Cloud Information Security from Intruders

K.Md.Waseem Iqbal, K Kishore,
[II-M.Tech]-CSE, Asst.Prof in CSE Dept.,DrKVSRIT Kurnool, Asst Prof in CSE Dept.

Abstract

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. 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 (www.mydatacontrol.com). 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.

1.INTRODUCTION

It's impossible to develop a single data-protection solution for the cloud because the term means too many different things. Any progress must first occur in a particular domain—accordingly, our work focuses on an important class of widely used applications that includes e-mail, personal financial management, social networks, and business tools such as word processors and spreadsheets. The following criteria define this class of applications:

• provide services to a large number of distinct end users, as opposed to bulk data processing or workflow management for a single entity;

• use a data model consisting mostly of sharable units, where all data objects have access control lists (ACLs) with one or more users; and

• Developers could run the applications on a separate computing platform that encompasses the physical infrastructure, job scheduling, user authentication, and the base software environment, rather than implementing the platform themselves. Overly rigid security is as detrimental to cloud service value as inadequate security. A primary challenge in designing a platform-layer solution useful to many applications is ensuring that it enables rapid development and maintenance. To ensure a practical solution, we considered the following goals relating to data protection as well as ease of development and maintenance:

• Privacy. Private data won't be leaked to any unauthorized entity.

• Access transparency. Logs will clearly indicate who or what accessed any data.

• Ease of verification. Users will be able to easily verify what platform or application code is running, as well as whether the cloud has strictly enforced their data's privacy policies.

• Rich computation. The platform will allow efficient, rich computations on sensitive user data.

• Development and maintenance support. Because they face a long list of challenges—bugs to find and fix, frequent software upgrades, continuous usage pattern changes, and user demand for high performance— developers will receive both development and maintenance support. minimizing system

2.IMPLEMENTATION

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods. 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. 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**.**

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. 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.

3.SYSTEM ARCHITECTURE

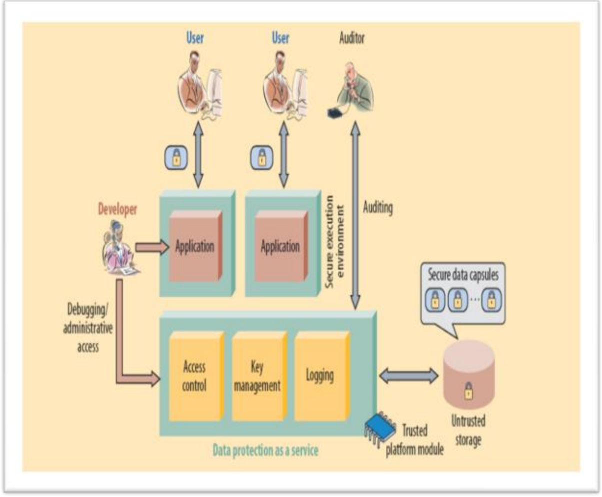

Fig 1. Sample architecture for data protection

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. DPaaS enforces fine-grained access control policies on data units through application confinement and information flow checking. It employs cryptographic protections at rest and offers robust logging and auditing to provide accountability. Crucially, DPaaS also directly addresses the issues of rapid development and maintenance. To truly support this vision, cloud platform providers would have to offer DPaaS in addition to their existing hosting environment, which could be especially beneficial for small companies or developers who don't have much in-house security expertise, helping them build user confidence much more quickly than they otherwise might.

4.DESIGN GOAL

A. INPUT DESIGN

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things:

(a) What data should be given as input?
(b) How the data should be arranged or coded?
(c) The dialog to guide the operating personnel in providing input.
(d) Methods for preparing input validations and steps to follow when error occur.

OBJECTIVES

1. Input Design is the process of converting a user-oriented description of the input into a computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system.

2. It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities.

3. When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so that the user will not be in maize of instant. Thus the objective of input design is to create an input layout that is easy to follow.

B. OUTPUT DESIGN

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

1. Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.

2.Select methods for presenting information.

3.Create document, report, or other formats that contain information produced by the system.

The output form of an information system should accomplish one or more of the following objectives.

- Convey information about past activities, current status or projections of the
- Future.
- Signal important events, opportunities, problems, or warnings.
- Trigger an action.
- Confirm an action.

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, classes of applications, many other applications also need solutions.

6.REFERENCES

1. C. Dwork, “The Differential Privacy Frontier Extendedm Abstract,” Proc. 6th Theory of Cryptography Conf. (TCC 09), LNCS 5444, Springer, 2009, pp. 496-502.
2. C. Gentry, “Fully Homomorphic Encryption Using Ideal Lattices,” Proc. 41st Ann. ACM Symp. Theory Computing (STOC 09), ACM, 2009, pp. 169-178.
3. E. Naone, “The Slow-Motion Internet,” Technology Rev.,Mar./Apr.2011;www.technologyreview.com/files/54902/GoogleSpeed_charts.pdf.
4. A. Greenberg, “IBM’s Blindfolded Calculator,” Forbes,13July2009;www.forbes.com/forbes/200/0713/breakthroughsprivacysupersecretencryption.html.
5. P. Maniatis et al., “Do You Know Where Your Data Are?Secure Data Capsules for Deployable Data Protection,”Proc. 13th Usenix Conf. Hot Topics in Operating Systems(HotOS 11), Usenix, 2011;www.usenix.org/events/hotos11/tech/final_files/ManiatisAkhawe.pdf.
6. S. McCamant and M.D. Ernst, “Quantitative Information Flow as Network Flow Capacity,” Proc. 2008 ACM SIGPLAN Conf. Programming Language Design and Implementation (PLDI 08), ACM, 2008, pp. 193-205.
7. M.S. Miller, “Robust Composition: Towards a Unified Approach to Access Control and Concurrency Control,” PhD dissertation, Dept. of Philosophy, Johns Hopkins Univ., 2006.
8. A. Sabelfeld and A.C. Myers, “Language-Based Information- Flow Security,” IEEE J. Selected Areas Comm., Jan. 2003, pp. 5-19.
9. L. Whitney, “Microsoft Urges Laws to Boost Trust in the Cloud,” CNET News, 20 Jan. 2010; http://news.cnet. com/8301-1009_3-10437844-83.html.

About The Authors

K.Md Waseem Iqbal received his B.Tech degree in Electronics and Commun cation and Engineering at . Pulliah College Of Engineer ng and techonology, kurnool affiliated to Jawaharlal Nehru Technological University, Anantapur, Andhra Pradesh, India, in 2011. Currently pursuing M.Tech in Computer Science and Engineering at Dr. KVSR Institute of Technology, Kurnool, affiliated to Jawaharlal Nehru Technological University, Anantapur, Andhra Pradesh, India.

K Kishore, received his MCA from Jawaharlal Nehru Technological University, Hyderabad, India in 2006. M.Tech in Computer Science from Jawaharlal Nehru Technological University, Anantapur, India.in 2012. He is an Asst.Professor at DR.K.V.S.R.I.T, Kurnool, Andhra Pradesh, India.