IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 3 Issue 1, January 2016.
www.ijiset.com
ISSN 2348 – 7968

Survey on Trust Management in Distributed Cloud Environment

V.JaganRaja [1], P.SathishKumar [2] Dr.V.Venkatachalam [3]
[1]M.E Computer Science and Engineering(with Specialization in Networks)
[1]jaganrajav@gmail.com
[2]Head of department/Computer Science and Engineering,[2]psathishsivam@gmail.com
[3]Principal, The Kavery Engineering College, Mecheri

Abstract-As more and more information on individuals and companies are placed in the cloud, concerns are beginning to grow about just how safe an environment it is. It is better to prevent security threats before they enter into the systems and there is no way how this can be prevented without knowing where they come from. Cloud Security and Privacy is the seminal tome to guide information technology in their pursuit of trust in "on-demand computing" as the demand for computing increases ,security and privacy become more critical, Cloud computing is a nascent and rapidly evolving model, with new aspects and capabilities being announced regularly. Although we have done our best in this survey paper to examine risks, trust, trends and solutions to consider when using Distributed Environment as cloud in a mathematical way.

Introduction

Cloud computing is the next generation paradigm in computation, which is continuously growing and emerging. Cloud computing is a new era of computing which refers to both the applications and resources delivered on demand over the Internet as services. The hardware and software resources in the data centers that provide diverse services over the network or the Internet to address the user requirements are called "cloud". According to National Institute of Standards and Technology (NIST),[9] cloud computing provides a convenient on demand network access to a shared pool of configurable computing resources cloud computing is based on five attributes: multitenancy (shared resources), massive scalability, elasticity, pay as you go, and self-provisioning of resources. Multitenancy Unlike previous computing models, which assumed dedicated resources cloud computing is based on a business model in which resources are shared at the network level, host level, and application level. Massive scalability although organizations might have hundreds or thousands of systems, cloud computing provides the ability to scale to tens of thousands of systems, as well as the ability to massively scale bandwidth and storage space. Elasticity Users can rapidly increase and decrease their computing resources as needed, as well as release resources for other uses when they are no longer required. Pay as you go Users pay for only the resources they actually use and for only the time they require them. Self-provisioning of resources Users self-provision resources, such as additional systems and network resources.[1]

2. Public Clouds

Public clouds describe cloud computing in the traditional mainstream sense, whereby resources are dynamically provisioned on a fine-grained, self-service basis over the Internet, via web applications or web services, from an off-site, third-party provider who shares resources and bills on a fine-grained, utility-computing basis. A public cloud is hosted, operated, and managed by a third-party vendor from one or more data centers. The service is offered to multiple customers over a common infrastructure; In a public cloud, security management and day-to-day operations are relegated to the third party vendor, who is responsible for the public cloud service offering. Hence, the customer of the public cloud service offering has a low degree of control and oversight of the physical and logical security aspects of a private cloud.

3. Private Clouds

Private clouds and internal clouds are terms used to describe offerings that emulate cloud computing on private networks. These products claim to deliver some benefits of cloud computing without the pitfalls, capitalizing on data security, corporate governance, and reliability concerns. Organizations must buy, build, and manage them and, as such, do not benefit from lower upfront capital costs and less hands-on management. The organizational customer for a private cloud is responsible for the operation of his private cloud. Private clouds differ from public clouds in that the network, computing, and storage infrastructure associated with private clouds is dedicated to a single organization and is not shared with any other organizations (i.e., the cloud is dedicated to a single

ISSN 2348 – 7968

organizational tenant). As such, a variety of private cloud patterns have emerged: Dedicated Private clouds hosted within a customer-owned data center or at a collocation facility, and operated by internal IT departments Community Private clouds located at the premises of a third party; owned, managed, and operated by a vendor who is bound by custom SLAs and contractual clauses with security and compliance requirements Managed Private cloud infrastructure owned by a customer and managed by a vendor[14]

4. Hybrid Clouds

Hybrid clouds combine both public and private cloud models. [8] They can help to provide on-demand, externally provisioned scale. The ability to augment a private cloud with the resources of a public cloud can be used to maintain service levels in the face of rapid workload fluctuations. This is most often seen with the use of storage clouds to support Web 2.0 applications. A hybrid cloud also can be used to handle planned workload spikes. Sometimes called "surge computing," a public cloud can be used to perform periodic tasks that can be deployed easily on a public cloud. Hybrid clouds introduce the complexity of determining how to distribute
Applications across both a public and private cloud. Among the issues that need to be considered is the relationship between data and processing resources. If the data is small, or the application is stateless, a hybrid cloud can be much more successful than if large amounts of data must be transferred into a public cloud for a small amount of processing. [2]

5. Security

Because cloud computing represents a new computing model, there is a great deal of uncertainty about how security at all levels can be achieved. That uncertainty has consistently led information executives to state that security is their number one concern with cloud computing [4]

6. Secure Software Development Life Cycle (SecSDLC)

The SecSDLC involves identifying specific threats and the risks they represent, followed by design and implementation of specific controls to counter those threats and assist in managing the risks they pose to the organization and/or its customers. The SecSDLC must provide consistency, repeatability, and conformance. The SDLC consists of six phases, and there are steps unique to the SecSLDC in each of phases:

6.1 Phase 1.Investigation:

Define project processes and goals, and document them in the program security policy.

6.2 Phase 2.Analysis:

Analyze existing security policies and programs, analyze current threats and controls, examine legal issues, and perform risk analysis.

6.3 Phase 3.Logical design:

Develop a security blueprint, plan incident response actions, plan business responses to disaster, and determine the feasibility of continuing and/or outsourcing the project.

6.4 Phase 4.Physical design:

Select technologies to support the security blueprint, develop a definition of a successful solution, design physical security measures to support technological solutions, and review and approve plans.

6.5 Phase 5.Implementation:

Buy or develop security solutions. At the end of this phase, present a tested package to management for approval.

6.6 Phase 6.Maintenance:

Constantly monitor, test, modify, update, and repair to respond to changing threats. In the *SecSDLC*, application code is written in a consistent manner that can easily be audited and enhanced; core application services are provided in a common, structured, and repeatable manner; and framework modules are thoroughly tested for security issues before implementation and continuously retested for conformance through the software regression test cycle. Additional security processes are developed to support application development projects such as external

ISSN 2348 – 7968

and internal penetration testing and standard security requirements based on data classification. Formal training and communications should also be developed to raise awareness of process enhancements.
IaaS (Infrastructure as a Service), as the name suggests, provides you the computing infrastructure, physical or virtual machines and other resources like virtual-machine disk image library, block and file-based storage, firewalls, load balancers, IP addresses, virtual local area networks etc.

Example: Amazon EC2, Microsoft Azure, Rackspace, Google Compute Engine.

7. IaaS

In the most basic cloud-service model & according to the IETF (Internet Engineering Task Force), providers of IaaS offer computers physical or virtual machines and other resources. IaaS clouds often offer additional resources such as a virtual-machine disk image library, raw block storage, and file or object storage, firewalls, load balancers, IP addresses, virtual local area networks (VLANs)[15], and software bundles. IaaS-cloud providers supply these resources on-demand from their large pools installed in data centers. For wide-area connectivity, customers can use either the Internet or carrier clouds[8][11]

8. PaaS (Platform as a Service)

PaaS allows platform access for clients so that they can put their own software's and applications on to the cloud.[8][11] In the PaaS models, cloud providers deliver a computing platform, typically including operating system, programming language execution environment, database, and web server. Application developers can develop and run their software solutions on a cloud platform without the cost and complexity of buying and managing the underlying hardware and software layers. With some PaaS offers like Microsoft Azure and Google App Engine, the underlying computer and storage resources scale automatically to match application demand so that the cloud user does not have to allocate resources manually. The latter has also been proposed by an architecture aiming to facilitate real-time in cloud environments. Even more specific application types can be provided via PaaS. [3]

8. Solutions for Security

8.1 Encrypt Everything

In the cloud our data is stored somewhere you just don't know exactly where . however we some basic parameters

- Our data lies with in a virtual machine guest operating system, and we control the mechanisms for access to that data
- Net work traffic exchanging data between instances is not visible to other virtual hosts
- For most cloud storage services, access to data is private by default. Many including Amazon s3, nevertheless allow you to make that data public

8.2 Encrypt your network traffic

No matter how lax our current security practices,we probably have network traffic encrypted at least for the most part .A nice future of Amazon cloud is that virtual servers. I still recommended against relaying on this feature ,since it may not be true of other providers .Furthermore ,Amazon might roll out a future feature that renders this protect ion measure obsolete .we should therefore encrypt all network traffic ,not just web traffic

8.3 Encrypt your Backups

When we bundle our data for backups, we should be encrypting it using some kind of strong cryptography, such as PGP etc .we can then store it in a moderately secure cloud storage environment like Amazon S3 etc, or even in an insecure environment .Encryption eats up CPU. As a result, I recommended first copying our files in plain text over to a temporary backup server whose job it is to perform encryption, and then uploading the backups into our cloud storage system .not only does the use of a backup server avoid taxing our application server and database server CPUs, it also enables we to have a single higher security system holding our cloud storage access credentials rather than giving those credentials to every system that needs to perform a backup

8.4 Encrypt your file systems

Each virtual server we manage will mount ephemeral storage device or block storage devices , the failure to encrypt ephemeral devises poses only a very moderate risk in an EC2 Environment because the EC2 Xen system zeros out that storage when your instance terminates ,snapshots for block storage devices however ,sit in Amazon S3 unencrypted unless you take special action to encrypt them. The most secure approach to both scenarios is to mount ephemeral and block storage devices using an encrypted file system. Managing the startup of a virtual server using encrypted file systems ultimately ends up being easier in cloud and offers more security The Challenge with encrypted file systems on server's lies in how we manage the decryption password .A given server needs our decryption Password before it can mount any given encrypted file system. The most common approach to this problem to store the password on the unencrypted root file system. Because the objective of the file system encryption to protect against the physical access to the disk damage , the storage of the password on a separate , unencrypted file system is not as problematic as it appear on the face of it –but still it's problematic .In the Cloud ,we don't have to store the decryption password .Instead ,we can provide the decryption password to our new virtual instance when we start up .The server can then grab the encryption key out of the servers startup parameters subsequently mount any ephemeral or block devices using an encrypted file system.

8.5 Password Assurance Testing

If the SaaS security team or its customers want to periodically test password strength by running password "crackers," they can use cloud computing to decrease crack time and pay only for what they use. Instead of using a distributed password cracker to spread the load across nonproduction machines, you can now put those agents in dedicated compute instances to alleviate mixing sensitive credentials with other workloads

9. Data Security

The ultimate challenge in cloud computing is data-level security, and sensitive data is the domain of the enterprise, not the cloud computing provider. Cloud users face security threats both from outside and inside the cloud. Many of the security issues involved in protecting clouds from outside threats are similar to those already facing large data centers. In the cloud, however, this responsibility is divided among potentially many parties, including the cloud user, the cloud vendor, and any third-party vendors that users rely on for security-sensitive software or configurations.[6]

10. Virtual Machine Security

The main purpose of virtualization is to improve the performance of a server by providing users virtual machines within an operating system.[7] In the cloud environment, physical servers are consolidated to multiple virtual machine instances on virtualized servers. Not only can data center security teams replicate typical security controls for the data center at large to secure the virtual machines, they can also advise their customers on how to prepare these machines for migration to a cloud environment when appropriate. Firewalls, intrusion detection and prevention, integrity monitoring, and log inspection can all be deployed as software on virtual machines to increase protection and maintain compliance integrity of servers and applications as virtual resources move from on-premises to public cloud environments.

11.Mathematical model of cloud computing data center based on OpenFlow

Cloud computing data center can be represented as a weighted undirected graph of the form:

$$Cloud = (Devices, Links, type, wn., wsw., wst., wl.), (1)$$,where

set of vertices Devices = Nodes ∪ Switches ∪ Storages ∪ {Cont 0} denotes network devices including computing nodes Nodes = {N1,N2,...,Nn}, OpenFlow switches = {S1,S2,...,Sm}, network storages = {F1,F2,...,Fr} and OpenFlow controller Cont 0, edges Links = {Lij} represent bidirectional network links. Type of each network device d ∈ D can be determined by function type: $Devices \rightarrow \{"node","switch","storage","controller"\}$. Cont0 is a special computing node executing OpenFlow controller (network operating system). Function wn. for each computing node Ni calculates the vector of its characteristics

ISSN 2348 – 7968

$$wn.(Ni) = (wn.stat.(Ni),wn.dyn.(Ni,t)), (2)$$

Where wn.stat.(Ni) and wn.dyn.(Ni,t) are respectively denote static parameters and dynamic characteristics of Ni. Node static parameters are represented by a vector

$$wn.stat.(Ni) = (Mi,Di,Ci,Pi) (3)$$

of its RAM size Mi, local disk size Di, computing cores count Ci and their performance characteristics Pi = (Pi1,Pi2,...,PiCi). Dynamic characteristics can be described by vector function:

$$wn.dyn.(Ni,t)= (mi(t),di(t),uik(t),vmi(t)). (4)$$

Here mi(t), di(t) are respectively denote available RAM and disk size at the time $t \geq 0$, uik(t) utilization of node Ni core k at the time t. vmi(t) is a set of virtual machine instances running at the time t. All this information can be collected at regular intervals by SNMP protocol. Each OpenFlow switch Sj ∈ Switches also has static parameters and dynamic characteristics:

$$wsw.(Sj)=(wsw.stat.(Sj),wsw.dyn.(Sj,t)). 5)$$

Static parameters of Sj include the following values:

$$wsw.stat.(Sj) = (Tpj,Pcj,OFj,Tcj,Tsj), (6)$$

where Tpj ∈{"100 Mbit Ethernet","1 Gbit Ethernet","10 Gbit Ethernet"} denotes supported version of Ethernet protocol, Pcj is a number of switch ports, OFj ∈{"1.0","1.1","1.2","1.3"} is a version of supported OpenFlow protocol. Tcj denotes a number of flow tables in the switch Sj. Each table has maximum Tsj flow entries. Dynamic characteristics of the switch are represented by vector:

$$wsw.dyn.(Sj,t) = (Ftj(t),Qj(t),Ptj(t)). (7)$$

Here Ftj(t) = (Ftj1(t),...,FtjTcj(t)) reflects the current state of all Tcj flow tables. At the moment t each flow table Ftjk(t) contains Rcj(t) OpenFlow rules (flow entries). Each of them has the following form:

$$Rl = (Mtl,Cnl,Acl). (8)$$

Mtl is a matching part of the rule, Cnl - statistical counters and Acl represents the set of actions. All incoming packets are compared against flow entries of the flow tables. If a matching entry is found (its Mtl part is matched against incoming packet), then all actions of Acl are performed on the packet and counters Cnl are updated. Otherwise packet is forwarded to controller Cont0. The contoller is responsible for determining how to process packets without flow entries in switches flow tables, it manages the switches flow tables by adding and removing flow entries

12. Summary and Further Research

Trust is a critical aspect of cloud computing. We examined and categorized existing research and practice of trust mechanisms for cloud computing in five categories– reputation based, SLA verification based, transparency mechanisms (self-assessment and information revealing), trust as a service, and formal accreditation, audit, and standards. Most current work on trust in the cloud focus narrowly on certain aspects of trust; our thesis is that this is insufficient. Trust is a complex social phenomenon, and a systemic view of trust mechanism analysis is necessary. In this paper we take abroad view of trust mechanism analysis in cloud computing and develop a somewhat informal and abstract framework as a route map for analyzing trust in the clouds. In particular, we suggest: (1) a policy-based approach of trust judgment, by which the trust placed on a cloud service or a cloud entity is derived from a "formal" audit proving that the cloud entity con- forms to some trusted policies; (2) a "formal" attribute- based approach of trust judgment, by which particular attributes of a cloud service or attributes of a service provider are used as evidence for trust judgment, and the belief in those attributes is based on formal certification and chains of trust for validation. To support this mechanism, we propose a general structure of evidence- based trust judgment, which provides a basis to infer the trust in a cloud entity from the belief in the attributes that entity has, and in which, based

ISSN 2348 – 7968

on the semantics of trust, we define the attributes to be examined are in a space of two-dimensions–domain of expectancy and source of trust including competency, integrity, and goodwill. Future research will focus on mathematical formal frameworks for reasoning about trust, including modeling, languages, and algorithms for computing trust.[13]

Information Data Security
Encryption (transit, rest, processing)
User Security & Monitoring
Identity Services –AuthN/Z, delegation, provisioning
Application Level Security
Application stack , Service , Database
Infrastructure and Architectural Security
PaaS –Storage *Guest OS Level –Firewall,Monitoring* *Hypervisor- Security FirewallNetworkLevel* *BGP,Load Balancing*

Figure-1 Introduction to Cloud Security

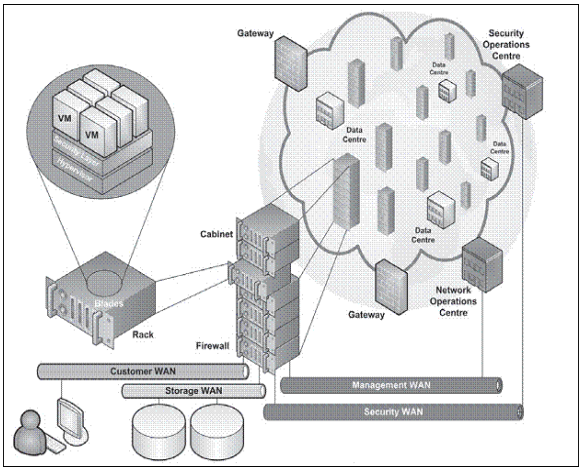

Figure- 1 Cloud Security Architecture

ISSN 2348 – 7968

References :

[1] "Cloud Security and Privacy " An Enterprise Perspective on Risks and Compliance by Tim Mather ,Subra Kumaraswamy , Shahed Latif

[2] "Introduction to Cloud Computing Architecture " by Sun Microsystems White Paper 1st Edition, June 2009

[3] en.wikipedia.org/wiki/Cloud_computing

[4] "Cloud Application Architectures",Building Applications and Infrastructure in the Cloud by George Reese

[5] "Mathematical model of cloud computing data center based on OpenFlow" by P.N. Polezhaev, A.E. Shukhman, U.A. Ushako

[6] "Clearing the clouds away from the true potential and obstacles posed by this computing capability". by Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin,, and Matei Zaharia

[7] "Network Security for Virtual Machine in Cloud Computing" by Hanqian Wu, Yi Ding, Chuck Winer, Li Yao

[8] "Emerging Security Issues and Challenges in Cloud Computing" S C Rachana ,Dr. H S Guruprasad

[9] Security and Privacy Issues in Cloud Computing Environment: A Survey Paper Kaleem Ullah and M. N. A. Khan

[10]Security and Privacy Issues in Cloud Computing Environment: A Survey Paper Kaleem Ullah and M. N. A. Khan
10 Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments by Dawei Suna, Guiran Changb, Lina Suna and Xingwei Wanga

[11]Trust in Cloud Computing Prasad I. Bhosle andSwapnil A. Kasurkar PADM. DR. V B KOLTE COE Malkapur

[12] Enhancing Trust Management in Cloud Environment Soon-Keow Chong, Jemal Abawajy, Masitah Ahmad, Isredza Rahmi A. Hamid

[13] Research on Trust Management Strategies in Cloud Computing Environment Wenjuan LI , Lingdi PING , Qinlong QIU , Qifei ZHANG

[14] Cloud Computing Trust Models: A Survey by Shweta Tharwani, Ajit Kumar Shrivastava Computer Science and Engineering Department Truba Institute of Engineering & Information Technology Bhopal, India

[15] Trust Management in Cloud Computing: A Critical Review Mohamed Firdhous, Osman Ghazali and Suhaidi Hassan