Enhancing Security and Privacy by Integrating the Trusted Computing and TClouds

N.Suganya[1] D.Arthi[2] M.Brindha Devi[3] V.Yamini Priya[4]
[1,2,3,4]Assistant Professor
[1,2,3,4]Department of Computer Science & Engineering
[1,2,3,4]VSB College of Engineering Technical Campus, Coimbatore, India

Abstract— Cloud computing is a network based technology. Cloud computing has it origin from distributed computing, grid computing, utility computing. In cloud the users can pay for what they can use. To reduce the infrastructure the users move the data from their environment to the cloud environment. The users can loss the control over the data. While the data moving on infrastructure can pose severe security and privacy issues and the data store is insufficiently protected by access policies. There is a chance that the attacker can easily spoof an authorized user's data. In this paper we are focusing to enhance the data security in cloud computing using Tclouds and trusted computing.
Key words: Cloud Computing, Threats and Attacks

I. INTRODUCTION

Cloud computing change the way the people using the computer and the internet. Cloud computing is a subscription-based service where we can obtain networked storage space and computer resources [3]. The Cloud makes it possible to access the information from anywhere at any time. The cloud provides many facilities to the computer users and the large as well as small businesses. The resources are provided as a service to the user such as SAAS (software as a service), PAAS (Platform as a service), IAAS (Infrastructure as a service) [10] .The cloud provides storage in the form of data centres where the datum are stored in a centralized location. Cloud has a service-level agreement which exists between the provider and the end-user. The SLA can identify the needs of the end-user, eliminate expectations and reduce complex issues.

II. CHARACTERISTICS

A. Improved Availability

If there exists a fault in one machine it does not affect other virtual machine. Single point of failure is avoided in cloud.

B. Network Access

Cloud resources can be accessed only through internet. The cloud computing uses the internet as a media for communication [10].

C. Increased Storage

The cloud can change dynamically and can handle large volume of data.With dynamic workloads it can work effectively.

III. SERVICE MODELS

A. Software-as-a-service:

A complete application is provided to the end-user as a service. Multiple users can access it by running a single instance of the service

B. Platform-as-a-service:

Development environment is provided as a service from which higher layers of developed. The end-user can develop their own platform depending on their need [9].

C. Infrastructure-as-a-service:

The storage and computing capabilities are provided as a service to end-users over the network.

IV. DEPLOYMENT MODELS

The different cloud models are as follows:

A. Private cloud:

The private cloud can be developed and hosted by any specific organization. Only the members of the organization can access or control the cloud which leads to secure information access.

B. Public cloud:

These clouds are operated and used by general public. They can be an organization or an enterprise or government bodies or any combination of them. The capabilities are provided to multiple customers with more data centers, hardware and infrastructures.

C. Hybrid cloud:

Hybrid cloud is a combines both public cloud and private cloud .The cloud users can store their information securely in private cloud and for processing large amount of information private cloud will be used.

D. Community cloud:

Community cloud shares infrastructure between several organizations from a specific community with common concerns whether managed internally or by third-party.

V. PROBLEM STATEMENT

Although cloud computing is an emerging technology, the recent increased use of cloud services require up-to-date insights into necessary security requirements and its solutions .cloud computing as an emerging technology have different issues and challenges.

The objective of this paper is to provide a detailed overview of the types of security issues investigated in the area of cloud computing and the proposed solutions to deal with the issues. It moreover helps cloud developers with a detailed overview to quickly find and address gaps in cloud security issues.

When storing data on cloud, one might want to make sure if the data is correctly stored and can be retrieved later. The information stored on the cloud is often seen as valuable to individuals with malicious intent. The loss of control

outside the secured corporate perimeter increases the complexity of protecting data and increases the risk of compromise. Tclouds and trusted computing are used to improve the security of the user's data.

VI. SECURITY ISSUES IN CLOUD COMPUTING:

Top seven security threats to cloud computing discovered by "Cloud Security Alliance" (CSA) are [6]:

- Abuse and Nefarious Use of Cloud Computing
- Insecure Application Programming Interfaces
- Malicious Insiders.
- Shared Technology Vulnerabilities
- Data Loss/Leakage
- Account, Service & Traffic Hijacking.

VII. RELATED WORK

The paper is mostly related to works in security of the user's data. Some of the works are listed below.

In [4] third party auditor and auditing mechanisms are proposed. Auditing is the process of tracing and logging the events that happen during the system run time. A third party auditor who has resources can audit the user's data in cloud. Privacy preserving public auditing and challenge-response protocols were implemented to ensure data integrity by auditing. To enforce the security policies, a master checklist for internal and external auditors are used during auditing. Checklist of Iaas includes: data location awareness, data ownership awareness, data protection plan. Saas model checklist consists of: data surrender activity, data format check and performance.

In [8] proposed data integrity requires only authorized users can change the data and confidentiality refers that only authorized users can read the data. Cloud computing also provides strong user access control for data management and licensing. The data stored in the cloud can be stolen so these data can be encrypted before [7] storing in the cloud. The encryption methodologies such as asymmetric key encryption, symmetric key encryption. Asymmetric encryption uses public and private keys for encryption and decryption whereas symmetric key encryption uses only single key for both encryption and decryption. Asymmetric key can get high security but encryption and decryption is slow. Encryption mechanism depends on the reliability of the difficulty of decryption.

The operational and maintenance are responsible for the data storage and backup. Since the data are not stored in client area, implementing security measures cannot be applied directly. When there exist a situation in which the data is not available, the backup data are used .Cloud computing storage security enforces data isolation, data location, data long term survivability. Customers [8] should have the right of the supervision and audit of cloud computing services in order to ensure the security of the customer data. The cloud provider is responsible for security but monitoring and auditing by the cloud provider is a problem. The disaster recovery management includes system backup and data disaster recovery. The network transparent security is protected by the virtual private network technology.

In [1] discusses the security issues in cloud and the methods to resolve those issues. Multi-tenancy arises due to sharing of the resources in cloud which can be used by many users. Due to the sharing of the resources create confidentiality issues. In order to avoid this issue isolation is maintained among the tenant data. Isolation should be done in VM's, storage, API's as well as in operating system. The consumers scale up and down the resources based on the consumer demand. Placement Engines are used to maintain a list of available resources. This list is used to allocate resources to the users based on the demand. When the users move the data to the cloud, the users calculate the risk based on the non-availability of the data. LA includes the maximum time for which the resources are not available and the penalty rate for the risk.

In [2] the service models and security issues are discussed. In IAAS the virtual server is used instead of the dedicated server because of the server capacity problems. In PAAS, the IDE is provided as a service where the developer can develop, deploy and complete the application life cycle. In SAAS, instead of installing the software in the desktop system it is provided as a service and the customer can pay for what they can use.

Providing authentication and access control is important to prevent from unauthorized users accessing the data. If a company is not satisfied with any of the service provider then the company can change the provider .When transferring the data from the customer environment to the cloud encryption is used to protect the data. For more security VPN or SSH tunnelling can be implemented. The hardware components may be attacked by the people. Due to the availability, the data should be available at all the time. The backup plan of the user's data is provided either to the customers or to the provider.

VIII. PROPOSED FRAMEWORK

To improve the security of the user's data Tclouds and trusted components are implemented. The Tcloud provide [5] a secure environment and it is resilient in which only the authorized users can access and store the data. In trusted component hardware enhancements and software associations are implemented by using various technologies. The trusted component provides the services such as authentication, encryption, integrity and confidentiality.

IX. TECHNOLOGIES IN TRUSTED COMPUTING

A. Endorsement Key

A Trusted Platform Module (TPM) is a dedicated chip on an end-user device that stores RSA encryption keys for authentication. Each TPM chip contains an RSA key pair called the Endorsement Key (EK).

B. Sealed storage

The data can be accessed by the machine only if the machine is in the particular hardware or software configuration. The sealed storage provides more privacy whenever the data access occurs.

C. Remote attestation

It allows changes to the user's computer to be detected by authorized parties.. It works by having the hardware generate a certificate affirming what software is currently running. To show that unaltered software is currently executing the computer can then present this certificate to a remote party

D. Trusted third party

Due to loss of control over the data by the endusers the third party mechanism is implemented. The third party who has the resources and the knowledge that the user does not have can access the data to check for the data privacy. If any malicious event occur then it will be notified to the end-user.

X. CONCLUSION

We believe that data security in Cloud Computing, an area full of challenges and of paramount importance, is still in its infancy now, and many research problems are yet to be identified. From this review, different modes of algorithms are used for security concern. Even encryption is implemented, there exists a problem. More advanced encryption methodologies are used to prevent the threats.

REFERENCES

[1] Akhil Bhel and Kanika Bhel (2012) "An Analysis of Cloud Computing security issues" World Congress on Information and Communication Technologies.
[2] Eystein Mathisen (2011) "Security Challenges and Solutions in Cloud Computing" 5th IEEE International Conference on Digital Ecosystems and Technologies (IEEE DEST), Daejeon, Korea
[3] Esh Narayan,Mohit Malik,Aman preet singh and Prem Narain "To Enhance the Data Security of Cloud in Cloud Computing using RSA Algorithm" International Journal of Software Engineering vol.1 No.1 sep 2012.
[4] Irfan Gul, Atiq ur Rehman and M Hasan Islam (2011) "cloud computing security Auditing", 2nd International Conference on Next Generation Information Technology (ICNIT).
[5] Mina Deng, Milan Petkovi, Marco Nalin and Ilaria Baroni (2011) "A home healthcare system in the cloud – addressing security and privacy challenges" -IEEE 4th International Conference on Cloud Computing.
[6] "Security Guidance for Critical Areas of Focus in Cloud Computing", April 2009, presented by Cloud Security Alliance (CSA).
[7] Shivlal Mewada , Umesh Kumar Singh and Pradeep Sharma (2011)"Security Based Model for Cloud Computing", IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), Vol. 1, No. 1.
[8] Wentao Liu (2012)" Research on Cloud Computing Security Problem and strategy" 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet).
[9] Cloudcomputing: http://en.wikipedia.org/wiki/Cloud_computing,Accessed:28/08/13
[10] Ayesha Malik, Muhammad Mohsin Nazir "Security Framework for Cloud Computing Environment: A Review" Journal of Emerging Trends in Computing and Information Sciences VOL. 3, NO. 3, March 2012

