RESEARCH ON SECURITY INDEX ACCOMPLISHED BY AN EVALUATED CLOUD COMPUTING NETWORK

[1]K SOWMYA PRIYA, [2]G CHINNA PULLAIAH

[1]Assistant Professor Deapartment of CSE Gokaraju Rangaraju Institute of Engineering and Technology, Hyderabad

[2]Assistant Professor of Department of CSE, Srinivasa Ramanujan Institute of Technology, Anantapur India

ABSTRACT

New developments in information technology (IT) provide opportunities for a better quality of life through benefits such as increased comfort and convenience. Compared to dedicated infrastructures such as cluster and grid computing, cloud computing can better cater to users' needs by increasing effectiveness, efficiency and functionality at a potentially lower cost. This research aims to provide insights into the challenges and issues faced by implementers and users of cloud computing by comparing the extant literature about this issue with current insights provided by IT managers. A systematic literature review and in-depth interviews with IT managers in local government councils were conducted for this research. The research indicated that the factors in the extant literature were supported; additional challenges and issues emerged which are related to effective network, data storage location, availability of different service providers, policy makers, a limited understanding of the cloud and business transformation.

Desirable requirements of cloud computing are to avoid wasting underused resources and increasing response time due to shortage of resources. We notice that recent literature in the field prioritizes the administration of resource provisioning and the allocation algorithms for an energy-efficient management of cloud computing environments. Security metrics can be seen as tools for providing information about the security status of a certain environment. With that in mind, we tackle the management of cloud computing security by using GQM methodology to develop a cloud computing security metrics hierarchy. The main goal of the proposed hierarchy is to produce a security index that describes the security level accomplished by an evaluated cloud computing environment.

1. INTRODUCTION

1.1 CLOUD COMPUTING

Information Technology practitioners always require rapid application development and deployment, but it is very difficult to build business environment. Therefore, the computing aspects of

information society have been revolutionized from distributed to cloud. Cloud is a natural evolution of distributed computing and the general variation of virtualization and Service Oriented Architecture (SOA) [1]. Cloud emphasizes on various service oriented architectures. .

Cloud computing is now proving a bonus to IT users and developers by reducing time and effort required to deploy the application

[2]. Cloud computing refers the means, where everything comes from computing power to application, infrastructure, and the business processes. It is delivered as service whenever , whatever, and wherever it is required. NIST defines cloud computing as a model for enabling ubiquitous, convenient, on -demand network access to a shared poo l of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort s or service provider interaction [1, 3]. This cloud model is composed of f ive essential characteristics (i.e., on demand capabilities, broad network access, resource pooling, rapid elasticity, and measured services), three service models (i.e., IaaS, SaaS, and PaaS), and four deployment models (i.e., public, private, hybrid, and community) [1, 2]. The importance of cloud computing and its adoption can be best described in terms of its underlying characteristics, delivery, and deployment models These models and characteristics lie at the top of each other, thereby forming a stack of a cloud [1, 3].

Amazon refers to cloud computing as, the on-demand delivery of IT resources, and applications via the Internet with pay as you go pricing [3]. Cloud provides rapid access to flexible and low cost IT resources by supporting the critical operations of business applications. The most common aspects for researchers in cloud computing are cloud brokering, cloud workflow management systems, big data cloud services, cloud analytics, cloud configuration and capacity management, mobile cloud architectures and models, IoT-cloud integration, cloud standards, QoS for applications on clouds, privacy, trust, and cloud security etc. Cloud security has been a significant attention for organizations in securing data and useful information on the cloud. Cloud security is still depend upon traditional approaches such as, authentication, authorization, data confidentiality, integrity, availability, and privacy issues, with some additional attacks. Cloud security faces different challenges and issues at various levels in the form of vulnerabilities and attacks. These challenges include multitenancy, cloud secure federation, secure information management, service level agreement, vendor lock -in, loss of control, confidentiality, data integrity and privacy, data intrusion, virtualization vulnerabilities, cloning and resource pooling, motility of data, VM hopping, XML signature attack, XSS attack, browser security, SQL injection attack, and flooding attack [8]. Our research work focuses on various aspects of cloud security such as, authentication, authorization, reliability, and data integrity .

1.2 CLOUD SERVICES

Cloud services are the numerous resources that are provided over the Internet. Standard services are accessed via standard platforms (i.e., desktop, laptop, mobile etc.). There are three standard service models used to describe cloud service delivery. These service models are Software Platform Infrastructure (SPI) model; i.e., Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) [1]. These services are designed to provid e easy, scalable access to applications, resources , and other services that are fully managed by CSP. SaaS is based on the concept of renting an entire finished application from a service provider rather than buying, installing, and running that software. Software licensing is not a critical issue for the SaaS users. SaaS application s such as word processors, CRM, application services etc., are executed on the Internet to process data and propagate information. Some conventional services are also combined with third party commercial services via orchestration to create new application [7]. SaaS increases the speed and reduces the hardware footprint . It also eliminates the version compatibility Some challenges while using the SaaS based application are governance and billing management, synchronization of client -

vendor migration etc. PaaS is all about providing a platform as a service via the Internet upon which the applications can be developed and executed. It works on pay as you go model in a distributed computing environment. The concerns of PaaS are code and data privacy, security, and scalability. Some of its challenges are governance, vendor lock-in, and connectivity. Examples of PaaS are Amazon EC2, Etelos Coghead, Microsoft Azure, Boomi, LongJump,

Google App engine etc. IaaS is offered to provide on-demand computing and storage capabilities. It is also based on a pay as you go model. The computing resources (i.e., processor, memory, storage, and bandwidth) are provided to users by the use of virtualization technology or Virtual Machines (VM). It is based on utility computing architecture. It reduces cost by less hardware, less floor space from the smaller hardware footprint, less cooling cost , and less power consumption. Main challenges in IaaS are the portability of

applications, maturity of system management tools, integration of service boundaries , and scheduling of huge amount of resources a vailable at Cloud Service Provider (CSP) side. Examples of IaaS based applications are HP-Electronic Data Systems (EDS), IBM BlueCloud, SunGrid, Joyent etc.

IaaS vendors deploy virtualization technologies that provide the computing power, whereas Pa aS allows accessing an environment upon which applications can be deployed. In IaaS, a VM is created for the user application and all other things required by the application rather than being restricted to a certain development environment. The user can select own choice of OS images, development environment , and host it on the IaaS vendor in frastructure. In the same way, Data Center or Data as a Service (DaaS) provides data storage services with IT infrastructure moving towards the cloud. It is feasible to offer endeavor level data safety and higher uptime guarantees at a reasonable cost. In order to achieve this, DaaS solution has many layers of built –in redundancy features.

2. LITERATURE REVIEW

Security in cloud is one of the major areas of research. Many researchers have investigated on cloud security.

Chen, D. et al. [4] address that data security affect a lot on the performance of cloud services. They do not help to maintain privacy and originality of content but also help to maintain trust and reliability on service as well service provider. The provide privacy protection mechanism concise all round analysis. They compare their solution with airawet and their concern is to avoid

information leakage from cloud environment. They uses MapReduce framework for deployment of proposed solution.

Tumpe Moyo et al [5] discusses the different types of cloud computing technology and discusses about open source cloud is quickly developing and provides some benefit over proprietary, but currently the proprietary method appears to be best route to take due its stability. Security is still an issue within cloud computing but the research indicates that this is taking a positive turn and is greatly improving as the cloud technology and adoption develops. The survey results demonstrate the popularity of cloud technology. The survey findings will inform the development and deployment of a Cloud based e-learning tool with the required security features.

Dimitrios Zissis et al. [6] introducing a Trusted Third Party, tasked with assuring specific security characteristics within a cloud environment. This paper evaluates cloud security by identify security requirements and attempt to present a possible solution that eliminates these potential threats. In this paper identified generic design principles of a cloud environment which stem from the

requirement to control relevant vulnerabilities and threats. A combination of PKI, LDAP and SSO can concentrate on most of the identified threats in cloud computing dealing with the integrity, confidentiality, authenticity and availability of the data and communications .Security requires a systemic point of view, from which security will be constructed on trust and mitigating protection to a trusted third party in a cloud computing environment.

K. Nasrin, et. al. [7] address that cloud storage frameworks are one of the key research area for cloud computing. Security is one of the major important concerns for research work. They derived a mechanism which is the combination of asymmetric and symmetric key method using RSA and AES algorithm. AES is good for key sharing and low overhead cryptographic mechanism further, RSA is good to create complex phenomena for attackers. The focus of the attackers was on proving secure file communication from vulnerable network.

Jayant, D. et al. [8] proposed role base access control mechanism using AES and RSA algorithm to provide a secure environment for public cloud environment. Here, they uses RSA and AES model for encryption and decryption purpose where RBAC is used for access control purpose. It gives the uploading rights and different rights to different user as per RBAC model.

Cindhamani.J et. al. proposed an improved design for data security. It proposed a concept to achieve integrity, confidentiality and authentication in single architecture. They uses 128 bit key for RSA and Third party auditor for authentication purpose. Here, proposed solution consist two main parts one is storing data into storage and another is retrieve data from storage. This paper ensures the security goals during storage operations and guaranty about valid authentication and access.

Kawser Wazed Nafi et al also introduced a improved framework for security similar with above researchers. They have also proposed OTP mechanism

and security services for secure communication.

Mrudula Sarvabhatla et al. introduced an improved mutual authentication scheme, which is secure and opposed to all major

cryptographic attacks. proposed authentication scheme avoids the expensive resource consuming operations. With negligible computational overload on client and server side and ability to resists all major cryptographic attacks makes our scheme more practical and can be deployed in resource less environment. This scheme is mainly built upon less expensive operations like one-way hash computations and negligible resource consuming XOR operations. Improved mutual authentication scheme is divided into three stages: Registration stage, Login stage, Mutual authentication stage.

Hussain Aljafer et al. describe about some of the major approaches for secure data sharing in cloud computing environment and Specifically focus on the use of encryption schemes and also provide a comparative study of the major schemes,

through implementation of some representative frameworks. The survey is to show how encryption is used in every of the covered technique, and discusses the corresponding open issues The objective is to provide a concise survey of existing solutions, discuss their benefits, and point out any shortcomings for future research.

3. CLOUD COMPUTING SECURITY PROBLEMS

3.1 Cloud Computing Lacks Uniform Standards of Security

At present, the cloud computing security standards are in the initial stage, yet haven’t a complete set of security standards. There are more and more standard organization set out to make cloud computing security standards to increase interoperability and security, reduce repeated investment or repeat invention. For example, Cloud Security Alliance (CSA), Distributed Management Task Force (DMTF) have already launched cloud computing standard work, and made progress [3]. Cloud computing security standards are the measure of clouds user security goals and the ability of cloud service providers. With the uniform standard, the user can choose through the cloud service standard authentication, establishing trust, and once accident happens, also can quickly realize that responsibility.

2.2 Security Problems of Cloud Computing Network Layer

Traditional network attacks: Cloud computing is based on the network structure, so there exist great menace for the traditional network attacks. Basically they are the following kinds: distributed denial of service (DDOS) attack, utilization type attack, information collection type attack and the false news attack. Cloud computing has the characteristics of its own: huge user information resources, highly centralize, complicated management, so are also more likely to become the target of hackers, hackers probably attack the whole cloud computing services via a user, and the damage and loss will be obvious more than the traditional enterprise nets application environment.

Priority access control: Generally speaking, the cloud services has the priority right to access data but not the users, so the user's data may be leaked out by the administrative staff and other employees, unable to guarantee the user's important and confidential data security. SSL attack: Secure Sockets Layer (SSL) is the encryption method to provide security for network communication; a lot of cloud providers employ SSL to guarantee cloud security. Now many hackers and communities are studying the SSL, different from the general way of network attack, at present the SSL attacks are rare, but SSL has become a worry to cloud computing security.

3.3 Data Security of Computing Clouds

Data Location: When use cloud computing services, customers don't know where the data are placed on the servers, even don't know which country these servers are placed in [4]. When these countries need to investigate these data, due to the different law, providers may be forced to submit data and be unable to guarantee the security of user data.

Data separation: In the cloud computing services, a large amount of user data are in a shared environment. In order to reduce spending, providers usually reuse the IP address, the IP address of one user may be reused to another, so often leads to the abuse of the data, there is no guarantee to data privacy. The data encryption is the way to ensure the data security in one way, but encryption does not always guarantee the security of the data, the fail of decryption may cause damage to the data [9]. To users and cloud services the data can't use, this reduces efficiency of data, causes waste of resources.

Data backup: To the important and confidential data, if cloud services dose not backup the data, when data lost by the server problems, or users accidentally delete data, important data can’t be restored.

4. OBJECTIVES

The research objectives of investigation of cloud adoption issues and design of a secure cloud computing environment are as follows:

Performance analysis of various cloud computing tools and technologies.

There are various tools available for the needs of an individual or the organization for deployment of their cloud infrastructure plan. Cloud infrastructure plan include tools such as , Eucalyptus, OpenNebula, Nimbus, OpenStack, ABICLOUD, CloudSim, and CloudStack etc. [1].

Design a framework for cloud environment with log maintenance scheme to improve cloud security and also provide a solution for authentication and authorization in cloud environment

Cloud computing is comprised of major demand from the every group of an organization because of easy availability and cost effectiveness but security has remain a major challenges for the practitioners. Authentication is constantly the biggest concerned for IT industries to adopt cloud computing environment. The availability, performance, key logger attack, malicious insiders, outsider attacks and service disruptions explore are the key research challenges at authentication level. The traditional user name and password is not enough as a single factor for authentication. In this objective, we have proposed a secure cloud computing framework , which uses the first factor as a crypt user name and password along with second factor, i.e., M-pin authentication server, which is similar to ATM pin . Also, this objective focuses on a solution to the threats that are the major issues for the cloud adoption.

Investigation of location signature to improve the performance of cloud computing.

The increasing demand of cloud computing in enterprise architectures allows users to remotely store their data and receive the benefits of on-demand high-quality cloud applications. The existing cloud security approaches are limited to satisfy users for the demand of cloud services and are observed to be insecure, complex , and costly. In this objective, we have proposed a security approach for a cloud environment using location signature and HTML5 WebDB. **Investigation of various virtualization tools for improvement in virtualization aspects.**

Cloud virtualization has created an enormous impact on IT and networking worlds. Virtualization and its exclusive architecture have numerous features and advantages over non -conventional virtual machines. However, it has some new vulnerabilities and attacks on a virtualization based cloud system. XSS based attack is among the top cloud vulnerabilities. This exposure occurs when a user uses the input from a cloud environment application without properly looking into them. It allows an attacker to execute malicious scripts in the cloud environment. The scripts execute harmful actions whe n a user visits the exploited cloud. Existing approaches to mitigate this problem, especially on effective detection of XSS vulnerabilities in the application or prevention of real -time, XSS attacks are not enough. Therefore, the survey of different vulner ability attacks on cloud virtualization is performed and also a concept for the removal of XSS vulnerabilities to secure the cloud environment is presented.

Develop a secure, reliable, and available application using cryptographic algorithm.

Cloud computing provides a service based environment for data storage and resource sharing that are available to user through the Internet with on-demand basis. Thus, users can access their data from any geographical location at any time. Cloud environment also provides better scalability, flexibility, high performance, availability and less storage cost as compared to other physical storage of data. Maintaining data integrity and security in the cloud environment is difficult especially when the stored data is not compl etely reliable, and trustworthy. However, the security of stored data is the major concern for organizations and individual user to adopt cloud based environment. In this objective, we have proposed and enhanced the functionalities of Third Party Auditor (TPA) server to protect the availability and integrity of outsourced data in a cloud environment. The proposed approach uses the functionality such as public verifiability, metadata generation, data dynamics, storage access point, encryption and decryption of data through RSA algorithm and IP range in case of private cloud.

Design a suitable web service API for the secure cloud in mobile cloud environment.

Cloud computing frameworks such as , Google App Engine, Amazon Web Services, Windows Azure, and open source frameworks such as, OpenStack have become increasingly popular among practitioners. Also, the growth in usage and deployment of smartphone platforms and applications worldwide is increasing rapidly. Mobile Cloud Computing (MCC) promotes the use of cloud based services in a mobile environment. Data and complex computing modules are processed in clouds and mobile devices do not need a powerful configuration such as, CPU speed and memory capacity. Mobile devices are unable to utilize resources , communication delay, and unexpected mobile vulnerabilities or attacks. These challenges have a great effect in the improvement of service qualities of mobile cloud. In this objective, the survey of different vulnerabilit ies and attacks on mobile cloud computing are identified and also, we have designed a secure mobile cloud storage environment through an encryption algorithm. The proposed work focuses on the solution for the threats that are the major issues for MCC adoption.

5. PROPOSED METHODOLOGY FOR SECURITY MANAGEMENT INCLOUD COMPUTING

Figure 1 represents the proposed life cycle of security management for cloud computing environments.

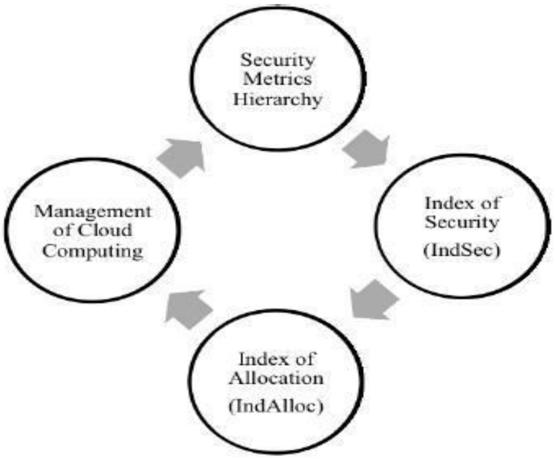

Security Metrics Hierarchy
Index of Security (IndSec)
Index of Allocation (IndAlloc)
Management of Cloud Computing

Fig. 1. Life cycle of Security Management

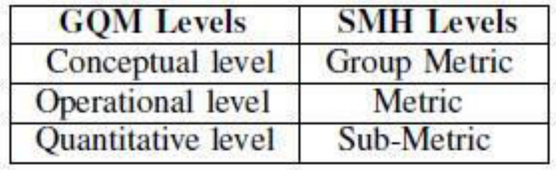
The proposed methodology for security management in cloud computing is based on the following components: i) security metrics hierarchy; ii) security index (IndSec); iii) allocation index (IndAlloc); iv) management of cloud computing.

A security metrics hierarchy is derived from the GQM methodology. A security index (IndSec) will be computed using the security metrics hierarchy, which in turn allows for the calculation of the allocation index (IndAlloc). Finally, the cloud management scheduler will use the allocation index as a reference for the the resource allocation process. In the context of the life cycle of security management (Fig. 1), a security metrics hierarchy is presented as a new form of visualization of security-related information that is collected from the cloud computing environment. A. GQM Methodology

In the 1970s, the GQM method (Goal-Question-Metric) was designed to move testing for software defects from the qualitative and subjective state it was currently in to an empirical model, in which defects would be measured against defined goals and objectives that could then be linked to results.

The GQM methodology defines a measurement model on three levels: i) Conceptual level (goal) - a goal is defined for an object for a variety of reasons, with respect to various models of quality, from several points of view and relative to a particular environment; ii) Operational level (question) - a set of questions is used to define models of the object under study and then attention is focused on that object to characterize the assessment or achievement of a specific goal; iii) Quantitative level (metric) - a set of metrics, based on the models, is associated with every question in order to answer it in a measurable way. In our methodology, the security metrics hierarchy is generated directly from the GQM definition process, during which stage security features are mapped to corresponding security metrics. Table I shows the relationship between the GQM methodology and the security metrics hierarchy (SMH)

TABLE I RELATIONSHIP BETWEEN THE GQM METHODOLOGY AND SMH



GQM Levels	SMH Levels
Conceptual level	Group Metric
Operational level	Metric
Quantitative level	Sub-Metric

For each goal statement identified in the conceptual level, a group metric will be defined. The operational level identifies which objects or activities must be observed or collected to measure the individual components of the goal statement. Lastly, the quantitative level defines which metrics remains explicitly aligned with the higher level goal statement.

B. Security Metrics Hierarchy

The security metrics hierarchy (Fig. 2) is derived from the GQM methodology.

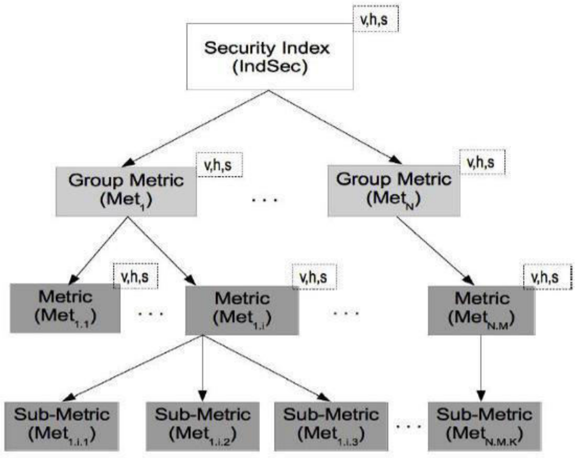


Fig. 2. Security Metrics Hierarchy.

The sub-metric represents a sub-part of a metric; it is used when a metric can be specialized in several ways, with each one having a different contribution to the overall metric. The values in the column Type are: G = Group Metric, M = Metric and S = Sub-metric.

CONCLUSION AND FUTURE WORK

In this article we proposed a methodology for management of cloud computing using security criteria. We presented two strategies for resource management that addresses scalability and granularity in cloud computing. The security index (IndSec) transparently conveys the security level measured in the cloud computing environment for the various security features modeled in the metrics hierarchy. Moreover, this approach has the advantage of supporting hierarchical decomposition, which allows the model to be more scalable and distributed. As for future work, we currently use security metrics that can be measured automatically from the environment, but the process still requires experts to set up limiting values for the ranges, which means that our model is highly dependent on human intervention. Another formulation for calculating the security index can be obtained by combining a weight value for each metric, where each weight value represents the degree of importance among metrics toward composing the metrics set. The security metrics at an upper level could be calculated as a weighted average of the metrics of the level immediately below it. Also, we plan to extend the comparison of strategies for management of cloud computing that were presented (AA and AR), in relation to overhead and performance, for a preliminary set of 180 metrics derived from accepted GQM methodology.

REFERENCES

[1] Daryl C. Plummer, Thomas J. Bittman, Tom Austin, David W. Cearley, David Mitchell Smith, "Cloud Computing: Defining and Describing an Emerging Phenomenon", in Research at Gartner Publication, ID Number: G00156220, 2008.

[2] http://www.cloudsecurityalliance.org.

[3] "Security Breaches-Challenges and Solutions", White Paper at CA Technologies Security Management, 2012.

[4] Deyan Chen and Hong Zhao “Data Security and Privacy Protection Issues in Cloud Computing” 2012 IEEE International Conference on Computer Science and Electronics Engineering.

[5] Tumpe Moyo, Jagdev Bhogal “Investigating Security Issues in Cloud Computing” 2014 IEEE Eighth International Conference on Complex, Intelligent and Software Intensive Systems.

[6] Dimitrios Zissis, Dimitrios Lekkas “Addressing cloud computing security issues” Future Generation Computer System Volume 28, Issue 3, March 2012, (583–592) , Elesvior.

[7] Nasrin Khanezaei, Zurina Mohd Hanapi “A Framework Based on RSA and AES Encryption Algorithms for Cloud Computing Services” IEEE Conference on Systems, Process and Control (ICSPC 2014), 12 - 14 December 2014, Kuala Lumpur, Malaysia.

[8] Bokefode Jayant D, Ubale Swapnaja A, Pingale Subhash V, Karande Kailash J., Apate Sulabha S., “Developing Secure Cloud Storage System by Applying AES and RSA Cryptography Algorithms with Role based Access Control Model” International Journal of Computer Applications (0975 – 8887) Volume 118– No.12, May 2015.

[9] Cindhamani.J, Naguboynia Punya, Rasha Ealaruvi, L.D. Dhinesh babu “An enhanced data security and trust management enabled framework for cloud computing systems” IEEE 5th International Conference on Computing, Communications and Networking Technologies July 11-13, 2014, Hefei, China.

[10] Kawser Wazed Nafi, Tonny Shekha Kar, Sayed Anisul Hoque, Dr. M. M. A Hashem “A Newer User Authentication, File encryption and Distributed Server Based Cloud Computing security architecture” (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 3, No. 10, 2012.

[11] Mrudula Sarvabhatla, Chandra Sekhar Vorugunti “A Robust Mutual Authentication Scheme for Data Security in Cloud Architecture” IEEE Future Information Security Workshop, COMSNETS 2015.

[12] Hussain Aljafer, Zaki Malik, Mohammed Alodib, Abdelmounaam Rezgui “A brief overview and an experimental evaluation of data confidentiality measures on the cloud” journal of innovation in digital ecosystems 1 (2014) 1 – 11, Elesvior.

[13] Nikhil Gajra, Shamsuddin S. Khan, pradnya Rane “Private Cloud Security: Secured User Authentication by using Enhanced Hybrid Algorithm” IEEE 2014 International Conference on Advances in Communication and Computing Technologies.