International Journal of
Advances in Scientific Research and Engineering (ijasre)

E-ISSN : 2454-8006

DOI: 10.31695/IJASRE.2020.33653

Volume 6, Issue 1
January - 2020

Users versus Cloud Service Providers, on the Trust, Threats, Confidentiality and Reliability in Using Cloud Computing Services

OKONKWO NGOZI U[1] & DR. MRS A.AJIBOLA[2]

Research Scholar [1], Senior Lecturer [2]

[1-2]Depatment of computer science

University of Abuja, Abuja

Nigeria.

ABSTRACT

Cloud Computing refers to applications and services that run on a distributed network using virtualized resources and accessed by common protocol and networking standards. Cloud computing, abstracts the details of system implementation from users and developers. Cloud computing is portioned in three different types of service provision. In each case, the service is hosted remotely and accessed over the network (usually the internet) through software called a web browser, rather than been installed locally on a customer's computer. the first among the service is; SaaS (Software as a service), which refers to the provision of software in the cloud. Secondly, PaaS (Platform as a service), refers to the provision of service that enables customers to deploy in the supply. Thirdly, IaaS (Infrastructure as a service) refers to services providing computer processing power, storage space and network capacity, which enables customers to run arbitrary software (including operating systems and network applications) in the cloud. Moreover, there is a need for cloud computing in the society today to obtain an optimum service. APA referencing format was used to acknowledge those who have done some work in this area. The method adopted for the analysis of the system in this project work questionnaire development is sampling and data collection. The intention of this project work is of two folds; first; to identify the level of trust the users have in using cloud computing services; secondly; to identify the societal challenges for adopting cloud computing, and the solutions from real-world for the challenges that do not have proper mitigation strategies identified through literature review.

KEYWORDS: *Cloud, Cloud Services, web hosting, Mitigation Techniques, Secure Socket Layer, Virtual Private Network.*

1.0 INTRODUCTION

Cloud computing (CC) is a developing technology which is one of the branches of distributed system, others being grid and cluster computing. The purpose of both grid and cloud computing is to attain resource virtualization. Nonetheless, grid computing and cloud computing have significant difference. The main emphasis of grid computing is to achieve maximum computing, while that of cloud computing is to optimize the overall computing capacity. Thus cloud computing can simply be defined as the practice of using remote server hosted on the internet to store, manage and process data. Cloud computing also provides a way to handle wide range of organizational needs by providing dynamically scalable servers and application to work with which is according to [1].

Top cloud computing service providers such as Amazon, IBM, Drop box, Apple's cloud, Google's applications, Microsoft Azure, etc, are able to attract normal users throughout the world. Cloud computing have presented a new Para grim, which helps its users to store or develop applications dynamically and access them from anywhere and anytime just by connecting to an application using internet in reference to [2]. Depending on user's requirement, cloud computing provides easy and customizable services to access or work with cloud applications. Based on the user necessity, cloud computing can be used to provide platform for designing applications, infrastructure to store and work on company's data and also provide applications to do user's routine tasks.

Identifying security challenges, improvising and updating solutions for handling these challenges is essential in implementing Cloud computing in reference to [3]. This research presents a good literature review and a survey to analyze the most prominent security challenges face during cloud computing between users and their cloud service providers. It will also prove detailed

challenges description and also the challenging situation faced by practitioners, models and architectures. Practices and solutions that help to migrate the challenges are also recommended.

One of the ways in which cloud computing is able to compete with traditional modes of computing is to reduce the costs through the pooling and sharing of the available resources. Traditionally, if a corporate entity wanted to deploy a new database, they would acquire the hardware, software and staff with technical knowledge to lunch and maintain the network. This would generally result in under usage of the network, at least in the initial stages of deployment and operation. In fact, Amazon discovered that their networks were being run at 10% capacity at any given time, to account for occasional spikes in the demand and usage of the network by [4]. Brief descriptions of the platforms, and what each has to offer, both in terms of the advantages and possible disadvantages, following [5].

Cloud computing (CC) is a term given to a technological evolution of distributed computing. Cloud computing has been evolving over a period of time and many companies are effective to use. Without the development of ARPANET (Advance Research Projects Agency Network) by [6] and many other researchers who dreamt of improving the interconnection of the systems, Cloud Computing would never have come into existence. The advent of ARPANET, which helped to connect (for sharing, transferring, etc) a GROUP OF COMPUTERS as stated by [7] led to the invention of internet (where bringing the gap between systems became easy). This internet helped to accelerate multifarious activities such as human interaction (social media, instant messaging, etc), business needs of an organization (online shopping).

Some common benefits of cloud computing according to [8] are;

- Reduced Cost
- Increased Storage:
- Flexibility:
- Greater Mobility
- Shift of IT Focus

These benefits of cloud computing draw lot of attention from information and technology Community (ITC).A survey by ITC in the year 2008, 2009 shows that many companies and individuals are noticing that CC is proving to be helpful when compared to traditional computing methods in [9] .

There are three architectural which exhibits certain characteristics in Cloud Computing which is referred as; The SPI MODEL.

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

Each of these deployment models are explained as follows:

- Public Cloud
- Private Cloud
- Hybrid Cloud
- Community Cloud

DOI: 10.31695/IJASRE.2020.33653

Table 1. Summary of various features of cloud deployment models.

Deployment Model	Manage By	Infrastructure Owned By	Infrastructure Located at	Accessibleand Consumed By
Public	Third party provider	Third party provider	Off-premise	Untrusted
Private				
Hybrid	Both organization and Third party provider	Both organization and Third party provider	Bottom-premise and off-premise	Trusted or untrusted
Community	Third party provider	Third party provider	On-premise	Trusted or untrusted

The users are provided with features rich in applications, dynamically scalable storage services, application developing interfaces and many more by just signing into a web browser/dedicated app. In addition to this, since CC support remote access feature and automatic updates (by cloud SP), any application once updated on a site gets to all its users.

2.0 LITERATURE REVIEW OF RELATED WORK

There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, loading balancing, concurrency control and memory management. Therefore, security issues for many of these systems and technologies are applicable to cloud computing. For example, the network that interconnects the systems in a cloud has to be secure.

Furthermore, virtualization paradigm in cloud computing leads to several security concerns. For example, mapping the virtual machines to the physical machines has to be carried out securely. Data security involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing. In addition, resource allocation and memory management algorithms have to be secure. Finally, data mining techniques may be applicable for malware detection in the clouds – an approach which is usually adopted in intrusion detection system (IDSs).

Organizations using cloud computing as a service infrastructure, critically like to examine the security and confidentially issues for their business critical insensitive applications. Yet, guaranteeing the security of corporate data in the "cloud" is difficult, if not possible, as they provide different services like SaaS, PaaS, and IaaS. Each service has its own security issues.

2.1 The Evolution of Cloud Computing

Long before the term cloud computing was coined; software suppliers were providing services to their customers from remote servers via internet – enabled computers. This was called Application Service Provision (ASP) and was the original platform of IT service delivery to emerge from the convergence of computing and communications in the mid – 1990s. However, the ASP model ultimately was an experiment that failed. Firstly, it involves more complicated initial installation and configuration (at the customer end) than is involved with todays on – demand cloud services. Secondly, it originated as a means of providing software on a one – to – one basis rather than on the one – to – many (multi – tenant) basis of cloud computing, where one supplier has many customers. Consequently, ASP lacked the huge advantage that cloud computing enjoys of being very scalable.

The emergence of software as a service (SaaS) in around 2001 signified the beginning of software delivery based on multi – tenant architecture involving network – based access to software managed from a central location and removing the need for customers to install patches or upgrades.

DOI: 10.31695/IJASRE.2020.33653

The term SaaS is useful because it highlights the principal difference between the internet – based model of software provision and the more orthodox license and installation – based model. The latter involves a customer being granted a license to use a software package, while the former involves the provision of a web – based service under a contract for services. Laconically, the below concept events will x-ray out the evolution of cloud computing in summary:

- 1950s: using mainframe computers the start of automation phase and localized infrastructure were commissioned
- 1960s: this marks the birth of IT service industries, decentralized computing and rise in demand of PCs
- 1990s: demand for high bandwidth, virtual private networks and dot com revolution we emerge
- 2000: IT infrastructure and increase in virtualization
- Beyond 2010: delivery of IaaS, PaaS, SaaS, NaaS and collaborative computing model

2.2 Architecture of Cloud Computing

Cloud computing enhances collaboration, agility, scale, availability and provides the potential for cost reduction through optimized and efficient computing. More specifically, cloud describes the use of a collection of distributed services, applications, information and infrastructure comprised of pools of compute, networks, information and storage resources. These components can be rapidly orchestrated, provisioned, implemented and decommissioned using an on demand utility like model of allocation and consumption. Cloud services are most often, but not always utilized in conjunction with an enabled by virtualization technologies to provide dynamic integration, provisioning, orchestration, mobility and scale. While the very definition of cloud suggests the decoupling of resources from the physical affinity to and location of the infrastructure that delivers them, many descriptions of cloud go to one extreme or another by either exaggerating or artificially limiting the many attributes of cloud. This is often purposely done in an attempt to inflate or marginalize its scope. Some examples include the suggestions that for a service to be cloud – based, that the internet must be used as a transport, a web browser must be used as an access modality or that the resources are always shared in a multi – tenant environment outside of the "perimeter".

Cloud Services are based upon five principal characteristics that demonstrate their relation and differences from traditional computing approaches. These characteristics are:

- Abstraction of infrastructure
- Resource democratization
- Service oriented architecture
- Elasticity/dynamism
- Utility model of consumption and allocation

There are certain services and models working behind the scene making the cloud computing feasible and accessible to end users. Following are the working models for cloud computing, NIST cloud computing definition in [10].

- Deployment Models
- Service Models

The four dimensions of Cloud Cube Model are shown in Figure 2.1 and listed here:

- Physical Location of the Data
- Ownership
- Security Boundary

Sourcing: In sourced or outsourced means whether the service is provided by the customer or the service provider, among the numerous security challenges are;

- Insider user threats
- External attacker threats:
- Data Leakage:
- Integrity

DOI: 10.31695/IJASRE.2020.33653

- Data Segregation:
- User Access:
- Data Quality:
- Availability
- Change Management

3.0 RESEARCH METHODOLOGY

The work aims to use an effective and efficient data collection method in order to guarantee credible results and enable reproduction of work if or when needed. This will involve gathering information or eliciting data in the subject of interest by asking questions which responses will be used to generalize on the subject matter.

From the literature review, most of the writers enumerated the lapses encountered in using cloud computing based on the numerous challenges and changes. The main security issues for the cloud computing comprises more of technologies like; network data base, operating system virtualization, resource scheduling, transaction management, loading balancing, concurrency control and memory management.

I then developed a questionnaire which I administered to the respondents as; IT administrator, IT staffs and students in which I was able the get the responses used for the result and analysis as seen in chapter 4

3.1 Research Design

In the course of conducting this research, the stages involved were; Questionnaire development, Sampling and Data collection

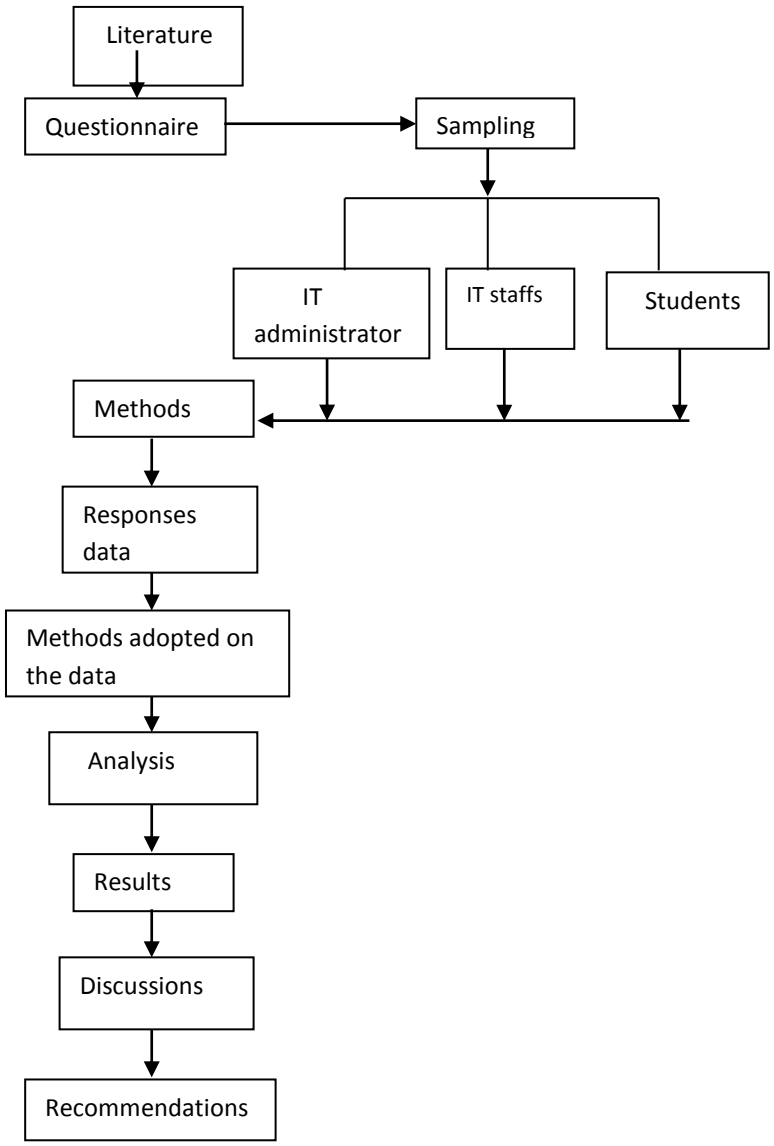

Figure.1 The steps adopted in achieving the research design and analysis.

DOI: 10.31695/IJASRE.2020.33653

3.2 Population Design / Sampling place

This survey is conducted on IT administration and IT staff of the below listed places in and outside Nigeria where more than 50 prospective IT practitioners responded. Survey included thirty one questions. The questionnaire including its rating scale is designed to evaluate the user's perception and security issues of cloud computing. An inquiry tool was developed to assess this questionnaire. Users are rating each question from the given value for evaluation and to promote the cloud computing security and threat concepts. This design method is selected due to its easiness, manageable and security. The work involved from a range of relevant industry users of cloud computing services and universities. The following groups were targeted for the study:

1. Technical officers in Department of Information Technology (IT) in universities. The following universities were used: Nile University of Nigeria, Base University, Gombe State University, Federal University Kashere and Cavendish University Uganda.

2. Technical officers in Department of Information Technology (IT) in the private and public industries. The following industries were used: Kaduna Electricity Distribution Company (KEDCO), Gombe Jewel Café, Mu'azzams Multi-Media, UnlockArewa School of Open Technology.

3. Students in computer science departments; Uniabuja

3.3 Sampling Description

The cluster sampling adopted in the above listed places involves a great concern to the head of the IT of the organizations which are responsible for expressing the capability of their respective staffs in terms of information technology and cloud computing usage. Workshop, conferences, and other academic activities participated by the prospective respondent is very important in choosing respondents.

3.4 Sampling Procedures

In sampling, everyone has an equal chance of being selected. This scheme is one in which every unit in the population has a chance of being selected in the sample. In terms of this research, the chance of been selected as a respondent depend directly on the knowledge of IT (Information Technology) with great emphasis on cloud computing. And the probability of been choose as a respondent is inversely proportional to the knowledge of cloud computing, non – updates on cloud computing practices.

There are two basic types of sampling procedures adopted during this study. These include simple random and cluster sampling.

3.5 Data Collection

The research in the process of collection of data, online facility such as Googles' https://docs.google.com/forms/ was adopted due to its simplicity. It does not require web hosting account or PHP expertise and survey analytics are automatically transcribed into analyzed info-graphics and charted formats, this ensure that the data is adequately utilized to generate accurate summaries and conclusions from the surveyors.

The study was targeted at Cloud – security functionaries of SMEs in Nigeria (based on local knowledge and industry contacts in the country, about 100 respondents are expected). The survey targets ICT – based SMEs, financial organizations and government agencies, which are the internet and cloud services for business communications and/or operations and will be selected by a simple random sampling. Based on the respondents, targets will be identified for further strategic level interviews as expert opinions.

3.6 Method of Analysis

The method of analysis is one respondent's submission, of the complete questionnaire's questions, because while designing the questionnaire, all the questions were marked as required which means they must not be empty. Responses are expended from the above listed sample places invited via email, SMS, Facebook and other social networks. By using Google forms, responses are easily and timely recorded as well as analyzed accordingly.

DOI: 10.31695/IJASRE.2020.33653

4.0 SYSTEM IMPLEMENTATION AND EVALUATION

This comprises result of the survey, where report and identified security challenges and perception of cloud users in terms of the security are depicted, information about the survey participants were also gathered. Also explanation and analysis of results from the survey using bar graphs, pie charts and a software program that proffers a solution to one or two of the threats encountered in using cloud computing etc, as shown;

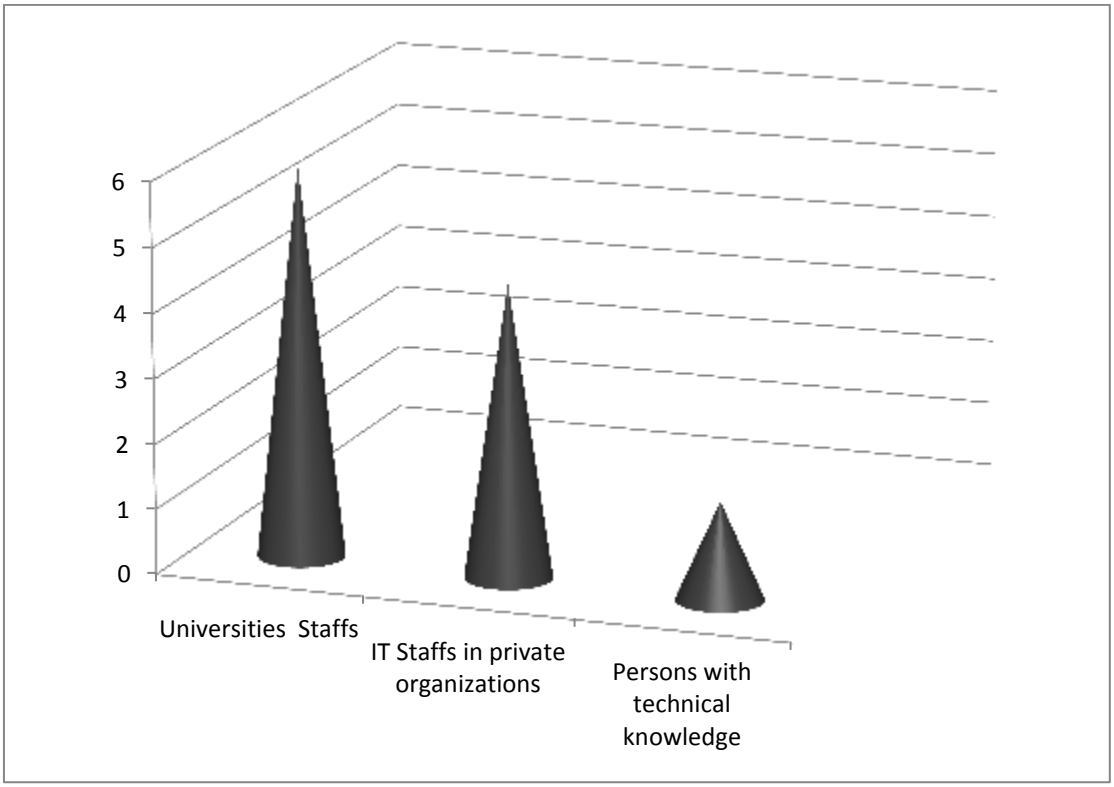

Figure 2: Survey responses bar graphs

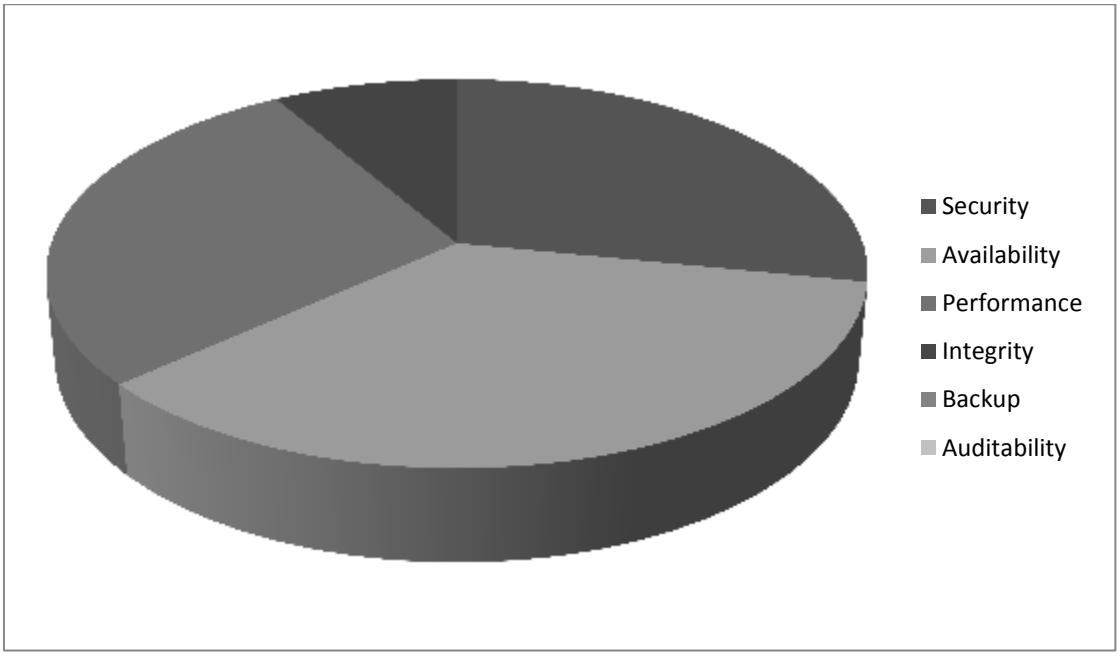

Figure 3: Survey Question 1 response depicted in the pie chart.

The above diagram shows the result of some responses from the respondents which emphasis on the level of Availability, Security, Accountability, Reliability, Performance and Auditability. The records of the most threaten attributes in figure 4.1 shows that security 31% confidentiality 14% and integrity and performance 0%, auditability and backup 28% each.

DOI: 10.31695/IJASRE.2020.33653

A summary of these future security challenge based on the opinions from experts. The results are as follows:

- ✓ Malicious insiders
- ✓ Hypervisor viruses
- ✓ Legal interception point
- ✓ Virtual machine security
- ✓ Trusted transactions
- ✓ Risk of multiple cloud tenants
- ✓ Insecure application programming interfaces
- ✓ Business intelligence
- ✓ Availalability
- ✓ Espionage
- ✓ Privacy
- ✓ Transparency etc

Reported Mitigation Techniques

From analysis of the results, the following security threat techniques were identified. The major security techniques that are used in the current world are:

- ✓ **SSL (Secure Socket Layer) Encryption:** Encryption between browser and web server. I
- ✓ **VPN (Virtual Private Network):** VPN's are not most commonly used for home based or mobile applications.
- ✓ A proper use of encryption can give good protection against eaves dropping.
- ✓ A proper use of encryption can give good protection against active attacks.
- ✓ Intrusion detection system
- ✓ Monitoring agent

Also suggested summarized practices from experts to mitigate future challenges to be faced in Cloud Computing are depicted. The summary includes:

- ✓ Increased efforts in risk management.
- ✓ Standardized security methods and solutions
- ✓ Increased efforts to mitigate harmful code.
- ✓ Analyze the security model of cloud provider interfaces.
- ✓ Ensure strong authentication and access controls are implemented in concert with encrypted transmission.
- ✓ Enforce strict supply chain management and conduct a comprehensive supplier assessment.
- ✓ Analyzes data protection at both design and run time.
- ✓ Better algorithms etc

5.CONCLUSION

The identification of cloud users' security perceptions in Cloud Computing is challenged by considering the large number of services. Most of the responses from the survey, noted that Cloud Computing is use by many users in handling their confidential information. Because it offers many flexible services, provides easy individualized and instant access control to the services and information where they are stored and processed for the users. In the process of identification from the research methods, the research identified satisfactorily number of challenges and mitigation techniques in current and future Cloud Computing.

Additionally, most organizations lack knowledge of Cloud Computing technology. This opens them to various threats as highlighted previously risking resources.

REFERENCES

1. Ruoyu et al (2010). Advent of Cloud Computing Technologies in Health Informatics, pp. 32 – 39.
2. Vaquero et al., (2008). A break in the Clouds: Towards a CloSud Definition, pp. 1 – 6.
3. Tanzim et al (2012). Securing Cloud from Cloud Drain, pp. 1 – 4.
4. Tharam, D. (2010). Cloud Computing: Issues and Challenges, 19 – 21.Dec.p. 43.
5. Mell and Grance (2011). NIST Computer Society Special Publication, pp. 1 – 7.
6. J.C.R. Lincklider in (1960), (Advance Research Projects Agency Network), pp 12-15

DOI: 10.31695/IJASRE.2020.33653

7. James et al (2009). Cloud Computing and Emerging IT Platforms: Vision, Hype and Reality for Delivering Computing as the 5th Utility, pp. 1 – 18.
8. Kresimir and Zeljko (2010). Cloud Computing Security Issues and Challenges, pp. 1 – 3.
9. Ramgovind et al (2010). Tackling Cloud Security Issues and Forensics Model, High Capacity Optical Networks and Enabling Technologies (HONET), 19 – 21, Dec, pp. 190 – 195.
10. National Institute of Science and Technology, Special Publications (2011), spp. 1 – 7.
11. Ahuja, R. (2011). SLA Based Scheduler for Cloud Storage and Computational Services, International Conference on Computational Science and Application (ICCSA), pp. 258 – 262.
12. [2] Albeshri, A. and Caelli, W. (2010). Mutual Protection in A Cloud Computing Environment, 12th IEEE International Conference on High Performance Computing and Communications (HPCC), pp. 641 – 646.
13. [3] Almulla, S. and Chon YeobYeun (2010). Cloud Computing Security Management, 2nd International Conference on Engineering Systems Management and its Applications, pp. 1 – 7.
14. Brenner, M. and Wiebelitz, J. (2011). Secret Program Execution in the Cloud Applying Holomorphic Encryption, Digital Ecosystems and Technologies Conference (DEST), 5th IEEE International Conference 2011, pp. 114 – 119.
15. Hof, R. D. (2006). Cloud Computing as a Facilitator of SME Entrepreneurship, pp. 1 – 6.
16. Iagesse, B. (2011). Challenges in Securing the Interface between the Cloud and Pervasive Systems', 2011 IEEE International Conference on Pervasive Computing and Communications Workshops, pp. 106 – 110.
17. Jaydip (2013). Enterprise Security and Privacy
18. Vijay, T. TREASURE: Trust Enhanced Security for Cloud Environments, Trust, Security and Privacy in Computing and Communications (Trustcom), 2012 IEEE 11th International Conference, Liverpool, 25 – 27, June 2012, pp. 145 – 152.

DOI: 10.31695/IJASRE.2020.33653