ISSN No. 0976-5697

Volume 5, No. 4, April 2014 (Special Issue)

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Trusted Environment in Virtual Cloud

Arif Mohammad Abdul
Department of Computer Science
GITAM University
Hyderabad, INDIA

M Balraju
Department of Computer Science
Mallareddy College of Engg. For Womens
Hyderabad, INDIA

Sudarson Jena
Department of Information Technology
GITAM University
Hyderabad, INDIA

S. Durga Prasad
Department of Computer science
GITAM University
Hyderabad, INDIA

Abstract- On the basis of services provided by the cloud environment, business and IT industries are highly focused to adopt the cloud services. The services provided by cloud are IaaS, PaaS, SaaS on demand basis in terms of low cost and accessibility of data, but customers are threatened by security. Cloud security has gained increasingly emphasis in the research community, with much focus primary concentrated on how to secure the operation system and virtual machine on which cloud system runs on. A trust management system will match the service providers and the customers based on the requirements and offerings. In this paper, we proposed a new method to build a secure and trusted computing system for cloud environment. It includes some important security services, including authentication, confidentiality and integrity, are provided in cloud computing system.

Keywords- Cloud Computing, Trusted System, Virtual Private network, Virtual Private Cloud.

I. INTRODUCTION

Every organization and each user is very much worried about the security of their data storage and maintaining of hardware device at their work places because of data size is increasing rapidly from terabyte to zeta byte. To store this data, increase the memory size of hard disk simultaneously lots of effort is required to maintain this data in the sense of cost.

To overcome the problem of maintaining and storing data the concept of cloud computing was introduced. Cloud computing provides a facility that enable large scale control sharing and inter operation among resources that are dispersedly owned and managed [2]. The opportunities afforded by cloud computing are too attractive for the consumers to ignore in today's highly competitive service environments. The way to realizing these opportunities, however, is not free of obstacles. In cloud computing, with a large amount of various computing resources, users can easily solve their problems with the resources provided by a cloud. The customers are worried to move the data to the cloud because of public. Cloud security has gained increasingly emphasis in the research community, with much focus primary concentrated on how to secure the operation system and virtual machine on which cloud system runs on. A trust management system will match the service providers and the customers based on the requirements and offerings.

Cloud computing has many new characteristics compared with traditional computing mode. Cloud security Alliance (CSA) describes these characteristics as: abstraction of infrastructure, resource democratization, services oriented architecture, elasticity/dynamism of resources and utility model of consumption & allocation [3]; NIST summarizes these characteristics as: on-demand self-service, ubiquitous network access, resource pooling, rapid elasticity and pay per use [4]. Since these cloud facilities are shared resources and generally located in the data center of Cloud Security Provider (CSP), they are under the full control of CSP. Security devices in cloud are also owned and controlled by CSP. On the other hand, customers have no control over the facilities on which their businesses run [5].

They should be security duty separation in cloud computing between CSP and customers. The mechanism of security duty separation must be based on what services the security provides the customers.

Cloud services are currently marketed on their different categories namely Infrastructure as a Service (IAAS), Platform as a Service (PAAS), and Software as a Service (SAAS) [6].

CSP must be responsible for the security of computing platforms and applications they provide. Trust the measure concern of the consumers and provider of services that participate in cloud computing environment. In this paper, we address some limitations of cloud computing for data storage by launch of Amazon Virtual Private Cloud (VPC) [1] resources in to a virtual network. The following limitations are overcome by VPC in this paper:

Loss of Authentication: Authentication is the basic to trust. Each customer is thinking about trust against third party before transferring data to cloud. The customers have to be aware of the identity of cloud service provider and cloud service provider has to be aware of the identity of users who interact with it. To provide authentication VPC allocates a private subnet and logically isolates from other virtual networks in the cloud.

Loss of Confidentiality: The intruders are wide spread security problem, they attack on critical information. Solution is that the customers encrypt the data before storing, but if the data is accessed by distributed applications

CONFERENCE PAPER
Two day National Conference on Innovation and Advancement in Computing
Organized by: Department of IT, GITAM UNIVERSITY Hyderabad (A.P.) India
Schedule: 28-29 March 2014

then required key distribution concept that has difficult on different machines. In VPC, data is placed in a private subnet.

Loss of Availability: When data is moved from company to cloud they face problem of availability due to Daniel-of-service. VPC provides Amazon Web Services (AWS) resources.

Loss and Corruption of Data: Due to data is public intruders are make problem on the data by damaging and deleting from cloud.

The rest of the paper is organized as follows.

Section 2 presents related work on trusted cloud. Section 3 presents Virtual Private cloud computing. The section 4 of this paper presents Security in Virtual cloud computing. The authentication and architecture of Virtual Private Cloud is discussed in section 5, The section 6 of this paper presents concludes the paper.

II. RELATED WORK ON TRUSTED CLOUD

The issue of establishing trust in the Cloud has been discussed by many authors. Much of the discussion has been centred on reasons to "trust the Cloud" or not to. Paper [11] discusses factors that affect consumer's trust in the Cloud and some of the emerging technologies that could be used to establish trust in the Cloud including enabling more jurisdiction over the consumers' data through provision of remote access control, transparency in the security capabilities of the providers, independent certification of Cloud services for security properties and capabilities and the use of private enclaves. The issue with jurisdiction is echoed [9], who further suggest some technical mechanisms including encrypted communication channels and computation on encrypted data as ways of addressing some of the trust challenges. The use of hardware based attestation mechanisms to improve transparency into the enforcement of critical security properties. Cachin [12] contains a survey of security issues in the context of cloud storage services and recent research addressing these issues; Armbrust [13] is a more general survey of cloud computing. Both of these papers point out some of the same challenges that motivate our work. Trusted cloud computing platform (TCCP) which enables laaS providers to serve a closed box execution environment that guarantees confidential execution of guest virtual maschines (VMs).

This system allows a customer to verify if its computation will run securely, before requesting the service to launch a VM. TCCP assumes that there is a trusted coordinator hosted in a trustworthy external entity, however, it is impossible to make the backend of the cloud visible to the third part. Moreover, TCCP lacks the mechanism to protect cloud user's data, once the cloud backend nodes are compromised. Our mechanism is different. TSSC allows the cloud users to indirectly measure the cloud backend, which relies on a remote attestation delegation service (RDS) provided by the cloud provider. So, TSSC can seamlessly cooperate with the current cloud architecture. Further, TSSC provide sealed storage to reduce the leakage risk of cloud user's sensitive data. Krautheim[15] provides a Private Virtual Infrastructure (PVI) that shares the responsibility of security in cloud computing between the service provider and client, decreasing the risk exposure of both. The challenge of PVI is similar to TCCP, which need exposure of every implementation detail to the cloud user and lacks sealed storage ability.

III. VIRTUAL PRIVATE CLOUD COMPUTING

A. *Virtual Private Cloud:*

Trust in cloud computing is more complex than in a traditional IT scenario where the information owner owns his own computers. Before the user uses the cloud, the user of the cloud may want to verify the trusted status of the platform which actually carries out the computing task in the cloud. Trust is the major concern of the consumer and provider of services that participate in a cloud computing environment [16].The remote attestation mechanism in Trusted Computing is suited for the cloud user's verification need. Since cloud computing share heterogeneous distributed resources via the network through in the open Internet Technology environment, thus it makes security problems necessary for us, trusted computing environment including some important security services, authentication, confidentiality and integrity for cloud computing system. Trust is the basis of secure interaction between human society and cyberspace [17].Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.'[18].

Trusted computing implies a redesign of systems architecture in such a way as to support its factorization into relatively discrete components with well-defined characteristics. This permits, in particular, rational decisions based upon reasonable expectations of behavior. Any such systems thinking must be motivated by an analysis of risks so that effort is expended where it may give the best return and an awareness of the limitations of such risk assessment. The most prominent approach to Trusted Computing technology has been specified by the Virtual Private Cloud Computing.

A Virtual Private Cloud (VPC) is a virtual network dedicated to Amazon Web Services (AWS). It is logically isolated from other virtual networks in the AWS cloud. It can select its IP address range, create subnet, route tables, network gateways and security.

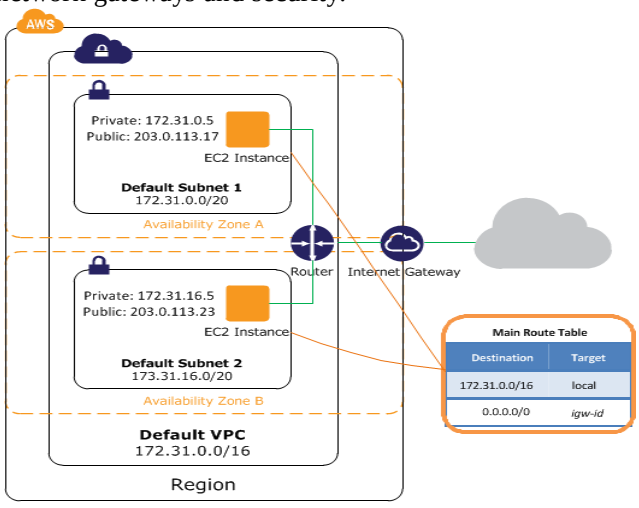

Figure: 1

B. Components of VPC:

When we create a default VPC, we do the following to set it up for you:

a. Create a default subnet in each Availability Zone.
b. Create an Internet gateway and connect it to your default VPC.
c. Create a main route table for your default VPC with a rule that sends all traffic destined for the Internet to the Internet gateway.
d. Create a default security group and associate it with your default VPC.
e. Create a default network access control list (ACL) and associate it with your default VPC.
f. Associate the default DHCP options set for your AWS account with your default VPC.

The following figure illustrates the key components that we set up for a default VPC.

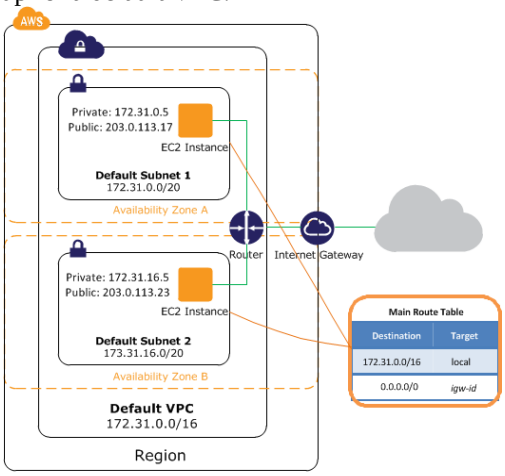

Figure: 2

Instances in a default subnet also receive both public and private DNS hostnames. Instances that launch into a non-default subnet in a default VPC don't receive a public IP address or a DNS hostname.

Using a default VPC as user would use any other VPC; you can add subnets, modify the main route table, add additional route tables, associate additional security groups, update the rules of the default security group, and add VPN connections. User can also create additional VPCs.

C. Default Subnets:

The CIDR block for a default VPC is always 172.31.0.0/16.This provides up to 65,536 private IP addresses. The net-mask for a default subnet is always /20, which provides up to 4,096 addresses per subnet, a few of which are reserved for our use.

By default, a default subnet is a public subnet, because the main route table sends the subnet's traffic that is destined for the Internet to the Internet gateway. You can make a default subnet a private subnet by removing the route from the destination 0.0.0.0/0 to the Internet gateway. However, if you do this, any EC2 instance running in that subnet can't access the Internet or other AWS products, such as Amazon Simple Storage Service (Amazon S3).

D. Creating a VPC:

There are two ways to create a VPC using the Amazon VPC console: the **Create VPC** dialog box and the VPC wizard.

E. Deleting Your VPC:

User can delete your VPC at any time (for example, if you decide it's too small). However, you must terminate all instances in the VPC first. When you delete a VPC, we delete all its components, such as subnets, security groups, network ACLs, route tables, Internet gateways, and DHCP options.

IV. SECURITY IN VIRTUAL PRIVATE NETWORKS

To protect the AWS resources in each subnet, user can use multiple layers of security, including security groups and network access control lists (ACL).

Amazon VPC provides two features that increase security in cloud:

a. Security groups—Act as a firewall for associated Amazon EC2 instances, controlling both inbound and out-bound traffic at the instance level
b. Network access control lists (ACLs)—Act as a firewall for associated subnets, controlling both inbound and outbound traffic at the subnet level. When user launches an instance in a VPC, it associates security groups that created. Each instance in your VPC could belong to a different set of security groups.

V. AUTHENTICATION AND ARCHITECTURE OF VIRTUAL PRIVATE CLOUD

The Virtual Private cloud provides only one way to enter in to the subnet with secure gateway. There is no other way to enter into the subnet so here security, confidentiality and authentication is ensuring by VPC. The auditing result not only ensures strong cloud storage correctness guarantee, but also simultaneously achieves fast data error localization, i.e., the identification of misbehaving server. Considering the cloud data are dynamic

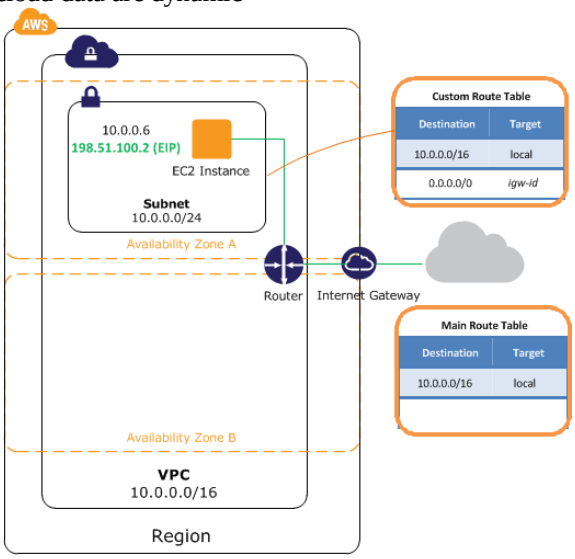

Figure: 3

In nature, the proposed design further supports secure and efficient dynamic operations on outsourced data, including block modification, deletion, and append. Analysis shows the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks.

VI. CONCLUSION

Cloud providers need to safeguard the privacy and security of personal data that they hold on behalf of organizations and users. We have analyzed the trusted computing in the cloud computing environment. Our proposed approach are to extend the trusted computing technology into the cloud computing environment to achieve the trusted computing requirements for the cloud computing and then fulfill the trusted cloud computing. This is achieving by using Virtual Private Cloud.

VII. REFERENCES

[1]. Amazon Virtual Private Cloud, API Version 2013-10-15

[2]. S.Berger, R.Caceres, K.A.Goldman, R.Pervez, R.Sailer and L.van Doom. VTPM: Virtualizing the Trusted Platform Module.In Proc. Of USENIX-SS'06, Berkeley, CA, USA,2006.

[3]. Cloud Security Alliance. Security Guidance for Critical Areas of Focus in Cloud Computing.

[4]. Peter Mell, Tim Grance. Effectively and Securely Using the Cloud Computing Paradigm. NIST, Information Technology Laboratory,3-19-2009 .http://csrc.nist.gov/groups/SNS/cloud-computing-v26.ppt

[5]. Xiao-Yongli, Li-Tao Zhou, Yong Shi, "A Trusted Computing Environment Model in Cloud Architecture" IEEE 11 July 2010.

[6]. C.Vecchiola, S.Pandey, R.Buyya, "High Performance Cloud Computing:A view of Scientific Applications" in 10th International Symposium on Pervasive Systems, Algorithms and Networks, Kaohsiung, Taiwan, pp.4-16, 2009.

[7]. Tim Marher, Subra Kumaraswamy and Shahid Latif "Cloud Security and Privacy" published by O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472.

[8]. Frank E.Gillet, "Future View: The new Technology Ecosystem of Cloud. Cloud services and cloud Computing" Forrester report Aug 2008.

[9]. Krauthiem, F.J., Phatak, D.S., Sherman, "A.T.: Private Virtual Infrastructure: A Model for Trustworthy Utility Cloud Computing". TR-CS-10-04. University of Maryland Baltimore County, Baltimore, MD (2010)

[10]. Krauthiem, F.J: "Private Virtual Infrastructure in Cloud Computing". In: Workshop on hot topics in Cloud Computing, San Diego, CA (2009)

[11]. T. Garfinkel, B. Pfaff, J. Chow, M. Rosenblum and D. Bonch. Terra: " A Virtual Machine-Based Platform for Trusted Computing. In Proc. Of SOSP'03, 2003

[12]. C Cachin, L Keidar, and A. Shraer, "Trusting the Cloud," ACM SIGACT News, 40(2):81-86, June 2009.

[13]. M. Armbrust, A Fox, R. Griffith, A D. Joseph, R. H. Katz, AKonwinski, G. Lee, D. A Patterson, A. Rabkin, 1. Stoica, and M.Zaharia, "Above the Clouds: A Berkeley View of Cloud Computing,"Technical Report EECS-2009-28, University of Cal ifornia at Berkeley, February 2009.

[14]. N. Santos, K. P. Gummadi, and R. Rodrigues, 'Towards Trusted Cloud Computing," Proc. HotCloud, June 2009.

[15]. F. J Krautheim, "Private Virtual Infrastructure for Cloud Computing," Proc. HotCloud, June 2009.

[16]. Zhidong Shen, Qiang Tong. The Security of Cloud Computing System enabled by Trusted Computing Technology. Proc.International Conference on Signal Processing System.

[17]. MELL,P., and GRANCEE,T. The NIST Definitionof Cloud Computing 2009.

[18]. S.ChangXiang,Z.HuanGuo,W.HuaiMin"Research on Trusted Computing and its Development".

CONFERENCE PAPER
Two day National Conference on Innovation and Advancement in Computing
Organized by: Department of IT, GITAM UNIVERSITY Hyderabad (A.P.) India
Schedule: 28-29 March 2014