

# Data Protection Service for Securing Data in Cloud

Shyam Babu Rachamalla & Swathi Amancha

<sup>1,2</sup>Assistant Professor, CSE, St. Martin's Engineering college

## Abstract:

*Offering powerful data protection to cloud users while authorizing 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. 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.*

## Keywords

*Authorizing, cloud applications, storage, cloud services,*

## 1. 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 [10] found that "...58% of the public and 86% of business leaders are excited about the possibilities of cloud computing. But, more than 90% of the public and business leaders are worried about security, availability, and privacy of their data as it resides 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. 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, It constrain ourselves to a particular domain.

It focuses 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

The principle challenge in designing a rostrum-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, it considers 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.

**Evolution and perpetuation support:** Any designer 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. Literature Survey

Literature survey is the most important step in software development process. Before developing the tool it is necessary to determine the time factor, economy in company strength. Once these things are satisfied, the next steps are to determine which operating system and language can be used for developing the tool. Once the developers start building the tool the developers need a lot of external support. This support can be obtained from senior programmers, from books or from websites. Before

building the system the above considerations are taken into account for developing the proposed system.

## 3. Existing System

Cloud computing ensures cheaper costs, quicker scaling, simple 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 % of the public and business leaders are worried about security, availability, and privacy of their data as it rests in the cloud.

### DISADVANTAGES OF EXISTING SYSTEM.

- ▶ There is no security for the data from the unauthorized users.
- ▶ If any unauthorized user changes the information, there is no chance of getting alert messages.

## 4. Proposed System

In this paper we propose 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 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.

### ADVANTAGES OF PROPOSED SYSTEM

- ▶ Data protection as a service (DPaaS), through this the data is secure and automatic keys will be generated and also provides the message alerts.

## METHODOLOGY

In this paper an efficient well known mechanism is designed by the following framework oriented fashion in

which there should be an accurate outcome in the systems performance based aspect respectively. Here the implementation of the present method is shown in the below figure in the form of the block diagram. This is the basic approach and here we explain in an elaborative fashion respectively. There is a huge challenge for the presently designed method where it is supposed to be accurate and analyze the entire previous methods followed by the implementation and drawback based strategy where it is finalized with theoretical concept The implementation of the present method is rather easier when compared to previous methods.



Figure 2:UserLoginPage

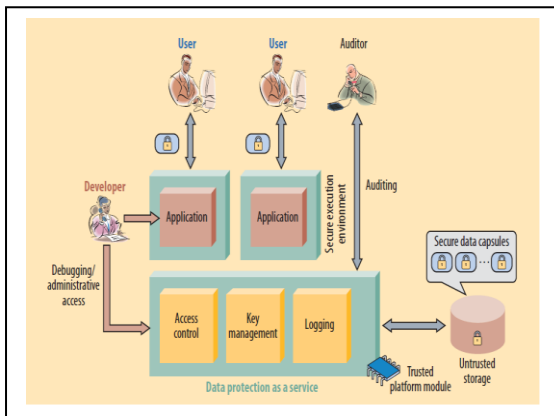
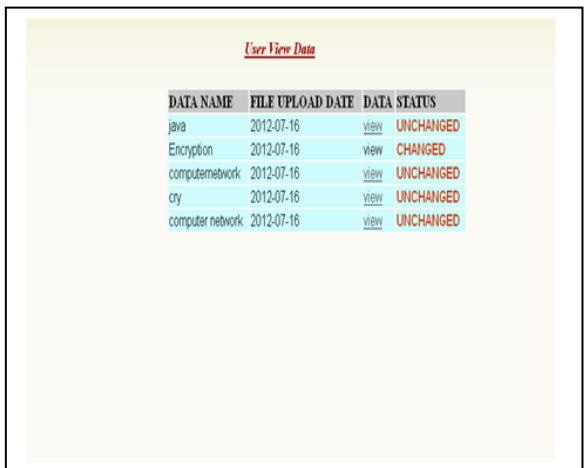


Figure 1:Architecture Diagram

## 5. Results



DATA NAME	FILE UPLOAD DATE	DATA STATUS
java	2012-07-16	view UNCHANGED
Encryption	2012-07-16	view CHANGED
computernetwork	2012-07-16	view UNCHANGED
cry	2012-07-16	view UNCHANGED
computer network	2012-07-16	view UNCHANGED

Figure 3:UserViewData



Figure 2: AdminHomepage



DATA NAME	FILE UPLOAD DATE	DATA STATUS
java	2012-07-16	view UNCHANGED
Encryption	2012-07-16	view CHANGED
Testing	2012-07-16	view CHANGED
Software	2012-07-16	view UNCHANGED
computernetwork	2012-07-16	view UNCHANGED
cry	2012-07-16	view UNCHANGED
computer network	2012-07-16	view CHANGED

Figure 4:Auditor checking details

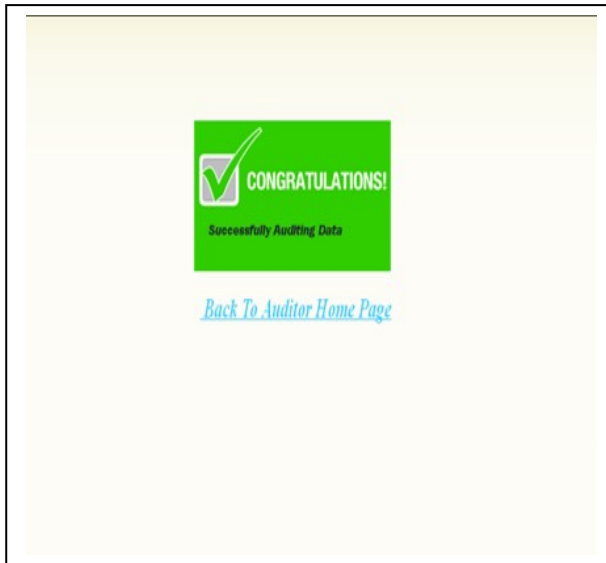


Figure 5: Auditing Success

## 6. Conclusion:

In this paper we have come up with a new technology for storing data in cloud. This technique provides flexibility in storing the data in cloud for the users

## 7. References:

- [1] <http://www.mydatacontrol.com>.
- [2] The need for speed. <http://www.technologyreview.com/files/54902/GoogleSpeedcharts.pdf>.
- [3] C. Dwork. The differential privacy frontier. In TCC, 2009.
- [4] C. Gentry. Fully Homomorphic Encryption Using Ideal Lattices. In STOC, pages 169–178, 2009.
- [5] A. Greenberg. IBM's Blindfolded Calculator. Forbes, June 2009. Appeared in the July 13, 2009 issue of Forbes magazine.
- [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. In PLDI, pages 193–205, 2008.

[8] M. S. Miller. Towards a Unified Approach to Access Control and Concurrency Control. PhD thesis, Johns Hopkins University, Baltimore, Maryland, USA, May 2006.

[9] A. Sabelfeld and A. C. Myers. Language-Based Information-Flow Security. IEEE Journal on Selected Areas in Communications, 21(1):5–19, 2003.

[10] L. Whitney. Microsoft Urges Laws to Boost Trust in the Cloud. [http://news.cnet.com/8301-1009\\_3-10437844-83.html](http://news.cnet.com/8301-1009_3-10437844-83.html).

## 8. Author's Biography



Mr. Shyam Babu Rachamalla, Post Graduated in Computer Science and Engineering (M. Tech) from JNTUH in 2013 and graduated in Computer Science and Engineering (B. Tech) from JNTUH in 2011. Having 3 years of experience as Asst. Professor. He is presently working as Asst. Professor in Computer Science and Engineering department in St. Martin's Engineering College, Hyderabad. Area of interest in Network Security, Cloud Computing, Big Data, Information Security



Ms Swathi Amancha, Post Graduated in Computer Science and Engineering (M. Tech) from JNTUH in 2012 and graduated in Computer Science and Engineering (B. Tech) from JNTUH in 2009. Having 8 years of experience as Asst Professor. She is presently working as Asst Professor in Computer Science and Engineering department in St. Martin's Engineering College, Hyderabad. Area of interest in Computer Networks, Network Security, Big Data, Information Security, Image processing, Cloud Computing, etc.