EasyChair Preprint

№ 2533

Cloud Computing Security Issues, Challenges and Solutions

Harsh Pratap Singh, Rashmi Singh and Vinay Singh

February 4, 2020

CLOUD COMPUTING SECURITY ISSUES, CHALLENGES AND SOLUTIONS

HARSH PRATAP SINGH
Ph.D. Scholar
Sri Satya Sai University of Technology and Medical Sciences, Sehore (M.P.), India singhharshpratap@gmail.com

RASHMI SINGH
Assistant Professor, CSE Dept.
Radharaman Institute of Technology and Science, Bhopal (M.P.), India
rashmi.singh1610@gmail.com

VINAY SINGH
Assistant Professor, CSE Dept.
SISTec Gandhi Nagar, Bhopal (M.P.), India
vinay.cse5@gmail.com

Abstract—The cloud computing is an emerging and extensively used technology in the field of Information Technology only because of its scalability, throughput, easy and cheap access and on demand up and down grading of cloud services characteristic. Cloud computing is gaining concentration due to the development of internet technologies, reduced cost of storage and processing, growth technologies of visualization, SOA (Service Oriented Architecture) and encroachment in internet security. But cloud security and privacy becomes the major issues because of its salient feature. In this study, present the literature work for the security issues and challenges with their solutions.

Keywords—Cloud Computing, Security Issues, Cloud Services, SOA

1. Introduction

Cloud computing is an advancing paradigm, as per National Institute of Standards and Technology (NIST), cloud computing is not having impeccable definition. NIST characterizes cloud computing as a model for empowering expediency, on–demand network access to a widespread group of configurable computing resources like servers, stockpiling, applications and services that can be quickly provisioned and discharged with optimal management exertion or specialist organization connection, around us its definition, attribution and qualities are still being battered by people in public and private sectors. So we can acknowledge it as "advancing paradigm" [GTSI (2011)] .Cloud computing advances the accessibility of information, for this objective, it is made out of five fundamental attributes. Service models and deployment models [GTSI (2011)] in cloud registering administrations and applications will move towards this paradigm. Fig. 1 gives the entire picture of Cloud Module. The three primary services of the cloud are appeared in this module. The thin-client1 on client devices access, over the networks applications hosted in server farm by application service provider. In cloud computing the basic circumstance is that the services are deployed from areas that are the best for the current set of clients. This can likewise be accomplished when the services will be facilitated on Virtual Machine (VM) in interconnected server applications and these VMs additionally relocate towards the region which suits for current client populations [F. Hao et al. (2010)]. In fact cloud computing can be characterized as a Transport Control Protocol/Internet Protocol(TCP/IP) based high development Clients are a development and integrations of computer technologies such as fast microprocessor, colossal memory rapid system and dependable framework design. Today we are using the cloud computing which is exist as a result of standard between associated protocols and developed amassing server application advances [Gong et al. (2010)]. Prophet CEO L Ellison said that, "cloud computing is simply everything that we as of now do" [D. Farber (2008)]. The other advanced technical meaning of cloud computing as the development and

espousal of quickly advancing technology, strong fault tolerance, TCP/IP based and virtualized. These characteristics are somewhat supported by grid computing. High security is not so far guaranteed completely. There are abundant more definitions for cloud computing these will contemplate on definite sections of the technology. From these definitions any one can get mystification about what cloud computing truly is the thing that the services are given by it and how it is deployed so on. The responses to these inquiries are not definite. Cloud computing is additionally separates itself from other registering standards like network figuring, worldwide registering, web processing in the different angles like on-request benefit arrangement with ensured Quality of Benefit [QoS], self-governing framework, client driven interfaces, alternate methods that adds to the distributed computing are virtualization, Web Service and Service Oriented Design (SOA), Web 2.0 and crush up Application Programming Interface (API). It additionally incorporates SOA and virtual utilizations of both equipment and programming. The cloud situation additionally gives a compliant administrations transference stage. It makes obvious its resources at dissimilar level customer's sellers and accomplices.

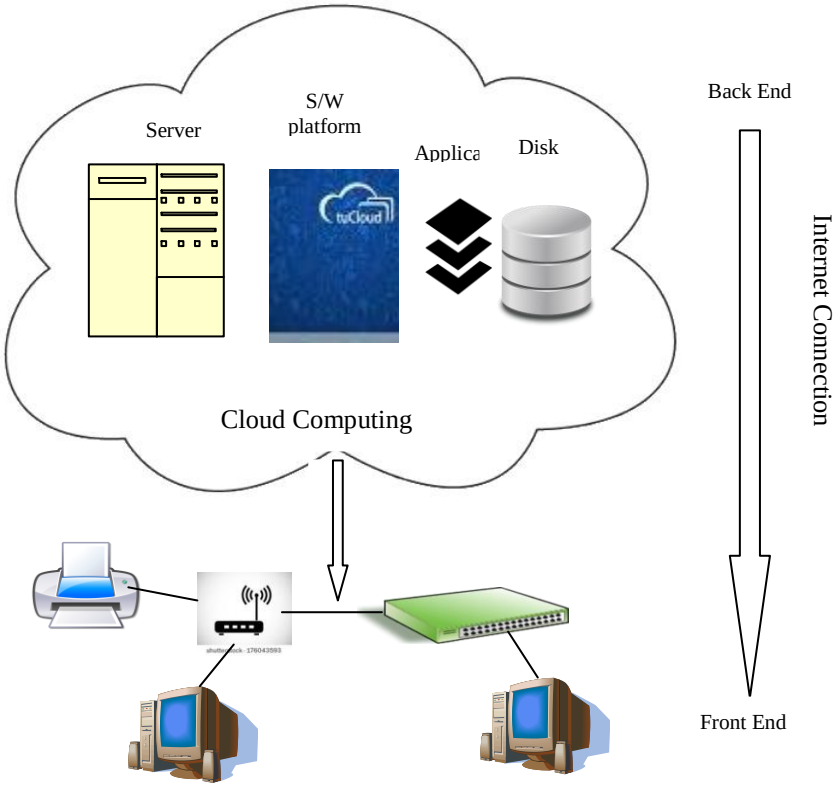

Fig.1 Cloud Architecture

2. Cloud Service Model

Clouds use architectural models in order to provide different services to the users. Service models are not tied to a specific deployment type, public, private, hybrid and community, rather each deployment type can use each service model [Cloud Security Alliance (2015)]. Just as with the different deployment methods the service models can have implications for a clouds security state, it is therefore important to have knowledge of these service models. The common service models are explained below.

2.1. Infrastructure as a Service

Infrastructure as a Service, mostly abbreviated to 'IaaS', comprises of offering infrastructure solutions as a service. The major benefit of this is the ability to only pay for what you actually use. An example of this is Dropbox where the user can pay more or less depending on how much storage they need [Sarukesi et al.(2012)].

2.2. Software as a Service

Software as a Service, generally abbreviated to 'SaaS', utilises an instance of an application and the underlying database to offer the software to various customers simultaneously [Sarukesi et al.(2012)].

2.3. Platform as a Service

Platform as a Service, generally abbreviated to 'PaaS', provides a platform that can be used during the development of an information system, e.g. for testing and distribution. Examples of these kinds of services are GAE and Microsoft Azure [Sarukesi et al.(2012)].

2.4 Hardware as a Service

Hardware as a Service is generally abbreviated to 'HaaS'. It brought forth a significant improvement because it allows for easy access to physical hardware devices, distributed among several geographical locations. If the cloud consumers subscribe to this service, it will appear as if they are connected to the local machine. The HaaS cloud middleware will ensure transparency between data exchanges while the local system considers all connected hardware to be locally connected, even though this is not always the reasons [Hovestadt et al.(2012)].

3. Cloud Security Challenges And Issues

3.1. Security Challenges

There are some key security [Arockiam et al. (2012] challenges are:

- **Authentication:** Throughout the internet data stored by cloud user is available to all unauthorized people. Henceforth the certified user and support for cloud must have interchangeability supervision entity.
- **Access Control:** To ensure and uphold only legalized users, cloud must have right access organized policies. Such services must be adaptable, well planned, and their distribution is overseeing conveniently. The method governor prerequisite must be assimilated on the basis of Service Level Agreement (SLA).
- **Policy Integration:** There are several cloud providers such as Amazon, Google which are accessed by end users. Lowest number of conflicts among their policies because they user their own policies and approaches.
- **Service Management:** In this diverse cloud providers such as Amazon, Google, comprise together to fabricate a novel composed services to meet their customers need. At this stage there should be get hold of divider to get the easiest localized services.
- **Trust Administration:** The trust administration systems must be developed as cloud surroundings is service provider and it should consist of trust negotiation factor among both parties such as user and provider. For example, to liberate their services provider must have slight bit trust on user and users have equivalent trust on provider.

3.2. Security Issues

- The security of commercial data in the cloud is intricate, as they makes available dissimilar services like NaaS (Network as a service), IaaS (Infrastructure as a service), PaaS (Platform as a service) and SaaS(Software as a service). Every services has their possess protection issues [Rakshit et al. (2009)]
- **Data Security:** It is refers as a secrecy/confidentiality, integrity/reliability and availability. These are the main issues for cloud vendors. Confidentiality is defined as an isolation of data. Confidentiality is designed to thwart the perceptive information from unauthorized or immoral people. In this stores the encryption key data from venture C, stored at encrypted format in venture D. that data must be safe from the employees of venture D. Integrity is defined as the correctness of data, there is no general policies exist for approved data exchanges. Availability is defined as data is accessible on time.
- **Privileged user access:** Exterior the resource data that is processed surrounds anindigeneous risk, as deploy services, avoid the mortal, consistent and human resource manage IT shops works on the house programs.
- **Trust Issue:** Trust is also a major issue in cloud computing. Trust can be in among human to machine, human to human, machine to human. Trust is revolving around assurance and confidence. In cloud computing, user stores their data on cloud storage because of trust on cloud. For example people utilize Gmail server, Yahoo server because they trust on giver.

- **Data Recovery:** It is defined as the process of restoring data that has been lost, corrupted or accident
- **Regulatory Compliance:** Customers are in the end responsible when the sanctuary and completeness of their individual data is taken by a service provider. Conventional service providers more parallel to outsource surveys and security certifications. Cloud computing providers purge to undergo the scrutiny as signaling so these customers can simply make usage of paltry operations [Hussain et al.(2010)].
- **Data Locations:** When users use, they probably won't recognize precisely where their data will hosted and which location it will stored in. In really, they might not even know what country it will be stored in. Service providers requisite to be asked whether they will bring about to storing and alter data in meticulous arbitration, and on the basis of their customers will they create a fair accomplishment to trail local privacy requirement [Lin et al. (2010)].

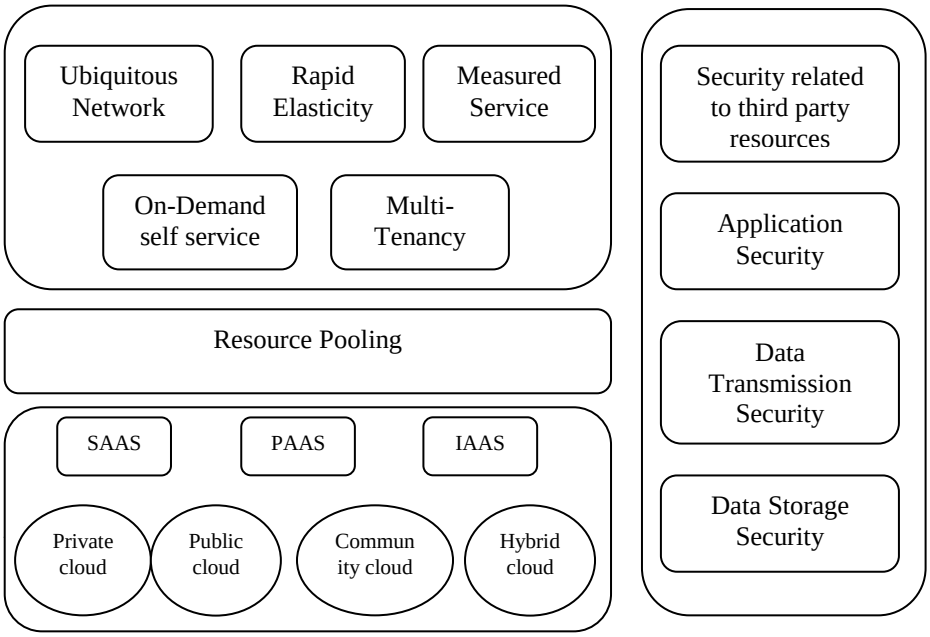

Fig.2 Cloud Security Environment

4. Solution for Cloud Security Issues

The cloud computing have become more popular because many users start to realize its benefits. It allows the user to easily shrink the operation and also help to save cost. However, with the increased adoption rate of the cloud service, the security issues and risk have been increased as well [Grance et al.(2011)]. In order to make cloud computing a better option to increase the user storage capacity and save their confidential information securely, there are few solutions and practice that helps.

4.1. Vulnerability shielding

The cloud service provider should improve the patch management. They should check the vulnerability of their cloud service frequently and always update and maintain the cloud to limit the possible access point and reduce the risk of attack of the cloud by the hackers. The cloud service provider might also use the Intrusion Detection System (IDS) to make sure the cloud service provided is secure and safe.

4.2. Identification management and authentication

When the users want to access the data stored in the cloud, they must be authenticated not only by using the username and password but also the digital data. Multi-level authentication technique introduced by [Kobara et al.(2010)] can also be implemented in cloud computing. The technique generates password in several levels before the user can access the cloud services. Anonymous authentication (i.e. identity of user is protected from the cloud) can also be implemented where only valid users are able to decrypt the

information [Sengar et al. (2012)]. Other than that, proposed scheme by [Kumari et al.(2010)] can also be applied in cloud computing where they claimed that their new password authentication scheme are secured from masquerade , man in the middle attack and off-line guessing. Furthermore, leakage-resilient authentication can also be utilized in order to improve the security of the cloud services.

4.3. Authenticated cloud service provider

The user should make sure that they unearthen the right cloud service provider. Each cloud service provider has diverse approaches on data management in the cloud. Well established and experienced cloud service provider is more trust worthy and better choice. Besides, the standards and regulations of the cloud service provider are also very important. Examples of authenticated clouds service providers are Google and Microsoft, Amazon Web Services (AWS) and IBM. [Ramanathan et al.(2011)] Shares the evaluation of cloud database so that user can have better understanding of every database and prefer the appropriate database accordingly. In order to guide users in choosing the best cloud service provides, CloudCmp have been developed in studies by [Correia et al. (2011)]. They claimed that the application compares the cost and performance of cloud service providers and ensure fairness, representativeness and compliance while limiting measurement cost structure.

4.4. Use cloud service wisely

The data stored in the cloud should be confidential and even the cloud service provider should not have access to those information [Mujinga M. (2013)]. The data stored in the cloud should be well encrypted to ensure the security of the users' information. Anyone who needs access to the data in the cloud should ask for the permission of the users before doing so.

4.5. Facilities for recovery

Cloud service provider should take the responsibility to recover the data of the users if there is any data loss due to certain issues [Bhanumathy et al. (2015)]. Cloud service provider should make sure that they have proper backup and can retrieve and recover the confidential data of the users that might be costly. Moreover, the cloud service providers can also implement the following solutions to ensure data recovery [Sen J (2013)]:

i. By means of fastest disk technology in event of disaster for reproduction of data in hazard.

ii. Altering dirty page threshold.

iii. Forecasting and replacement of risky devices.

4.6. Enterprise infrastructure

The user must secure the data that they want to keep in the cloud infrastructure. The cloud service provider should provide an infrastructure which give facilitates for the users to install and configure hardware components like firewalls, routers, server and proxy server.

4.7. Access control

The cloud service provider should set up the data access control with rights and the users who access the data should be verified by the cloud service provider every time. The cloud service provider must ensure that only the authorized users may have access to the data stored in cloud. The method can help to reduce the risk of the data access by the unauthorized users and thus provide a much secure environment to store sensitive data. In addition, third party auditing can also be one of the alternatives to ensure data integrity of the storage in the cloud [Sengar et al. (2012)]. However, the auditing course of action should have the following properties:

i). Confidentiality/Secrecy: Auditing protocols should maintain user's data confidential against auditor.

ii). Dynamic auditing: The auditing protocol should sustain renews of data in the cloud.

iii). Batch auditing: The auditing protocol should sustain batch auditing for manifold users and clouds.

4.8. Security check events

The users should have clear contract with the cloud service provider so that the users can claim if any accidents or breaches of the sensitive data/information stored in the cloud. The users must have clear agreement with the cloud service provider before using the cloud services provided by that particular cloud service provider. The users should ensure that the cloud service provider give adequate details about fulfillments of guarantees, break remediation and reporting eventuality.

4.9. Data storage regulations

The architecture of the cloud environment is an important aspect to ensure the security of the data stored in the cloud. The users must understand the concept of the data storage regulations which the cloud service provider follows. Cloud service provider that provide security solution compliant with regulations such as HIPAA, PCI DSS, and EU data protection laws are some of the best choice.

5. Applications of Cloud Computing

Aneka has been used in creating more than a few interesting applications in domains such as life sciences, engineering, and imaginative media. Applications created using Aneka are able to run on enterprise or public Clouds devoid of any change. The three case studies on the implement of Aneka for constructing applications in geospatial, engineering and life science domains are explained below.[Sukumar et al. (2012)]

5.1. Manufacturing and Engineering

The Manufacturing and Engineering sectors comprises of a broad variety of market segments, from aerospace to self-propelled. Manufacturing organizations face a number of computing challenges as they pursue to elevate their IT environments, including high infrastructure costs and complexity to meager visibility into aptitude and utilization. Today's design engineers requisite access to unrestrained, bendable computing competence on demand, so that design cycles can be as swift, inexpensive, and productive. The GoFront group, a dissection of China Southern Railway, is accountable for constructing the high speed electric locomotive, metro car, urban transportation vehicle and the motor train. The unprocessed design of the prototypes necessitates utmost quality 3D images using auto desk's rendering software called Maya. By exploring the 3D images, engineers identify problems in the original design and create the suitable design improvements. Nevertheless, such designs on a single four core gave out used to 3 days to submit scenes with 2000 frames. To moderate this time, GoFront has used Aneka and created a venture Cloud (see Figure 3) contained by their company by utilizing networked PCs. They used Aneka Design Explorer, a tool for hasty creation of parameter sweep applications, in which the similar program is executed many times on dissimilar data items (in this case, executing the Maya software for rendering dissimilar images).

5.2. Geospatial Sciences and Technologies

Because of the unremitting intensification of GIS sciences and technologies, there have been even supplementary geospatial and non-spatial data involved owing to intensification in number of data sources and improvement of data gathering methodologies. The spatial analysis and geo-computation are getting elaborate and computationally demanding. The Department of Space, Government of India (GOI), agrees to Aneka as the Cloud computing platform supporting the improvement of high enactment GIS applications [Varadan et al. (2010)].

5.3. Health and Life Science

With the elevated volume and density of data, along with the growing complication of IT ecosystem and the pressures of competition and dictatorial groups, life sciences organizations need IT infrastructure and management tools that can respond quickly to altering needs and, additional outstandingly, enable rather than hamper the aptitude to innovate.

5.4. IT Education and Research

When the IT field is swiftly moving towards Cloud Computing, software industry's emphasis is shifting from developing applications for PCs to Data Centers and Clouds that authorize millions of users to produce exercise of software simultaneously. This is creating a gigantic demand for manpower with skills in this area. Educational and research organizations require a platform that can sustenance (1) manifold models of application programming, (2) manifold classes of Cloud deployments (public, private and hybrid), and (3) extensible outline enabling authors/researchers to develop their own programming models and application schedulers.

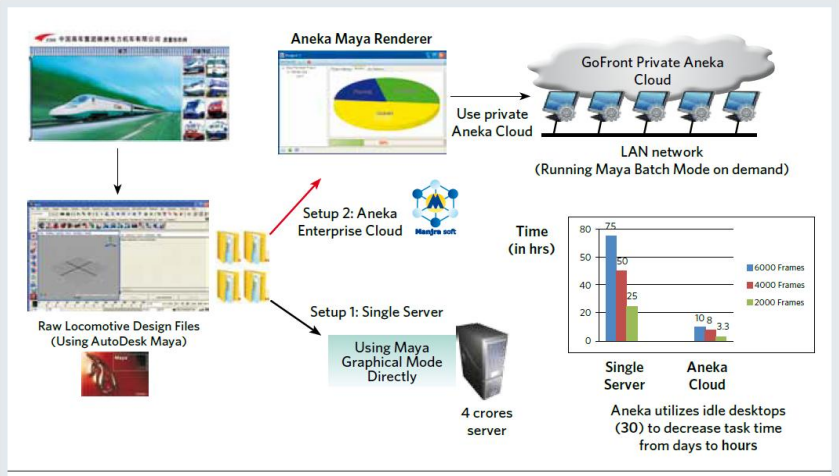

Fig. 3: Rending images of Locomotive design on GoFront's Private Cloud Using Aneka

6. Conclusion

Cloud Computing technology is extensively used technology for data processing and management today. It helps to speed up and enhance the flexibility of data management with less cost. It is incontrovertible that cloud computing has brings us lots of advantages and becoming more popular. Several huge industries have started to use cloud service in their business purpose. While the cloud computing is widely used, the security becomes an apprehension to everyone who use cloud services. There is a lot of security issues arises incessantly while there are improvements as well on the security model of the cloud service provided. Although the increasing employ of the cloud service, the user should use the cloud service provided prudently in a way that always make certain good security practices so that this technology have the prospective to bring the information technology to the subsequent level. Cloud computing might help us to take apart he software from the hardware as more technologies are used as service using cloud and software might have a highly abstract space with the computer hardware. It is expected that this paper provides some basis or foundation in regards to issues and challenges and solutions of cloud computing.

References

[1] GTSI (2011). White Paper on Cloud Computing Building a Framework for Successful Transition.

[2] F. Hao et al. (2010). Enhancing dynamic cloud based services using network virtualization. ACM SIGCOMM Computer Communication Review, vol. 40, no. 1.

[3] C. Y. Gong, J. Liu, Q. Zhang, H. T. Chen, and Z. H. Gong (2010). The characteristics of cloud computing. In Proc. 39th International Conference on Parallel Processing Workshops, pp. 275-279.

[4] D. Farber (2008). Oracle"s Ellison nails cloud computing. [Online]. Available: http://news.cnet.com/8301-13953_310052188.html.

[5] Cloud Security Alliance (2015). Security Guidance for Critical Areas of Focus in Cloud Computing" V3, fromhttps://downloads.cloudsecurityalliance.org/initiatives/guidance/csaguide.v3.0.pdf

[6] Srinivasan, M. K., Sarukesi, K., Rodrigues, P., Manoj, M. S., & Revathy, P (2012). "State-of-the-art Cloud Computing Security Taxonomies: A Classification of Security Challenges in the Present Cloud Computing Environment" In Proceedings of the International Conference on Advances in Computing, Communications and Informatics, pp. 470–476. New York, NY, USA: ACM.

[7] Stanik, A., Hovestadt, M., & Kao, O. (2012). Hardware as a Service (HaaS): Physical and virtual hardware on demand. In 2012 IEEE 4th International Conference on Cloud Computing Technology and Science (CloudCom) pp. 149–154.

[8] Chandrahasan, R. Kalaichelvi, S. Shanmuga Priya, and L. Arockiam (2012). Research Challenges and Security Issues in Cloud Computing. International Journal of Computational Intelligence and Information Security 3.3, pp 42-48.

[9] B.R kandukuri, R.Paturi V, and A.Rakshit (2009). Cloud security issues. IEEE International Conference on Services Computing, Bangalore, India, pp. 517-520.

[10] G. Hughes, D. Al-Jumeily & A. Hussain (2010). Supporting Cloud Computing Management through an Object Mapping Declarative Language. Developments in E-systems engineering.

[11] Feng-Tse Lin, Teng-San Shih (2010). Cloud Computing: The Emerging Computing Technology. ICIC Express Letters Part B: Applications (ISSN: 2185-2766), v1, pp. 33-38.

[12] Mell P and Grance T (2011). The NIST definition of cloud computing Retrieved from http://dx.doi.org/10.6028/NIST.SP.800-145

[13] Sharma S, Soni S and Sengar S (2012). Security in cloud computing National Conf. on Security Issues in Network Technologies 1-6
[14] Shin S H and Kobara K (2010). Towards secure cloud storage Demo for CloudCom.
[15] Sirisha A and Kumari G G (2010). API access control in cloud using the role based access control model Trendz in Information Sciences & Computing (TISC) 135-137
[16] Ramanathan S, Goel S and Alagumalai S (2011). Comparison of cloud database: Amazon's SimpleDB and Google's Bigtable International Journal of Computer Science Issues **8** 6 2 243-246.
[17] Rocha F and Correia M (2011). Lucy in the sky without diamonds: Stealing confidential data in the cloud Proc. of the 1st Int. Workshop on Dependability of Clouds Data Centers and Virtual Computing Environments (DCDV) 1-6
[18] Mujinga M. (2013). Privacy and legal issus in cloud computing SMME position in South Africa Proc. Of the 11th Autralian Information Security Management Conf. 49-59
[19] Sekhar R V, Nandini N, Bhanumathy D and Hemalatha M (2015). Identity based authentication for data stored in cloud International Journal of Advanced Research in Computer Science and Software Engineering **5** 3 243-247.
[20] Sen J (2013). Security and privacy issues in cloud computing. Retrieved from arxiv.org/pdf/1303.4814.
[21] K. Raghavendra, A. Akilan, N. Ravi, K. P. Kumar, and G. Varadan (2010). Satellite Data Product Generation Using Aneka Cloud, Research Demo at the 10th IEEE International Symposium on Cluster, Cloud, and Grid Computing (CCGrid), Melbourne, Australia.
[22] Rajkumar Buyya and Karthik Sukumar(2011) "Platforms for Building and Deploying Applications for Cloud Computing", CSI Communications.