# Cloud Data Protection for the Masses

**Mr. Mahesh Nandkumar Chopade[1], Mr. SwikarNavnath Lad[2], Mr. InzamamSadik Waikar[3], Mr. SubhashDundappa Ambi[4] Prof. Ms. Anisa B. Shikalgar[5]**

[1]Department of Computer Science and Engineering, Student at Dr. J. J. Magdum College of Engineering, Jaysingpur, India.
*maheshchopade@hotmail.com*

[2]Department of Computer Science and Engineering, Student at Dr. J. J. Magdum College of Engineering, Jaysingpur, India.
*swikar25@yahoo.com*

[3]Department of Computer Science and Engineering, Student at Dr. J. J. Magdum College of Engineering, Jaysingpur, India.
*inzamamwaikar@hotmail.com*

[4]Department of Computer Science and Engineering, Student at Dr. J. J. Magdum College of Engineering, Jaysingpur, India.
*ambisubhash@yahoo.in*

[5]Department of Information Technology
Assistant Professor at Dr. J. J. Magdum College of Engineering, Jaysingpur, India.
annu.shikalgar@gmail.com

---

## Abstract:

*Offering 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. 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." 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, and key management.*

*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.*

***Key Words:*** **Data protection, DPAAS, DES, Key management, Security etc..**

## 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 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.

### 1.1 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.

### 1.2 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. 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."

This tension makes sense: users want to maintain control of their data, but they also want to benefit from the rich services that application developers can provide using that data. So far, the cloud offers little platform-level support or standardization for user data protection beyond data encryption at rest, most likely because doing so is nontrivial. Protecting user data while enabling rich computation requires both specialized expertise and resources that might not be readily available to most application developers.

## 3. PROPOSED SYSTEM

Building in data-protection solutions at the platform layer is an attractive option: the platform can achieve economies of scale by amortizing expertise costs and distributing sophisticated security solutions across different applications and their developers.

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, and key management.

## 4. 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 and company strength. 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.

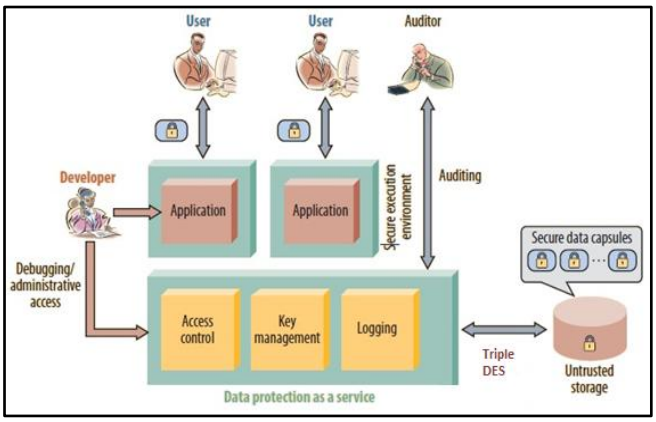


**Figure 4.1: System Architecture**

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.

The data-protection-as-a-service cloud platform architecture dramatically reduces the per-application development effort required to offer data protection while still allowing rapid development and maintenance.

## 5. METHODOLOGY

### 5.1 Proposed Work

Building in data-protection solutions at the platform layer is an attractive option: the platform can achieve economies of scale by amortizing expertise costs and distributing sophisticated security solutions across different applications and their developers. 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.

### 5.2 Design Approaches

***5.2.1. DFD Level 0:-***

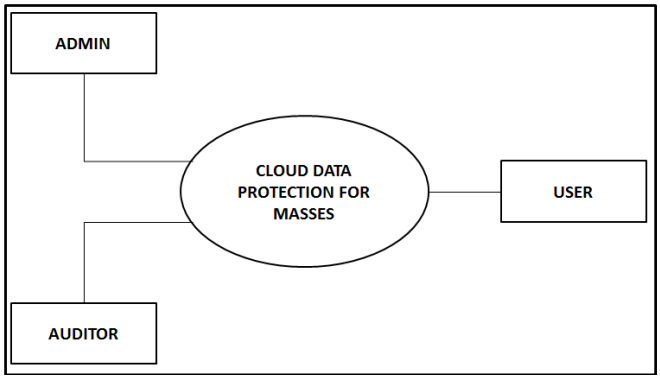


**Figure 5.1 DFD Level 0**

***5.2.2 DFD Level 1:-***

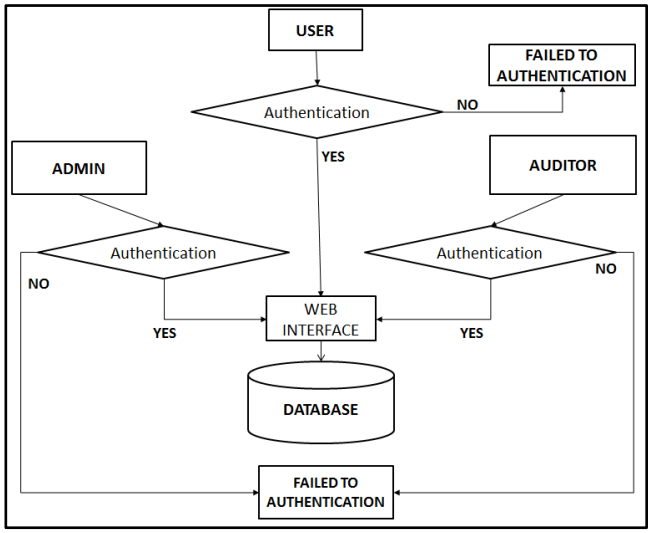


**Figure 5.2 DFD Level 1**

***5.2.3 Sequence Diagram:***

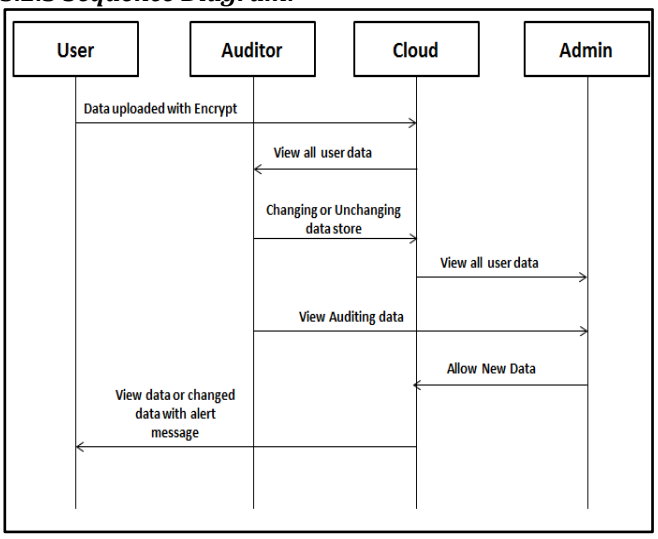


**Figure 5.3 Sequence Diagram**

***5.2.4. Use Case Diagram:***

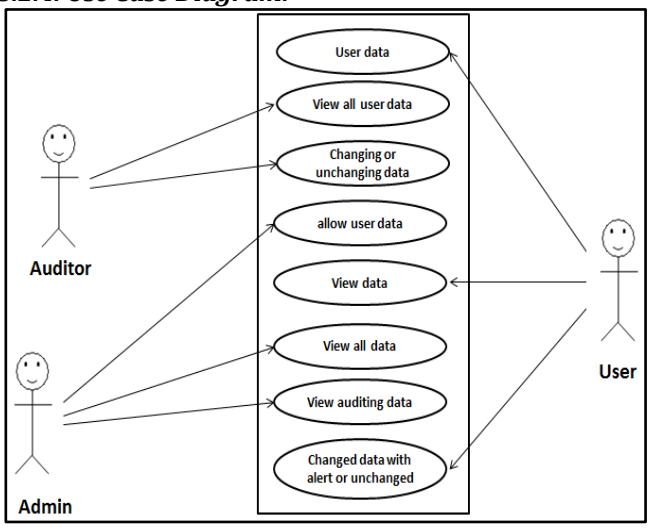


**Figure 5.4 Use Case Diagram**

***5.2.5 Class Diagram:***

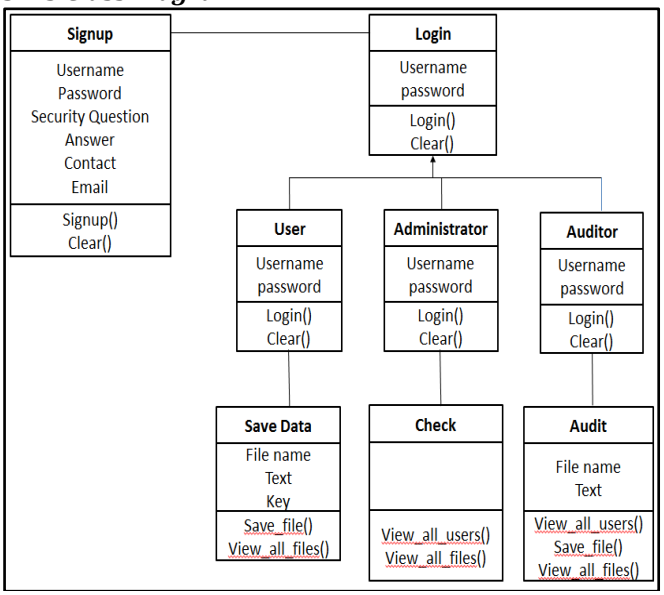


**Figure 5.5 Class Diagram**

## 6. CONCLUSION

In the first phase of our project we have developed two modules out of four modules. Our first module is User module with registration with his login session. In the second module we have implemented data storage with encryption and decryption.

In the Second Phase of our project we have tried to develop the cloud Server and making it secure and one more thing is we are tried to develop an auditor module. In its future scope this can be done as Android application.

## 7. REFERENCES

1. Dawn Song, Elaine Shi, and Ian Fischer, *University of California, Berkeley,* Umesh Shankar, *Google* Published by the IEEE Computer Society
2. http://www.mydatacontrol.com.
3. The need for speed. http://www.technologyreview.com/files/54902/GoogleSpeedcharts.pdf.
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. A. Greenberg. IBM's Blindfolded Calculator. Forbes, June 2009. Appeared in the July 13,2009 issue of Forbes magazine.
7. 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.
8. S. McCamant and M. D. Ernst. Quantitative information flow as network flow capacity.In PLDI, pages 193–205, 2008.
9. M. S. Miller. Towards a Unified Approach to Access Control and Concurrency Control.PhD thesis, Johns Hopkins University, Baltimore, Maryland, USA, May 2006.
10. A. Sabelfeld and A. C. Myers. Language-Based Information-Flow Security. IEEE Journalon Selected Areas in Communications, 21(1):5–19, 2003.
11. L. Whitney. Microsoft Urges Laws to Boost Trust in the Cloud. http://news.cnet.com/8301-10093-10437844-3.html.

**Authors Profile**

**Mr. Mahesh N. Chopade –** Completed Diploma in Computer Engineering from Shantiniketan Polytechnic, Sangli, MSBTE, Mumbai.Pursuing BE degree in Computer Science from Dr. J.J. Magdum college of Engineering, Jaysingpur, Shivaji University, Kolhapur. Research interests are in the field of Cloud Computing and Data Mining.

**Mr. Swikar N. Lad –** Completed Diploma in Computer Engineering from Government Polytechnic, Sangli, MSBTE, Mumbai.Pursuing BE degree in Computer Science from Dr. J.J. Magdum college of Engineering, Jaysingpur, Shivaji University, Kolhapur. Research interests are in the field of Cloud Computing and Data Mining.

**Mr. Inzamam S. Waikar –** Completed Diploma in Computer Engineering from Shantiniketan Polytechnic, Sangli, MSBTE, Mumbai.Pursuing BE degree in Computer Science from Dr. J.J. Magdum college of Engineering, Jaysingpur, Shivaji University, Kolhapur. Research interests are in the field of Cloud Computing and Data Mining.

**Mr. Subhash D. Ambi –** Completed Diploma in Computer Engineering from SantGajananMaharaj Rural Polytechnic, Mahagaon, MSBTE, Mumbai.Pursuing BE degree in Computer Science from Dr. J.J. Magdum college of Engineering, Jaysingpur, Shivaji University, Kolhapur. Research interests are in the field of Cloud Computing and Data Mining.

Prof. (Ms.) A. B. Shikalgar – received BE degree in Information Technology from PadmabhooshanVasantraodada Patil Institute of Technology, Budhgaon, Shivaji University, Kolhapur, and pursuing ME degree from same University, Currently working as an Assistant Professor in the Department of Computer Science & Engineering, Dr. J. J. Magdum College of Engineering, Jaysingpur, Shivaji University, Kolhapur. Research interests are in the field of Cloud Computing and Artificial Neural Network.