IPHV2I20009X
International Journal Of Advanced Research and Innovation -Vol.II, Issue .2
ISSN Online: 2319 – 9253
Print: 2319 – 9245

DATA FORTIFICATION IN CLOUD BASED STORAGE

A.Vainathi[1], Mruthyunjaya Mendu[2]

1. M.Tech (CSE) , Dept. of Computer Science & Engineering, SCCE, Karimnagar.
2. Associate Professor, Dept. of Computer Science & Engineering, SCCE, Karimnagar.

ABSTRACT

Cloud is a common area for data centers and services now days. These services are works through cloud to the client. Offers the services with optimal price methods but requires the protection to the data. Clouds are not offering that much of security services but a platform providing protection called Data Protection As a Service. DPaS which reduce lot of data protection problems with development and maintenance issues also.

Key terms: *Cloud, Security, Protection, DPaS, Encryption*

Introduction

Cloud computing provides many benefits like low cost and accessibility of data. To provide the security to the cloud is a major issue because of thousands of services and lack of users sensitive data are saved in cloud. Cloud uses the security but those may be untrusted to ensure the security to the cloud we require basic security mechanism is encryption is as follows.

Data Protection through Encryption

1) Key Policy Attribute-Based Encryption (KP-ABE):

KP-ABE is a public key cryptography primitive for one-to-many communications. In KP-ABE, data are associated with attributes for each of which a public key component is defined. User secret key is defined to reflect the access structure so that the user is able to decrypt a cipher text if and only if the data attributes satisfy his access structure. A KP-ABE scheme is composed of four algorithms which can be defined as follows:

- Setup Attributes
- Encryption
- Secret key generation
- Decryption

Setup Attributes:

This algorithm is used to set attributes for users. From these attributes public key and master key for each user can be determined. The attributes, public key and master key are denoted as

Attributes- $U = \{1, 2. . . N\}$
Public key- $PK = (Y, T1, T2, . . . , TN)$
Master key- $MK = (y, t1, t2, . . . , tN)$

Encryption:

This algorithm takes a message *M*, the public key *PK*, and a set of attributes *I* as input. It outputs the cipher text *E* with the following format

***E* = (*I*, ˜ *E*, {*Ei*}*i*)** where $\tilde{}E = MY, Ei = Ti.$

Secret key generation:

This algorithm takes as input an access tree *T*, the master key *MK*, and the public key *PK*. It outputs a user secret key *SK* as follows.

***SK* = {*ski*}**

IPHV2I20009X
International Journal Of Advanced Research and Innovation -Vol.II, Issue .2
ISSN Online: 2319 – 9253
Print: 2319 – 9245

Decryption:

This algorithm takes as input the cipher text ***E*** encrypted under the attribute set **U**, the user's secret key ***SK*** for access tree ***T***, and the public key ***PK***.

Finally it output the message ***M*** if and only if **U satisfies T**.

2) Proxy Re-Encryption (PRE):

Proxy Re-Encryption (PRE) is a cryptographic primitive in which a semi-trusted proxy is able to convert a cipher text encrypted under Alice's public key into another cipher text that can be opened by Bob's private key without seeing the underlying plaintext. A PRE scheme allows the proxy, given the proxy re-encryption key ***rka↔b,*** to translate cipher texts under public key ***pk1*** into cipher texts under public key ***pk2*** and vise versa.

3) Lazy re-encryption:

The lazy re-encryption technique and allow Cloud Servers to aggregate computation tasks of multiple operations. The operations such as

- Update secret keys
- Update user attributes.

EXISTING MODEL

Cloud computing promises lower costs, rapid scaling, easier maintenance, and service availability anywhere, anytime, a key challenge is how to ensure and build confidence that the cloud can handle user data securely. A recent Microsoft survey found that "58 percent of the public and 86 percent of business leaders are excited about the possibilities of cloud computing. But more than 90 percent of them are worried about security, availability and privacy of their data as it rests in the cloud."

PROPOSED WORK

We propose a new cloud computing paradigm, *data protection as a service* (DPaaS) is a suite of security primitives offered by a cloud platform, which enforces data security and privacy and offers evidence of privacy to data owners, even in the presence of potentially compromised or malicious applications. Such as secure data using encryption, logging, key management.

DATA PROTECTION AS A SERVICE

Currently, users must rely primarily on legal agreements and implied economic and reputational harm as a proxy for application trustworthiness. As an alternative, a cloud platform could help achieve a robust technical solution by •• making it easy for developers to write maintainable applications that protect user data in the cloud, thereby providing the same economies of scale for security and privacy as for computation and storage; and •• enabling independent verification both of the platform's operation and the runtime state of applications on it, so users can gain confidence that their data is being handled properly. Much as an operating system provides isolation between processes but allows substantial freedom inside a process, cloud platforms could offer transparently verifiable partitions for applications that compute on data units, while still allowing broad computational latitude within those partitions. DPaaS enforces fine-grained access control policies on data units through application confinement and information flow checking. It employs cryptographic protections at rest and offers robust logging and auditing to provide accountability. Crucially, DPaaS also directly addresses the issues of rapid development and maintenance. To truly support this vision, cloud platform providers would have to offer DPaaS in addition to their existing hosting

IPHV2I20009X
International Journal Of Advanced Research and Innovation -Vol.II, Issue .2
ISSN Online: 2319 – 9253
Print: 2319 – 9245

environment, which could be especially beneficial for small companies or developers who don't have much in-house security expertise, helping them build user confidence much more quickly than they otherwise might.

SYSTEM ARCHITECHTURE

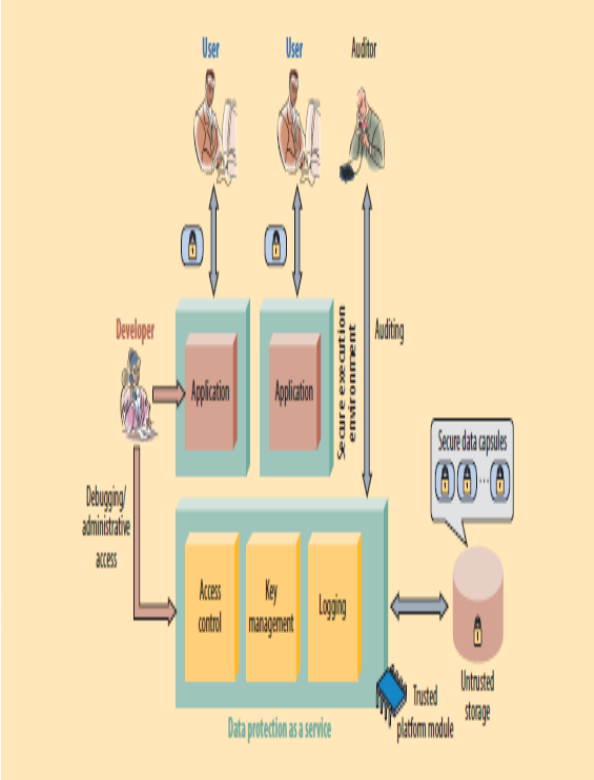

Figure 1. Sample architecture for data protection as a service illustrates how it's possible to integrate various technologies, such as application confinement, encryption, logging, code attestation, and information flow checking to realize DPaaS.

1. **Cloud Computing**
2. **Trusted Platform Module**
3. **Third Party Auditor**
4. **User Module**

1. Cloud Computing

Cloud computing is the provision of dynamically scalable and often virtualized resources as a services over the internet Users need not have knowledge of, expertise in, or control over the technology infrastructure in the "cloud" that supports them. Cloud computing represents a major change in how we store information and run applications. Instead of hosting apps and data on an individual desktop computer, everything is hosted in the "cloud"—an assemblage of computers and servers accessed via the Internet.

Cloud computing exhibits the following key characteristics:

1. Agility improves with users' ability to re-provision technological infrastructure resources.

2. Multi tenancy enables sharing of resources and costs across a large pool of users thus allowing for:

3. Utilization and efficiency improvements for systems that are often only 10–20% utilized.

4. Reliability is improved if multiple redundant sites are used, which makes well-designed cloud computing suitable for business continuity and disaster recovery.

5. Performance is monitored and consistent and loosely coupled architectures are constructed using web services as the system interface.

6. Security could improve due to centralization of data, increased security-focused resources, etc., but concerns can persist about loss of control over certain sensitive data, and the lack of security for stored kernels. Security is often as good as or better than other traditional systems, in part because providers are able to devote resources to solving security issues that many customers cannot afford. However, the complexity of security is greatly increased when data is distributed over a wider area or greater number

of devices and in multi-tenant systems that are being shared by unrelated users. In addition, user access to security audit logs may be difficult or impossible. Private cloud installations are in part motivated by users' desire to retain control over the infrastructure and avoid losing control of information security.

7. **Maintenance** of cloud computing applications is easier, because they do not need to be installed on each user's computer and can be accessed from different places.

2 .Trusted Platform Module

Trusted Platform Module (TPM) is both the name of a published specification detailing a secure crypto processor that can store cryptographic keys that protect information, as well as the general name of implementations of that specification, often called the "TPM chip" or "TPM Security Device". The TPM specification is the work of the Trusted Computing Group.

Disk encryption is a technology which protects information by converting it into unreadable code that cannot be deciphered easily by unauthorized people. **Disk encryption** uses disk encryption software or hardware to encrypt every bit of data that goes on a disk or disk volume. Disk encryption prevents unauthorized access to data storage. The term "full disk encryption" (or **whole disk encryption**) is often used to signify that everything on a disk is encrypted, including the programs that can encrypt bootable operating system partitions. But they must still leave the master boot record (MBR), and thus part of the disk, unencrypted. There are, however, hardware-based full disk encryption systems that can truly encrypt the entire boot disk, including the MBR**.**

3. Third Party Auditor

In this module, Auditor views the all user data and verifying data and also changed data. Auditor directly views all user data without key. Admin provided the permission to Auditor. After auditing data, store to the cloud.

4. User Module

User store large amount of data to clouds and access data using secure key. Secure key provided admin after encrypting data. Encrypt the data using TPM. User store data after auditor, view and verifying data and also changed data. User again views data at that time admin provided the message to user only changes data.

CONCLUSION:

It is mandatory to provide the security to data in personal/private involves in online nature. Some of the data centers are utilizes the high-end protection systems to provide the security to the data. we know that the data centers are nothing but a cloud adding protection to the single cloud it leads to all services provided by client means thousands o services are benefited and TBs of client data are protected.

REFERENCES:

[1] H. Abu-Libdeh, L. Princehouse and H. Weatherspoon, "RACS: a case for cloud storage diversity", SoCC'10:Proc. 1st ACM symposium on Cloud computing, 2010, pp. 229-240.

[2] P. Ammann and S. Jajodia, “Distributed Timestamp Generation in Planar Lattice Networks,” ACM Trans. Computer Systems, vol. 11, pp. 205-225, Aug. 1993.

[3] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable Data Possession at Untrusted

[4] Stores,” Proc. ACM Conf. Computer and Comm. Security, pp. 598-609, 2007.

[5] E. Barka and A. Lakas, "Integrating Usage Control with SIP-Based Communications," J. Computer Systems, Networks, and Comm.,vol. 2008, pp. 1-8, 2008.

[6] D. Boneh and M.K. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. Int'l Cryptology Conf. Advances in Cryptology, pp. 213-229, 2001.

[7] R. Bose and J. Frew, "Lineage Retrieval for Scientific Data Processing: A Survey," ACM Computing Surveys, vol. 37, pp. 1-28, Mar. 2005.

[8] P. Buneman, A. Chapman, and J. Cheney, "Provenance Management in Curated Databases," Proc. ACM SIGMOD Int'l Conf.

[9] Management of Data (SIGMOD '06), pp. 539-550, 2006.

[10] B. Chun and A.C. Bavier, "Decentralized Trust Management and Accountability in Federated Systems," Proc. Ann. Hawaii Int'l Conf. System Sciences (HICSS), 2004.

[11] C. Dwork, "The Differential Privacy Frontier Extended Abstract," *Proc. 6th Theory of Cryptography Conf.* (TCC 09),LNCS 5444, Springer, 2009, pp. 496-502.

[12] C. Gentry, "Fully Homomorphic Encryption Using Ideal Lattices," *Proc. 41st Ann. ACM Symp. Theory Computing* (STOC 09), ACM, 2009, pp. 169-178.

[13] E. Naone, "The Slow-Motion Internet," *Technology Rev.*, Mar./Apr. 2011; www.technologyreview.com/files/54902/

[14] GoogleSpeed_charts.pdf.Greenberg, "IBM's Blindfolded Calculator," *Forbes*,13 July 2009; www.forbes.com/forbes/2009/0713/breakthroughs-privacy-super-secret-encryption.html.