloud Computing Use Case Discussion Group. "Cloud Computing Use Cases Version
22. 3.0," 2010.
23. [R.K. Balachandra, P.V. Ramakrishna and A. Rakshit. “Cloud Security Issues.” In PROC
24. ‘09 IEEE International Conference on Services Computing, 2009, pp 517-520.