International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-9, Issue-2, March 2021
https://doi.org/10.21276/ijircst.2021.9.2.4
Article ID IRP1131, Pages 21-27
www.ijircst.org

Detail Study of Cloud Infrastructure Attacks and Security Techniques

Surendranath Singh B.G.[1] **Dr. Sunil Phulre**[2]

[1]Research Scholar, Department of Computer Science & Engineering, LNCT University, Bhopal, Madhya Pradesh, India.
[2]Associate Professor, Department of Computer Science & Engineering, LNCT University, Bhopal, Madhya Pradesh, India.

Correspondence should be addressed to Surendranath Singh.B.G.; surendranathsingh.bg@gmail.com

ABSTRACT- Cloud computing is Internet-based computing and the next stage in the evolution of the internet. The uses of the cloud attract different industries in the recent decade, but this brings security challenges against attacks from insider or outsider, human or bot. Many researchers are working continuously to resolve the issues by introducing policies, algorithms for accessing and storage of client data. This paper gives a detailed survey on IAAS security issues. A 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 the cloud. Tenant-based measures were also in the solutions to various issues. Paper has listed some of the trust techniques developed by researchers for identifying any malicious machine.

KEYWORDS- Cloud Computing, Multi-tenant, Trust Computing, Resource Management.

I. INTRODUCTION

Companies are eventually changing their IT strategies and are turning towards the cloud to meet their data storage requirements to improve their scalability and to reach globally. There are several benefits of cloud computing among which the major ones are lower cost, fault tolerance, flexibility, and efficient response to the latest business needs. But with the advent of this new technology brings new threats and challenges as concerned with the privacy of data that is processed or stored within the cloud. Out of which one of the major challenges of cloud computing is that the consumers who are the actual owners of information while sending their information into the cloud lose control of their precious data. This increases the chances of information theft considerably. Cloud computing indeed offers many benefits but steps have to be taken to improve the trust of people in cloud computing to ensure that the information stored in it is private and confidential. One of the problems with cloud computing is the management and the owners of the website hosting services are removed from the control of a solitary owner. And many important organizations such as government agencies, financial institutes, and health care providers are lawfully required to keep their data secure. Normally such organizations maintain their own data centers to keep their data safe and secure. Such organizations cannot move towards the cloud due to the risk of a data leak that they cannot control.

II. CLOUD COMPUTING SERVICES

A. SAAS (software as a service)

It is the permission provided to any user to use the providers' applications that run on cloud infrastructure. Such applications are easily reachable from client devices and applications such as web browsers, e-mail, or any program interface, shown in fig. 1. But the main point to notice is that the consumer cannot manage the cloud infrastructure including storage, operating system, servers, and network, and he is allowed to limited configuration settings.

B. PAAS (platform as a service)

It is the capability that is granted to the user to have control over the deploy applications that are created using programming language, tools, library, and services [5]. But he does not have control over servers, networks, and storage of the cloud.

C. IAAS (Infrastructure as a service)

The capability that is allowed to any user is to operate basic computing necessities where he can able to upload and run fundamental software that can include applications and operating systems. The consumer cannot manage or have control over the infrastructure of the cloud such as operating systems, deploy any application, and have limited control over selected network components.

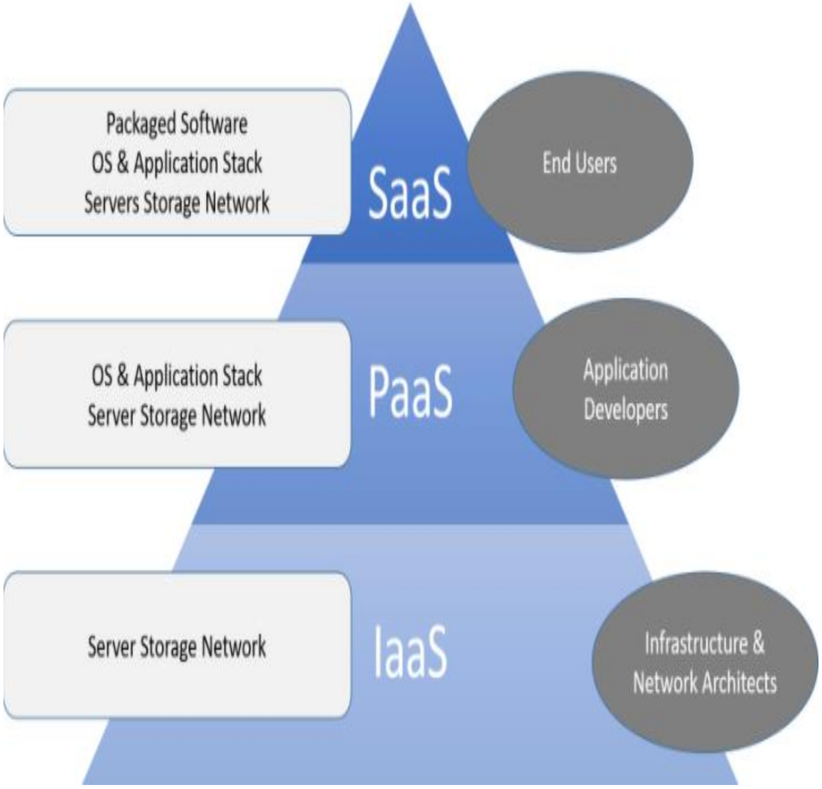

Fig. 1: Cloud computing architecture [6].

Virtualization and elastic computing are the two main technologies which enable IAAS cloud computing. In IAAS, all the facilities are available for clients on the internet which the client purchase in form of outsourced service which is shared with other consumers at a lower cost. Many trusted cloud technologies are not related to the cloud and their merging with the cloud is the focus of this survey.

D. Virtualization

It is the procedure of decoupling the hardware from the system on the machine. Virtual machines are the illustration of the physical machines which are maintained to run on some host by the virtual machine monitor software or a hypervisor [7]. These hypervisors are responsible to implement virtualization on the physical machine and it can be of one or two varieties. Variety 1 type hypervisors also know as native hypervisors run on bare metal or can directly control host's hardware and monitor the guest operating systems. While type 2 types of the hypervisor are hosted hypervisors and run within an environment of OP.

E. Elastic Computing

It provides on-demand and scalable computing resources that are delivered in form of service over the Internet [8]. In elastic compute the clouds have mechanized management which handles the provision and allocation of VMs on the resources of cloud computing. This layer provides the scalability both up and down of the infrastructure resources. An example of elastic computing is Amazon's cloud. Elastic computing or EC2 [9] can have several servers and different applications from many clients that are simultaneously running within a cloud. The view of one client may be different from the other. The biggest advantage of cloud computing is its pay and use model. Earlier the IT organizations have to purchase their requirements regarding network hardware, storage, as well as space, power, and provision for cooling of the hardware. In EC2 one can purchase storage or bandwidth as per their actual usage. Thus elastic computing has reduced TT cost through paying only for the resources that they are using without any additional cost.

III. LITERATURE SURVEYS

Azad et al.[10]: proposed reputation system run by the concept of machine to machine that evaluates the credibility of the machines in the IoT. In this study, preference was given to only the reputation and also social trust metric. The participants in this experiment were allowed to assign a trust value to any machine was allotted which were based on their experiences and interactions with that particular machine. After this, the trust value was cryptogram to the board. Using the secure multi-party methods, the client calculates the global reputation of the machine. Rafey et al. [11] calculated the trusted nodes based on the behavior of the node. In his representation transaction attributes of nodes such as confidence, power, context importance, and social attributes such as relationship, centrality, and friendship were considered to calculate the overall trust value of the machines. The trust based accuracy given by this model is affected by results from dishonest nodes. Chen et al. [12] In this model consider both the QoS also the trust metrics that include energy status and also the reputation in terms of quality together with social trust metrics. But for some reason, this study was not considered to achieve perfect results. Pei Yun Zhang et al. [13] proposed a trust model related to the algorithm to decrease the trust management load and worked to improve the node detection ability that was malicious on the domain partition. Partitioning such nodes into domains was helpful to decrease the load of trust managing in terms of computation and storage. Cross-domain sliding of windows and domain were proposed and were used to save the latest trust values. After this, an algorithm was designed to compute the cross-domain and domain trust value of the nodes, a procedure called filter was applied to remove the malicious nodes and malicious trust evaluations from the domain. D. Eyers et. al. in [14] A camFlow model as a trial was launched in data-centric model in the PAAS cloud was also proposed by the authors. It enforces the data flow strategy and executes the information between the machines at the hardware kernel part while exchanging of the messages. Z. Wu et. al. in [15] Two-layer data flow model was again adopted for the cloud that provides data flow tracking and controlling which was proposed as a protection mechanism from system attacks like buffer and stack overflow. N. E. Moussaid et. al. in [16] Security attributes were formulated in a dynamic fashion when the behaviors of these collected entities were linked with security classes and trust level and it also enhanced the information flow together with security control. It was difficult to identify the information flow boundary due to the sharing of machines (virtual). X. Lu et. al. in [17] also proposed a control method that was dynamic and was used to know the virtual boundary recognition by sensitive information flow. It combines the concepts of decentralized and centralized information flow control. Omar Abdel Wahab et. al. in [18] Two-fold type solution was also adopted that allows the hypervisor to make a trust relationship with the guest virtual machines by knowing the subjective and objective trust resources and employing them with Bayesian inference to combine them. We design a game that was trust based among the hypervisor that tries to maximize the minimization that was caused to a cloud system by DDoS attackers under the inadequate budget of the resources. This game control the hypervisor to detect the load distribution in real-time among VMs that maximizes attacks and detects the DDoS.

IV. THE TENANT ADOPTING CLOUD COMPUTING

Seven security apprehensions were identified by the world's important IT technology, an advisory company that is needed to clear with cloud computing companies before giving them approval [19].

- Regulatory Compliance: The provider should be willing to submit audits reports and also security certifications
- User Access: Major companies should enforce their own principles in hiring for operating their cloud computing company. It is necessary to ask providers for any unambiguous information on hiring
- Data Segregation: It is to realize what steps are taken to isolate your data, and proof of the encryption scheme that has been adopted.
- Data Location: The enterprise should process the data within jurisdictions.
- Disaster Recovery: The provider should able to commit to supporting any type of investigations and research during the discovery phase and should verify that the company has helped in all such activities before.
- Disaster Recovery Verification: The provider should be capable to restore all the data and service in case of any adversity.
- Long Term Viability: It is to ask the new providers that how they can get the data return if failing to assimilate and also ask their replacement application.

A. The solution to Security Issues

- The Right Discovery key: It is to identify the genuine cloud company provider as different providers have dissimilar data management procedures and security levels. A cloud vendor need to be professional and well established and should have the necessary experience and principles.
- Clear Contract: There should be a contract with the cloud vendor which can be necessary during claims
- Recovery Facilities: The cloud vendor should provide excellent recovery facilities which are necessary in case of fragment or data lost conditions.
- Enhanced Enterprise: The enterprise should have the proper infrastructure to maintain all the necessary software and hardware components, routers, firewall, and proxy servers to prevent themselves from cyber-attacks conditions.
- Usage of Data Encryption technology for Security Purpose: A solicitation is to be developed by the developers which provide encryption of data. The leader must define the approach and the basic security components where the data encryption is needed.
- Need to Organize Chart Apropos information Flow: A chart apropos must be present at the group of data. So that the IT managers will know where the data has been stored.

V. ATTACKER TYPES AND THEIR RISKS

There are many security fear and problems in the cloud, these attackers can be broadly divided into two groups shown in fig. 2.

A. *Internal Attackers*

- They are any third-party provider, customer, or cloud service provider that supports the operation or maintenance of the service
- Those who have current authorization access to services, data of the customers, or access to application and infrastructure.
- Those who use their existing privileges and support the third party in executing attacks to leak the data which is on the cloud environment.

B. *External Attackers*

- It is not a member of cloud company by the current consumer, third parties, or cloud providers They have no authorization to services of cloud or their infrastructure
- Uses the operation, technical process, and engineering to attack the cloud service providers, customers, or third-party organization supported.

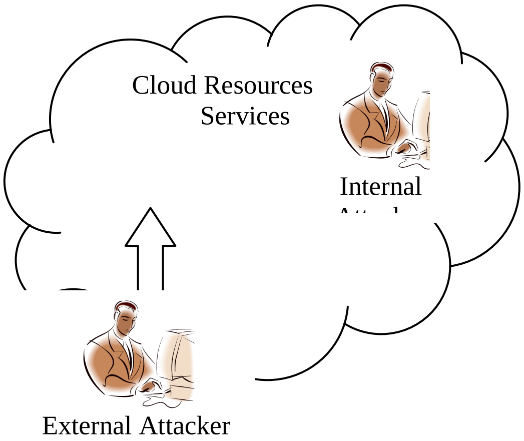

Fig. 2: Attacks on cloud resources.

C. *Cloud Security Risks*

The risk of securities varies with every cloud model and is dependent on the range of factors that includes the sensitivity of information assets, cloud architectures, and security control. Below are some of the general factors to discuss these risks in the cloud delivery model [20].

1. *Privileged User Access*

The cloud companies normally have much control over the consumer data which is risky. Data Location and Segregation: Many Customers sometimes are not aware where their information is stored and there is a risk that these data have been stored with the data of the other customers.

2. *Data Disposal*

Deletion and disposal of the data on the cloud are risky particularly where the hardware is issued according to the needs of the customer dynamically. There is a worry regarding data is not being erased from, backups and data stores.

3. *E-investigations and the Protective Monitoring*

It is the capability for consumers to perform their investigation with the cloud investment is very limited due to the delivery model that is used. Customers cannot deploy the monitoring systems effectively and rely on cloud service providers to support the investigation.

4. *Assuring Cloud Security*

The users may not believe in the security of the systems because they do not have direct control over them. They have to use SLAs and the right to audit for security control in their agreements.

VI. TRUST MODELS

The trust in the cloud computing environment is divided into many categories which are SLA verification-based trust, Evidence-based trust, Reputation-based trust, the Policy-based trust and Societal Trust shown in fig. 3 [21, 22, 23].

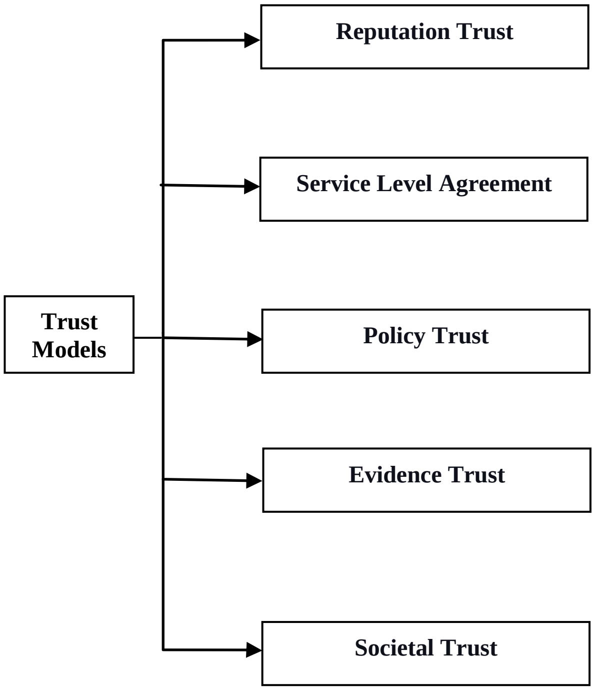

Fig. 3: Types of trust model for virtual machine.

A. *Reputation Based Trust*

It is the collection of public trust towards an entity. Generally, many people living in a community often trust those entities which have a higher reputation. The trustee is required to maintain or build a reputation to meet the trust level. Similarly, the reputation of the cloud depends on the choosing process of the cloud services. And so CSP tries to develop and preserve its high reputation. Reputation is usually measured by a board score that reflects the complete outlook, or sometimes less points based on performance.

B. SLA

It is that type of verification-based trust that is established after accessing a service, the user needs to examine and verify the trust value of the cloud services. SLA is an agreement between two parties which are provider and consumer. And so checking the Qos parameters are essential in the SLA document, in CSP party it is required to offer such services.

C. The Policy-based trust

In this, it is essential to follow formal trust methodologies. The PKI(Public key infrastructure) constructs this formal trust methodology to support its digital signature, validation, and support key certification. The trust in CA or certification authority relies on CA certificate policies. The CA plays an important role in PKI trust roles and procedures.

D. Evidence-based trust

In this, the known behavior of the company owner, which is based on the pieces of evidence, honesty, helpfulness, and honesty.

E. Societal trust

This type of trust may consist of any individual or an organization. In a cloud computing environment, the entities need to be trusted and the IT security service sector plays an important role between the client and the supplier for the growth of the business..

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest.

VII. CONCLUSIONS

This survey paper has discussed an overview of trust management which includes the highlights on the semantics of trust, types of trust, and attributes used for evaluating trust. Further, the paper identifies the various trust models classified by many researchers. It was found that node or virtual machine trust was evaluated based on continuous monitoring of sessions established between machines. As trust changes may depend on pattern, hence in the 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 medical 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., Stamford, CT, 2008.

[3] M. Armbrust, A. Fox, It Griffith, et al., 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 Environments. Annals of Emerging Research in Information Assurance, 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 Model”. International Journal of Intelligent Information Systems Volume 4, Issue 1, February 2015, Pages: 8-15.

[6] I. Odun-Ayo, M. Ananya, F. Agono and R. Goddy-Worlu, "Cloud Computing Architecture: A Critical Analysis," 2018 18th International Conference on Computational Science and Applications (ICCSA), Melbourne, VIC, 2018.

[7] S. Campbell, and M. Jeronimo, Applied Virtualization Technology, Hillsboro, OR: Intel Press, 2006.

[8] D. Nurmi, R. Wolski, C. Grzegorczyk, et aL, Eucalyptus: A Technical Report on an Elastic Utility Computing Architecture Linking Your Programs to Useful Systems, Technical Report 2008-10, University of California Santa Barbara Computer Science, Santa Barbara, CA, 2008.

[9] "Amazon Elastic Compute Cloud (Amazon EC2)," http://aws.amazon.com/ec2/.

[10] Azad M.A., Bag S., Hao F., Salah K. M2m-rep: Reputation system for machines in the internet of things. Comput. Secur. 2018.

[11] Rafey S.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. Wu, X.-Y. Chen, and X.-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.

[16] N. E. Moussaid and M. 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 boundary recognition," IEEE Access, vol. 8, pp. 162548_162568, 2020.

[18] Omar Abdel Wahab, Jamal Bentahar, Hadi Otrok, and Azzam Mourad. “Optimal Load Distribution for the Detection of VM-based DDoS Attacks in the Cloud”. IEEE Transaction, Services Computing Nov. 2020.

[19] B. Hari Krishna, S. Kiran, G. Murali, R. Pradeep Kumar Reddy. "Security Issues in Service Model of Cloud Computing Environment". Procedia Computer Science, Volume 87, 2016.

[20] Security and Security andPrivacy Privacy Privacy Issues in Cloud Computing Computing Jaydip Sen Innovation Labs, Tata Consultancy Services Ltd., Kolkata, INDIA.

[21] 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.

[22] 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.
[23] D. Grawrock, Dynamics of a Trusted Platform, Hillsboro, OR: Intel Press, 2009.

ABOUT THE AUTHORS

Surendranath Singh B. G, Research Scholar, Department. of Computer Science & Engineering, LNCT University, Bhopal, Madhya Pradesh, India.

Dr. Sunil Phulre, Associate Professor, Department. of Computer Science & Engineering, LNCT University, Bhopal, Madhya Pradesh, India