Secured data in cloud computing using Trusted platform

Harini Chitta
PG Student
Master of Computer Application
Mount Carmel College, Bangalore
harinisowjanya@gmail.com

***Abstract*—The most rapidly developing field of current trends in present world is cloud computing. It delivers all basic services required for IT industry as well as other industry. Storage as service is most widely used services provided by the cloud where the space is given to store their data on a subscription basis. The main challenge here is the security of data stored. This paper emphasis more on cloud computing security challenges, data protecting techniques and discuss about the strategies for secure transition to the cloud. We analyze the importance of trusted platform.**

Keywords—cloud,Trusted platforms;

I. INTRODUCTION

Cloud computing has transformed the It organization approach, allowing them to move quickly, meet their goals, expand their business, provide more services with reduced cost. Cloud computing technology can be implemented in a wide variety of architectures, different services and deployment models, along with the software design approaches. The services provided by cloud are Software as a Service (Saas), platform as a Service (PaaS) and Infrastructure as a Service (IaaS). SaaS deploys the provider applications running on the cloud infrastructure. It offers access at any place. PaaS is a shared development environment, where the consumer controls deploy applications but does not manage the underlying cloud infrastructure. IaaS lets the consumer provision processing, storage, networks, and other fundamental computing resources and controls operating systems, storage, and deployed applications. Some of the Cloud provides are Windows Azure, Amazon Elastic Compute Cloud, Hadoop etc.

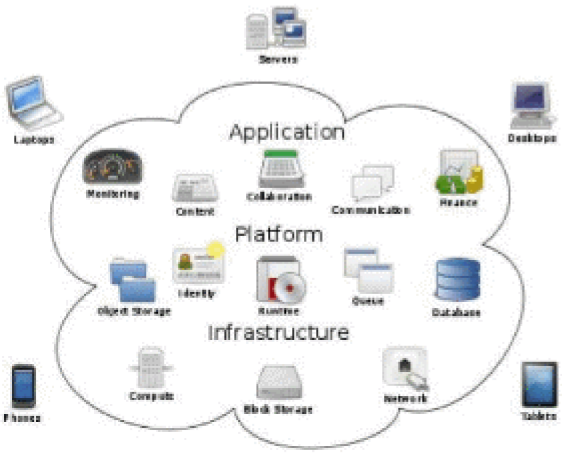

Fig. 1 *Services provided by the cloud*

The cloud computing landscape continues to realize explosive growth. The worldwide public cloud services market was projected to grow nearly 20 percent in 2013, to a total of $132 billion, with 45.6 percent growth for Infrastructure as a Service (IaaS), which is the fastest growing market segment. A decade ago, enterprise data typically resided in the organization's physical infrastructure, on its own servers in the enterprise's data center, where one could segregate sensitive data in individual physical servers. Today, with virtualization and the cloud, data may be under the organization's logical control, but physically reside in infrastructure owned and managed by another entity. This is the reason for requirement of new approaches and techniques to ensure organizations can maintain data security.

II. CLOUD COMPUTING SECURITY CHALLENGES

Storage as a Service is generally seen as a good alternative for a small or mid-sized business that lacks the capital budget and/or technical personnel to implement and maintain their own storage infrastructure. Data protection tops the list of cloud concerns. The benefits of cloud computing are economies of scale, potential cost savings, fast deployment and easy scalability. According to the research report, security is the biggest obstacle to cloud adoption followed closely by legal, compliance, and privacy issues.

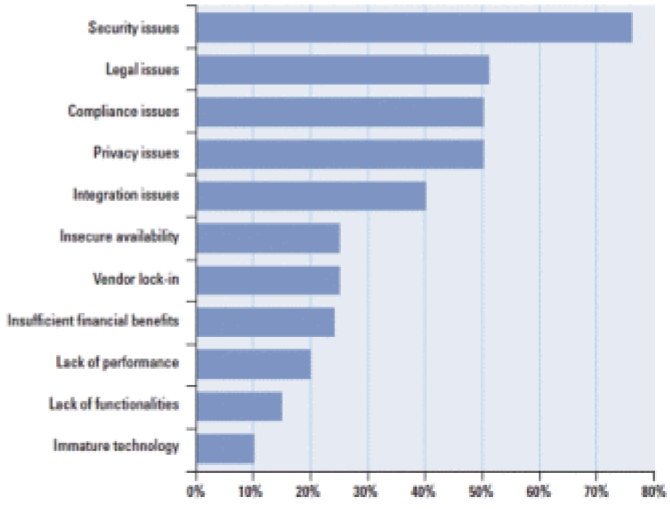

Fig. 2 *Main concern regarding the use of cloud computing*

There are complex data security challenges in the cloud:

- The need to protect confidential business government, or regulatory data.

- Cloud service models with multiple tenants sharing the same infrastructure
- Data mobility and legal issues relative to such government rules as the EU Data Privacy Directive
- Lack of standards about how cloud service providers securely recycle disk space and erase existing data
- Auditing, reporting, and compliance concerns
- Loss of visibility to key security and operational intelligence that no longer is available to feed enterprise IT security intelligence and risk management
- A new type of insider who does not even work for your company, but may have control and visibility into your data.

III. TECHNIQUES FOR PROTECTING DATA IN THE CLOUD

Traditional models of data protection have often focused on network-centric and perimeter security, frequently with devices such as firewalls and intrusion detection systems. But this approach does not provide sufficient protection against APTs, privileged users, or other insidious types of security attacks. Many enterprises use database audit and protection (DAP) and Security Information and Event Management (SIEM) solutions to gather together information about what is happening. But monitoring and event correlation alone do not translate into data security. Many organizations have implemented encryption for data security. They often overlook inherent weaknesses in key management, access control, and monitoring of data access. If encryption keys are not sufficiently protected, they are vulnerable to theft by malicious hackers. Vulnerability also lies in the access control model; thus, if keys are appropriately protected but access is not sufficiently controlled or robust, malicious or compromised personnel can attempt to access sensitive data by assuming the identity of an authorized user. Therefore, any data-centric approach must incorporate encryption, key management, strong access controls, and security intelligence to protect data in the cloud and provide the requisite level of security.

By implementing a layered approach that includes these critical elements, organizations can improve their security posture more effectively and efficiently than by focusing exclusively on traditional network-centric security methods.

An effective cloud security solution should incorporate three key capabilities:

- Data lockdown
- Access policies
- Security intelligence

First, one make sure that data is not readable and that the solution offers strong key management. Second, one must implement access policies that ensure only authorized users can gain access to sensitive information, so that even privileged users such as root user cannot view sensitive information. Third, one must incorporate security intelligence that generates log information, which can be used for behavioral analysis to provide alerts that trigger when users are performing actions outside of the norm.

IV. TRUSTED COMPUTING

Encryption is one of the major reasons why online backup is the preferred choice for computer storage. Encryption prevents malicious parties from attempting to access, change or damage files by storing them in a why which is inaccessible without the key. Encryption prevents unwanted individuals from being able to access, tamper with or vindictively change files to cause harm to you personally or to your business. Encryption is the process whereby you use a program to scramble data in a way which can only be rectified by using a key. This protects the files while they are on our data servers, by simply storing them away from your PC. Public and private cloud services, also known as multi-tenant infrastructure, are used increasingly in the enterprise and by government agencies. It should maintain below mentioned properties:

Confidentiality: The nature of hardware-based cryptography ensures that the information stored in hardware is better protected from external software attacks. A variety of applications storing secrets on a TPM can be developed. These applications make it much harder to access information on computing devices without proper authorization. *Authentication:* It ensures only authorized users and authorized PCs are on an enterprise network. It also acts as a secure vault for certificates, keys and passwords, negating the need for costly tokens.
Platform Integrity: Measures and reports on the integrity of platform, including the BIOS, disk MBR, boot sector, operating system and application software, to ensure no unauthorized changes have occurred. The TPM, a secure cryptographic integrated circuit (IC), provides a hardware-based approach to manage user authentication, network access, data protection and more that takes security to higher level than software-based security.

V. TRUSTED CLOUD STORAGE ARCHITECTURE

For the vast majority of cloud storage, the security and privacy options provided are perfectly acceptable. The fact is that most people just don't care about privacy. For those of us that do, however, there is a relatively easy solution that can allow you to continue using cloud storage and keep your data secure, Using Trusted Cloud; you can create encrypted folders within your cloud storage, which gets synched like any other file from the Trusted Cloud. Trusted Cloud provides you with the ability to create a unified data protection policy across all clouds. As an in-line security gateway that sits between your users and your cloud applications, Trusted Cloud applies encryption on the fly before sensitive data leaves the enterprise. By applying encryption in a cloud security gateway, Cipher Cloud eliminates the inherent security and privacy risks of cloud computing. Your business never loses control of its sensitive data, yet you can achieve the full benefits of cloud computing. The Trusted Gateway provides a way to encrypt sensitive information to the enterprises as it moves to any cloud application and then decrypt it again as data is delivered to end users. This protects the data from being accessed by others. This revolutionary technology maintains the cloud application user experience, with near zero latency, and without making any changes to the cloud application itself. Trusted Gateway takes

a revolutionary approach to protecting sensitive data before it leaves an organization's secure enterprise network.

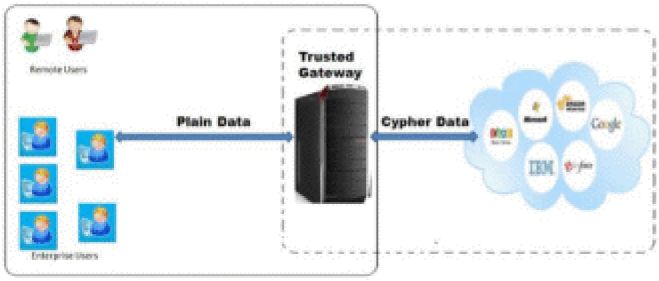

Fig 3 *Trusted Cloud Storage Architecture*

There also may be possible that in the internal network some intruder gain access pretend to be another genuine user. So it is necessary to authenticate the user to retain security. For authenticate the users we use the famous Kerberos authentication service [2]. The entities of the authentication service are as follows: End User (U): User, who aims to stores encrypted credentials to the cloud storage. So to encrypt data user should authenticate itself to the Trusted Gateway. Remote User: Remote User, who access the cloud storage outside the internal enterprise network. Trusted Gateway (TG): Trusted gateway is the work station having TPM which maintains the data to be encrypted comes from end users and encrypt them and store to the cloud storage and vice versa. Authentication Server (AS): Authentication Server verifies user's access right in database; create ticket granting ticket and session key. Ticket Granting Server (TGS): Ticket Granting Server issues ticket to request the Trusted Gateway.

Database: The Kerberos service must have a database to store user id (ID) and hashed passwords.

The details of the Kerberos Authentication Service Exchange are: A. Authentication Service Exchange to obtain ticket-granting Ticket

(1) U □ AS : IDu, IDtgc, TS1

(2) AS □ U : E (Ku , [Ku,tgs||IDtgs||TS2 ||Lifetime2 ||Tickettgs])

Tickettgs= E(Ktgs, [Ku,tgs||IDu||ADu||IDtgs||TS2 ||Lifetime2])

B. Ticket-granting service Exchange to obtain trusted gateway service-granting ticket

(3) U □ TGS : IDtg||Tickettgs||Authenticatoru

(4) TGS □ U : E(Ku,tgs,[Ku,tg||IDtg||TS4 ||Tickettg])

Tickettg= E(Ktg,[Ku,tg||IDu||ADu||IDtg||TS4 ||Lifetime4])

Authenticatoru= E(Ku,tgs||IDu||ADu||TS3)

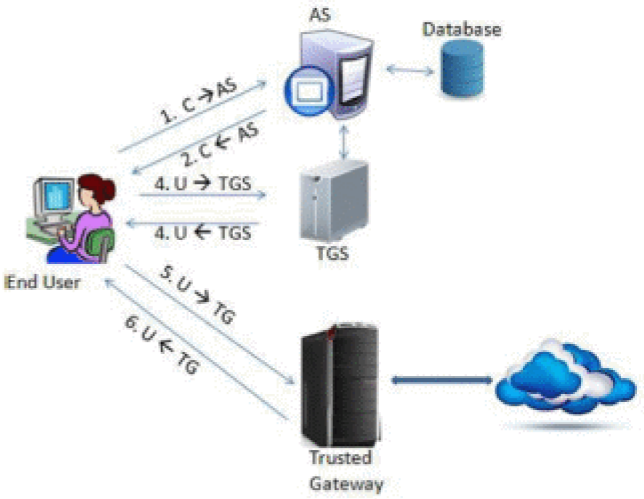

Fig. 4 *Kerberos authentication service*

Once the session is created between end user and trusted gateway then the end user can send data to store in the cloud in encrypted form and also can retrieve data from the cloud with the help of Trusted Gateway. Records of data sent and retrieved to the cloud from various end users is maintains by the Trusted Gateway. As we clarify that the data which is stored in the cloud in the encrypted form in highly confidential so to keep the security of data we assume that the remote users who want to retrieve the data from cloud have TPM chip in his system. So remote users have to authenticate itself to the trusted gateway and then it can exchange keys, by which it can retrieve data directly from the cloud and decrypt itself.

VI. CONCLUSIONS

In this paper we have discuss about cloud computing security issues and discussed about the Trusted platform and its architecture as a Solution which helps to encrypt and decrypt the data efficiently which gives better security in the Cloud storage.

REFERENCES

[1] William Stallings, *Cryptography and Network Security- Principles and Practices*, 3rd Edition, Prentice Hall of India, 2003.

[2] A research on cloud computing security.

[3] Data security in cloud computing.

[4] Using location based encryption to improve the security of data access in cloud computing.

[5] A Proposed Model for Data Security of Cloud Storage Using Trusted Platform Module by Abhishek Patel and **Mayank Kumar**