Cloud Data Protection for the Masses

N.Janardhan[1], Y.Raja Sree[2], R.Himaja[3],
[1,2,3]*{Department of Computer Science and Engineering, K L University, Guntur, Andhra Pradesh, India}*

***Abstract*— Cloud computing enables highly scalable services to be easily consumed over the Internet on an as-needed basis. 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. 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.**

Key Terms: Cloud computing, DPaaS, Security

I. INTRODUCTION

Even though the Cloud computing is emerging in these days and the number of providers and the clients are rapidly increasing there is much more concern about the security. 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.

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]

III. PROPOSED SYSTEM

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.

In this system for encrypting the data we use AES[3](Advanced Encryption Standard) algorithm . AES is based on a design principle known as a substitution-permutation network, and is fast in both software and hardware. Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits.

In figure 1: We have 4 modules. They are below

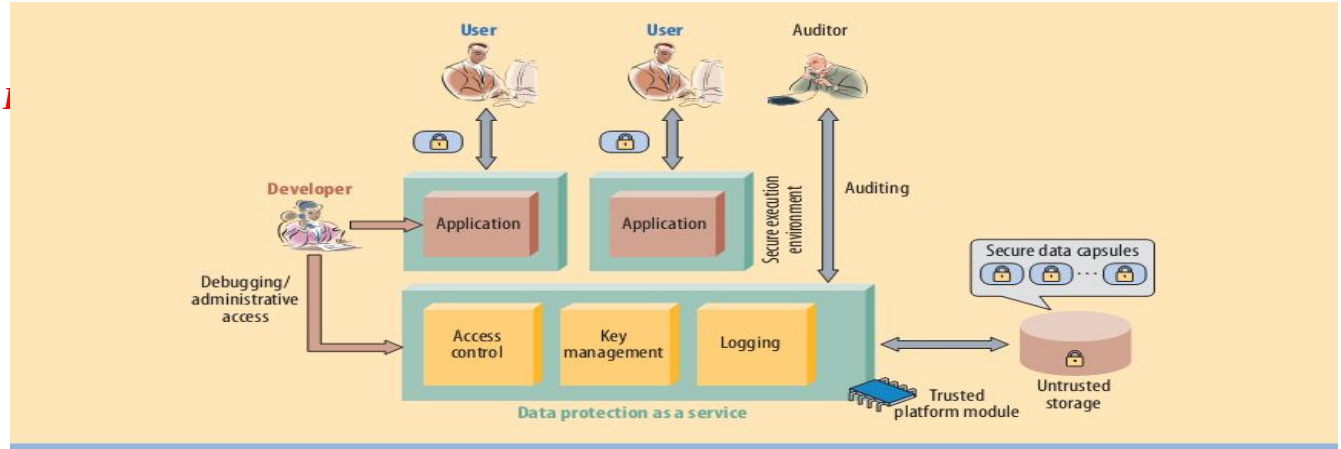


Figure 1. Sample architecture for data protection as a service illustrates how it's possible to integrate various technologies, such as application confinement, encryption, logging, code attestation, and information flow checking to realize DPaaS.

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 for enabling 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 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)[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

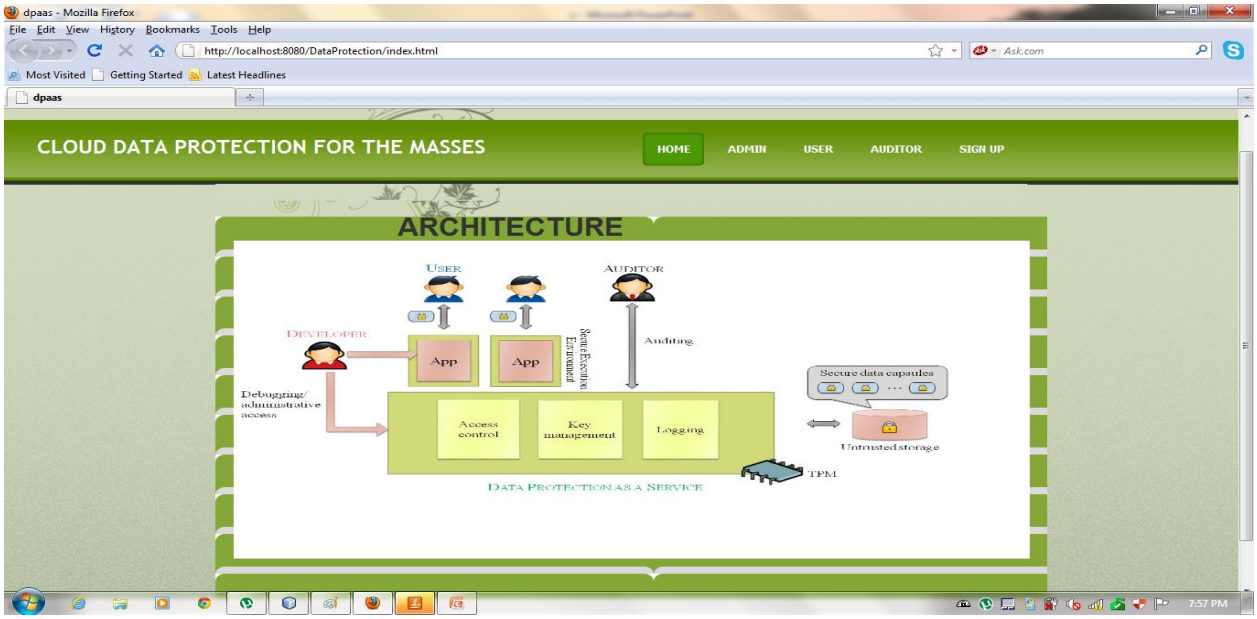
User store large amount of data to clouds and access data using secure key. Secure key provided admin after encrypting data. Encrypt the data using TPM. User store data after auditor, view and verifying data and also changed data. User again views data at that time admin provided the message to user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

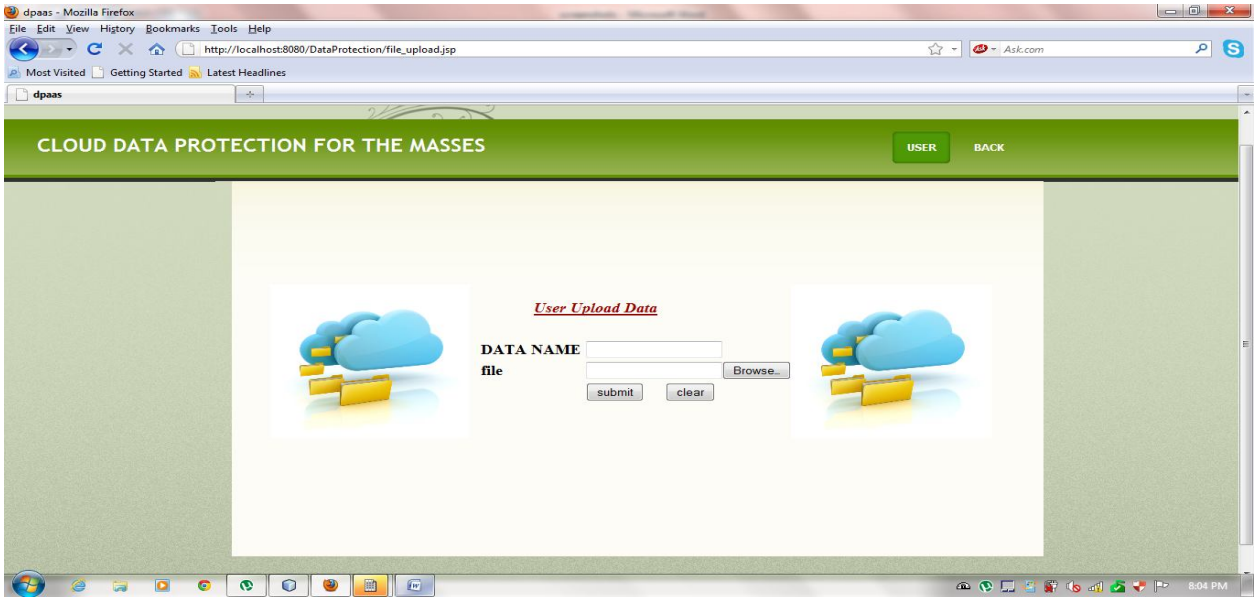
Much as an operating system provides isolation between processes but allows substantial freedom inside a process, cloud platforms could offer transparently verifiable partitions for applications that compute on data units, while still allowing broad computational latitude within those partitions.

IV OUTPUT ANALYSIS



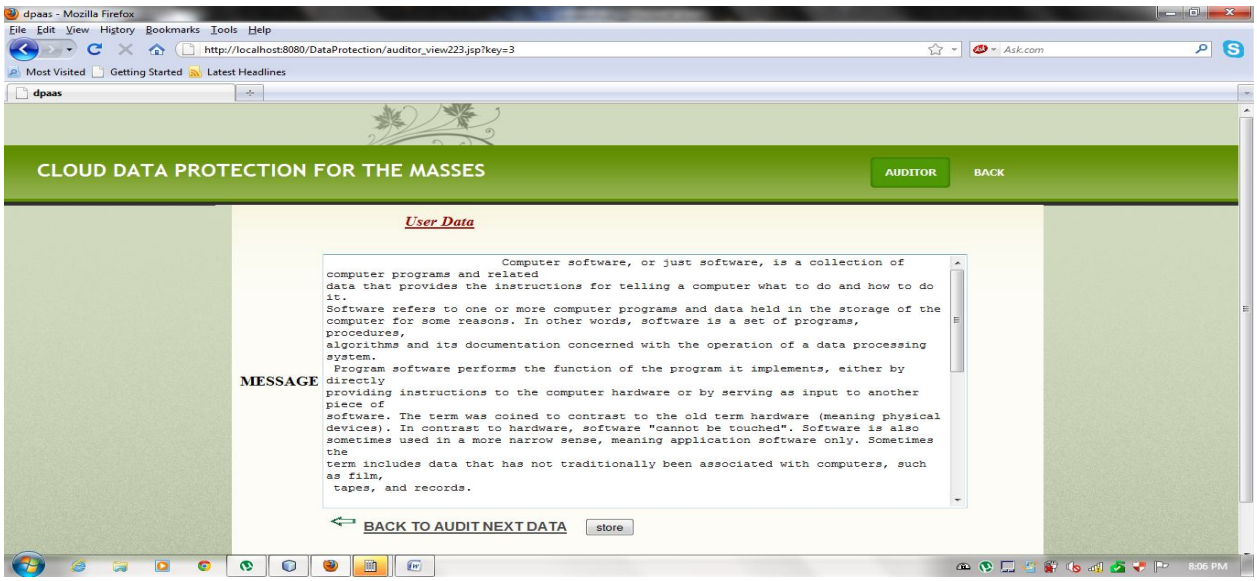
SCREEN SHOT 1: Home page

The home page of this system describes the architecture of the system. It provides sign up of the user, user profile, auditor profile and admin profile results.



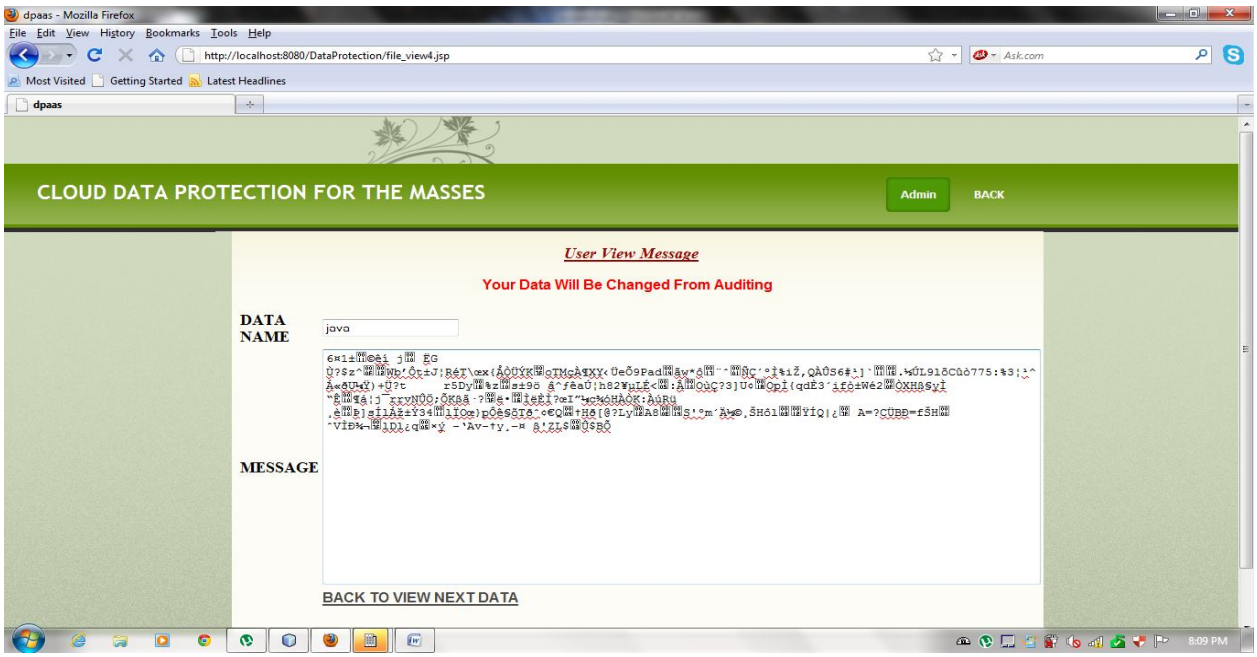
SCREEN SHOT 2: User profile

The user will give the name of the file in the field data name and upload a file in the field file. Then click submit then the data file is uploaded.



SCREEN SHOT 3:Auditor profile

The auditor will see the user uploaded data files and check whether the data file is virus free or not . After checking the data of the user then the auditor click store the the file is stored.



SCREEN SHOT 4:Admin profile

The admin checks the user data file but the data which is viewed by admin will be in the form of encryption which shows that any unauthorized user can not see the actual data of the user.

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. 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, class of applications, many other applications also needs solutions.

VI FUTURE ENHANCEMENT

In our system we are uploading the data files and protecting the files by encrypting the data. In future not only uploading the data file but also we can enhance the number of users by providing download option also.

VII REFERENCES

[1]Dawn Song, Elaine Shi, Ian Fischer, Umesh Shankar."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, Yongtae Shin, Department of Computing, Soongsil University."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.HotTopicsin OperatingSystems(HotOS11),Usenix,2011; www.usenix.org/events/hotos11/tech/final_files/ManiatisAkhawe.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.