Identify the key security threats in Trust as a Service (TaaS) and Trust Services Principles in cloud Security

[1]Dushyant Singh, [2]Arun Singh Chouhan ,[3]Shalini Agarwal
[1]Hod Of Computer Science, [2]Assistant Professor, [3] M.Tech Pursing RTU
[1] Chandravati Group of Institutions, Bharatpur, India.
[2] Department of Computer science, [2] SRITS, Datia (M.P.) India.
[3] Department of Computer science, [3] Chandravati Group of Institutions, Bharatpur, India.

***Abstract* - Cloud computing security is the main concern area to design a trusted and secure cloud platform between a cloud service providers and cloud customer. The Trust as a Service (TaaS) is very important for secure cloud platform because it is a mutual relation between the cloud service provider and cloud customers. To design such type of cloud computing security environment in this research paper we identify the key issues of security and threats in TaaS. When a third party build some software interfaces or APIs are what cloud customers use to interact with cloud services, those must have extremely secure authentication, access control, encryption and activity monitoring mechanisms. We are also consider here the Cloud Security Alliance(CSA)' s top seven key threats in cloud computing and TaaS security .The trust services principles are very important to achieve the trust management and its criteria is used in trusted cloud environment.**

***Index Terms* - Cloud computing, Trust as a Service (TaaS), Trust services principles, Trust management.**

I. INTRODUCTION

Cloud computing is the most emerging area in business, education, Industry and Financial system. All the areas need a good security mechanism so that they can save the data on cloud and transaction of any type become more secure. To design such type of cloud computing security environment in this research paper we identify the key issues of security and threats in TaaS.[1] When a third party build some software interfaces or APIs are what cloud customers use to interact with cloud services, those must have extremely secure authentication, access control, encryption and activity monitoring mechanisms.[2] We are also consider here the Cloud Security Alliance(CSA)' s top seven key threats in cloud computing and TaaS security that are Abuse and Nefarious Use of Cloud Computing, Insecure Application Programming Interfaces, Malicious Insiders, Shared Technology Vulnerabilities, Data Loss/Leakage, Account, Service & Traffic Hijacking, Unknown Risk Profile [3] . Trust services principles covers the all aspects of trust management in cloud environment.

II. KEY THREATS IN CLOUD COMPUTING SECURITY AND TRUST AS A SERVICE(TAAS)

The Cloud Security Alliance determines top seven key threats in cloud computing security that is also used in TaaS[3].

i. Abuse and Nefarious Use of Cloud Computing

Abuse and nefarious use of cloud computing is the top threat identified by the CSA. A simple example of this is the use of botnets to spread spam and malware. Attackers can infiltrate a public cloud, for example, and find a way to upload malware to thousands of computers and use the power of the cloud infrastructure to attack other machines.

ii. Insecure Application Programming Interfaces

As software interfaces or APIs are what customers use to interact with cloud services, those must have extremely secure authentication, access control, encryption and activity monitoring mechanisms - especially when third parties start to build on them.

iii. Malicious Insiders

The malicious insider threat is one that gains in importance as many providers still don't reveal how they hire people, how they grant them access to assets or how they monitor them. Transparency is, in this case, vital to a secure cloud offering, along with compliance reporting and breach notification.

iv. Shared Technology Vulnerabilities

Sharing infrastructure is a way of life for IaaS providers. Unfortunately, the components on which this infrastructure is based were not designed for that. To ensure that customers don't thread on each other's "territory", monitoring and strong compartmentalization is required.

v. Data Loss/Leakage

Be it by deletion without a backup, by loss of the encoding key or by unauthorized access, data is always in danger of being lost or stolen. This is one of the top concerns for businesses, because they not only stand to lose their reputation, but are also obligated by law to keep it safe.

vi. Account, Service & Traffic Hijacking

Account service and traffic hijacking is another issue that cloud users need to be aware of. These threats range from man-in-the-middle attacks, to phishing and spam campaigns, to denial-of service attacks.

vii. Unknown Risk Profile

Security should be always in the upper portion of the priority list. Code updates, security practices, vulnerability profiles, intrusion attempts – all things that should always be kept in mind.

III. OTHERS SECURITY THREATS IN CLOUD SECURITY

The top seven threats are not fulfill the all aspects of cloud security some others threats are also affecting the cloud environment security. These are following: [4]

a. **Failures in Providers Security**. Cloud providers control the hardware and the hypervisors on which data is stored and applications are run and hence their security is very important while designing cloud.

b**. Attacks by other customer**. If the barriers between customers break down, one customer can access another customer's data or interfere with their applications.

c. **Availability and reliability issues**. The cloud is only usable through the Internet so Internet reliability and availability is essential.

d. **Legal and Regulatory issues**. The virtual, international nature of cloud computing raises many legal and regulatory issues regarding the data exported outside the jurisdiction.

e. **Perimeter security model broken**. Many organizations use a perimeter security model with strong security at the perimeter of the enterprise network. The cloud is certainly outside the perimeter of enterprise control but it will now store critical data and applications.

f. **Integrating Provider and Customer Security Systems**. Cloud providers must integrate with existing systems otherwise the bad old days of manual provisioning and uncoordinated response will return.[5]

IV. TRUST SERVICES PRINCIPLES IN CLOUD SECURITY

Trust services principles represent attributes of a reliable system that help support the achievement of management's objectives. For each of the principles there are detailed criteria that serve as benchmarks used to measure and present the subject matter and against which the practitioner evaluates the subject matter. The attributes of suitable criteria are as follows:[6]

- **Objectivity.** Criteria should be free from bias.
- **Measurability**. Criteria should permit reasonably consistent measurements, qualitative or quantitative, of subject matter.
- **Completeness**. Criteria should be sufficiently complete so that those relevant factors that would alter a conclusion about subject matter are not omitted.
- **Relevance**. Criteria should be relevant to the subject matter.

The following are the trust services principles

a. Security. The system is protected against unauthorized access, use, or modification.

The security principle refers to the protection of the system resources through logical and physical access control measures in order to support the achievement of management's commitments and requirements related to security, availability, processing integrity, and confidentiality. Controls over the security of a system prevent or detect the breakdown and circumvention of segregation of duties, sys-tem failure, incorrect processing, theft or unauthorized removal of data or system resources, misuse of software, and improper access to, or use of, alteration, destruction, or disclosure of information.

b. Availability The system is available for operation and use as committed or agreed.

The availability principle refers to the accessibility of the system, products, or services as committed by contract, service-level agreement, or other agreements. This principle does not, in itself, set a minimum acceptable performance level for system availability. The availability principle does not address system functionality (the specific functions a system performs) and system usability (the ability of users to apply system functions to the performance of specific tasks or problems), but does address whether the system includes controls to support system accessibility for operation, monitoring, and maintenance.

c. Processing integrity. System processing is complete, valid, accurate, timely, and authorized. The processing integrity principle refers to the completeness, validity, accuracy, timeliness, and authorization of system processing. Processing integrity addresses whether the system achieves its aim or the purpose for which it exists, and whether it performs its intended function in an unimpaired manner, free from unauthorized or inadvertent manipulation. Processing integrity does not automatically imply that the information received and stored by the system is complete, valid, ac-curate, current, and authorized. The risk that data contains errors introduced prior to its input in the system often cannot be addressed by system controls and detecting such errors is not usually the responsibility of the entity. Similarly, users out-side the boundary of the system may be responsible for initiating processing. If such actions are not taken, the data may become invalid, inaccurate, or otherwise inappropriate.

d. Confidentiality Information designated as confidential is protected as committed or agreed.

The confidentiality principle addresses the system's ability to protect information designated as confidential in accordance with the organization's commitments and requirements through its final disposition and removal from the system. In-formation is confidential if the custodian of the information, either by law or regulation, commitment, or other agreement, is obligated to limit its access, use, and retention, and restrict its disclosure to a specified set of persons or organizations (including those that may otherwise have authorized access within the boundaries of the system). The need for information to be confidential may arise for many different reasons. For example, the information is proprietary information, information intended only for company personnel, personal information, or merely embarrassing information. Confidentiality is distinguished from privacy in that

(i) privacy deals with personal information whereas, confidentiality refers to a broader range of information that is not restricted to personal information; and

(ii) privacy addresses requirement for the treatment, processing, and handling of personal information.

e. Privacy The privacy principle addresses the system's collection, use, retention, disclosure, and disposal of personal information3 in conformity with the commitments in the entity's privacy notice and with criteria set forth in generally accepted privacy principles (GAPP). GAPP is a management framework that includes the measurement criteria for the trust services privacy principle.

V. TRUST MANAGEMENT IN CLOUD SECURITY

Trusted cloud computing can be viewed as a computer security architecture that is designed to protect cloud systems from malicious intrusions and attacks, and ensure that computing resources will act in a specific, predictable manner as intended. A trusted cloud computing system will protect data in use by hypervisors and applications, protect against unauthorized access to information, provide for strong authentication, apply encryption to protect sensitive data that resides on stolen or lost devices, and support compliance through hardware and software mechanisms.Numerous trust-related issues should be raised with, and satisfied by, a cloud provider. They range from concerns about security, performance, cost, control; availability, resiliency, and vendor lock in.[7]

VI. CONCLUSION

Now, we conclude this research paper. In this paper we identified top seven cloud computing security threats Abuse and Nefarious Use of Cloud Computing, Insecure Application Programming Interfaces, Malicious Insiders, Shared Technology Vulnerabilities, Data Loss/Leakage, Account, Service & Traffic Hijacking, Unknown Risk Profile. Trust services principles is very important to setup the trust management between cloud service providers and cloud user/customers. These are describe as Security, Availability, Processing, Confidentiality, Privacy. In the last section of this research paper we describe the trust management and role of trusted cloud computing.

REFERENCES

[1] NIST Special Publication 800-14, "Generally Accepted Principles and Practices for Securing Information Technology Systems," September 1996

[2] Almulla S, Chon Yeob Yeun. (March 2010) 'Cloud Computing Security management ', 2nd International Conference On Engineering Systems Management and Its Applications , 1-7..

[3] Security Guidance for Critical Area of Focus in Cloud Computing,. 2009.

[4] R.Chow, et al. Controlling Computation without Outsourcing Control. in CCSW'09, ACM workshop on Cloud computing security. 2009.

[5] S.Hanna, A security analysis of Cloud Computing. Cloud Computing Journal.

[6] TRUST SERVICES PRINCIPLES AND CRITERIA, EXPOSURE DRAFT, Prepared by the AICPA Assurance Services Executive Committee Trust Information Integrity Task Force, September 30, 2013.

[7] Shalini Agarwal et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (5) , 2015, 4568-4570.