INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

PROTECTING LARGE CLOUD DATA AS A SERVICE

Krishna Kunsoth[1], Dr. G. Venkata Rami Reddy[2]

[1]PG Scholar, Department of Computer Science, School of Information Technology, JNTUH Hyderabad, Telangana State, India.

[2]Assistant Professor, Department of Computer Science, School of Information Technology, JNTUH Hyderabad, Telangana State, India.

krishna535.kittu@gmail.com, gvr_reddi@yahoo.co.in

Abstract

The cloud computing technology refers to providing of services over the internet. The cloud provider owns, the cloud servers facilitate clients to store data on cloud without bothering aspects like correctness and integrity of data. Cloud data storage has its own advantages over the data storage at local. The uploaded data on cloud can be accessed from any place without any additional burden. Even cloud computing provides easy maintainability, availability of service, less cost; an important challenge is how to ensure and build confidence that user data on cloud managed securely.

This paper gives possible solutions to data protection at platform layer (Dpass) and homographic encryption of data; it includes secrecy of user data, even to external hack attacks. By ensuring protection of cloud data decreases burden of per-application development.

Keywords: *Data protection as a service, cloud computing security issues, homomorphic encryption*

1. Introduction

The cloud computing brings newly founded and challenging security threats on user outsourced data. Although cloud infrastructures are reliable and powerful over personnel computing devices, the cloud computing still faces many threats of data integrity.

A Microsoft survey depicts "58 percent of public and 86 percent of business leaders excited over the possibilities of cloud computing. But 90 percent of industrial people and public are worried about secrecy, availability of services and security of user data on cloud. Cloud computing facilitates downloading and uploading data on cloud without compromising on security. Users can access data from anywhere, any time on demand. The charge of cloud services depends on usage.

Data protection issues:

The protection of data is a major issue in cloud computing. These include network security or data security. The cloud data protection refers to broad set of policies, application & the associated infrastructure of cloud computing and technology and controls deployed to protect data. Some data protection and privacy policies that need to be considered are as follows

1) Authentication: Limiting to only authorized users to access data in cloud.

2) Easy accessibility: Easy data accessing and retrieval. The authorized and unauthorized users indicated and identified easily with help of logs.

3) Rich computation: The platform provides many computations on user private data, and run those computations efficiently.

4) Application security and data integrity: the cloud applications secured with following the integrity, acceptance and testing procedures for outsourced application.

DATA PROTECTION AS A SERVICE

The cloud users depend on preliminary legal agreements and implied economic and reputational harms as a proxy for application trustworthiness. It provides fine grained access control policies on data units through application confinement and information flow checking. To overcome this we prefer robust technological solution as a base.

For achieving this two most important things that a cloud does are to:

- Availing the developers to write maintainable applications that protect user data in the cloud, thereby providing the same economies of scale for security and privacy for computation and storage; and
- Providing independent verification of platforms operation and the runtime state of applications on it, so users can gain confidence that their data is being handled properly.

ENCRYPTION PROCESS

Encryption process involves the transformation of data into unreadable format. In the process user data security , the developers assumes encryption of cloud data is of utmost secured ,but in real encryption is just an tool- albeit a powerful one- to help achieve user data protection properties. The full disk encryption and computing on encrypted data have recently gained attention, but these techniques shortfall on answering all security and maintenance challenges mentioned earlier.

HOMOMORPHIC ENCRYPTION

For all operations performed over the cipher texts generated by an encryption scheme is reflected over the corresponding plaintexts (possibly with the same or a different operation), such an encryption is called homomorphic encryption. To perform arbitrary computations over the encrypted data, the encryption scheme must support both addition and multiplication over the cipher texts unlimitedly, the notion of
Which is called Fully Homomorphic Encryption (FHE)[3].

If a limited number of additions and multiplications are supported the scheme is called Somewhat Homomorphic Encryption (SHE)[3]. A homomorphic encryption scheme consists of four algorithms KeyGen, Encrypt, Decrypt, and Evaluate.

We have several efficient homomorphic cryptosystems. The proper treatment of homomorphism leads to performing computations securely.

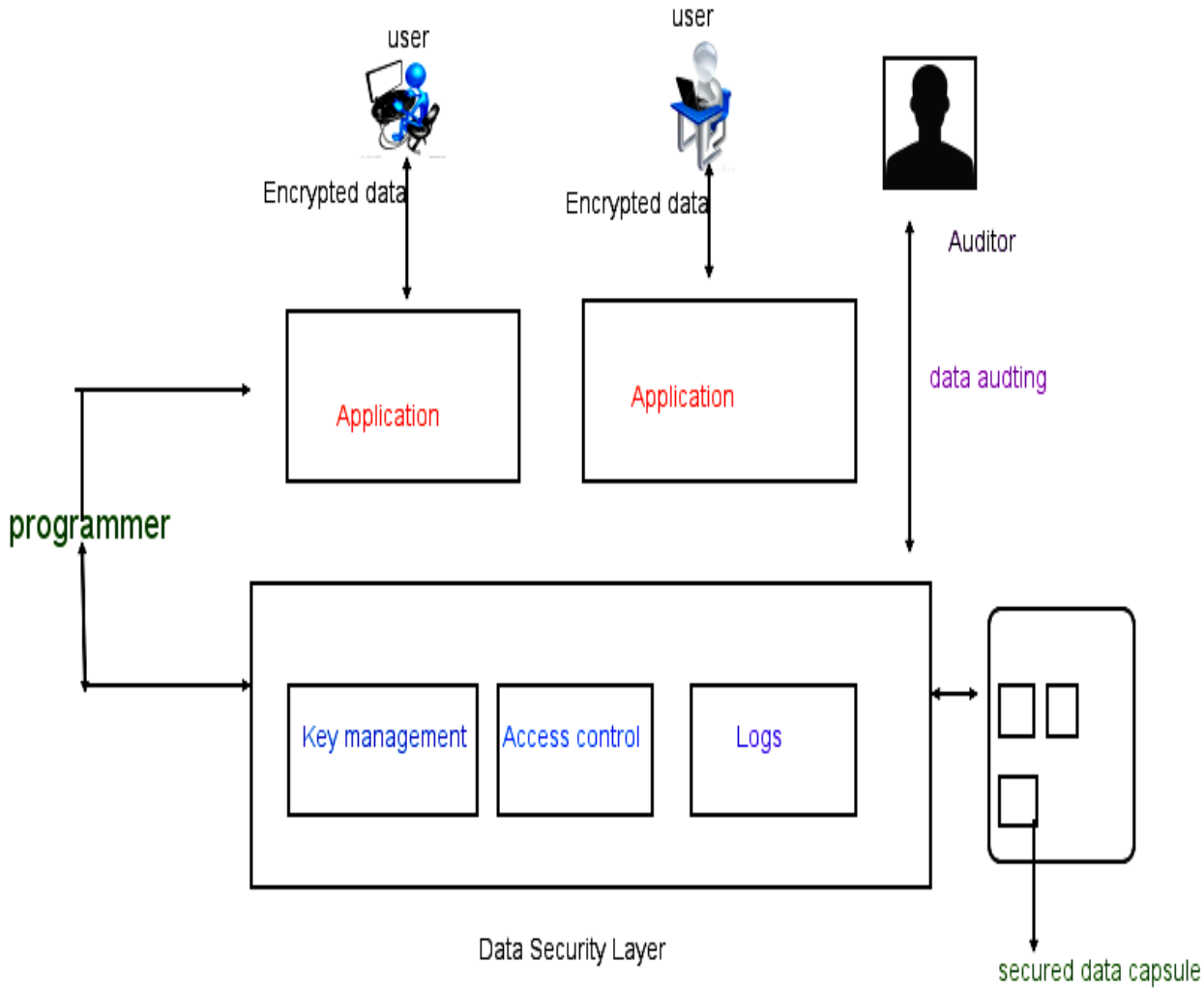

Figure: data security layer

The key management, encryption, logging, and access controls acts like barriers for secure shortage of data.
Implementation of data security layer offers evidence of privacy to the data owners, even in the presence of malicious applications.

The implantation modules includes: admin, auditor i.e. third party and user. The administrator deals with all signup and registration details of the user, coming to auditor deals with the user data and verifies the data. The encryption of user data done at the platform level.

Platform- level verifiable support:

The platform development involves support for confinement and auditing in a verifiable manner. It provides many advantages to developers do not all have to reinvent the wheel; the application code is independent from control; third party auditing and standards compliance are easy; and it allows for hardware support even in a virtualized environment.

Conclusion:

The user private data moves online, the need of data protection becomes ever urgent. By adding protection to a single cloud platform immediately benefits to hundreds of applications and, by extension, hundreds of users. This application can be enhanced by providing an online help line service to help the authorized users finding it difficult to work with the application or to help the new users who want to use the application. This can be further enhanced by allowing the users, not only to upload the text files but also allowing the users to upload music, videos and documents.

REFERENCES

[1] L.whitney. Microsoft urgues laws to boost trust in the cloud.http://news.cnet.com/8031-10093-10437844-83.html.
[2] C.Gentry. fully homomorphic encryption using ideal lattices.in STOC pages 169-178,2009.
[3] Greenberg. IBM's Blindfolded Calculator. Forbes, June 2009. Appeared in the July 13, 2009 issue of Forbes magazine.
[4] C. Dwork, "The Differential Privacy Frontier Extended Abstract," Proc. 6th Theory of Cryptograph Conf. (TCC 09), LNCS 5444, Springer, 2009, pp. 496-502.
[5] C. Dwork, "The Differential Privacy Frontier Extended Abstract," Proc. 6th Theory of Cryptography Conf. (TCC 09), LNCS 5444, Springer, 2009, pp. 496-502.
[6] Hamlen, K. W., Morrisett, G., & Schneider, F. B. (2006). Certified In-lined Reference Monitoring on. NET. In Proceedings of the ACM SIGPLAN Workshop on Programming Languages and Analysis for Security (PLAS)