SAFETY THREAT CONSEQUENCES IN CLOUD COMPUTING

Chandraiah.T

Assistant Professor, Department of Computer Science,
Yuvaraja's College, Mysore - 570005

ABSTRACT

Cloud computing is a exemplary for permitting lodging user's pervasive, opportune and on-claim network access to a joint pool of configurable computing assets. The safety for Cloud Computing is evolving area for study and this paper afford security topic in terms of cloud computing predicated on analysis of Cloud Security threats and Technical Components of Cloud Computing.

Keywords: Cloud Computing, Security Threats, Future Technology

INTRODUCTION

Cloud computing is a model for enabling accommodation user's ubiquitous, convenient and on-claim network access to a shared pool of construct computing resources (e.g., networks, servers, storage, applications, and lodgings), that can be expeditiously provisioned and renounced with minimal management effort or accommodation provider communication. Cloud computing enables cloud lodgings.

The security building and utilities highly depend on the allusion design, and this paper shows the allusion design and the main safety issues regarding this structural design.

Bureaucratic Mechanisms of Cloud Computing

As shown within the Figure 1, key functions of a cloud management system is split into four layers, respectively the Resources & Network Layer, Services Layer, Access Layer, and User Layer. Each layer includes a group of functions:

- The Resources & Network Layer achieves the carnal and cybernetic resources.
- The Services Layer embraces the most classes of cloud services, namely, NaaS, IaaS, PaaS, SaaS/CaaS, the service adaptation function and consequently the cloud operative function.
- The Access Layer includes API closure function, and Inter-Cloud scrutinizing and coalition function.
- The User Layer includes End-user utility, Companion function and Administration function.

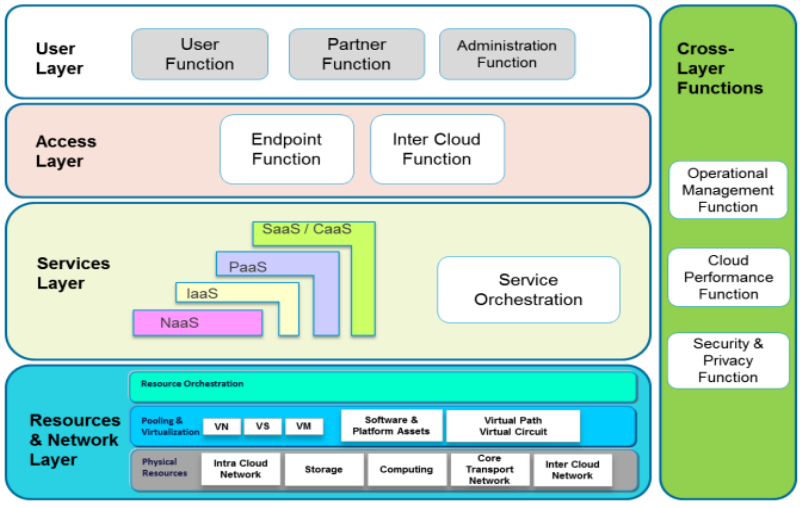

Figure 1: Components of Cloud Computing

Other utilities like Controlling, Security & Privacy, etc. are measured as crosslayer a function that covers all the layers. The most principle of this structural design is that each one these layers are alleged to be optional. This suggests that a cloud benefactor who wants to use the allusion architecture may select and implement only a subset of those layers. However, from the safety perspective, the principal of separation requires each layer to require charge of certain responsibilities.

In event the safety controls of 1 layer are by passed (e.g. admittance layer), other safety functions could reimburse and thus should be executed either in other layers or as cross-layer utilities.

THREATS FOR CLOUD SERVICE USERS

Responsibility Ambiguity

Cloud amenity customers devour supplied resources through service models. The customer-built IT structure thus be dependent on the services. The shortage of a transparent definition of responsibility among cloud service users and Providers may evoke conceptual conflicts. Furthermore, any votive discrepancy of provided services could induce anomaly, or incidents. However the matter of which entity is that the data controller which on is that the data processor stays open at a world scale (even if the international aspect is reduced to a minimal third party outside of the precise region like EU).

Loss of Governance

For an enterprise, migrating a neighborhood of its own IT system to a cloud infrastructure suggests to partly give mechanism to the cloud service sources. This loss of governance depends on the cloud service models. as an example , IaaS only delegates hardware and network administration to the benefactor, while SaaS also envoys Operating System, application, and service integration so as to supply a turnkey service to the cloud service user.

Loss of Trust

It is sometime difficult for a cloud service user to acknowledge his provider's trust level owed to the black-box article of the cloud service. There's not at all measure the way to get and share the provider's safety level in formalized manner. Furthermore, the cloud service users haven't any abilities to gauge security implementation level achieved by the provider. Such a scarcity of sharing security level in sight of cloud service provider will become a significant security threat in use of cloud services for cloud service users.

Service Provider Lock-in

A consequence of the loss of governance might be a scarcity of freedom regarding how to replace a cloud provider by another. this might be the case if a cloud provider relies on non-standard hypervisors or virtual machine image format and doesn't provide tools to convert virtual machines to a uniform format.

Unsecure Cloud Service User Access

As maximum of the source deliveries are over distant linking, non-protected APIs, (mostly management APIs and PaaS services are one among the simplest attack vector). Attack methods like phishing, fraud, and exploitation of software vulnerabilities still achieve results. Authorizations and keys are often reprocessed, which intensifies the impact of such attacks. Cloud solutions add a replacement threat to the landscape. If an attacker gains access to your credentials, they will pay attention to your activities and transactions, deploy data, return forged data, and readdress your clients to illegal sites. Your account or service instances may become a replacement base for the attacker. From here, they'll leverage the facility of your reputation to launch subsequent attacks.

Lack of Information/Asset Management

When applying to use Cloud Computing Services, the cloud service user will have serious concerns on lack of information/asset management by cloud service providers like location of sensitive asset/information, lack of corporal control for data loading, consistency of data backup (data retention issues), and countermeasures for BCP and Calamity Recovery then on. Furthermore, the cloud service users even have important concerns on exposure of knowledge to foreign government and on compliance with privacy law like EU data protection directive.

Data loss and leakage

The damage of encrypted key or restricted access code will bring severe problems to the cloud service users. Therefore, absence of cryptographic supervision information like encryption secrets, endorsement ciphers and access privilege will heavily lead sensitive damages on data loss and unexpected leakage to outside. For instance, inadequate endorsement, approval, and review (AAA) controls; unpredictable use of encryption and/or validation keys; functioning failures; removal problems; authority and political issues; data center consistency; and disaster recovery are often recognized as major behaviors during this threat category.

THREATS FOR CLOUD SERVICE PROVIDERS

Responsibility Ambiguity

Different user roles, like cloud service provider, cloud service user, client IT admin, data owner, could also be defined and utilized in a cloud system. Uncertainty of such customer roles and tasks definition associated with data rights, access control, infrastructure maintenance, etc, may induce business or legal dissention (Especially when handling third parties. The cloud service worker is someway a cloud facility user).

Protection Inconsistency

Due to the dispersed structural design of a cloud organization, its safety mechanisms are likely to be contradiction among distributed security modules. For case, an admittance denied by one IAM section could also be granted by alternative. This threat could also be profited by a possible attacker which compromises both the confidentiality and integrity.

Evolutional Risks

One abstract upgrading of cloud computing is to rearrange some choices from the planning phase to the execution phase. This suggests, some dependent software components of a system could also be selected and implemented when the system executes. However, conventional risk assessment methodology can't match such an evolution. A system which is assessed as secure during the planning phase may exploit vulnerabilities during its execution thanks to the newly implemented software components.

Business Discontinuity

The "as a deal" feature of cloud computing gives resources and distributes them as a service. The entire cloud infrastructure alongside its business workflows thus relies on an outsized set of services, starting from hardware to application. However, the discontinuity of service delivery, like black out or delay, may bring out a severe impact associated with the supply.

Supplier Lock-in

The platform of a service provider is made by some software and hardware components by suppliers. Some merchant needy modules or workflows are executed for amalgamation or functionality postponement. However, thanks to the shortage of ordinary APIs, the portability to migrate to a different supplier isn't obvious. The consequence of provider locked-in might be a scarcity of freedom regarding the way to replace a supplier.

License Risks

Software licenses are usually supported the amount of installations, or the numbers of users. Since created virtual machines are going to be used only a couple of times, the provider may need to acquire from more licenses than really needed at a given time. the shortage of a "clouded" license management scheme which allows to pay just for used licenses may cause software use conflicts.

Bylaw Conflict

Depending on the bylaw of hosting country, data could also be protected by different applicable jurisdiction. as an example , the USA Patriot Act may authorize such seizures. EU protects cloud service user's private data, which shouldn't be processed in countries that don't provide a sufficient level of protection guarantees. a world cloud service provider may commit bylaws of its local data centre's which may be a legal threat to be taken under consideration .

Bad Integration

Migrating to the cloud implies moving large amounts of knowledge and major configuration changes (e.g., network addressing). Relocation of a neighbourhood of an IT organisation to an outside cloud service provider requires deep changes within the infrastructure design (e.g. network and security policies). a nasty integration caused by incompatible interfaces or inconsistent policy enforcement may evoke both functional and non-functional impacts.

Unsecure Administration API

The administration middleware standing between the cloud infrastructure and therefore the cloud service user could also be unsure with insufficient attention dedicated to sanitation of cloud service user inputs and authentication. Non threatened APIs, typically administration APIs develops a objective of choice for attackers.

This is often not specific to cloud environment. However, the facility sloping approach makes APIs a basic structure block for a cloud infrastructure. Their defence becomes a main anxiety of the cloud safety.

Shared Environment

Cloud resources are virtualized, different cloud service users (possibly competitors) share an equivalent infrastructure. One key concern is said to architecture compartmentalization, resource isolation, and data segregation. Any unlawful and ferocious access to cloud service user's delicate data may negotiation both the integrity and concealment.

Hypervisor Isolation Failure

The hypervisor technology is taken into account because the basis of cloud infrastructure. Various simulated machines co-held on unique physical server share both CPU and memory resources which are virtualized by the hypervisor. This risk concealments the failure of mechanisms separating attack" might be propelled on a hypervisor to understand unlawful access to other virtual machines' memory.

Service Unavailability

Availability isn't specific to cloud environment. Though, due to the amenity concerned with design principle, service distribution could also be impacted while the cloud infrastructure in not available. Moreover, the dynamic dependency of cloud computing offers far more possibilities for an attacker. A typical Denial of Service attack on one service may clog the entire cloud system.

Data Unreliability

Data protection includes access to data for the confidentiality also as its integrity. Cloud service customers have disquiets about how benefactors handle with their information, and whether their data is disclosed or illegally altered. The cloud service user trust isn't within the central of cloud security, it's a serious marketing differentiator for a cloud service provider to advance the migration of IT system to cloud environment.

Abuse Right of Cloud Service Provider

For a cloud service user, migrating a neighborhood of its own IT to a cloud infrastructure implies to partially give control to the provider. This becomes a significant threat to cloud service user's data, notably regarding role and privileges assignment to providers. Including lack of transparency regarding cloud provider practices may conduce mis-configuration or malicious insider attack. Such security breaches will lower the provider's reputation, leading to lower cloud service user confidence.

CONCLUSION

In any cloud service (infrastructure, software or platform) the top service provider or enterprise will control the access to the services. If these services are being hosted on the cloud, then the cloud provider (which could also be different from the service provider or enterprise) also must protect their network from unauthorized accesses. However, since the cloud provider and therefore the service provider or enterprise is legally different entities, they'll in certain cases got to isolate their respective user information. In this paper, we offer Cloud Security treats in terms of Cloud Service user and provider. Supported these Cloud Security treats, the subsequent items are main topic for

Cloud Security standardization

Security Architecture/Model and Framework

- Security Management and Audit Technology
- Professional Permanency Planning (PPP) and Calamity Rescue
- Storage Security
- Data and Privacy Protection
- Account/Identity Management
- Network Monitoring and Incident Response
- Network Security Management
- Interoperability and Portability Security
- Virtualization Security
- Obligatory Predicates

REFERENCES

1) N. Fernando, S. W. Loke, and W. Rahayu. (2013). “Mobile cloud computing: a survey,” Future Generation Computer Systems, vol. 29, no. 1, pp. 84–106.
2) Ali, Maaruf, and Mahdi H. Miraz. (2013). "Cloud Computing Applications." In Proceedings of the International Conference on Cloud Computing and eGovernance, p. 1
3) Miraz, Mahdi H.; Ali, Maaruf; Excell, Peter S.; Picking, Rich. “A Review on Internet of Things (IoT), Internet of Everything (IoE) and Internet of Nano Things (IoNT)”. Proceedings of the fifth international IEEE conference on Internet Technologies and Applications (ITA).
4) Y. Ren, R. Werner, N. Pazzi, A. Boukerche. (2010). “Monitoring patients via a secure and mobile health-care system”. IEEE Wirel. Commun. 17, pp. 59–65.
5) J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos. (2017). “Security and privacy for cloud-basedIoT:challenges.” IEEE Communications Magazine, vol. 55, no. 1, pp. 26–33.
6) N. Angelova, G. Kiryakova, L. Yordanova. (2017). "The Great Impact Of Internet Of Things On Business". Trakia Journal Of Sciences, Vol. 15, Suppl. 1, pp 406-412.
7) G. Khanna and S. K. Chaturvedi. (2018). “A Comprehensive Survey on Multi-hop Wireless Networks: Milestones, Changing Trends and Concomitant Challenges”, Wireless Personal Communications. Vol. 101, No. 2, pp. 677–722.
8) Hwang, K., Dongarra, J., & Fox, G. C. (2013). “Distributed and cloud computing: from parallel processing to the internet of things” Morgan Kaufmann.
9) S. Midya. (2016). “An Efficient Handoff Using RFID Tags. Proc. of Intl. Conf. on Intelligent Communication, Control and Devices”, Advances in Intelligent Systems and Computing 47, pp. 779.
10) S. Misbahuddin, R. Olson, J. A. Zubairi, M. Irfan, S. M. Arif, S. Mansoor, S. Saeed, Z. Irfan. (2012). “Client-Server Based Transmission Scheme over GSM Network for MEDTOC with Patient Classification”. In: International Conference on Collaboration Technologies and Systems (CTS), pp. 176–179.
11) H. Huang, T. Gong, N. Ye, R. Wang, Y. Dou. (2017). “Private and Secured Medical Data Transmission and Analysis of Wireless Sensing health-care System”. IEEE Trans. on Inf. 13, pp. 1227–1237.