Megha Sharma, 2022, 10:4
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

A Survey on Cloud Computing and Security Methods

Megha Sharma, Asst. Prof. Sumit Sharma
Dept. of Computer Science Engg.
Vaishnavi Institute Of Technology And Science
Bhopal,MP,India

Abstract- Computing in the cloud is a form of internet-based computing that represents the subsequent stage in the development of the internet. In recent years, it has received a significant amount of attention, but one of the most significant factors that is slowing down the growth of cloud computing is the concern over security. However, because of this one aspect of cloud computing, there are many security issues that must be resolved and clearly understood. This article provides a comprehensive review of the various concerns regarding IAAS security. To protect one's data and one's privacy, a virtual machine needs to have adequate security. Methods that have been suggested by a variety of academics and can either directly or indirectly improve the cloud's security are discussed here. Tenant-based measures were also considered to be potential solutions to the many problems that arose. A paper has outlined some of the trust techniques developed by researchers for determining whether or not a machine is malicious.

Index Terms- Cloud Computing, Multi-tenant, Trust Computing, Resource Management.

I. INTRODUCTION

Cloud computing's increasing dominance is having an impact on every aspect of the information technology (IT) industry [1, 2, 3, 4]. By utilising virtualization and shared infrastructures, it is possible to increase business agility while simultaneously lowering costs for information systems. Multi-tenancy is used by most cloud providers to isolate tenants from one another in order to protect user data and configurations. The isolation strategy, on the other hand, is detrimental to multi-tenant collaborations, which are essential in the cloud [2]. Fine-grained, secure resource sharing among tenants is not encouraged in today's commercial clouds, which is particularly problematic. Using existing access control models, cloud providers can maintain tight control over the activities of users within a single tenant environment. This approach, on the other hand, is limited to dealing with multi-tenant access control in databases and cannot be directly extended to protect other critical types of resources such as files and virtual machines. Because of this, in order to enable secure multi-tenant collaborations in the cloud, it is necessary to implement a general fine-grained access control model.

[2][3] Multi-tenancy is the ability to share the same service instance among multiple tenants[2][3]. One of the most important applications provided by SaaS is a multi-tenant data management system (MDS). Furthermore, multi-tenant jobs running on a set of shared computing workers can increase energy efficiency by 20% [4] while simultaneously reducing the number of active servers by 50% [5]. Although cloud computing has numerous advantages, it also presents a number of significant challenges. In today's world, the majority of information services are hosted online, and accessing online services has become a daily routine for almost everyone.

There are also significant security concerns arising from malware and attacks in the cloud, which not

only have access to the data and services of a large number of users, but also have the capability of spreading to a large number of systems through the cloud infrastructure. In addition, there is the issue of trust in the cloud service providers themselves to consider. So it has become necessary for service providers to provide guarantees regarding the security, the level of quality, and the availability of their services. The reputation of Cloud Providers (tenant's employees) can be used to increase the trust of tenants in cloud service providers [6, 7, 8]. Because it assists the tenant in selecting an appropriate tenant's employee. A reputation management mechanism (RMM) is designed to take note of the selfish and malicious behaviours of a tenant's employees and to reflect these behaviours on the tenant's reputation [7].

II.CLOUD COMPUTING SERVICES

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 underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

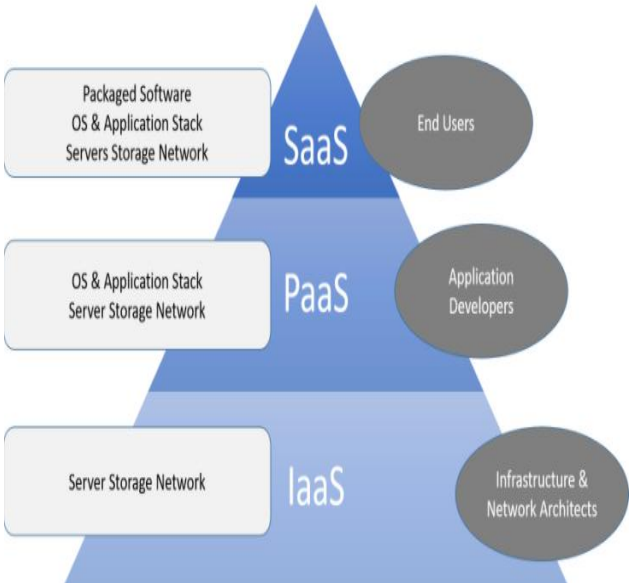

Fig. 1 Cloud computing architecture [6].

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

2.Infrastructure as a Service (IaaS) : The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems 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 networking components.

The two major technologies that enable IaaS cloud computing 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 consumers 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.Virtualization Virtualization is the process of decoupling hardware from the operating system on a physical machine. A Virtual Machine (VM) is the virtualized representation of a physical machine that is run and maintained on a host by a software virtual machine monitor or hypervisor [7]. The hypervisor implements the virtualization on the physical machine and can be one of two types. Type 1 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. Type 2 hypervisors are hosted hypervisors, meaning they are software applications running within a conventional operating-system environment.

4.Elastic Computing - Elastic computing provides scalable on-demand computing resources that are delivered as a 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 within 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 traditional IT approach, organizations would have to purchase enough processing, storage, and network hardware to support their peak computing requirements, as well as provide for space, power, and cooling for the hardware. In elastic computing, processing, storage and bandwidth 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 paying for the resources when they are used.

III.LITERATURE SURVEY

A new method for recognising fake feedback in cloud trust management systems has been proposed by Charband and Navimipour [8]. The method makes use of a feedback assessment component as well as a Bayesian game model. They presented two new methods for identifying fake feedbacks, including the feedback assessment component and the Bayesian game model, as well as the feedback assessment component. The feedback assessment component is responsible for examining the received feedback and determining whether it is likely to be a fake identity. The results of the experiments demonstrate that the feedback assessment component is capable of correctly identifying and rectifying fictitious feedback. A Bayesian game model is demonstrated for the purpose of identifying troll users and preventing their feedback. The simulation results were consistent with the analytical results, indicating that the Bayesian game model is capable of correctly identifying troll users. Feedbacks received from troll users are immediately identified as fake feedbacks. However, while its mechanism has improved security and dependability, its dependability and scalability have both been rated as low.

A cloud-based trust evaluation framework for vehicular social networks has been proposed by Navimipour and Charband [9], according to the authors. An advanced trust management model and disposition scheme based on a vehicular cloud computing system were demonstrated in the paper. They proposed a layered trust management approach that takes advantage of the efficient use of physical resources and determines its disposition in a VSN scenario based on a three-layer cloud computing architecture, which they believe will be effective. Moreover, the efficiency modelling of the proposed trust management scheme is carried out using a novel formal compositional method performance assessment process algebra, which has improved features in compositionality and parsimony, and thus is capable of modelling systems with layered architectures and multifaceted behaviours with efficiency. Many numerical analyses are supported by presentation assessment process algebra, which can be assessed using its underlying incessant time Markov chains directly or by solving a set of approached usual differential equations, among other things. According to the results of the examination, they looked at several key performance characteristics of the scheme as well as related volume issues in disposition. A more efficient investigation approach for evaluating the performances of the trust models is revealed as a result of these detections. This mechanism provided adequate security and scalability, but it was unreliable and unconfidentially transmitted information.

According to Tang et al. [10], an innovative method for recognising the moderating effect of trust on the adoption of cloud-based services has been developed. Specifically, the goal of this study is to identify the factors that influence trust in the hypothesis of cloud computing services in the semiconductor industries. A hypothesis has been advanced regarding the moderated effectivity of these trust elements in relation to the success factors in the technical, organisational, and environmental domains. In accordance with the findings of a literature review, an assumptive model has been expanded, and relationships between the hidden variables have been investigated through the use of structural equations. Although the proposed method provided adequate security, it was hampered by a lack of dependability and dynamicity.

Selvaraj and Sundararajan [11] have proposed a fuzzy-based trust evaluation scheme for cloud services, which is based on the concept of uncertainty. It was also suggested that a dynamic trust model based on evidence be used to define the dynamic trustworthiness of cloud-based services. It makes use of fuzzy logic to develop trust in order to deal with uncertainty, and it employs the ordered weight averaging operator to gather the trust values, allowing it to operate in real time without sacrificing performance. The proposed scheme makes use of the QoS parameters as a form of validation in order to assess the level of trust in cloud services. In order to determine the model's efficiency and effectiveness, simulations were used to arrive at the final conclusions. Despite the fact that it provided adequate security, dependability, and dynamicity, it was hampered by deficiencies in integrity, dependability, confidentiality, and safety.

In [12], authors proposed a two-fold solution that allows, firstly, the hypervisor to establish credible trust relationships toward guest Virtual Machines (VMs) by considering objective and subjective trust sources and employing Bayesian inference to aggregate them. On top of the trust model, we design a trust-based maximin game between DDoS attackers trying to minimize the cloud system's detection and hypervisor trying to maximize this minimization under limited budget of resources. The game solution guides the hypervisor to determine the optimal detection load distribution among VMs in real-time that maximizes DDoS attacks' detection.

IV.ATTACKER TYPES AND RISKS

Many of the security threats and challenges in cloud computing 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 [13].

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 services, customer data or supporting infrastructure and applications, depending on their organizational role
- Uses existing privileges to gain further access or support third parties in executing attacks against the confidentiality integrity and availability of information within 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 engineering vulnerabilities to attack a cloud service provider, customer or third party supporting organization to gain further access to propagate attacks against the confidentiality, integrity and availability of information 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 [20].

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. 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 customers' information.

Data disposal: Cloud data deletion and disposal is a risk, particularly where hardware is dynamically issued 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. 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 systems on

infrastructure they do not own; they must rely on the systems in use by the cloud service provider to support investigations.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

Trust in cloud computing can be broken down into a few different categories, including reputation-based trust, trust that is based on SLA verification, trust that is based on policy, trust that is based on evidence, and trust that is based on society [14, 15, 16].

1.Trust That Is Determined By Reputation An organization's reputation can be defined as the aggregated estimate of the public's level of trust in that organisation. In general, many entities within a community will trust an entity that has a strong reputation; an entity that is required to build a trust decision on a trustee will use the trustee's reputation to compute or approximate the trust level of the trustee. Because the reputation of the cloud has an impact on the process by which cloud services are selected, cloud service providers (CSPs) work hard to build and maintain a positive reputation. A person's reputation is traditionally represented by either a broad score that reflects the overall outlook or a small number of scores on numerous foremost aspects of performance. Alternatively, reputation can also be represented by a combination of the two.

2.Service Level Agreement (SLA): After establishing the preliminary trust and gaining access to a cloud service, the cloud user is required to validate and re-examine the trust value as part of the Service Level Agreement (SLA) for verification-based trust. A SLA, or Service Level Agreement, is a legal agreement that is made between two communicating parties user and provider. As a result, monitoring the QoS parameters and verifying the SLA document are essential components of cloud computing's trust management infrastructure. When participating in CSP, parties are required to offer these kinds of services.

3.Policy-based trust: in order to build one, you need to follow the "formal" procedures. In a related domain, the Public Key Infrastructure (PKI) is a widely implemented technology that supports key certification, digital signature and validation through the use of "formal" trust methodologies. It also supports data attribute certification and validation. In this context, confidence in a Certification Authority (CA) is predicated on the CA's demonstration of compliance with specific certificate policies. It is done with regard to the delivering and keeping of public key certificates that have been validated. Trust in PKI is largely dependent on the policies governing certificates.

4.Trust that is based on evidence:, The evidence that an individual possesses adeptness, helpfulness, and honesty is the foundation upon which a trusting belief in the predictable behaviour of a trustee is built. In relation to that presumption, evidence-based trust was communicated.

A societal trust is made up of any individual in addition to a business. Even within the cloud, each entity needs to be trusted. When it comes to the information security service industry, trust between the provider and the customer is absolutely necessary for the expansion of the company.

VI.CONCLUSIONS

In this survey paper, an overview of trust management was discussed, including key points on the semantics of trust, types of trust, and attributes that are used for evaluating trust. In addition, the paper describes the various trust models that have been categorised by a number of researchers. It was discovered that the basis for determining whether a node or virtual machine is trustworthy is the continuous monitoring of sessions that are established between machines. Considering that shifts in trust may be dependent on pattern, academics may in the future propose a method that can learn the behaviors of sessions in order to generate attack alarms.

REFERENCES

[1] S. Singh, Y. Jeong, and J. H. Park, "A survey on cloud computing security: Issues, threats, and solutions," Journal of Network and Computer Applications, vol. 75, pp. 200–222, 2016.

[2] NIST, Final Version of NIST Cloud Computing Definition Published, 2011.

[3] L. Turnbull and J. Shropshire, "Breakpoints: An analysis of potential hypervisor attack vectors," in Proceedings of the IEEE SoutheastCon 2013: Moving America into the Future, 2013.

[4] S. Udaykumar, T. Latha Trusted computing model with attestation to assure security for software services in a cloud environment Int. J. Intell. Eng. Syst., 10, 2017

[5] S. Berger, R. C´aceres, K. A. Goldman, R. Perez, R. Sailer, and L. van Doorn. vtpm: Virtualizing the trusted platform module. In Proceedings of the 15th Conference on USENIX Security Symposium - Volume 15, USENIX-SS'06, Berkeley, CA, USA, 2006.

[6] E. Christian, M. Ficco, F. Palmieri, A. Castiglione Smart cloud storage service selection based on fuzzy logic theory of evidence and game theory IEEE Trans. Comput., 65 (2016

[7] D. E. Kouicem, Y. Imine, A. Bouabdallah and H. Lakhlef, "A Decentralized Blockchain-Based Trust Management Protocol for the Internet of Things," in IEEE Transactions on Dependable and Secure Computing, doi: 10.1109/TDSC.2020.

[8] Y. Charband, N.J. Navimipour Online knowledge sharing mechanisms: a systematic review of the state of the art literature and recommendations for future research Inf. Syst. Front. (2016), pp. 1-21

[9] N.J. Navimipour, Y. Charband Knowledge sharing mechanisms and techniques in project teams: literature review, classification, and current trends Comput. Human Behav., 62 (2016), pp. 730-742

[10] M. Tang, X. Dai, J. Liu, J. Chen Towards a trust evaluation middleware for cloud service selection Future Gener. Comput. Syst., 74 (2017), pp. 302-312.

[11] A. Selvaraj, S. Sundararajan Evidence-based trust evaluation system for cloud services using fuzzy logic Int. J. Fuzzy Syst. (2017), pp. 1-9.

[12] 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.

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

[14] 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.

[15] 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.

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