ACHIEVING DATA PRIVACY AND SECURITY BY USING FHE IN CLOUD COMPUTING

[1] MR. NILESH B. PARGHI, [2] PROF. TRUPTI KODINARIYA

[1]M.E. [C.E.] Student, Department of Computer Engineering, Atmiya Institute of Technology and Science, Rajkot, Gujarat
[2] Professor, Department of Computer Engineering, Atmiya Institute of Technology And Science, Rajkot, Gujarat

pani.ourlife@gmail.com, tmkodinariya@aits.edu.in

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.*

Keywords—Cloud Computing, Security in cloud computing, FHE in cloud computing, FHE

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.

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."

3. PROBLEM FORMULATION

Cloud data protection is the main important issues in the field of security issue of cloud computing in the owner's perspective. There are some efficient approaches designed for Data privacy and security in cloud computing even in the presence of compromised or malicious applications. This dissertation work focus on DPaaS called "Data Protection as a Service" to protect the owners data in the privacy and security issue of cloud computing.

4. IMPLEMENTATION

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.

MODULE DESCRIPTION:

I. **Cloud Computing**
II. **Trusted Platform Module**
III. **Third Party Auditor**
IV. **User Module**

I. 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 users' 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.

II. **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**.**

III. 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.

IV. 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.

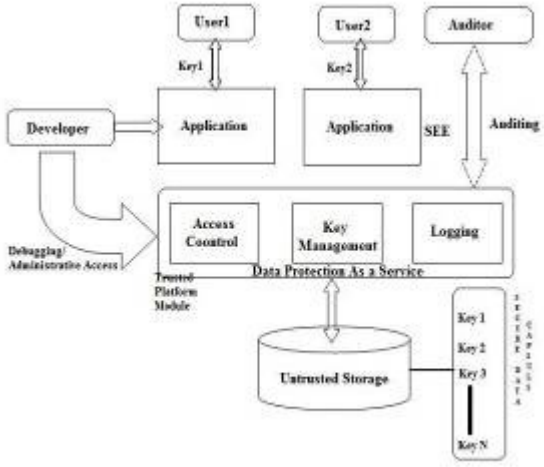

FIG.1 DATA PROTECTION AS A SERVICE

5. 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 datacenters 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.

REFRENCES

[1] http://iosrjournals.org/iosr-jce/papers/voll-issue3/S0132836.pdf

[2]T. Mather, S. Kumaraswamy, and S. Litif, Cloud Security and Privacy: enterprise perspectives on Risks and Compliance (Theory in Practice). O' Reilly, 2009

[3]C. Gentry, "Fully Homomorphic Encryption Using IdealLattices," Proc. 41st Ann. ACM Symp. Theory Computing(STOC 09), ACM, 2009, pp. 169-178.

[4] K.Valli Madhavi, R.Tamilkodi, K.Jaya Sudha, " Cloud Computing: Security Threats and Counter Measures" International Journal of Research in

Computer and Communication technology, IJRCCT, ISSN 2278-5841, Vol 1, Issue 4, September 2012.
[5] B.R. Kandukuri, R.P.V., and A. Rakshit. Cloud security issues. In IEEE International Conference on Services Computing (SCC). 2009.
[6] IEEE International Conference on Cloud Computing. 2009.
[7]http://www.researchgate.net/publication/45926884_A_Taxonomy_and_Survey_of_Energy-Efficient_Data_Centers_and_Cloud_Computing_Systems?ev=sim_pub
[8]http://en.wikipedia.org/wiki/Cloud_computing.