Cloud Computing: An Overview of Data Security Issues

Ayokunle Omotunde
Computer Science Department
Babcock University

Faith Adekogbe
Computer Science Department
Babcock University

Onuiri Ernest
Computer Science Department
Babcock University

Precious Uchendu
Computer Science Department
Babcock University

ABSTRACT

Cloud computing can be explained as a technology that enables user access to computing services over a network, different technologies have been existing over the years bearing a canny resemblance to what is termed "Cloud Computing" today, and these technologies have helped to shape its functionalities. Security is a fundamental factor that affects each and every field of study of which cloud computing is not exempted. Delivering computing resources over a network usually the Internet, creates problems associated with protecting information from unauthorized and malicious persons. The implementation of the cloud for infrastructure provides facilities such as data storage, servers and operating systems, which could result in unauthorized access to important information on the cloud. This can lead to data manipulation, data loss and breach of privacy. This paper provides an insight into the field of cloud computing, with discussions on issues related to data security.

Keywords

Technology, Security, Internet, Network, Infrastructure, Data Storage.

1. INTRODUCTION

Cloud computing is a technological model whose prominence has increased in recent years, and has therefore resulted in an exponential rise in its adoption by individuals, cooperate organizations and government establishments. The term "Cloud" denotes a major characteristic of this paradigm, which is an abstraction of the core infrastructure whereby the entire computing environment is remotely located and an instance of this environment is delivered to the client. The term 'cloud' as defined by Harjit and Singh (2011) is an "environment where resources are executed elastically with the involvement of stakeholders and is also associated with the delivery of services in measured quantities for a certain service quality as an instance" [1]. Computing as a whole has undergone a wide spread revolution over the past two decades with the successive development of computing techniques that have undisputedly given rise to what is term as cloud computing today. These techniques include utility computing, virtualization and grid computing. A major proponent of these computing techniques has been the ever increasing need to share resources. Cloud computing can be referred to as a model offering the delivery of computing resources as services over a network to clients, the services provided can be obtainable within the bounds of a company (private cloud) or to the general public (public cloud), the services delivered to clients include access to applications (SaaS), development platforms (PaaS) and computing infrastructure (IaaS), these three layers arguably encompasses all services required by clients. Data is a fundamental building block of the economy today and so its processing, development and storage is an important task, cloud computing thereby offers these services to clients whilst minimizing hardware and software implementation details. The emergent trends in cloud computing offers cloud customers the distinctive benefit of unimpeded access to important information which may be converted to useful knowledge aiding the accomplishment of different business related goals [2]. Cloud computing uses the Internet in addition to remote central servers to control information and software with the added benefit of unhindered customer access to software without the need to install and maintain them. This technology offers increased efficiency in computing by the centralization of storage facilities, information processing and also bandwidth. Examples of cloud computing include Yahoo email, Gmail and Outlook. With just an Internet connection, mails can be easily sent and these mails are retrievable on any device that has Internet access. The underlying infrastructure which includes servers and mail control application resides on the cloud and is entirely managed by the corresponding cloud provider such as Microsoft or Google [3].

2. CLOUD COMPUTING

There have been many attempts by researchers and cooperate bodies to define cloud computing based on different perspectives. This results in the existence of countless definitions and interpretations of cloud computing.

Cloud Computing has been explained by the United States National Institute of Standards and Technology (NIST) as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [4].

[5] as well [6] both delimit cloud computing with regards to the components that comprise it. [5], explains cloud computing as a collection of the software provisioned as a service over the Internet and the infrastructure and system software in a location designated by the service provider [5]. [6], explains the cloud as "a kind of parallel and distributed system comprising of a group of interconnected and virtual computers which are provided on demand and is displayed to the user as one or more centralized resources based on service-level agreements, determined by negotiation amongst the cloud provider and cloud client" [6].

Cloud computing has also been explained with regards to its function. This entails that cloud computing provides numerous functions which include but are not limited to: The provision of access to shared computing resources and centralized hardware, that offers services as demanded over a networks to accomplish tasks that meet evolving needs in business [7] and "…using of fast, high-bandwidth Internet connections to provide services which are controlled centrally, in most cases by third parties, and thus reduce the cost of maintenance of IT personnel and support for the customers that make use of those services" [8]

Some researchers also look at it from the cloud client's perspective: The Cloud encompasses the use of computing resources (hard and software) which are provisioned as services over the Internet [9]. Cloud computing has also been defined from a business perspective by Foster, Zhao, Raicu, and Lu (2008), they described it as "a large-scale distributed computing model whose goal is to achieve economies of scale, where a set of abstracted, virtual, dynamically-scalable, platforms and services are provisioned on demand to consumers over the Internet. [10][11]".

3. TECHNICAL ASPECTS OF THE CLOUD

The cloud as explained previously enables fast, on-demand and convenient access to computing resources, this section discusses the underlying infrastructure in the cloud that controls delivery and access to these resources.

3.1 Service delivery models

The service models that make-up cloud computing is a representation of the several services delivered by the cloud for use by consumers. Cloud computing delivers its characteristics via three major services which define cloud computing and the means through which customers are granted access to resources, as a whole these services make up the "cloud computing stack" [12]. The services are discussed as follows:

3.1.1 Software as a Service (SaaS)

This layer is characterized by the delivery of applications as a service via the Internet. Instead of installing and maintaining software, an instance of it can simply be accessed via the Internet, thereby relieving the user of the need for complex software and hardware management. The customer sees the SaaS model as a web-based application interface that delivers services and software applications over the Internet with access via a web browser [13]. Maintenance of applications no longer concern users as they relinquish control over software versions and requirements. SaaS vendor advertently takes responsibility for the deployment and supervision of the IT infrastructure and the processes needed to run and manage the entire solution. A great benefit of SaaS is that the user has access to their work and services from anywhere in the world via any device with Internet connection. Examples of SaaS today are Google's Gmail and Microsoft's Office Live [12][14].

3.1.2 Platform as a Service (PaaS)

This layer is characterized with the delivery of computing platforms as a service without the need to download and install software for developers, IT personnel or customers. It is a technology that provides a high degree of integration for cloud software test and implementation [14]. Berry and Reisman (2012), explain it as a cloud-based service where programmers can create or customize software applications. An example would be a platform that allows developers to build applications (apps) [15]. This service delivery model is one layer above IaaS. The consumer has no control over the core cloud hardware including network, servers, or data storage, nevertheless can control the software used and how the development platforms are configured for use. Everything else is abstracted away from the "view" of developers. PaaS is widely used and a few examples of them are Google-App, Elastic Compute Cloud by Amazon and Azure platform [4][12]. This enables developers to take advantage of added benefit of PaaS which includes verification and access to data provisioned by the platform and it abstracts the core infrastructures which includes servers, with the aim of providing a computing environment that is primarily focused on application management [7].

3.1.3 Infrastructure as a Service (IaaS)

This involves resource sharing by using virtual instances of the infrastructure. Services obtainable through IaaS comprise a remote provision of computing resources (for example; virtual computers, network, servers, data storage applications and bandwidth) [13][14]. This model allows business organizations to focus more on areas of competence which improves their level of productivity since the burden of provisioning and management of infrastructure is on the cloud provider. A few IaaS providers today include Serve-Path by Go Grid and Elastic Compute Cloud by [12][16]. IaaS delivers computing resources on demand, where the underlying technicalities like location and infrastructure are abstracted from the view of the consumers. It also allows client configuration, deployment, and running of Operating Systems and software [7].

3.2 Service deployment models

Cloud computing is categorized as public cloud, private cloud, community cloud and hybrid cloud [17]. These groups are referred to as deployment models which define the level of services obtainable by customers.

3.2.1 Public Cloud

This model is available for general use by the members of the public including individuals, corporations and government agencies. Its ownership and administration may be controlled by third parties or vendors over the Internet [7]. It exists on the premises of the cloud provider. The cloud which is owned and managed by a cloud service provider offers services to consumers on a pay-per-use basis which eradicates under-utilization. The cloud service provider assumes full responsibility for installation; management, provisioning, and maintenance [14]. They can also be referred to as provider clouds. Public clouds are by default treated as untrustworthy; therefore, security and privacy are major concerns about this type of cloud. In this model, access restrictions are applicable while authorization and authentication techniques are not. Popular providers of these cloud services include Amazon EC2, Google Apps Engine and Salesforce.com [4][17].

3.2.2 Private Cloud

This cloud deployment model is designed for individual corporations that comprises of multiple consumers (e.g., business units). The ownership, management, and control of this model is carried out by the organization, a third party cloud service provider, or a combination of them, and it may be located on or off the premises. "These are also called internal clouds and may be built primarily by IT departments within enterprises seeking to optimize utilization of infrastructure within the enterprise by providing the infrastructure with applications using the concept of grid and virtualization" [7]. This model offers more in terms of security and also incurs large costs because it is deployed for a single organization.

Private clouds minimize the need for additional security regulations, legal requirements or bandwidth limitations that characterize a public cloud environment, the cloud service providers and the clients have optimized control of the infrastructure since user's access and the networks used are regulated. One of the best examples of a private cloud is Eucalyptus Systems [4][14].

3.2.3 Community Cloud

This service deployment model shares certain similarities with private clouds the difference is that the frame-work and resources are shared by multiple organizations with similar mission, policy and security requirements. The ownership, management, and control of this model is carried out by one or more of the organizations in the community, a third party, or a combination of them, and it may be located within the premises or otherwise. "These clouds are normally based on an agreement between related business organizations such as banking or educational organizations" [14]. The costs are therefore spread over fewer users than a public cloud so only a few revenue saving benefits of the cloud is achieved [4][17].

3.2.4 Hybrid Cloud

This comprises of two or more unique cloud infrastructures (private, community or public) which retain their distinct existence. The components of this cloud are then combined using standardized or proprietary technology enabling portability, the combination of these components are managed as a single unit. Hybrid clouds promote resource optimization by organizations, so the critical core tasks can be managed by the private cloud while other operations can be contracted out to the public cloud [4][14][17].

4. CLOUD COMPUTING SECURITY

Security is an aspect in any facet of computing that is given the highest priority, this makes it evident that security issues are given high importance in the cloud environment [18][19]. Albeit, the numerous advantages obtainable by the adoption of Cloud Computing, it is noteworthy to mention that there are also some obstacles that limit its implementation, of which security has been identified as a the most prominent, not excluding matters concerning compliance, privacy and legality [20][21]. The use of cloud computing requires that client relinquish part or in some cases full security of their personal and cooperate files to the provider, It inadvertently becomes the responsibility of cloud providers to provide effective security for client information. Security has always been at the core of safe computing practices and so security within cloud computing especially is a worrisome issue because of the fact that the devices used to provide services do not belong to the users themselves. Users have no control or knowledge of, what happens to their data when it is sent to the cloud. This is because to utilize advantages associated with using the cloud, allocation of resources and scheduling must be implemented. This concern is of high priority especially where client information is extremely valuable and confidential for example business and criminal records [14][22][23]. When intruders can 'spy' on confidential information employing diverse means of 'hacking', to gain access to private data, security concerns are ultimately raised. These 'loopholes' cannot be completely eliminated by the cloud as a result of its nature and mode of application and so security issues continue to plague the cloud [23].

In addition, information is the bed-rock on which many businesses are built, hence any event that could lead to information compromise must be strictly countered. Achieving a robust security system with secured computing techniques is not possible in a single effort, rather it is a gradual one with different layers of security added in every iteration – this demands consistent examination of contemporary security practices on a regular basis [23]. The Cloud Security Alliance (CSA) is one of the bodies dedicated to regulating security in cloud computing. In march 2015 CSA released a report directed at the provision of guidance to states in the European Union specifying guidelines on the development of secure frameworks that aid risk management in the case of clouds used by the government, this report identifies security as a main barrier in the adoption of the cloud and it offers a step by step implementation plan process with emphasis on governmental clouds [24].

5. SECURITY CONCERNS IN CLOUD COMPUTING

During any event of data transfer between two parties, some security concerns need to be factored in to avoid security breaches. This section discusses these security concerns using scenario cases.

5.1 Scenario 1

In this scenario Individual A is given control and access to a hard drive containing vital information that belongs to Individual B.

5.1.1 Likely Occurrences

5.1.1.1 Loss of Control

Individual B no longer has control over what happens to the content of the hard drive since control is relinquished to individual A.

5.1.1.2 Risk of Exposure

The content of the hard drive might have been exposed to some unwanted parties. Hence, Individual B cannot vouch for the confidentiality of the information contained on the hard drive.

5.1.1.3 No Established Contracts

In this case there is a huge possibility that no formal documentation exists to specify rules that Individual A has to adhere to in the handling of the hard drive.

5.1.1.4 Inherent Risk of Outsourcing

Inherent risk of outsourcing: In the event that Individual A decides to outsource the job of securing the hard drive to a third party who may be unknown to Individual B there is a great risk of information breach.

5.1.1.5 Data Compromise

In a situation where Individual A does not handle the hard drive securely the information on it may become compromised.

The bottom line is that despite the fact that Individual A may be a known party, the data stored in that hard drive has been rendered potentially unsafe and its integrity compromised. As regarding cloud computing with its characteristic communication over network, transmission of files and other networking activities, security becomes a very important issue and poses a threat to cloud computing as well. Despite the security techniques adopted by the network service providers and administrators the presence of hackers and other intruders who are continuously finding a way to break into the system poses great danger. Thus it all boils down to cloud computing, making sure that its computation and other activities involved are extremely secure to overcome its inherent security issues and those issues inherited from networking.

5.2 Scenario 2

Individual A, a programmer decides to upload some of his projects and other vital documents online for storage and for future use and he plans to select a service provider

5.2.1 Critical Questions from this Scenario

a. How sure is Individual A that an attacker does not have access to his files or even read them?
b. How sure is Individual A that the service provider does not have access to his files?
c. What is the probability that the files are intact and have not been tampered with, even as they are retrieved from the online storage?
d. How sure is Individual A that all the files that he uploaded arrived safely at the service provider's location?

The above listed questions highlight the major issues that cloud service users may have to deal with, by using cloud computing users relinquish control over their files to the cloud service providers, therefore providing a secure environment for such files becomes a high priority to the providers. It is clear that security issues have played a prominent role in hindering the general acceptance of Cloud Computing. Storing documents, executing applications on a hard disk owned by another person and making use of a CPU that belongs to someone else seems unnerving to a great number of people [16].

5.3 Data Security Issues

A few security issues encountered in cloud computing with an emphasis on data storage in the infrastructure layer include;

5.3.1 Data Privacy

A breach of data privacy implies that the data stored on the cloud has been accessed by someone other than the owner of such data, now this individual may either be the cloud service provider or a third party. The decision to move corporate data and/or personal documents to an external cloud environment may in its very nature lead to individuals within the service provider organization having access to the data stored in the cloud environment. If any service provider personnel gets access to the data stored, it could potentially result in loss of privacy of confidential data. Data in the cloud is usually globally distributed, which raises issues in jurisdiction, data exposure and privacy. In cases where the cloud service provider contracts a third party organization to back-up the data, the scope of privacy loss may be further widened [14][25].

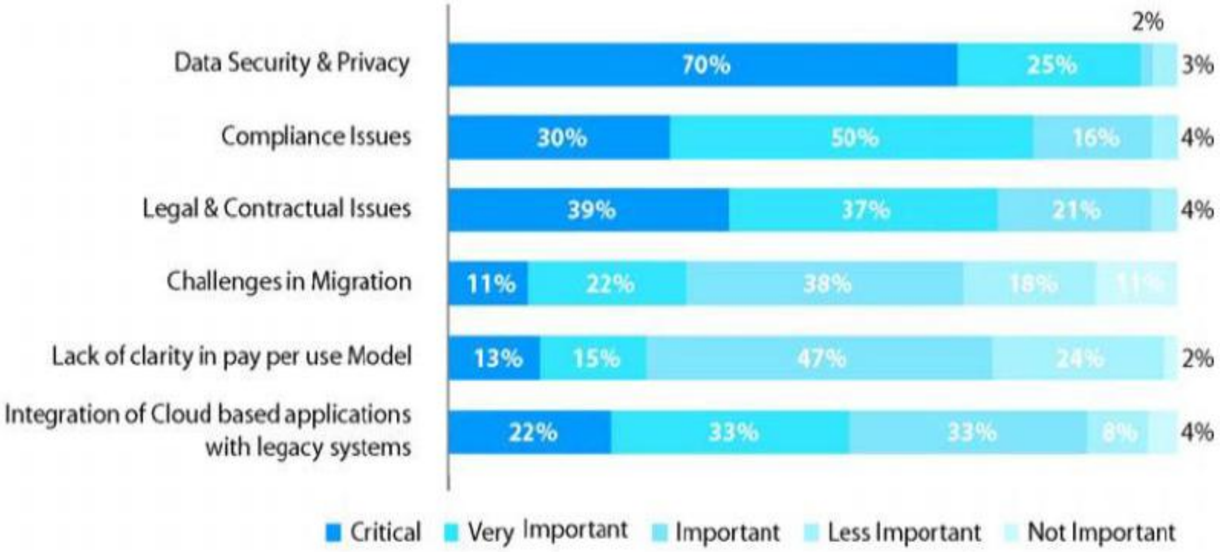

Fig 1: Survey results highlighting Data Security and Privacy as a major limitation in the cloud [26]

5.3.2 Data Breach or Loss

This occurs when all or significant part of client data is accessed by an unauthorized or malicious person, this is an evident concern in the cloud computing environment because of the never ending presence of hackers and the likes. Continuous effort must be made by the cloud service provider to ensure that no form of data is leaked both when the data is stored (at rest) and during transmission (transportation). The nature of cloud computing requires that data transfer is carried out over a network, where cloud computing inadvertently inherits security issues associated with networks which include Network Sniffing, Man in the Middle Attack and DDoS etc. Cloud service providers must be able to assure clients that no part of the data becomes missing or exposed to a third party when data is stored and when uploading and retrieving client data.

5.3.3 Data Integrity

Data stored in the cloud must be uploaded, stored and retrieved by the user without any change in its original format i.e. this data must be returned to the client with an assurance that it has not been tampered with, and any deviation from this will inadvertently lead to compromised integrity of client data. Data protection concerns data access for privacy along with data integrity. Consumers may be concerned about the way their information is handled, and whether this information is liable to disclosure or illegal alteration. At any storage phase, it is possible for client data to be corrupted using any media device and so monitoring the integrity is a prominent concern in the cloud, and its importance cannot be over emphasized in any data center [14][27].

5.3.4 Data Location

In most cases the client has little or no idea concerning the physical location of their data as this is abstracted from their view and the clients have no control over contact with their data. Some providers operate a distributed architecture in which this data might be physically located in separate places but appears as a whole to the client. Problems may arise from security and data management policies of the areas where this data is located for example in some European Union countries restriction are placed on moving certain kinds of data because the information may be sensitive [14].

5.3.5 Data Availability

This is an important concern for clients that adopt the cloud, continuous and uninterrupted delivery of document is an expected feature of a cloud computing environment, in a case where client’s data may be temporarily unavailable due to malfunctions on the part of the providers a great problem arises. If the Cloud goes out of business, information becomes inaccessible since it relies on the service provider. In such cases clients are denied access to their data and this causes a big problem for data critical organizations. Enterprises need be assured by the service providers that services will be available at all times [14].

5.3.6 Incomplete Data Deletion

Clients have no idea whatsoever if their data is physically deleted from the cloud providers’ storage and their backup, in a case whereby a client desires to move data from one vendor to another or totally remove it from the cloud, there is no assurance the cloud provider wont still have copies of this data and this could potentially lead to a major security breach in the case of sensitive data if data is not completely removed.

6. CONCLUSION

Cloud computing is a field that has great prospects for the emerging business world, with its provision of computing services at pay-per-use basis which is a major relief in consideration of the financial backing needed to provide these resources. However, security issues mitigate its adoption, since information is a very important currency for business transactions today, any breach or loss could cause untold financial damage. This paper discussed cloud computing and highlighted problems associated with data security in the cloud, these problems need to be continuously addressed with corresponding improvements on security. Data security in general is a major bottleneck in any data transfer process, with the inherent risk of data leakage and unauthorized manipulation of data, it is mandatory to develop a data transfer system that successfully mitigates these risks while maintaining optimal delivery of services. As the world of information management is tending towards the cloud, cloud service providers need to factor all risks involved in data sharing into any security system they adopt. Furthermore, it is noteworthy to mention that security breaching techniques like any other facet of computing is evolving every day, and so security systems need to evolve at a faster pace to keep up with these trends. Security forecasting must be carried out by every cloud service provider at regular intervals to review its current security status so as to make regular improvements to existing processes.

7. REFERENCES

[1] Harjit, S. L., & Singh, G. (2011, July). Cloud Computing-Future Framework for e-management of NGO's. *International Journal of Advancements in Technology, 2*(3), 400-408.

[2] Petre, R.-Ş. (2012). Data mining in Cloud Computing. *Database Systems Journal, 2*(3), 67-72.

[3] Kumar, D. A., & Sukumar, M. (2013, November). Development of cloud computing in integrated library management and retrieval system. *International Journal of Library and Information Science, 5*(10), 394-400.

[4] Mell, P., & Grance, T. (2011). NIST Definition of Cloud Computing. *Recommendations of the National Istitute of Standards and Technology NIST Special Publication 800-145.*

[5] Armburst, M. e. (2009). Above the Clouds: A Berkeley View of Cloud Computing. University of California, Berkeley. Retrieved from http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html

[6] Buyya, R., Yeoa, C. S., Venugopala, S., Broberg, J., & Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems, 599-616

[7] Srinivasa, R. V., Nageswara, R. N., & Kumari, K. (2009). Cloud Computing: An Overview. Journal of thoeritical and Applied Information Technology, 71-77.

[8] Borenstein, N., & Blake, J. (2011). Cloud Computing Standards: Where’s the Beef? IEEE Internet Computing, 15(3), 74-78.

[9] Ştefania, R. (2012). Datamining in Cloud Computing. Database Systems Journal, III(3).

[10] Foster, I., Zhao, Y., Raicu, I., & Lu, S. (2008). *Cloud Computing and Grid Computing 360-Degree Compared.* Texas: 2008 Grid Computing Environment Workshop (GCE ’08).

[11] Sarga, L. (2012). Cloud Computing. JOURNAL OF SYSTEMS INTEGRATION, 4, 3-15.

[12] Karlin, S., & Curran, K. (2012, June). Cloud Computing Technologies. International Journal of Cloud Computing and Services Science (IJ-CLOSER), 1(2), 59-65.

[13] Sultan, N. (2010). Cloud computing for education: A new dawn? International Journal of Information Management, 109-116.

[14] Padhy, R. P., Patra, M. R., & Satapathy, S. C. (2011, December). Cloud Computing: Security Issues and Research. International Journal of Computer Science and Information Technology & Security (IJCSITS), I(2), 136-145.

[15] Berry, R., & Reisman, M. (2012, May). Policy Challenges of Cross-Border Cloud Computing. Journal of International Commerce and Economics, 2-35.

[16] Kuyoro, S. O., Ibikunle, F., & Awodele, O. (2011). Cloud Computing Security Issues and Challenges. International Journal of Computer Networks (IJCN), 3(5), 247-255.

[17] Youssef, A. E. (2012, July). Exploring Cloud Computing Services and Applications. Journal of Emerging Trends in Computing and Information Sciences, 3(6), 838-848.

[18] Emam, A. (2013). Additional Authentication and Authorization using Registered Email-ID for Cloud Computing. International Journal of Soft Computing and Engineering, 3(2), 110-113.

[19] Kim, J., & Hong, S. (2012). A Consolidated Authentication Model in Cloud Computing Environments. International Journal of Multimedia and Ubiquitous Engineering, 151-160.

[20] Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. Journal of Internet Services and Applications, 4(5). Retrieved from http://www.jisajournal.com/content/4/1/5

[21] KPMG. (2010). From hype to future: KPMG’s 2010 Cloud Computing survey. Retrieved from KPMG: http://www.techrepublic.com/whitepapers/from-hype-to-futurekpmgs-2010-cloud-computing-survey/2384291

[22] Hamlen, K., Kantarcioglu, M., Khan, L., & Thuraisingham, B. (2010, April-June). Security Issues for Cloud Computing. International Journal of Information Security and Privacy, 4(2), 39-51.

[23] Ahmed, M., & Hossain, M. A. (2014, January). Cloud Computing and Security Issues in the Cloud. International Journal of Network Security & Its Applications (IJNSA), 6(1), 25-37.

[24] Cloud Security Alliance. (2015, March). Cloud Security Alliance Announces Release of Security Framework for Governmental Clouds. Retrieved January 2016, from Cloud Security Alliance.

[25] Mosher, R. (2011, July). Cloud Computing Risks. Information Systems Security Association.

[26] R. Velumadhava Rao & K. Selvamani (2015). *Data Security Challenges and Its Solutions in Cloud Computing.* International Conference on Intelligent Computing, Communication & Convergence, 204-209

[27] Lee, K. (2012, October). Security Threats in Cloud Computing Environments1. International Journal of Security and Its Applications, 6(4).