IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 5, May 2018

A Survey on Cloud Security Issues and Challenges (CSIC)

Rama Krishna K[1], Dr. K G Mohan[2]

Assistant Professor, Dept. of Computer Science & Engg, Presidency University, Bangalore, India[1]

Professor & Head, Dept. of Computer Science & Engg, Presidency University, Bangalore, India[2]

Abstract: Cloud computing security is a fast-growing service that provides many of the same functionalities as traditional IT security. This includes protecting critical information from theft, data leakage and deletion. One of the benefits of cloud services is that you can operate at scale and still remain secure. It is similar to how you currently manage security, but now you have new ways of delivering security solutions that address new areas of concern. Cloud security does not change the approach on how to manage security from preventing to detective and corrective actions. But it does however give you the ability to perform these activities in a more agile manner. This paper provides a survey on generic architecture of cloud and the challenges in making the cloud secure.

Keywords: Cloud Architecture, Security issues, challenges

I. INTRODUCTION

The history of cloud computing is endemic with data disclosures either premeditated or unpremeditated. This discloses the risks of privacy and privacy of the cloud data storage deployment. The first ever kind of the risk is the unintentional disclosure of data which happens because of the errors in the design of the cloud computing software of the providers. For instance, the non-authenticated users were allowed to view the documents by Google Docs due to a bug The history of cloud computing is endemic with data disclosures either premeditated or unpremeditated. This discloses the risks of privacy and privacy of the cloud data storage deployment. The first ever kind of the risk is the unintentional disclosure of data which happens because of the errors in the design of the cloud computing software of the providers. For instance, the non-authenticated users were allowed to view the documents by Google Docs due to a bug, whereas the Flicker and Facebook have also leaked the private pictures of the users due to flaws [2].

Cloud computing is nothing but Internet computing generally the internet is seen as set of clouds; thus the word cloud computing can be defined as utilizing the internet to provide technology enabled services to the people and organizations. Cloud computing is new utility of this era, which many enterprises wants to incorporate in order to improve their way of working. It implies sharing of computing resources to handle applications. Cloud computing offers reduced capital expenditure, operational risks, complexity and maintenance, and increased scalability while providing services at different abstraction levels, namely Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS). It is used in consumer-oriented applications such as financial portfolios delivering personalized information, or power immersive computer games. It is a pay as peruse kind of service, hence has become very popular in very less time.

To clearly understand the cloud security issues, we first need to understand the compound security challenges in a complete way. Specifically, we need to: (i) investigate various cloud security attributes including vulnerabilities, threats, risks, and attack models; (ii) identify the security requirements including privacy, integrity, availability, transparency, etc.; (iii) identify the involved parties (clients, service provides, outsiders, insiders) and the role of each party in the attack-defense cycle; and (iv) understand the impact of security on various cloud deployment models (public, community, private, hybrid). The main contribution of this paper is that it provides a holistic study of the security issues in the clouds that cover almost all the cloud components (data centers, computing infrastructure, interfacing and networking, etc.), network layers (application, transportation, IP, etc.), and cloud stakeholders [3] (providers, consumers, third party contractors, etc.). In this paper, we provide a comprehensive survey on the cloud security and privacy concerns that includes: (i) cloud computing security issues (vulnerabilities, threats, and attacks); (ii) attack classifications; (iii) relations and dependencies among attacks; (iv) known attacks; (v) comparative analysis of some of well-known countermeasures; (vi) insights from the current security solutions to identify and address unattended security challenges. Figure 1 illustrates a typical cloud based scenario that includes the cloud service provider and the cloud users in a cloud computing architecture

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 5, May 2018

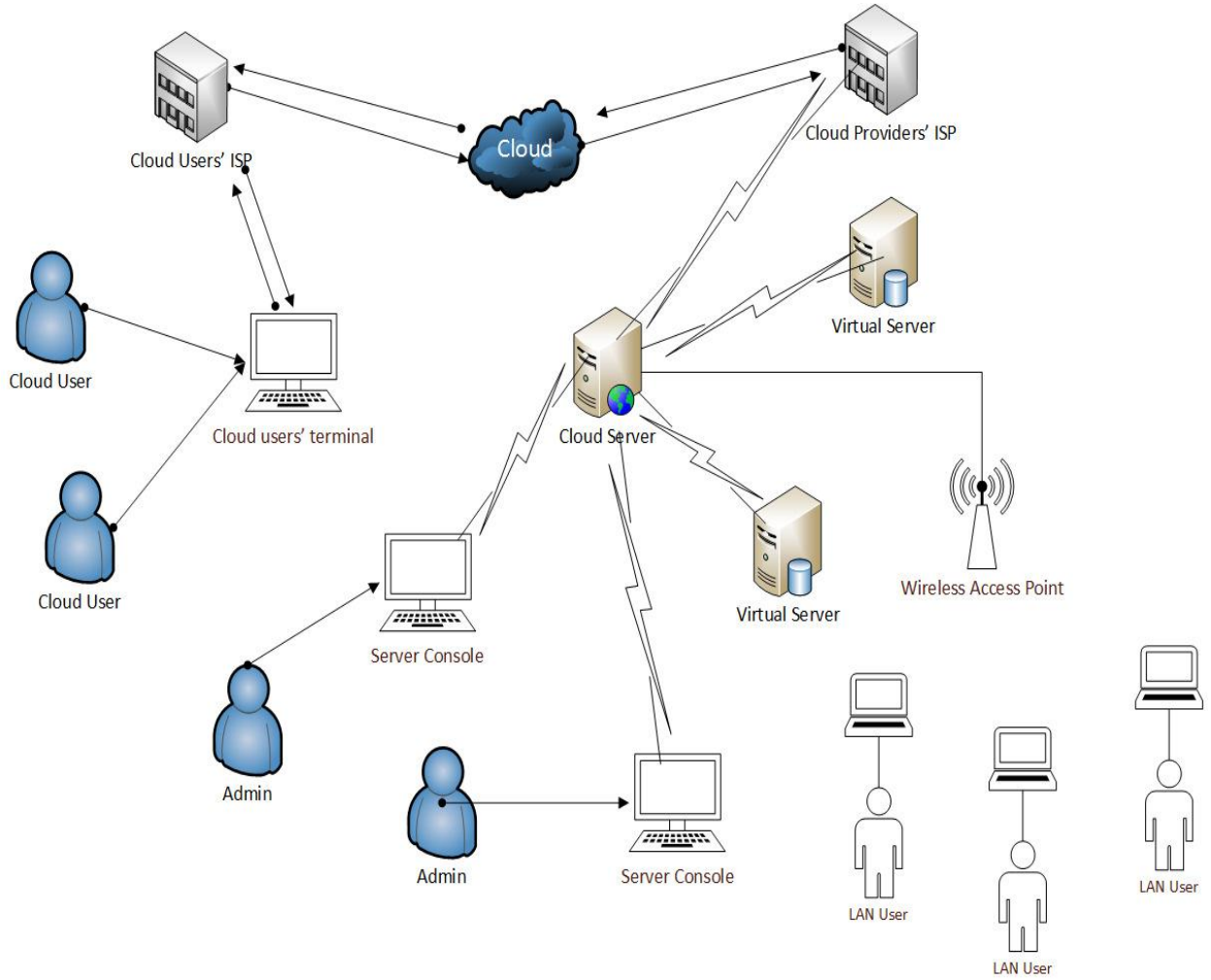

Figure 1: A Typical Cloud Architecture

The illustration of cloud architecture in figure 1 is a simplest one where few complex characteristics of cloud computing (e.g. redundancy, server replication, and geographic dispersion of the cloud providers' network) are not shown – the purpose of the illustration is to establish the arrangement that makes the concept of cloud computing a tangible one. The network architecture is self-explanatory with the identification of cloud users when considered in-line with the discussion of the cloud computing concept. One notable part from the architecture is that, while the cloud users are clearly identified and named accordingly due to their remote location and means of remote access to the cloud servers, the admin users who are administering the cloud servers are not cloud users in any form with respect to the cloud service provider's network in the scenario. It is arguable whether the LAN users in figure 1 are cloud users or not. Such room for argument could exist due to the phrase 'cloud computing' being a concept rather than a technical terminology. If the definition of cloud computing is taken to have essential arrangements of being the servers located remotely that are accessed through public infrastructure (or through cloud), then the LAN users in figure 1 may not be considered as the cloud users in the context. With respect to distributed and grid computing as the mother technology that define the infrastructural approach to achieve cloud computing, the LAN users in the scenario are essentially the cloud users when they use the cloud services offered by the servers; the LAN users in this perspective are essentially using resources that are 'borrowed' from the servers on an on-demand basis. Whereas the Flicker and Facebook have also leaked the private pictures of the users due to flaws [4].

Cloud computing is nothing but Internet computing generally the internet is seen as set of clouds; thus the word cloud computing can be defined as utilizing the internet to provide technology enabled services to the people and organizations. Cloud computing is new utility of this era, which many enterprises wants to incorporate in order to improve their way of working. It implies sharing of computing resources to handle applications. Cloud computing offers reduced capital expenditure, operational risks, complexity and maintenance, and increased scalability while providing services at different abstraction levels, namely Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS). It is used in consumer-oriented applications such as financial portfolios

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 5, May 2018

delivering personalized information, or power immersive computer games. It is a pay as peruse kind of service, hence has become very popular in very less time [6].

To clearly understand the cloud security issues, we first need to understand the compound security challenges in a complete way. Specifically, we need to: (i) investigate various cloud security attributes including vulnerabilities, threats, risks, and attack models; (ii) identify the security requirements including privacy, integrity, availability, transparency, etc.; (iii) identify the involved parties (clients, service provides, outsiders, insiders) and the role of each party in the attack-defense cycle; and (iv) understand the impact of security on various cloud deployment models (public, community, private, hybrid). The main contribution of this paper is that it provides a holistic study of the security issues in the clouds that cover almost all the cloud components (data centers, computing infrastructure, interfacing and networking, etc.), network layers (application, transportation, IP, etc.), and cloud stakeholders (providers, consumers, third party contractors, etc.). In this paper, we provide a comprehensive survey on the cloud security and privacy concerns that includes: (i) cloud computing security issues (vulnerabilities, threats, and attacks); (ii) attack classifications; (iii) relations and dependencies among attacks; (iv) known attacks; (v) comparative analysis of some of well-known countermeasures; (vi) insights from the current security solutions to identify and address unattended security challenges. Figure 1 illustrates a typical cloud based scenario that includes the cloud service provider and the cloud users in a cloud computing architecture [8].

The illustration of cloud architecture in figure 1 is a simplest one where few complex characteristics of cloud computing (e.g. redundancy, server replication, and geographic dispersion of the cloud providers' network) are not shown – the purpose of the illustration is to establish the arrangement that makes the concept of cloud computing a tangible one. The network architecture is self-explanatory with the identification of cloud users when considered in-line with the discussion of the cloud computing concept [11]. One notable part from the architecture is that, while the cloud users are clearly identified and named accordingly due to their remote location and means of remote access to the cloud servers, the admin users who are administering the cloud servers are not cloud users in any form with respect to the cloud service provider's network in the scenario. It is arguable whether the LAN users in figure 1 are cloud users or not. Such room for argument could exist due to the phrase 'cloud computing' being a concept rather than a technical terminology. If the definition of cloud computing is taken to have essential arrangements of being the servers located remotely that are accessed through public infrastructure (or through cloud), then the LAN users in figure 1 may not be considered as the cloud users in the context. With respect to distributed and grid computing as the mother technology that define the infrastructural approach to achieve cloud computing, the LAN users in the scenario are essentially the cloud users when they use the cloud services offered by the servers; the LAN users in this perspective are essentially using resources that are 'borrowed' from the servers on an on-demand basis..

2. THE GENERIC ARCHITECTURE

The generic architecture is composed of two modules, i.e. the client module and the server module. The general description of the model is given in the following figure.

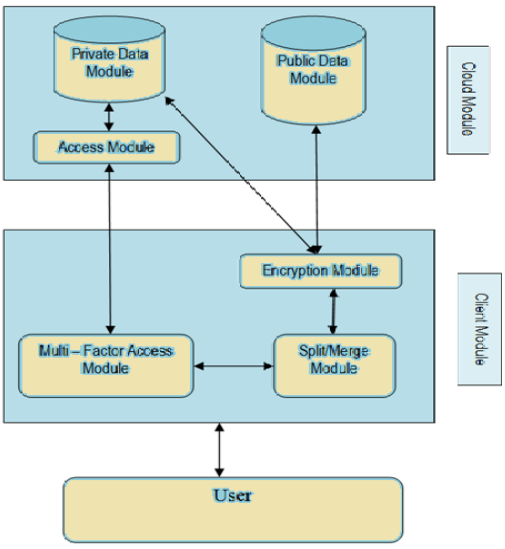

Figure 2. Block Diagram of the Generic Architecture

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 5, May 2018

2.1 The Client Module

The client module is mainly composed of three components. The access control component, the split and merge component and the encrypt/decrypt component. The working of each component is explained separately.

2.1.1. The Client Access Control Component:

The access control component is responsible of the authentication and authorization of the cloud user. The simplest mechanism of authentication is a user name and password. But this is too weak method of authentication for cloud computing. The user will login with its user credentials (User Name, Password) and the cloud access control component generates the two session password randomly. One is sent to the user's official email account and the other is sent to a mobile number of the user. The user can be authenticated using both of these session passwords. Once the authentication is complete the access control module will go into the back ground and the rest of the data access and storage will be done through split and merge and encrypt and decrypt components.

2.1.2. The Split and Merge Component:

After authentication, the user will be granted access to the cloud data storage services. When the client wants to send data, the data will be split first by the split by using the split algorithm. The data can be received and merge algorithm will be used to see the original data form. The split algorithm divide the data into even and odd bits of information and then the merge algorithm reverse the process.

2.1.3. Encrypt/Decrypt Component:

After the data is split by the split and merge component, it is then send to encrypt/decrypt component. The encrypt/decrypt component after applying the AES encryption techniques send the encrypted data to cloud storage server, where the data is stored in the public component of the data storage server while the key will be store in the private data component. The same mechanism is applied when the data is requested back from the storage. The key is taken from the private data component and data from the public data component after decrypting the data is given back to split and merge component where the merger algorithm is used to generate the original data.

2.2. The Server Module

The cloud server module of our architecture is also composed of three components. These components include the authentication component, the private data component and the public data component. The working of these components is explained as follows.

2.2.1 Authentication Component:

The authentication component works in close connection with the private data component of the server module. When the server receives a request for the authorization of data access, it is the responsibility of authentication module to randomly generate two session password and send one of it to user's official email account and the other to the mobile number. The user is then authenticated after checking the session passwords from the user.

2.2.2. Private Data Component:

The private data component is not only responsible the storage of the user's credentials (Login Information). But it is also responsible for the storage of secrete keys needed for the decryption of the data store in the public section of the cloud storage. Only the owner of the data is able to access the private data section of the cloud storage and perform operation like update, delete, append on the data. The user cannot perform data operations on private data section.

2.2.3. Public Data Component:

The public component stores the data which will be shared among all the authorized users of the specific data. All the data stored in the public data section will be present in encrypted form. The owner is not only responsible for the creation of data in this component, but also for the different data operations as well

3. SECURITY ISSUES IN CLOUD COMPUTING

Security of Cloud Implementation Models Basically, the deployment of a cloud is managed in-house (Private Cloud) or over a third-party location (Public Cloud). While, for various reasons, it is deployed as an integrated private-public cloud(Hybrid Cloud). A "Community Cloud" is a fourth type of cloud implementation models, where the infrastructure spreads over several organizations and is accessed by a specific community. The different cloud implementation models are shown in above Figure. In private cloud configuration an organization may have control over its infrastructure or delegate that to a third-party, being physically on-site or off-site. Securing the in-house cloud infrastructure is controllable and requires no need for extra trust mechanisms. While having a third-party service

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 5, May 2018

provider running the private cloud is prone to several doubts. Users adopt a private cloud implementation to increase the security level. That decreases the isolation level between the services and the infrastructure. For instance, managing the security of the provided service in conjunction with the existing firewalls and protection services [13]. Furthermore, operating over a secure virtual private network is an option to isolate the private cloud hosted by a third-party. Despite the benefits of a private cloud, several issues need attention as unbalanced resources utilization. A sluggish infrastructure is a wasted resource for example.

3.1 Security challenges in Cloud

Before any organizations wishes to move towards cloud computing seems they have to overcome various challenges. Existing scenario of the services offered by cloud, provides many solutions for problems. Few to name them, are security stuffs, viability, and interoperability in addition to others. Probable answers have been put forth by some authors to the various challenges, while few researchers highlighted the necessity for additional improvements. Security is a critical issue that worries those considering an external outsource to hold their data and processes. The concerns exceed the potential of data loss and corruption to matters of trust, service availability, and unpredictable issues. Some evidences reveal the availability challenge such as instances of Google services interruption going from 1.5 to 8 hour periods in 2008. Few Authors have highlighted ten hurdles to the expansion of cloud computing along with potential chances for recovery. Among the hurdles there is the privacy of data for which they suggest data encryption as an opportunity for resolution. Few authors put forth the need for serious acts toward improving the security of the clouds. One of the proposals is the assurance given by Service Level Agreement (SLA) that is between the users and the service provider. On the other hand, one of the many proposed possibilities is a “multi-tenancy” support in which customizable security options allow individuals to adapt to their desired context. It is challenging to justify the costing model in terms of cloud services. Cloud customers need to think of different tradeoffs regarding the cost of security mechanism, communication, computing power, and integration. The infrastructure cost will be substituted by the cost of data transfer and connectivity. Restraining the cost of communication is not an option, due to the high reliance on regular large amounts of data transfer. Taking the special case of hybrid clouds where constant data transfer is required between the private cloud, in-house IT infrastructure, and the public cloud. Few authors discussed the managerial decisions of selecting a suitable costing model based on the available alternatives. Also they stated that on-demand services offer reasonable usage-based fees for startups, in contrast to the high cost of in-house infrastructure. Cloud services will replace or integrate with an in-house infrastructure, which requires a serious study of the charge-back model. Cost analysis becomes more complex compared to the establishment of legacy infrastructure. One author presented three areas for billing customers over the cloud, which are the cost of storage, access, and processing. That increases the analysis dimensions considering a public cloud service. On the other hand, designing a secure architecture will have an overhead of optimization to minimize the public cloud cost. Considering a hybrid cloud is a possible solution to gain a better return on investment. A trade-off between the private or public cloud utilization is needed to maximize the benefits over the costs, taking in consideration the desired security level.

SLA is an important matter when considering public cloud services, as presented in. It is important to have an assurance before conducting serious business operations over third-party resources. The provider is expected To ensure service accessibility, availability, dependability and performance. Potential problems of the agreements include the interpretation of the conditions, as well as the evaluation criteria of the terms. That creates confusion on one hand; on the other hand the terms may omit the customers’ expectations or requirements. Furthermore, the terms vary and increase the SLA complexity for different cloud offerings as for Iaas, Paas, and Saas. For that the SLAs need to be flexible in a way that adapts to customer specific requirements, at the same time clear to both parties. Automated SLAs try to overcome the challenges here, but practically it is difficult as highlighted. Deciding what to migrate is challenging, customers may hesitate when determining what to put over the cloud. Despite the reduction in the capital and operational expenditures, trust and security concerns limit the migration decisions. The results of an investigation presented one author show that security is the most significant concern. Specifically, the respondents are apparently consider data protection and SLA at the top of the requirements for evaluating a service provider, while the security is almost a must when the migration to the cloud is already in place. That indicates the tendency to prohibit the migration of sensitive resources once security is not clear and highly assured. IDC’s survey shows an expected dramatic spending increase to develop public clouds by 2014, to be around 55.5 billion US Dollars. More than half of the spending is going to applications development, while infrastructure, servers and storage follow. Though, migration is expected to be with higher possibility towards SaaS, coming next IaaS and PaaS respectively. The interoperability of in-house systems and data with cloud services is not straightforward. The lack of common interface raises the issue of data lock-in. Furthermore, expanding the cloud services, possibly utilizing different clouds, is challenging and could be impossible in some cases. Adopting a hybrid cloud approach raises many questions about compatibility of data and operations as well [14]. Public and private clouds integration without common standards prevents a smooth and quick cloud expansion. Few authors pointed to the need of standardizing the security issue, possibly by adopting a well-

formulated security standard. Accordingly, a proposed solution in some paper suggests implementing standardized API's, which makes switching between clouds or services easier.

4. CONCLUSION

Cloud computing has seen a paradigm shift when it comes to exploiting the existing technologies. The inclination of having cloud services as part of a society seems to be gaining more significance. Particularly in this day and age the cycle of presenting more technological innovations is falling tinier. For many purposes, including the decrease of capital expenses, establishments need to consider exploiting cloud services as a vital part of their grounds. However, several challenges are keeping out the execution of vast placement and recognition levels. The primary shortcoming of the current cloud service implementations is their incapability to deliver a high security level. Additionally, security assertion necessities to cover the transmission channels which influences to include a third-party. To have better exploitation of cloud services many issues need to be improved in a way to ensure high level of security, privacy, genuineness, incorporation, quickness, scalability and trustworthy. Perhaps an automated SLA, third trusted party, or a new improvement would be a fascinating study domain to cover the security issues pertaining to cloud computing.

REFERENCES

1. Sarika Gupta, Sangita Rani Satapathy, Piyush Mehta, Anupam Tripathy.A Secure and Searchable Data Storage in Cloud Computing. 2013 3rd IEEE International Advance Computing Conference (IACC).
2. Hamid Banirostam, Alireza Hedayati, Ahmad Khadem Zadeh, Elham Shamsinezhad, A Trust Based Approach for Increasing Security in Cloud Computing Infrastructure. 2013 UKSim 15th International Conference on Computer Modelling and Simulation.
3. Sultan Ullah and Zheng Xuefeng. TCLOUD: A Trusted Storage Architecture for Cloud Computing. International Journal of Advanced Science and Technology Vol.63, (2014).
4 Monjur Ahmed1 and Mohammad Ashraf Hossain. Cloud Computing and security issues in Cloud. International Journal of Network Security & ItsApplications (IJNSA), Vol.6, No.1, January 2014.
5.Dr.P.K.Rai, R.K.Bunkar, Vivekananda Mishra. Data Security and Privacy Protection Issues in Cloud Computing. IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 1, Ver. IX (Feb. 2014).
6. Mr. Prashant Rewagad and Ms.Yogita Pawar. Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing. 2013 International Conference on Communication Systems and Network Technologies.
7. Osama Harfoushi, Bader Alfawwaz, Nazeeh A. Ghatasheh, Ruba Obiedat, Mua'ad M. Abu-Faraj, Hossam Faris. Data Security Issues and Challenges in Cloud Computing:A Conceptual Analysis and Review. Communications and Network, 2014, 6, 15-21 Published Online February 2014.
8. S C Rachana, Dr. H S Guruprasad Emerging Security Issues and Challenges in Cloud Computing. International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 3, Issue 2, March 2014.
9. Issa M. Khalil , Abdallah Khreishah and Muhammad Azeem. Cloud Computing Security: A Survey.Computers ISSN 2073-431X www.mdpi.com/journal/computers
10. Amit Goyal And Sara Dadizadeh. A Survey on Cloud Computing. University of British Columbia, Vancouver.
11. Keiko Hashizume , David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez. An analysis of security issues for cloud computing. Hashizume et al. Journal of Internet Services and Applications 2013, 4:5 http://www.jisajournal.com/content/4/1/5
12. Deepanchakaravarth i Purushothaman and Dr.Sunitha Abburu. An Approach for Data Storage Security in Cloud Computing. IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 1, March 2012 ISSN (Online): 1694-0814 www.IJCSI.org
13. Swetha Reddy, Lenkala , Sachin Shetty and kaiqi Xiong. Security Risks Assessment of Cloud Carrier. 2013 13th IEEE/ACM Internation Symposium on Cluster,Cloud and Grid Computing.
14 K Sri Prasad H, Sai Charan Srinivasan, O Pandithurai and A Saravanan. A Novel method to secure cloud computing through multicast key management.
15 Kandaswamy B and Papitha E. Flexible access control for outsourcing personal health services in cloud computing using Hierarchical attribute set based encryption.