International Journal of Science Engineering and Advance Technology

# Data Protection as a service in Cloud

Yemineni Ashok, Sri J. Bhargav
M. Tech (Cse), Assistant Professor, M.Tech (Software Engg.)
Chalapathi Institute Of Engineering And Technology
Chalapathi Nagar, Lam, Guntur,

*Abstract*

**Cloud computing enable highly scalable services to be easily consumed over the internet as and when needed. A major feature of the cloud services is that users' data are usually processed remotely in unknown machines that users do not own or operate. Providing a strong data protection to cloud users while enabling rich applications is a challenging task. We explore a new cloud platform architecture called Data Protection as a Service, which dramatically reduces the per-application development effort required to offer data protection, while still allowing rapid development and maintenance.**

**Key words: Cloud, data protection, rich applications.**

## INTRODUCTION

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

There is tension between user data protection and rich computation in the cloud. Users want to maintain control of their data, but also want to benefit from rich services provided by application developers using that data. At present, there is little platform-level support and standardization for verifiable data protection in the cloud. On the other hand, user data protection while enabling rich computation is challenging. It requires specialized expertise and a lot of resources to build, which may not be readily available to most application developers. We argue that it is highly valuable to build in data protection solutions at the platform layer: The platform can be a great place to achieve economy of scale for security, by amortizing the cost of maintaining expertise and building sophisticated security solutions across different applications and their developers.

**Target Applications**

There is a real danger in trying to "solve security and privacy for the cloud," because "the cloud" means too many different things to admit any one solution. To make any actionable statements, we must constrain ourselves to a particular domain.

We choose to focus on an important class of widely-used applications which includes email, personal financial management, social networks, and business applications such as word processors and spreadsheets. More precisely, we focus on deployments which meet the following criteria:

• applications that provide services to a large number of distinct end users, as opposed to bulk data processing or workflow management for a single entity;

• Applications whose data model consists mostly of sharable data units, where all data objects have ACLs consisting of one or more end users (or may be designated as public);

• And developers who write applications to run on a separate computing platform which Encompasses the physical infrastructure, job scheduling, user authentication, and the base Software environment rather than implementing the platform themselves.

**Data Protection and Usability Properties**

A primary challenge in designing a platform-layer solution useful to many applications is allowing rapid development and maintenance. Overly rigid security will be as detrimental to cloud services' value as inadequate security. Developers do not want their security problems solved by losing their users! To ensure a practical solution, we consider goals relating to data protection as well as ease of development and maintenance.

**Integrity:** The user's private (including shared) data is stored faithfully, and will not be corrupted.

**Privacy:** The user's private data will not be leaked to any unauthorized person.

**Access transparency**: It should be possible to obtain a log of accesses to data indicating who or what performed each access.

**Ease of verification:** It should be possible to offer some level of transparency to the users, such that

they can to some extent verify what platform or application code is running. Users may also wish to verify that their privacy policies have been strictly enforced by the cloud.

**Rich computation:** The platform allows most computations on sensitive user data, and can run those computations efficiently.

**Development and maintenance support**: Any developer faces a long list of challenges: bugs to find and fix, frequent software upgrades, continuous change of usage patterns, and users' demand for high performance. Any credible data protection approach must grapple with these issues, which are often overlooked in the literature on the topic.

2. Related Work A primary challenge in designing a platform layer solution useful to many applications is allowing rapid development and maintenance. Overly rigid security will be s detrimental to cloud service's value as inadequate security. Developers do not want their security problems solved by losing their users! To ensure a practical solution we consider goals relating to data protection as well as ease of development and maintenance.Integrity: The user's private data is stored faithfully, and will not be corrupted.

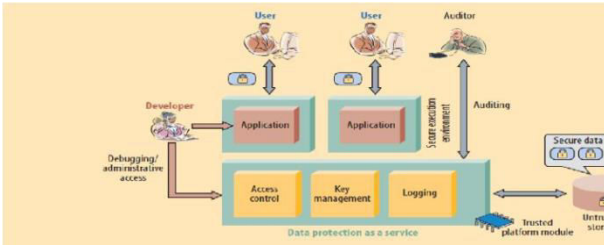
Privacy: The user's private data will not be leaked to any unauthorized person.Access transparency: It should be possible to obtain a log of accesses to data indicating who or what performed each access.Ease of verification: It should be possible to offer some level of transparency to the users, such that they can to some extent verify what platform or application code is running. Users may also wish to verify that their privacy policies have been strictly enforced by the cloud.Rich computation: The platform allows most computations on sensitive user data, and can run those computations efficiently.

Development and maintenance support: Any developer faces a long list of challenges: bugs to find and fix, frequent software upgrades, continuous change of usage patterns, and users' demand for high performance. Any credible data protection approach must grapple with these issues,which are often overlooked in the literature on the topic.Once these things are satisfied ten next steps are to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support. This support can be obtained from senior programmers, from book or from websites.Before building the system the above consideration are taken into account for developing the proposed system. 3. Usage of System modules 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:Agility improves with user's ability to re-provision technological infrastructure resources.Multi tenancy enables sharing of resources and costs across a large pool of users thus allowing for:Utilization and efficiency improvements for systems that are often only 10–20% utilized.Reliability is improved if multiple redundant sites are used, which makes well-designed cloud computing suitable for business continuity and disaster recovery.Performance is monitored and consistent and loosely coupled architectures are constructed using web services as the system interface.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.

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.4. 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" 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 hardware based full disk encryption systems that can truly encrypt the entire boot disk, including the MBR.4.1 Design space and a sample architecture Figure 4.1.1 illustrates example architecture for exploring the DPaaS design space. Here, each server contains a Trusted Platform Module (TPM) to provide secure and verifiable boot and dynamic root of trust. This example architecture demonstrates at a high level how it's potentially
possible to combine various technologies such as application confinement, encryption, logging, code attestation, and information flow checking to realize DPaaS.




MODULE DESCRIPTION:
1. Cloud Computing
2. Trusted Platform Module
3. Third Party Auditor
4. User Module

1. Cloud Computing

NIST DEFINITION: Cloud computing is a model forenabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks,servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential
characteristics, three service models, and four deployment models.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 computer 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 acrossa large pool of users thus allowing for:
3. Utilization and efficiency improvements for systems thatare often only 10–20% utilized.
4. Reliability is improved if multiple redundant sites are used,which makes well-designed cloud computing suitablefor business continuity and disaster recovery.
5. Performance is monitored and consistent and looselycoupled architectures are constructed using web services asthe 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, andthe lack of security for stored kernels. Security is often asgood as or better than other traditional systems, in partbecause providers are able to devote resources to solvingsecurity issues that many customers cannot afford. However,the complexity of security is greatly increased when data isdistributed over a wider area or greater number of devices andin multi-tenant systems that are being shared by unrelated users. In addition, user access to security audit logs may bedifficult or impossible. Private cloud installations are in partmotivated by users' desire to retain control over theinfrastructure 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)[4] 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"[5] (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)[6], 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

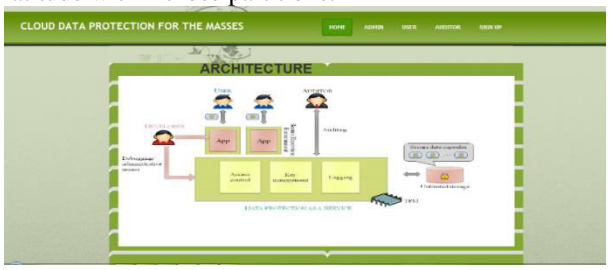
In this module, Auditor views the all user data and verifying data and also changed data. Auditor directly views all user data without key. Admin provided the permission to Auditor. After auditing data, store to the cloud.

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.

DATA PROTECTION AS A SERVICE (DPaaS)

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.





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 data enters will also aid in using collective security expertise more effectively. Addingprotections 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, class of applications, many other applications also needs solutions.

VII REFERENCES

[1] Dawn Song, Elaine Shi, Ian Fischer, UmeshShankar."Cloud Data Protection For The Masses" Computer,vol. 45(1),Jan 2012 page(s): 39-45.

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

[3] Hyubgun Lee, Kyounghwa Lee, YongtaeShin,Department of Computing, SoongsilUniversity."AES Implementation and Performance Evaluation on 8-bit Microcontrollers", International Journal of Computer Science and Information Security (pp. 070-074)

[4] P. Maniatis et al., "Do You Know Where Your Data Are? Secure Data Capsules for Deployable Data Protection," Proc.13thUsenixConf.HotTopics in OperatingSystems(HotOS11),Usenix,2011; www.usenix.org/events/hotos11/tech/final_files/ManiatisAkha we.pdf.

[5] Casey, Eoghan; Stellatos, Gerasimos J. "The impact of full disk encryption on digital forensics". Operating Systems Review 42 (3),2008 page(s); 93–98.

[6] Peter Norton and Scott Clark. "Peter Norton's New Inside the PC". Sams Publishing,2002, pp. 360–361.

[7] N.Janardhan ,Y.RajaSree , R.Himaja, Cloud Data Protection for the Masses publish in ijctt (volume4Issue4 –April 2013 )