SJIF Impact Factor: 6.260| ISI I.F.Value:1.241 Volume: 4 | Issue: 12 | December | 2019 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Peer Reviewed Journal

A SURVEY ON DATA SECURITY ISSUES IN CLOUD COMPUTING

P. Ram Kishor
Assistant Professor,CSE Department,AITAM, Tekkali
D. Sreenu Babu
Assistant Professor,CSE Department,AITAM,Tekkali
T. Ravikumar
Assistant Professor,CSE Department,AITAM, Tekkali

ABSTRACT
Cloud computing is set of resources and provide services over the Internet. The services which are delivered from data centers that are located in the entire the world. General example of cloud services is Google apps provided by Google and Microsoft SharePoint. In cloud computing, IT-related capabilities are provided as services, accessible with minimal management effort and without requiring detailed knowledge of technologies. The rapid growth in cloud computing also increases severe security concerns. Security has always remained a constant issue for internet, when we are talking about security cloud really suffers.Cloud computing is surrounded by many security issues like securing data. Lack of security is the only hurdle in wide adoption of cloud computing.
KEYWORDS: *Pooled resource, Denial-of-Service, hypervisor*

I.INTRODUCTION

Cloud computing has been developed by National Institute of Standards and Technology (NIST). Cloud computing is a model for on-demand network access to a shared pool of configurable computing resources i.e., networks, servers, storage, applications and services that can be hastily provisioned and released with minimal management effort or service provider interaction.

Cloud computing deliver the computing services over the Internet. Cloud provides the services to individuals and businesses to use software and hardware that are managed by third parties at remote locations. Online file storage, social networking sites, webmail, and online business applications are the examples of cloud services. This model allows access information and computer resources from anywhere that a network connection is available. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications.

Characteristics:

The characteristics of cloud computing include on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service. On-demand self-service means that customers (usually organizations) can request and manage their own computing resources. Broad network accessallows services to be offered over the Internet or private networks. Pooled resources means that customers draw from a pool of computing resources, usually in remote data centers. Services can be scaled larger or smaller; and use of a service is measured and customers are billed accordingly.

Service models:

The cloud computing service models are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). In Software as a Service model, a pre-made application, along with any required software, operating system, hardware, and network are provided. In PaaS, an operating system, hardware, and network are provided,

and the customer installs or develops its own software and applications. The IaaS model provides just the hardware and network; the customer installs or develops its own operating systems, software and applications.

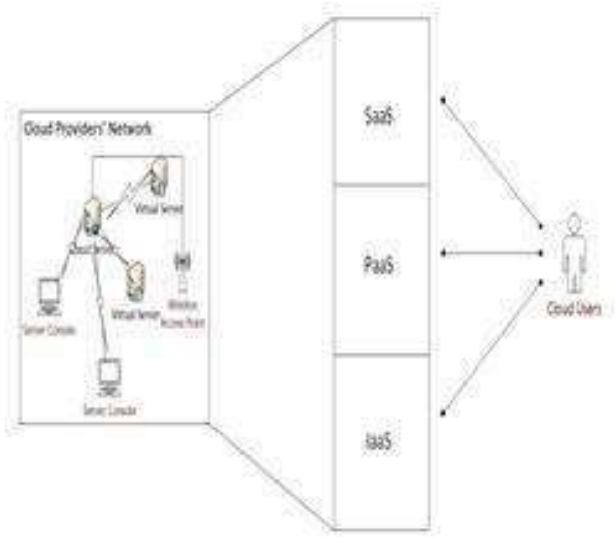
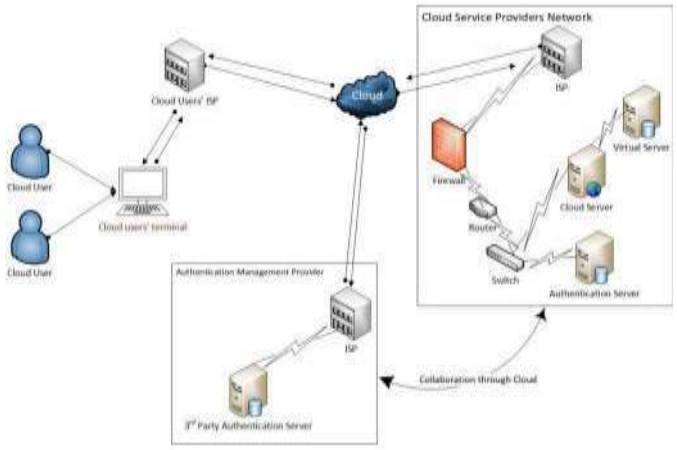


Fig. 1.Cloud Service Hierarchy

Authentication in cloud:

The way to interact with devices, software, data and processes is drastically changed by Cloud computing but still some things never change and one thing that remains true across the old. New computing paradigms are the importance of authentication to confirm the identity of the user and/or system with which we're communicating. Identity management and authentication form the basis for security whether in the cloud or on the local network. Managing identities has been enough of a challenge within the corporate network, and became more so as businesses formed federations for the purpose of sharing resources across organizational lines. Private, public and hybrid clouds are adding yet another layer of complexity. In a private cloud, to which users log on via a virtual private network, authentication can work effectively the same as on a local corporate network. Public clouds may be a different story, since it's all dependent on how the cloud vendor has implemented security.

Multi-factor authentication provides significantly more security but is being implemented slowly, even within local corporate networks, much less in the cloud. Biometric authentication has the potential to be the most secure form of single sign-on once the kinks are worked out, and solves some of the problems inherent in other forms of two-factor authentication. Users don't "forget" their fingerprints, lose them, or go off and leave them at home. And Hollywood fantasies aside, cases of the bad guys severing a finger or removing an eyeball to use it to gain unauthorized access are likely to be few and far between. However, a number of obstacles to adoption still exist, which include cost of biometric scanning equipment and users' fears of invasion of privacy.



Deployment of cloud services:

Cloud services are typically made available via a private cloud, community cloud, public cloud or hybrid cloud. Generally speaking, services provided by a public cloud are offered over the Internet and are owned and operated by a cloud provider. Some examples include services aimed at the general public, such as online photo storage services, e-mail services, or social networking sites. However, services for enterprises can also be offered in a public cloud.

In a private cloud, the cloud infrastructure is operated solely for a specificorganization, and is managed by the organization or a third party. In a community cloud, the service is shared by several organizations and made available only to those groups. The infrastructure may be owned and operated by the organizations or by a cloud service provider.

Problems Associated with Cloud Computing:

In generally most of the people faced these types of problems because people are new to the technology. Organizations also adopting these types of technologies they will take more time. Example Microsoft company launched this technique Windows8 operating system onwards but cloud computing launched1990's.Amazon is also adopted this technique in 2006 onwards.

Most security problems are Loss of control means most customers are aware of the danger of letting data control out of their hands and storing data with an outside Cloud Computing provider. Data could be compromised by the Cloud Computing provider itself or other competitive enterprises which are customers with the same Cloud Computing provider. There is a lack of transparency for customers on how, when, why and where their data is processed. This is in opposition to the data protection requirement that customers know what happens with their data.Many Cloud Computing providers are technically able to perform data mining techniques to analyseuser data. This is a very sensitive function and even more so, as users are often storing and processingsensitive data when using Cloud Computing services. This holds especially true for social mediaapplications that encourage users to share much of their private life e.g. private photos1.Mobile devices, in particular with their limited storage and computing capabilities are drivers forhaving services provided by Cloud Computing instead of using software on individual computers. Evendata that are only to be transferred from one mobile device to another (local) device, are oftentransferred via the cloud, when cloud oriented applications on the mobile devices are involved.Therefore users often put themselves at risk without noticing this, as they assume that the data istransferred locally.Since Cloud Computing is a service, it has to be accessed remotely. The connection between the CloudComputing provider and customer is not always adequately protected. Security risks that threaten thetransfer line include eavesdropping, DNS spoofing, and Denial-of-Service attacks. The paradigm shifts in Cloud computing makes the use of traditional risk management approaches harder even impossible. Irrespective of the fact that control over data is transferred to the CloudComputing provider, risk management and compliance issues are split between the Cloud Computingprovider, Internet provider and customer. However, compliance can be seen as one of the importanttrust factors between the Cloud Computing provider and customer. Regulatory and legislativecompliance is also problematic. Cloud data centers can be geographically dispersed. Thereforelegislative compliance is not currently adequately defined.As all technical control is given to the Cloud Computing provider, customers often want

to have anexternal audit of this provider. Therefore logging and auditing information has to be stored andprotected in order to enable verification. Appropriate logging could provide the possibility for forensicinvestigation in cases of incident.Concerns also exist with regard to deletion of data: It is difficult to delete all copies of electronicmaterial because it is difficult to find all copies. It is impossible to guarantee complete deletion of allcopies of data. Therefore it is difficult to enforce mandatory deletion of data. However, mandatorydeletion of data should be included into any forthcoming regulation of Cloud Computing services, butstill it should not be relied on too much:the age of a "Guaranteed complete deletion of data", if it everexisted has passed. This needs to be considered, when data are gathered and stored.Data Protection and Privacy legislation is not even similar in many countries around the globe yet.Cloud Computing is a global service of the future. Consequently the problems and risks that affect dataprotection rules in Europe must be considered properly when Cloud Computing platforms are locatedon servers in non-European countries.Cloud computing depends on a reliable and secure telecommunications network that assures andguarantees the operations of the terminal users of the services provided in the cloud by the cloudcomputing provider. Telecommunications networks are often provided separately from the Cloud computing services.

Lack of trust:

When it is not clear to individuals why their personal information is requested, or how and by whom it will be processed, this lack of control and lack of visibility of the provider supply chain will lead to suspicion and ultimately distrust. There are also security-related concerns about whether data in the cloud will be adequately protected. As a result, customers may hold back from using cloud services where personally identifiable information is involved, without an understanding of the obligations involved and the compliance risks faced, and assurance that potential suppliers will address such risks. This is particularly the case where sensitive information is involved, for example financial and healthcare information. Ultimately, usage of the cloud is a question of trade-offs between security, privacy, compliance, costs and benefits.Trust is key to adoption of SaaS, and transparency is an important mechanism. Furthermore, trust mechanisms need to be propagated right along the chain of service provision.

Securing the Multi-Tenant Environment:

Hypervisor-Based Segmentation:

Virtualization is quite often the platform that underpins IaaS offerings. Software, such as VMware VSphere, CitrixXenServer, and Microsoft Hyper-V, provides the means of turning a single piece of hardware into a physical host formany VMs. These virtual machines are the databases, file servers, application servers, and Web servers that comprisethe typical physical network, and enable the traffic that makes commerce and communication over the Internetpossible. They are also the servers offered to customers of IaaS for storing their data or running their web-basedbusinesses. At its core, the virtualization platform includes a very specialized and optimized OS called the hypervisor, which in part serves to map traffic from VMs to the underlying VM host hardware so that it can make its way through the data center and out to the Internet and vice versa. The majority of security concerns in the virtualized infrastructurerelate to the co-residency of machines owned by different customers. This places machines in a privileged positionrelative to one another. And this can elevate the risk for many types of breaches such as unauthorized connectionmonitoring, unmonitored application login attempts, malware propagation, and various "man in the middle" attacks.VM segmentation and isolation is also an absolute requirement for VMs containing regulation and compliance intensedata like employee details, customer information, etc. Most regulatory mandates such as Payment Card IndustryData Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act(SOX), and Gramm Leach Bliley Act (GLBA) require that access be limited to a business' need to know, and that controlpolicies be set in place to enforce blocking of unwarranted access. Since the hypervisor intercepts all traffic betweenVMs and VM hosts, it is the natural place to introduce segmentation for the resources of IaaS tenants where VMs mightbe housed within the same VM host or VM host cluster.

CONCLUSION

Cloud providers need to safeguard the privacy andsecurity of personal data that they hold on behalf of organisations and users. In particular, it is essential for the adoption of public cloud systems that consumers and citizens are reassured that privacy and security is notcompromised. Responsible management of personal data is a central part of creating the trust that underpins adoption of cloudbasedservices – without trust, customers will be reluctantto use cloud-based services. Privacy protection builds trust between service providers and users: accountability and privacy by design provide mechanisms to achieve the desired end effects and create this trust. This management can span a number of layers: policy, process, legal and technological. It is universally accepted as best practice that such mechanisms should be built in as early as possible into a system's lifecycle. We are currently carrying out research on ways to improve the protection of private data and thereby enable further

deployment of cloud technologies; these mechanisms include identity management, sticky policies and data obfuscation. By these means users and citizens can be provided with reassurance that their personal data will be protected, and cloud deployments can be made compliant with regulations, even within countries where such regulation is relatively strict. Conforming to legal privacy requirements and meeting client privacy and security expectations with regard to personal information require corporations to demonstrate a context-appropriate level of control over such data at all stages of its processing, from collectionto destruction. The advantages ofcloud computing – its ability to scale rapidly (through subcontractors), store data remotely (in unknownplaces), and share services in a dynamic environment –can become disadvantages in maintaining a level of assurance sufficient to sustain confidence in potential customers. In this paper we have assessed some of the key issues involved, and set out the basis of some approaches that we believe will be a step forward in addressing this situation.

REFERENCES

1. *"Understanding Cloud Computing Vulnerabilities," by B. Grobauer, T. Walloschek and E. Stöcker, IEEESecurity and Privacy, vol. 99, 2010.*
2. *"An analysis of security issues for cloud computing" Keiko*
3. *Hashizume1*, David G Rosado2, Eduardo Fernández-*
4. *Medina2 and Eduardo B Fernandez1*
5. *"Cloud Computing-A Practical Approach" byVelte, Tata McGraw-Hill Edition (ISBN-13:978-0-07-068351-8*
6. *"Addressing cloud computing security issuesDimitrios"Zissis, DimitriosLekkas Department of Product and Systems Design Engineering, University of the Aegean, Syros 84100, GreeceArticle history:Received 14 May 2010 Received in revised form 11 December 2010 Accepted 13 December 2010 Available online 22 December 2010*
7. *"A survey on security issues in service delivery models of cloud computing" S. Subashini, V.KavithaAnna University Tirunelveli, Tirunelveli, TN 627007, India Article history: Received 3 March 2010 Received in revised form11 July 2010Accepted 11 July 2010*
8. *"An Overview and Study of Security Issues & Challenges inCloud Computing"by Rajesh Piplode* Umesh Kumar SinghDepartment of Computer Science Institute Of Computer Science Govt. Holkar Science College Indore-India Vikram University Ujjain-India*
9. *http://www.conres.com/cloud-computing-deployment-models*