ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

Privacy Data Control and Data Protection as a Service in Cloud Computing

K.Bhima[1], S.Suresh[2]

Department of IT, Padmasri DR. B V Raju Institute of technology, Medak (Dist.), A.P, India [1]

Department of IT, Padmasri DR. B V Raju Institute of technology, Medak (Dist.), A.P, India [2]

Abstract: Offering strong data protection to the cloud users while enabling rich applications is a challenging task. Data protection in cloud has become unavoidable and is tremendously increasing feature in present scenario and in future. Many of the multinational organizations are interested in cloud computing and are excited about the features of the cloud. But they are worried about security, privacy and availability of the data as it rests in the cloud. As more and more sensitive information, privacy data is centralized in cloud, the data protection security and privacy issues must be strengthened tightly. I explore a new cloud platform architecture called Data Protection as a Service (Dpaas), which dramatically reduces the per-application development effort required to offer strong data protection, while still allowing rapid development and maintenance.

Keywords: - Cloud Computing, Data protection, Dpaas, Security, Privacy.

I. INTRODUCTION

The U.S. National Institute for Standards and Technology(NIST) has defined cloud computing as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (for example, networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"[1].

A cloud computing is a computing model that makes IT resources such as servers, middleware, and applications available over the Internet as services to business organizations in a self-service manner. The cloud is a set of hardware, networks, storage, services, and interfaces that enable the delivery of computing as a service. Cloud services include the delivery of software, infrastructure, and storage over the Internet (either as separate components or a complete platform) based on user demand. There are many participants of cloud such as end users, business management and cloud service provider. There will be an increasing number and diversity of clouds. In today's competitive market, companies must innovate and get the most from its resources to succeed. This requires enabling its employees, business partners, and users with the platforms and collaboration tools that promote innovation. Cloud computing infrastructures are next generation platforms that can provide tremendous value to companies of any size. As cloud consumers, enterprises have to improve cloud security. Corporate information must be secured in cloud computing. Cloud security is a joint responsibility of cloud providers and enterprises. There are three cloud models, ranging from software as a service (SAAS) to platform as a service (PAAS) to infrastructure as a service (IAAS). On one end of the spectrum, SAAS approaches are considered as security black box, where application security activities are largely not visible to the enterprise. On the other end IAAS, where an enterprise is principally responsible for the security of the application, data and possibly other levels of the infrastructure stack.. Moreover, vendors can update application/OS/middleware security patches faster because of higher availability of staff and resources. According to cloud vendors, most thefts occur when users with authorized access do not handle data appropriately. Upon a logout from the cloud session, the browser may be configured to delete data automatically and log files on the vendor side indicate which user accessed what data. The fact that cloud computing is not used for all of its potential is due to a variety of concerns. [2]

Even though cloud Computing is emerging as a rapid growing technology in the world as the number of providers and clients are rapidly increasing day by day. There is much concern about data protection, security and privacy challenges. Although 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" [3][4] Today, organizations that deal with large amounts of data (often termed "Big Data")—in various industries including media, banking and healthcare—are

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

increasingly adopting cloud technology to deliver faster services, protect data in real-time, provide seamless communication between employees, partners and suppliers, enable business continuity, and address the pressure to become more energy efficient—to be a greener organization.

II. EXISTING SYSTEM

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"[2]. In Cloud Computing till now we have seen Software-as a Service, Platform-as a service and Infrastructure-as a service. Let us see in detail, Software-as a Service is a software delivery method that provides access to software and it functions remotely as a web-based service. Software-as a Service allows organizations to access business functionality at a cost typically less than paying for licensed applications. When coming to Platform-as a Service, it is defined as a computing platform being delivered as a service. Here the platform is outsourced in place of company or data centre purchasing and managing their own hardware and software layers. Typically platform-as a service facilities deployment of applications, application development, testing and also supports the building, testing and hosting web applications and coming to Infrastructure-as a Service (Iaas), it is defined as a computer infrastructure such as virtualization being delivered as a service. Iaas is popular in the datacentre where software and servers are purchased as a fully outsourced service and usually billed on usage and how much of the resources are used.

III. PROPOSED SYSTEM

We proposed a new Cloud computing paradigm, Data-Protection as a Service (DpaaS). It is a suite of security primitives offered by a cloud platform, which enforces data security, privacy and offers evidence of privacy to data owners, even in the presence of potentially compromised or malicious applications. The figure illustrates an example architecture for exploring the Dpaas design space [6]. Dpaas enforces fine grained access control policies 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 [3]. To truly support this vision, cloud platform providers would have to offer DPaaS in addition to their existing hosting 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.

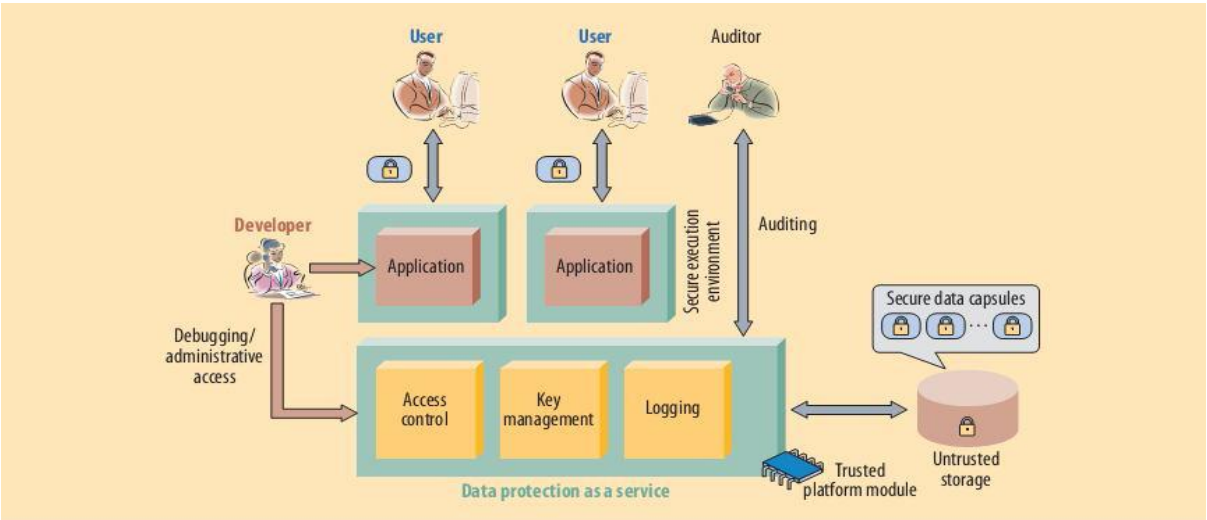

Figure 1. Sample architecture for data protection as a service illustrates how it's possible to integrate various technologies, such as application confinement, encryption, logging, code attestation, and information flow checking to realize DPaaS.

In figure 1, we have four modules, they are:

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

1. Cloud Computing:

A cloud computing is a computing model that makes IT resources such as servers, middleware, and applications

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

available over the Internet as services to business organizations in a self-service manner. The cloud is a set of hardware, networks, storage, services, and interfaces that enable the delivery of computing as a service. Cloud services include the delivery of software, infrastructure, and storage over the Internet (either as separate components or a complete platform) based on user demand. Now a day, "Cloud Computing" is the very useful and beneficial technology in business world. Cloud computing is internet – based technology which is combination of traditional and network technology. Cloud computing allows enterprises to achieve more efficient use of their hardware and software investments. Keeping resources into large clouds drives down costs and increases utilization by delivering resources only for as long as those resources are needed. Cloud computing allows individuals, teams, and organizations to streamline procurement processes and eliminate the need to duplicate certain computer administrative skills related to setup, configuration, and support.

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:

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

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

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

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

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

f. 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.

g. 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.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

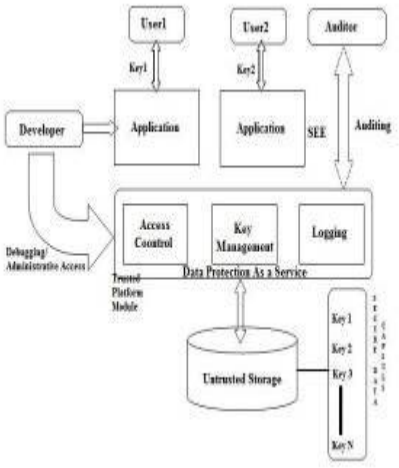

Fig 2: Data Protection as a Service

IV. THEORIES AND APPROACHES

A. Data Protection Goals:

- *Integrity.* The user's stored data won't be corrupted.
- *Privacy.* Private data won't be leaked to any unauthorized entity.
- *Access transparency.* Logs will clearly indicate who or what accessed any data.
- *Ease of verification.* Users will be able to easily verify what platform or application code is running, as well as whether the cloud has strictly enforced their data's privacy policies.
- *Rich computation.* The platform will allow efficient, rich computations on sensitive user data.
- *Development and maintenance support.* Because we face a long list of challenges, bugs to find and fix, frequent software upgrades, continuous usage pattern changes, and user demand for high performance, developers will receive both development and maintenance support.

B. Security and Privacy Challenges:

It's impossible to develop a single data-protection solution for the cloud because the term means too many different things. Any progress must first occur in a particular domain—accordingly, our work focuses on an important class of widely used applications that includes e-mail, personal financial management, social networks, and business tools

The following criteria define this class of applications:

- Provide services to a large number of distinct end users, as opposed to bulk data processing or workflow management for a single entity.
- use a data model consisting mostly of sharable units, where all data objects have access control lists (ACLs) with one or more users and
- Developers could run the applications on a separate computing platform that encompasses the physical infrastructure, job scheduling, user authentication, and the base software environment, rather than implementing the platform themselves.

C. Encryption:

Encryption is a powerful tool. When speaking about data protection, developers often view encryption as a kind of powerful one to help achieve data protection properties. Disk encryption is a technology which protects information by converting it into unreadable code that cannot be deciphered easily by unauthorised people. Disk encryption uses disk encryption software or hardware to encrypt every bit of data that goes on disk or volume. Disk encryption prevents unauthorised access to data storage. The term full disk encryption (FDE) is often used to signify that everything on a disk is encrypted, including the programs. Although FDE is effective in protecting private data in certain scenarios such as stolen laptops and backup tapes, the concern is that it can't fulfil data protection goals in the cloud, where physical threat isn't the main threat. According to performance when compared between FDE VS FHE, a recent survey, 49 percent of users abandon a site or switch to a competitor after experiencing performance issues.3 And the need for speed is only increasing: in 2000, a typical user was willing to wait 8 seconds for a webpage to load before navigating away; by 2009, that number dropped to 3 seconds.[5]

At the other end of the spectrum, Craig Gentry recently proposed the first realization of fully Homomorphic encryption (FHE)[4] which offers the promise of general computation on cipher texts. Basically, any function in plaintext can be transformed into an equivalent function in cipher text the server does the real work, but it doesn't know the data it's computing. Naturally, this property gives strong privacy guarantees when computing on private data, but the question of its practicality for general cloud applications still remains.

D. Key Management:

The concept of key came from the branch called as Cryptographs. There are basically two types of keys. They are:

(i) Public key (ii) Private key

A public key known to everyone and what a user wants to send the same message to another user, he uses public key to encrypt the message. Whereas private key or secret key known only to the recipient of the message. The same user after sending the message using public key then he can use his private key to decrypt it. In our system we encrypt the file using a key stored in the cloud. The user should enter

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

the key to decrypt the file, so multiple protection mechanisms are used here for protecting the files in the cloud.

E. Auditor:

The auditor is one who audits the overall performance of the system. He can track all the transactions and logins of users with correct time and date. Here auditor is software that is capable of tracking the transactions. Cloud storage offers movement of data into cloud. It has a great convenience to the user because users can store their data in the cloud safely without the knowledge about the storage space. There are several trends in cloud computing because of its wide variety of possibilities in the new era. Security in cloud computing have greater importance because users wants their data to be secure. The attack towards the data which is stored into the cloud is increasing. There are different security services implemented toward data storage. Researches for the security threats in cloud have great opportunities.

F. Audit Trails:

Because the platform mediates all data access, authenticates users, and runs binaries, it knows what data is accessed by what user, and with which application. It can generate meaningful audit logs containing all these parameters and optionally incorporate additional information from the application layer.
DPaaS can log four basic kinds of actions:

- Ordinary online data accesses that occur in response to external user requests when a user is online and operating an application;
- Access control modification by authorized users, the provenance of which can assist in forensics or problem diagnosis;
- Offline/batch access to handle requests while users are offline (for example, e-mail delivery) to compute aggregates or to reorganize data such as during schema changes; and
- Administrative access for maintenance operations such as debugging.

Users or developers can decide how detailed the logs are on a case-by-case basis.

G. Secure Data Capsule:

A Secure Data Capsule is an encrypted data unit packaged with its security policy. A main purpose of any cloud computing system should be to maintain users' data persistently in highly available remote storage. If it is also desirable to permit arbitrarily rich computations on this data while maintaining privacy, then careful attention must be paid to how that data is stored. Previous proposals for secure data capsules [7] have outlined key characteristics that such a mechanism should ideally have. Maniatis et al. argued that data should be stored as cryptographically secured \objects" that contain, in addition to a main payload of data, some sort of policy describing how and by whom that payload may be read or modified. Furthermore, any modifications to an existing object should be recorded in a log that preserves the history of that object since its inception and reveals which entities have accessed it. A more lightweight approach would be to use OS process isolation; an even lighter-weight approach would be to use language-based features such as information-flow controls or capabilities [7][8].

V. CONCLUSION

As private data moves online, the need to secure it properly becomes increasingly urgent. The good news is that the same forces concentrating data in enormous datacentres will also aid in using collective security expertise more effectively. Adding protections to a single cloud platform can immediately benefit hundreds of thousands of applications and, by extension, hundreds of millions of users. While we have focused here on a particular, albeit popular and privacy-sensitive, classes of applications, many other applications also need solutions.

In future, this work can be extended to develop a more formal model for data protection as a service in cloud computing. We can use this model for many other communications like client server communication etc..

REFERENCES:

[1] Effective Storage Management and Data Protection for cloud computing pdf.IBM.
[2] Traian Andrei, Cloud Computing Challenges and Related Security Issues,http://www.cs.wustl.edu/~jain/cse571-9/ftp/cloud/index.html#user.
[3] Cloud Data Protection for the Masses pdf. IEEE 2012
[4] C. Dwork. The differential privacy frontier. In TCC, 2009.
[5] C. Gentry. Fully Homomorphic Encryption Using Ideal Lattices. In STOC, pages 169–178, 2009.
[6] P. Maniatis, D. Akhawe, K. Fall, E. Shi, S. McCamant, and D. Song. Do You Know Where Your Data Are? Secure Data Capsules for Deployable Data Protection. In HotOS, 2011.
[7]. S. McCamant and M.D. Ernst, "Quantitative Information Flow as Network Flow Capacity," *Proc. 2008 ACM SIGPLAN* Conf. Programming Language Design and Implementation (PLDI 08), ACM, 2008, pp. 193-205.
[8]. M.S. Miller, "Robust Composition: Towards a Unified Approach to Access Control and Concurrency Control," PhD dissertation, Dept. of Philosophy, Johns Hopkins Univ.,2006.