International Journal of Scientific Research & Engineering Trends
Volume 7, Issue 1, Jan-Feb-2021, ISSN (Online): 2395-566X

A Survey on Security of Clouds and Trust Model Techniques

Sidharth Mohan, Asst. Prof. Jayshree Boaddh
Dept. of Computer Science &Engineering
Mittal Institute of Technology Bhopal,
Madhya Pradesh, India
jayshree.boaddh@gmail.com

Asst.Prof. Jashwant Samar
Dept. of Computer Science & Engineering
UIT-RGPV
Madhya Pradesh, India
jashwantsamar.samar2@gmail.com

***Abstract*- Cloud computing is an Internet-based computing and next stage in evolution of the internet. It has received significant attention in recent years but security issue is one of the major inhibitor in decreasing the growth of cloud computing. However, this sole feature of the cloud computing introduce many security challenges which need to be resolved and understood clearly. This paper gives a detailed survey on IAAS security issues. As virtual machine should be secured to handle data and maintain privacy. Methods proposed by various scholars are explained which directly or indirectly enhance the security of cloud. Paper has list some of trust techniques developed by researchers for identifying any malicious machine.**

***Keywords*- Cloud Computing, Fuzzy logic, Trust Computing, Resource Management.**

I.INTRODUCTION

Companies can fundamentally change their information technology strategies as they turn to the cloud for datac enter and information technology services to improve scal ability and global reach, and to lower overhead. There are many benefits to cloud computing: lower overall cost of IT ownership, increased flexibility, fault tolerance, locality flexibility ability, and to respond to new business require ments quickly and efficiently.As with any new technology, this new way of operating brings new risks and challenges, especially when considering the security and privacy of information stored and processed within the cloud [1].

One of the risks of cloud computing is that the users, who are the information owners, lose control of their data when they release the information into the cloud for processing. Relinquishing physical control of the datacenter infrastru cture and information increases the risk of data compro mise considerably[2]; however, benefits (including lower operating costs and increased availability [3]) of moving to cloud computing for services may be significant enough to justify the risk. This dissertation provides solutions for information owners to increase their trust level in cloud computing providers and assure that their private and confidential information is kept secure.

Ensuring the security and integrity of information in the cloud becomes an issue as the management and ownership of the hosting platforms is removed from the consolidated control of a single facility and a single owner. Many organ izations such as financial institutions,health care providers, and government agencies are legally required to protect their data from compromise due to the sensitivity of their information[4].Generally, these organizations are required to manage and maintain their own datacenters with strin gent physical and logical protection mechanicins ensuring that their data remains protected. These organizations simply cannot utilize cloud computing in a generic manner due to the inherent risk of data compromise from systems they do not control.

II. CLOUD COMPUTING SERVICES

1. Software as a Service (SaaS):
The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface,such as a web browser (e.g.,web-based email),or a program interface [5].

The consumer does not manage or control the under lying cloud infrastructure including network, servers, operating systems,storage,or even individual application capabilities, with the possible exception of limited user specific applic ation configuration settings.

2. Platform as a Service (PaaS):
The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired appl ications created using programming languages, libraries, services, and tools supported by the provider [6]. The consumer does not manage or control the underlying cloud infrastructureincluding network,servers,operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

3. Infrastructure as a Service (IaaS):
The capability provided to the consumer is to provision processing, storage, networks, and other fundamental com

© 2021 IJSRET

puting resources where the consumer is able to deploy and run arbitrary software,which can include operating sys tems and applications [7].

The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications and possibly limited control of select networ king components.
The two major technologies that enable IaaS cloud comput -ing are virtualization and elastic computing which are described in depth later in this section. In IaaS, all of the facilities required for a datacenter application are available over the Internet which clients purchase as an outsourced service and are shared among a large number of consu mers to allow for lower costs. This section also provides a brief introduction to trusted computing technologies. While trusted computing technologies are not specifically related to cloud, the merging of cloud and trusted computing technologies is the focus of this dissertation.

3.1 Virtualization:
Virtualization is the process of decoupling hardware from the operating system on a physical machine.A Virtual Machine (VM) is the virtualized repre sentation of a physical machine that is run and maintained on a host by a software virtual machine monitor or hype rvisor[7].The hypervisor implements the virtualization on the physical machine and can be one of two types.

- **Type1** hypervisors are sometimes referred to as native hypervisors as they run on "bare metal," or directly on the host's hardware to control the hardware and to monitor guest operating-systems.
- **Type2** hypervisors are hosted hypervisors, meaning they are software applications running within a conve ntional operating-system environment.

3.2 Elastic Computing:
Elastic computing provides scalable on demand computing resources that are delivered asa service over Internet technologies[8]. Elastic compute clouds have automated management that handles the allocation and provisioning of VMs on cloud computing resources. This management layer provides up and down scalability of infrastructure resources. Amazon's Elastic Compute Cloud (EC2)[9] is one implementation of elastic computing. EC2 can have many different applications and servers, from many clients, simultaneously running with in its cloud. Each client's view of the cloud will be different from another client's view.

Elastic computing biggest advantage is its payment and use model.In a traditiona lIT approach, organizations would have to purchase enough processing, storage, and network hardware to support their peak computing requir ements, aswell as provide for space,power,and cooling for the hard ware.In elastic computing, processing, storage and band width incur charges of actual usage based on a normalized unit of measurement. The elastic computing payment model allows clients to reduce their TT cost by only pay ing for the resources when they are used.

III. LITERATURE SURVEY

Azad et al. [10] proposed machine to machine reputation system to evaluate the trustworthiness of machines in IoT. Only reputation social trust metric is considered in this study. The participantsa ssign a trust value to the machine based on their experiences and interactions with the mac hine. Then, they send trust values' cryptograms to the bul letin board.Utilizing secure multi party computation meth ods, the reputation requester calculates the global reput ation of machine by utilizing the reported crypto grams in the bulletin board.

Rafey et al. [11] to enhance cooperation between trusted nodes and adjust the trust scores dynamically based on the node behavior. In this model, node transaction attributes (e.g.,node computation power, confidence, context import ance, and feedback),and node social attributes(e.g., friend ship, centrality, and relationship) are considered. In the trust computation phase,each node computes the overall trust values of other nodes based on its own direct intera ctions and recommendations from other nodes. Also, their model integrates the social relationships and context of interactions in the trust computation.The trust accuracy in this model can be affected by recommendations from dishonest nodes that assign higher trust values to their group of allies.

Chen et al. [12] for effective service composition and resi stance against trust-related attacks. In their model, they consider both QoS trust metrics including energy status and quality reputation and social trust metrics based on social similarities. However, this study doesn't consider the contextual and dynamic nature of trust.

Pei Yun Zhang et. al. in [13] paper proposes a new trust model and related algorithm to decrease trust management overhead and improve malicious node detection ability based on domain partition.Partitioning nodes into domains is helpful for decreasing the overhead of trust management in terms of trust storage and computation. Domain and cross-domain sliding-windows are proposed and utilized to store the most recent trust values. Then, an algorithm is designed tocompute domain and cross-domain trust values for nodes, and a filter procedure is adopted to remove malicious trust evaluations and malicious nodes from a domain.

The authors of [14] proposed a CamFlow model as a proto type implementation of a data-centric security model in PaaS cloud.CamFlow enforces the information flow cont rol strategy at the kernel level and executes the inform ation flow control strategy between machines while excha nging messages.

© 2021 IJSRET

The authors of[15] proposed a two layer information flow control model for the cloud environment, designed and implemented a prototype system, that can provide cloud tenants with information flow tracking and control as a service,and proposed a protection mechanism for common system attacks such as stack over flow and buffer over flow.
In [16], by analyzing the behavior of entities and linking them with trust levels and security classes,security attribu - -tes were dynamically formulated, thereby enhancing information flow control to ensure the security attributes of tenants and organizations. Due to the sharing of virtual machine resources, it is difcult to identify the information ow boundary of tenant virtual machines.

The authors of [17] proposed a dynamic control method for tenant sensitive information flow based on virtual bou ndary recognition, which combines the concepts of centra lized and decentralized information flow control. Thus, a dynamic control method was established for sensitive information flow.

IV. ATTACKER TYPES AND RISKS

Many of the security threats and challenges in cloud comp uting will be familiar to organizations managing in house infrastructure and those involved in traditional outsourcing models. Each of the cloud computing service delivery models threats result from the attackers that can be divided into two groups [18].

1. Internal Attackers:
- Is employed by the cloud service provider, customer or other third party provider organization supporting the operation of a cloud service
- May have existing authorized access to cloud servi ces, customer data or supporting infrastructure and applications, depending on their organizational role
- Uses existing privileges to gain further access or supp ort third parties in executing attacks against the confid entiality integrity and availability of information with in the cloud service.

2. External Attackers:
- Is not employed by the cloud service provider, customer or other third party provider organization supporting the operation of a cloud service.
- Has no authorized access to cloud services, customer data or supporting infrastructure and applications
- Exploits technical, operational, process and social eng ineering vulnerabilities to attack a cloud service provi der, customer or third party supporting organization to gain further access to propagate attacks against the confidentiality, integrity and availability of informati on within the cloud service.

3. Cloud Security Risks:
The security risks associated with each cloud delivery model vary and are dependent on a wide range of factors including the sensitivity of information assets, cloud architectures and security control involved in a particular cloud environment. In the following we discuss these risks in a general context, except where a specific reference to the cloud delivery model is made [18].

3.1 Privileged user access: Cloud providers generally have unlimited access to user data, controls are needed to address the risk of privileged user access leading to compromised customer data.

3.2 Data location and segregation: Customers may not know where their data is being stored and there may be a risk of data being stored alongside other cus tomers' information.

3.3 Data disposal: Cloud data deletion and disposal is a risk, particularly where hardware is dynamically issu ed to customers based on their needs. The risk of data not being deleted from data stores, backups and physical media during decommissioning is enhanced within the cloud.

3.4 E-investigations and Protective monitoring: The ability for cloud customers to invoke their own electronic investigations procedures within the cloud can be limited by the delivery model in use, and the access and complexity of the cloud architecture. Customers cannot effectively deploy monitoring syst ems on infrastructure they do not own; they must rely on the systems in use by the cloud service provider to support investigations.

3.5 Assuring cloud security: Customers cannot easily assure the security of systems that they do not directly control without using SLAs and having the right to audit security controls within their agreements.

V. TRUST MODELS

The trust in cloud computing is divided into various categories namely Reputation Based Trust, SLA verifi cation based trust, Policy-based trust, Evidence-based trust and Societal trust [19, 20].

1. Reputation Based Trust: The reputation of an entity is the collected estimation of public's trust towards that entity. Generally, many entities in a community trust an entity that has high reputation; an entity, which is required to build trust decision on a trustee, uses the reputation to compute or approximate the trust level of the trustee. The reputation of cloud affects the selection process of cloud services;therefore,CSPstryto construct and preserve higher reputation. Reputation is classically represented by a broad score reflecting the overall outlook,or a small number of scores on numerous foremost aspects of performance.
2. SLA: Verification based trust, after establishing the pre liminary trust and accessing a cloud service, the cloud user is required to validate and re-examine the trust value. SLA

© 2021 IJSRET

is a lawful agreement between the two communica ting parties, user and provider. Therefore, monitoring the QoS parameters and verification of SLA document are essential source of trust management for cloud computing. In CSP party is required to provide these types of services.

3. Policy-based Trust: It is required to construct a "formal".In a related area, Public Key Infrastructure (PKI) is an exte nsively used technology that utilizes "formal" trust method ologies to support key certification, digital signature and validation.It also supports data attribute certification and validation. In this, the trust in a Certifica tion Authority(CA) is dependent on the CA's confirmation with definite certificate policies. It is taken w.r.t to delivering and retaining public key certificates which are validated. Certificate policies play a main role in PKI trust.

4. Evidence-Based Trust: A belief of trustor in the pred ictable behavior of trustee is based on the proof about attri butes of adaptness, helpfulness and honesty. With respect to that expectation evidence-based trust is expressed as follows:believe(c,attrb1(sb,av1))∧... ∧ believe(c, attrbn(sb, avn)) → trust_ * (c, sb, x, ct) which states that if a cloud user c believes a subject sb has attribute attrb1 with value av1, ..., attribute attrbn with value avn, then u trusts (it is either trust in belief or other one)sbw.r.t x,the performance of sb or information is believed by sb, in a particular context ct.

5. Societal Trust: Consists of any individual and a com pany. In cloud also, each entity must be trusted. In Informa tion security service sector, trust plays a vital role between the supplier and the client to help the business grow.

VI. CONCLUSIONS

In this survey, paper have discussed an overview of trust management which includes the highlights on semantics of trust, types of trust and attributes used for evaluating trust. Further, paper identify the various trust models classified by many researchers. It was found that node or virtual machine trust was evaluate on the basis of continous monitoring of session established between machines. As trust changes may depends on pattern hence in future scholars can propose a technique that can learn behaviors of sessions to generate attack alarms.

REFERENCES

[1] Manoj, K., Manglem, S."CBMIR:Content based medi -cal image retrieval system using texture and intensity for eye images". International Journal of Scientific & Engineering Research, 2016.
[2] J.Heiser, and M.Nicolett,Accessing the Security Risks of Cloud Computing,G00157782,Gartner,Inc., Stamfo rd, CT, 2008.
[3] M.Armbrust,A.Fox,It Griffith,etal.,Above the Clouds: A Berkeley View of Cloud Computing, University of California Berkeley, Berkeley, CA, 2009.
[4] Zhang, Y.& Joshi, J.(2009). Access Control and Trust Management for Emerging Multidomain Environment s.Annals of Emerging Research in Information Assura nce,Security and Privacy Services, S.Upadhyay and R.O. Rao (eds.), Emerald Group Publishing, pp. 421-452, 2009.
[5] Tingwei Chen, China Jing Lei. "Research on Service Reputation Evaluation Method Based on Cloud Mo del".International Journal of Intelligent Informati on Systems Volume4, Issue1, February2015, Pages:8-15.
[6] Boniface, Michael & Nasser, Bassem & Papay, Juri & Phillips, Stephen & Servin, Arturo & Yang, Xiaoyu & Zlatev, Zlatko & Gogouvitis, Spyridon & Katsaros, Gregory&Konstanteli,Kleopatra& Kousiouris, George & Menychtas, Andreas & Kyriazis, "Platform-as-a-Service Architecture for Real-Time Quality of Service Management in Clouds".Conference:2010 Fifth Inter national Conference on Internet and Web Applic ations and Service. 2010.
[7] S. Campbell, and M. Jeronimo, Applied Virtualization Technology, Hillsboro, OR: Intel Press, 2006.
[8] D.Nurmi, R.Wolski,C.Grzegorczyk, etaL, Eucalyptus: A Technical Report on an Elastic Utility Computing Architecture Linking Your Programs to Useful Sys tems, Technical Report 2008-10, University of Calif ornia Santa Barbara Computer Science, Santa Bar bara, CA, 2008.
[9] "Amazon Elastic Compute Cloud(AmazonEC2)," http ://aws.amazon.com/ec2/.
[10] AzadM.A., BagS., HaoF., SalahK. M2m-rep: Reputa tion system for machines in the internet of things. Comput. Secur. 2018.
[11] RafeyS.E.A.,Abdel-Hamid A.,El-Nasr M.A. CBSTM-IoT: Context-based social trust model for the Internet of Things; Proceedings of the 2016 International Conference on Selected Topics in Mobile & Wireless Networking (MoWNeT); Cairo, Egypt. 11–13 April 2016; pp. 1–8.
[12] Chen Z., Ling R., Huang C.M., Zhu X. A scheme of access service recommendation for the Social Internet of Things. Int. J. Commun. Syst. 2016.
[13] Peiyun Zhang, Senior Member, IEEE, Yang Kong, And Mengchu Zhou."A Domain Partition-Based Trust Model For Unreliable Clouds". IEEE Transactions On Information Forensics And Security, VOL. 13, NO. 9, SEPTEMBER 2018.
[14] T.F.J.-M. Pasquier, J.Singh, D.Eyers, and J.Bacon, "Cam_ow: Managed data-sharing for cloud services," IEEE Trans.Cloud Comput., vol.5, no.3, pp. 472_484, Jul. 2017.
[15] Z.-Z.Wu,X.-Y.Chen,andX.-H.Du,Enhancing sensitive data security based-on double-layer information _ow controlling in the cloud," Acta Electron. Sinica, vol. 46, no. 9, pp. 2245_2250, Sep. 2018.

© 2021 IJSRET

[16] N.E.Moussaid andM.E. Azhari,``Enhance the security properties and information _ow control," Int. J. Electron. Bus., vol. 15, no. 3, pp. 249_274, 2020.
[17] X.Lu,L.Cao,and X. Du,``Dynamic control method for tenants'sensitive information_ow based on virtual bou ndary recognition,"IEEE Access, vol.8, pp. 1625 48_ 162568, 2020.
[18] Security and Security and Privacy issues in Cloud Computing Computing Jaydip Sen Innovation Labs, Tata Consultancy Services Ltd., Kolkata, INDIA.
[19] J.Li, N.Li, and W. H. Winsborough, "Automated trust negotiation using cryptographic credentials," in Proc. ACM Conf. Computer and Communications Security (CCS), Alexandria, VA, 2005.
[20] V.Goyal,O.Pandey,A.Sahai, and B.Waters, "Attibute-based encryption for fine-grained access control of encrypted data," in Proc. ACM Conf. Computer and Communications Security (ACM CCS), Alexandria, VA, 2006.

© 2021 IJSRET