Surveying and Analyzing Security challenges and Privacy in Cloud Computing

Vaibhav Jain
CSE Department
Amity University Rajasthan
Jaipur, Rajasthan

Mr. Varun Sharma
Senior Lecturer CSE Department
Amity University Rajasthan
Jaipur, Rajasthan

Abstract— Cloud computing is almost similar distributed computing over a network and means the power to run a program on many connected computers at the same time. The word is also, more commonly used to refer to network-based services which seems to be provided by real server hardware, which really are served up by virtual hardware, simulated by software running on one or more real machines. such type of virtual servers do not physically exist and can therefore be moved around and scaled up or scale down on the fly without affecting the end user - arguably, rather like a cloud. Cloud computing is a model to achieve more reliable, on-demand access to a shared pool configurable computing resources. In cloud computing, IT-related abilities are provided as services, accessible without requiring brief information of the underlying technologies, and with minimal management effort. It provides more efficient computing by centralizing storage, bandwidth and memory processing. Adopting cloud computing can result in both negative and positive effects on data security. This paper provides an overview of cloud computing, and discusses related security challenges. We emphasize that even there are many techniques that can improve cloud security, there are in present no one-size-fits-all solutions, and future work has to undertake challenges such as service level agreements for security, as well as holistic schemes for insure accountability in the cloud.

Keywords— Privacy and security; Cloud computing; formatting; security challenges; security strategies .

I. INTRODUCTION

Cloud computing is the latest step in evolution of distributed computing that takes benefit of technology innovations and the internet evolution. It provides suitable, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, applications, and services) that can be quickly provisioned and released with minimal management exertion or cloud provider interaction. Cloud computing technology can be implemented in a wide range of architectures, under diverse service and deployment models, and can coexist among other technologies and software design approaches. The security problems cloud computing presents, however these are difficult, especially for public clouds whose infrastructure and computational property are owned by an outside party that sells those services to the public.

Cloud computing is a new computing approach appeared in 2006, and the evolutionary offspring of parallel computing, grid computing, distributed computing and utility computing, and the developmental outcome of network storage, load balance and virtualization [1]. The core idea of cloud computing is to build a virtualized computing resource pool by centralizing rich computing resources connected with network and present the service of infrastructure, platform and software. This type of network which offers various computing resources is called "*cloud*" [2]. As a supercomputing model based on the Internet, cloud computing allows customers to dynamically share a mass of hardware, software and data resource, and charges according to their actual usage so, computing power can be sold and purchased as goods easily by network in a low price, just like water, electric power and gas. Cloud computing is an innovatory thing alike to electric power changing from a single generator to a centralized electric power plant.

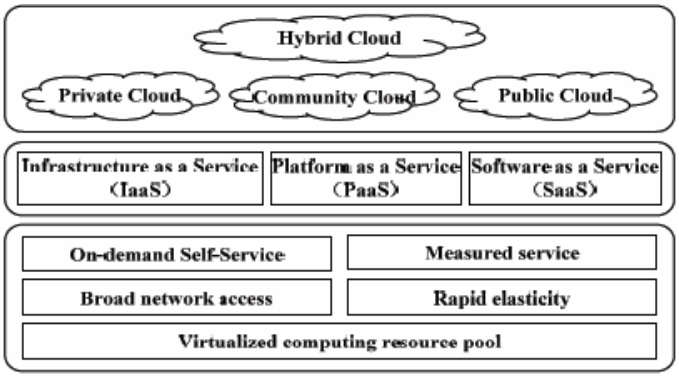

Fig.1. the NIST's definition model of cloud computing [1].

The concept of cloud computing has been introduced for more than a few years, however, there are still a variety of interpretations on what is cloud computing. Since the cloud computing specification of National Institute of Standards and Technology (NIST) has been proposed, the description of NIST about cloud computing becomes the most reliable one widely accepted by researchers. The cloud computing definition of NIST includes five essential features, four deployment models and three service models [3]. In this, the

five vital features includes virtualized computing resource pool, rapid elasticity, broad network access, on-demand self-service, measured service; the three service models are Infrastructure as a Service (IaaS), Software as a Service (SaaS),Platform as a Service (PaaS), the four deployment models are private cloud, public cloud ,community cloud and hybrid cloud.

A. *Cloud deployment model can be classified as private, public, community, and hybrid cloud.*

1) Private cloud : It is owned or rented by an association. The whole cloud resource is dedicated to that association for its private use. An instance of this model is a cloud built by an enterprise to serve their business critical applications.

2) Public cloud : It is owned by a service supplier and its resources are sold to the public. End-users can rent parts of the resources and can typically scale their resource use up (or down) to their requirements. Amazon, Google, Rackspace, Salesforce, and Microsoft are some examples of public cloud providers.

3) Community cloud : It is similar to a private cloud, except where the cloud resource is shared among members of a closed community with similar benefits. An example of a community cloud is the Media Cloud set up by Siemens IT Solutions and Services for the media industry [11]. A community cloud may be handled by a third party (as in the Siemens case), or may be controlled and handled in a collaborative fashion as in the Grid Computing model.

4) Hybrid cloud: It is the mixture of two or more cloud infrastructures, Hybrid cloud can be any private, public, or community clouds. The main purpose of a hybrid cloud is usually to provide additional resources in cases of high demand, for example enabling migrating some computation tasks from a private cloud to a public cloud.

B. *Cloud service models are normally classified as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) .*

1) Cloud SaaS: It is the use of applications running on a cloud infrastructure to offer services to end-users. SaaS can deliver business applications for example customer relationship management (CRM), accounting and enterprise resource planning(ERP). Examples of cloud SaaS are Google Apps [12] and Sales force CRM [13]. The customer does not control underlying infrastructure.

2) Cloud PaaS: It is the use of tools and resources running on a cloud infrastructure to provide services to end-users. The applications are developed and acquired by end-users on top of the tools provided. Microsoft Windows Azure [14] and Google App Engine [15] are instances of cloud PaaS. The customer does not control the underlying infrastructure or operating systems, however does control deployment of individual applications.

3) Cloud IaaS : It is the use of primary computing resources, e.g. storage, servers, networks, to provide services to end users. The end-users can install and run arbitrary software including both applications and operating systems. An instance of IaaS is Amazon EC2 [16]. The customer does not control the primary infrastructure, but can typically launch virtual machines with chosen operating systems which in turn are managed by the customer.

With its lots of advantages, cloud computing is currently being used in huge corporations such as Yahoo, Google, Amazon and Facebook. It is also beneficial for startups, as it saves their initial investment money. Dropbox [17] and Groupon [18] are examples of startups that utilize cloud computing for their daily operations. It is a trend that other organizations are moving their applications to the cloud to reduce investment and function costs and to increase their business efficiency [19].

II. CLOUD COMPUTING SECURITY CHALLENGES

The profit introduced by cloud computing are legion. According to IDC [20], the most beneficial aspects of using cloud include fast and easy deployment, the pay-per-use model, and lessening of in-house IT costs. Though, they also point out that security is the most vital issue to be addressed in order to encourage the widespread use of cloud computing.
Cloud computing providers need to solve the common security challenges of usual communication systems. At the same time, they also must deal with other issues inherently introduced by the cloud computing paradigm itself. In this section, we have categorized the main cloud security issues as traditional and new cloud security challenges.

A. *Traditional security challenges*

Though the security concerns in traditional communication systems also apply to the cloud, the use of cloud computing introduces new attack vectors that will make attacks either possible or simply easier to carry out. The authentication and authorization applications for organization environments may need to be changed to work with a cloud environment. Forensics tasks may become much more hard since the investigators may not be able to access system hardware physically. The availability of cloud service providers is also a big concern, since if the cloud service is disrupted, it affects more customers than in the traditional model. For example, the recent disturbance of the Amazon cloud service took down a number of websites including Reddit, Foursquare, and Quora.finally, virtual machine security is also a difficulty. The

hypervisor and virtual machines used in cloud providers may also have vulnerabilities, as exemplified by Xen [21]. Such vulnerabilities represent an even more serious problem in multi-tenant environments, where the compromise of a virtual machine can distress all users on the same physical server.
Cloud providers, as a result, might need to reconsider traditional security concerns from different angles.

B. Cloud security challenges of the Specifications

As end-users utilize the cloud services and store their information in the provider's infrastructure, the most critical security concern is about privacy and user information confidentiality. End-users want to know where their data is stored, and who is in control of that information in addition to the owners. They also want to be guaranteed that the critical information is not accessed and used illegitimately, even by the cloud providers.

1) Resource location: End-users use the services provided by the cloud providers without knowing exactly where the resources for such services are located, possibly in other governmental domains. This poses a potential trouble when disputes happen, which is sometimes away from the control of cloud providers.

Data stored at the cloud service providers is not only affected by the provider policies but also by the legislation of countries where the providers reside. When using such services, users have to agree to the ''Terms of Service'' which grant the providers the right to disclose user information in compliance with laws and law enforcement requests, for example, as noted in the recent Drop box's Terms of Service [22]. The European Union has issued Directive 95/46/EC [23] to protect user privacy. The directive prohibits transfers of personal data to countries which do not ensure an adequate level of protection. The transfer of personal data outside EU countries is legally possible if it is done with the owner's permission or if it is done to a country having ''safe harbor principle'' agreements with EU, or under some other special cases as mentioned in article 26 of the directive. Though, implementation and enforcement of this directive beyond the EU border in the general case remains an open challenge.

2) Multi-tenancy issue: This matter poses a challenge to protect user data against unauthorized access from other users running processes on the same physical servers. This is in fact not a new matter taking into thought ,the present concern with web hosting services. Even , with the widespread use of cloud computing and with the fact that users store more vital data in the cloud, this issue needs to be reconsidered seriously.

3) Authentication and faith of acquired information: As the critical data is situated in the cloud provider infrastructure, the data may be changed without the owner's consent. The modified information may then be retrieved and processed by the owner to make serious decisions. The authenticity of the information in this case is very essential, and therefore needs to be guaranteed. However, general standards to ensure data integrity do not exist.

4) System monitoring and logs: As more business serious applications are migrated to the cloud, clients may request that cloud providers provide more monitoring and log data for the customers' personnel. As the outcomes of monitoring and logs may have sensitive infrastructure information, and are traditionally used inside by the providers, sharing parts of

Such data to either customers or third-party examiners is not something all cloud providers are ready to do. It will require a lot of negotiation between cloud providers and clients to come up with appropriate monitoring and log information as part of any service contract.

5) Cloud standards: standards are wanted across different standard developing organizations to achieve interoperability between clouds and to increase their stability and security. For instance, the present storage services by a cloud provider may be unsuitable with those of other provider. In order to keep their customers, cloud providers may introduce so called ''sticky services'' which create difficulty for the users if they want to migrate from one provider to the other, e.g., Amazon's S3 is not compatible with IBM's Blue Cloud or Google storage. There are currently a large number of standards bodies with different interests, e.g. IEEE Cloud Computing Standard Study Group(IEEE CCSSG) [24], ITU Cloud Computing Focus Group [25], Cloud Security Alliance(CSA) [26], Distributed Management Task Force(DMTF) [27], Storage Networking Industry Association(SNIA) [28], Open Grid Forum(OGF) [29], Open Cloud Consortium(OCC) [30], and Organization for the Advancement of Structured Information Standards(OASIS) [31], and so on. To promote the wide use of cloud computing, those standards bodies require to sit down and work together for establishing common standards. Possible ''Inter cloud'' standards in the following domains are required to increase cloud interoperability and free data movement among clouds:

- Network architecture,
- Data format,
- Metering and billing,
- Quality of Service,
- Resource provisioning,
- Security, identity management and privacy.

Clearly, there are many general computing standards that may be reused in the cloud, but for the moment, there are to our information no dedicated cloud standards. This may add to the uncertainty for cloud users [32], and is something which must be addressed in the future.

There are currently many open problems in cloud computing security that should be addressed by cloud providers in order to convince end-users to use the technology. The greater part concerns, in our view, are to assurance that user

data integrity and confidentiality is attained while they are stored in the cloud systems. In a lengthy, non-transparent provider chain,

III. THE ORDINARY SECURITY ISSUE OF CLOUD COMPUTING

A. Seven Security Issues of Cloud Computing

Respectively by CSA and Gartner Cloud Security Alliance (CSA) has published a white paper titled Top Threats to Cloud Computing by summarizing a variety of security concerns of cloud computing in March, 2010 [7]. In this white paper, CSA has described seven security risks of cloud computing:

1) *abuse and nefarious use of cloud,*
2) *insecure interfaces and APIs;*
3) *malicious insiders;*
4) *shared technology issues;*
5) *data loss or leakage;*
6) *account or service hijacking;*
7) *unknown risk profile.*

Gartner, a global authoritative IT research and analyst firm, has made a widespread investigation, and summarized seven security risks of cloud computing [8]:

8) *privileged user access;*
9) *regulatory compliance;*
10) *data location;*
11) *data segregation;*
12) *recovery;*
13) *investigative support;*
14) *long-term viability.*

B. Three Parties' Security Issues of Cloud Computing

We analyze the security risks of cloud computing from the view of customer, service provider and government as follows.

1) The security risks confronted by clients. The security risks that customers need to confront in cloud computing environment include: a) The downtime of cloud computing environment that brings great depress to the confidence of clients cannot be avoided completely; b) The leak of commercial secrets that means a nightmare for customer cannot be avoided totally; c) How to face the privilege status of cloud service provider and the security concerns such as fault elimination, business migration and damage compensation etc.

2) The security risks confronted by service providers. The security risks that service providers need to confront in cloud computing environment include: a)How to assure the long-term secure operation of the cloud data center and isolate the fault to reduce its influence to a smallest extent are the security risks that service providers have to face with; b) How to fight against the numerous and aggressive network hackers is a disturbing security problem; c) For customers with various demands, how to effectively and securely manage these customers and identify and block the malicious customers is another unavoidable task.

3) The security risks confronted by government. The security risks that government administrators need to confront in cloud computing environment include: a) How to enhance the security protection of a mass-scale data center is one important concern; b) How to securely manage the numerous and various scale cloud service providers; c) How to evaluate and rank the security level of cloud service providers and the security credit of cloud customers, and publish the proactive alarm of malicious programs.

4) Privacy is the ability of an individual or group to seclude themselves or information about themselves and thereby expose themselves selectively, and it is include [33]: (a) when: a subject may be more concerned about her current or future information being revealed than information from the past, (b) how: a user may be comfortable if friends can manually request his information, but may not want alerts sent automatically, (c) extent: a user may rather have her information reported as an ambiguous region rather than a precise point. In the commercial, consumer context and privacy needs the protection and appropriate use of the information about customers and meeting the expectations of customers about its use. In the industries , privacy entails the application of laws, standards, mechanisms and processes by which personally identifiable information is managed [38].

The privacy issues vary according to different cloud scenario, and can be divided in four subcategories [36] [37] [38], which include: (a) how to make users remain control over their data at the time it is stored and processed in cloud, and avoid theft, nefarious use and unauthorized resale, (b) how to promise data replications in a authority and consistent state, where replicating user data to multiple appropriate locations is an usually choice, and avoid data loss, leakage and unauthorized modification or fabrication, (c) which party is responsible for ensuring lawful requirements for personal information, and (d) what extent cloud sub-contractors involved in processing can be properly recognized, checked and ascertained.

5) Faith is viewed as a measurable belief that utilizes experience, to make honest decisions. It is originally used in social science in constructing human beings' relationship and is now an essential substitute for forming security mechanism in distributed computing environments, as trust has many soft security attributes, such as, dependability, reliability, confidence, honest, trustfulness, belief, security, competence, and suchlike. In fact, faith is the most complex relationship among entities because it is extremely subjective, context-dependent, uncertain, non-symmetric, and partially transitive [9] [10]. Faith evaluation is a multi-phased and multi-faceted

phenomenon based on multi-dimensional factors and trust evaluation cycle, and it is used to find the answer to the question "With which node(s) should I interact and with which I should not?" A measurable trust view is adapted by [34], "Trust of a party A to a party B for a service X is the measurable belief of A in that B behaves dependably for a specified period within a specified context (in relation to service X)." Another mathematical trust view is given in [35], "Trust (or, symmetrically, distrust) is a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action, both before he can monitor such action (or independently or his capacity ever be able to monitor it) and in a context in which it affects his own action." To guard clouds, traditional solid security techniques such as encryption and authorization provide a solid foundation, but they fail when cooperating entities act maliciously because of scale and temporary nature of collaborations.

Faith as a soft social security thinking can fight against such security threats by restricting malicious entities from participating in interactions and consequently offers a high reliable cloud computing environment. Faith issues in cloud computing environments can be divided into four sub-categories [36] [37] [38] [39], which include: (a) how to definition and evaluation faith according to the exclusive attribute of cloud computing environments, (b) how to handle malicious recommend information, which is very vital in cloud computing environments, as faith relationship in clouds is temporary and dynamic, (c) how to consider and provide different security levels of service according to the faith degree, (d) how to manage faith degree change with interaction time and context, and to monitor, adjust, and really reflect faith relationship dynamic change with time and space.

IV. SOME SECURITY STRATEGIES OF CLOUD COMPUTING

When constructing or migrating client business to a cloud environment, its security have to be assured. Here, we give several strategies to contribute a secure cloud environment. Regarding to the security risks of cloud computing, we proposed a number of security strategies as follows.

A. Securely Construction Strategies of Cloud Computing

1) Traditional Security Practice Mechanism: Traditional security practice such as the security protection of physical facilities, computer system, network, software application, and data still work in a cloud environment, and constructing a cloud environment should obey the common global information security standards such as ISO27001. Therefore, the traditional security practice mechanisms should be assured for a secure cloud environment.

2) Virtualization Security Risks Assessment: Regardless of a public or private cloud, the construction and deployment of a cloud environment can't lack numerous virtualization products. Thus, we need to assess the merits and drawbacks and security level of various virtualization technology resolutions and suite products, and choose the best one to decrease the security risks brought by virtualization.

3) Development Outsourcing Risk Control: Constructing a cloud environment is a large-scale systematic engineering with serious work load and many sophisticated technologies, so it is hard to take charge of all development work for an association. A practical action is to handover partial development work to numerous outsourcing parties, which will introduce some security risks. Therefore, we should recognize the security risks incurred by outsourcing service and establish strict control strategies to promise their quality level and security requirements.

4) Portability and Interoperability: Clients must keep in mind that they may have to change service providers for the sake of unacceptable price raise at contract renewal time, business operations ceasing by service providers, unacceptable service quality decrease, partial cloud service closure without migration plans, and business dispute between cloud customer and provider etc. Therefore, portability and interoperability should be considered up front as piece of the risk management and security assurance of any cloud program.

V. CONCLUSIONS AND FUTURE WORK

Cloud computing is a very promising technique that helps organizations reduce operating costs while growing efficiency. Even though cloud computing has been deployed and used in production environments, security in cloud computing is still in its childhood and needs more research attention. Cloud computing is a kind of computing model that can access conveniently a dynamic and configurable public set of computing resources (e.g. storage, server, network, application and related service), provided and published rapidly and on-demand with minimal management and intervention. However, the prevalence of cloud computing is blocked through its security to a great extent. To contribute some attempt to improving the security of cloud computing, we surveyed the main existing security paradigm of cloud computing, and summarized the main security risks of cloud computing from different organizations. Finally, we gave a few security strategies in opposition to these common security problems of cloud computing. In the future, we will beat these security problems with technology and management ways.

REFERENCES

[1] Vaquero L.M., Rodero-Merino L, Caceres J., Lindner M. A break in the clouds: towards a cloud definition. In: ACM SIGCOMM, editor. Computer communication review 2009. New York: ACM Press; 2009.
[2] Boss G, Malladi P, Quan D, Legregni L, Hall H. Cloud computing, 2009. http://www.ibm.com/developerswork/websphere /zones/hipods/ library.html.
[3] Peter Mell, Timothy Grance. The NIST Definition of Cloud Computing (Draft). NIST. 2011.
[4] Cloud Security Alliance. Security guidance for critical areas of focus in cloud computing(v2.1). December, 2009.
[5] VMware. Inc. Understanding full virtualization, paravirtualization and hardware assist. Technical report, VMware, 2007.
[6] Jericho Formu. Cloud Cube Model: Selecting Cloud Formations for Secure Collaboration. April, 2009. http://www.opengroup.org/jericho/ cloud_cube_model_v1.0.pdf.
[7] Cloud Security Alliance. Top Threats to Cloud Computing, 2010. http://www.cloudsecurityalliance.org [accessed on: March,2010.
[8] Heiser J. What you need to know about cloud computing security and compliance, Gartner, Research, ID Number: G00168345, 2009.
[9] Ahamed S I, Haque M M, Endadul Hoque M, Rahman F, Talukder N. Design, analysis, and deployment of omnipresent
formal trust model (FTM) with trust bootstrapping for pervasive environments. *Journal of Systems and Software*; 2010
[10] Karaoglanoglou K, Karatza H. Resource discovery in a Grid system: Directing requests to trustworthy virtual organizations
based on global trust values. *Journal of Systems and Software*; 2011
[11] Siemens IT Solutions and Services. Community clouds: supporting business ecosystemswith cloud computing; 2011. <http://www.it-solutions.siemens.com/
b2b/it/en/global/Documents/-Publications/Community-Clouds-Whitepaper_PDF_e.pdf
[12] Google, Google Apps. <http://www.google.com/apps/>.
[13] Salesforce. Salesforce CRM applications and software solutions. <http://www.salesforce.com/eu/crm/products.jsp>.
[14] Microsoft. Microsoft Windows Azure. <http://www.microsoft.com/windowsazure/>.
[15] Google. Google App Engine. <http://code.google.com/appengine/>.
[16] Amazon. Amazon Elastic Compute Cloud (EC2). <http://aws.amazon.com/ec2/>.
[17] Dropbox, Where Are My Files Stored?; 2011. <http://www.dropbox.com/help/7> [retrieved 26.04.11].
[18] Salesforce. Groupon expands throughout the US and beyond with salesforce; 2011. <http://www.salesforce.com/showcase/stories/groupon.jsp>
[19] Lee Hong Joo. Analysis of business attributes in information technology environments. J Inform Process Syst 2011;7(2):385–96.
[20] IDC Blogs. IT cloud services user survey, pt.2: top benefits & challenges; 2011. <http://blogs.idc.com/ie/?p=210>.
[21] Secunia. Xen multiple vulnerabilities; 2011. <http://secunia.com/advisories/26986/>.
[22] Dropbox's Blog. Privacy, security & your dropbox; 2011. <http://blog.dropbox.com/?p=735>.
[23] European Union. Directive 95/46/EC of the European parliament and of the council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; 1995.
[24] IEEE Cloud Computing Standard Study Group. <http://www.computer.org/portal/web/sab/cloud>.
[25] ITU Cloud Computing Focus Group. <http://www.itu.int/en/ITUT/focusgroups/cloud/Pages/default.aspx>.
[26] Cloud Security Alliance. <http://www.cloudsecurityalliance.org/>.
[27] Distributed Management Task Force. <http://www.dmtf.org/>.
[28] Storage Networking Industry Association. <http://www.snia.org/>.
[29] Open Grid Forum. <http://www.gridforum.org/>.
[30]Open Cloud Consortium. <http://www.opencloudconsortium.org/>.
[31] Organization for the Advancement of Structured Information Standards. <http://www.oasis-open.org/>.
[32] Fogarty Kevin. Cloud computing standards: too many, doing too little;2011.
<http://www.cio.com/article/679067/Cloud_Computing_Standards_Too_Many_Doing_Too_Little>
[33] Krumm J. A survey of computational location privacy. *Personal and Ubiquitous Computing*; 2009
[34] Shekarpour S, Katebi S D. Modeling and evaluation of trust with an extension in semantic web. *Journal of Web Semantics*;2010.
[35] Iltaf N, Hussain M, Kamran F. A mathematical approach towards trust based security in pervasive computing environment.
Proceedings of the Third International Conference and Workshops, ISA 2009; IEEE Press, Jun. 2009.
[36] Paquette S, Jaeger P T, Wilson S C. Identifying the security risks associated with governmental use of cloud computing.
Government Information Quarterly; 2010.
[37] Subashini S, Kavitha V. A survey on security issues in service delivery models of cloud computing. *Journal of Network and
Computer Applications*; 2011.
[38] Pearson S, Benameur A. Privacy, security and trust issues arising from cloud computing. *Proceedings of the 2nd IEEE International Conference on Cloud Computing Technology and Science, CloudCom 2010*; IEEE Press, Nov. 2010, 693-702.
[39] Sangroya A, Kumar S, Dhok J, Varma V. Towards analyzing data security risks in cloud computing environments.
Communications in Computer and Information Science; 2010
[40] http://en.wikipedia.org/wiki/Cloud_computing

AUTHORS PROFILE

Vaibhav Jain Mtech CSE Final Year from Amity University Rajasthan. My sincere Thanks to my Respected Guide Mr. Varun Sharma Senior Lecturer CSE Department Amity University Rajasthan. I thanks all the Members of CSE department and my collegues for their support and help.