ISSN: 2320-1363

A Novel Data Protection for Masses in Cloud Computing

Sirisha.D*1, Mr.G.Rama Swamy*2

M.Tech (CSE) Student Department of CSE, Priyadarshini Institute of Technology & Science, Chintalapudi, Guntur(Dist), Ap, India.

Professor, Principle in Priyadarshini Institute of Technology & Science, Chintalapudi, Guntur(Dist), Ap, India

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. Although cloud computing promises numerous benefits, including lower costs, rapid scaling, easier maintenance, and ubiquitous availability, a key challenge is how to protect users data in the cloud. Today users effectively lose control of their data in the cloud and if the either the cloud infrastructure or applications are compromised users privacy will be at risk. This article we propose a new cloud computing paradigm, data protection as a service is a suite of security primitives offers evidence of privacy to data owners, even in the presence of potentially compromised or malicious application. Such as secure data using encryption, logging, and key management.

Keywords: Trusted Platform Module, Encryption, Dpaas

1. Introduction

It is the ICT subject of the last few years: cloud computing. Nowadays everyone is connected to the internet and working in "the cloud". Updating your profile on Face-book, using an online office application or uploading files to an online storage service, these are just small examples of the use of cloud services. Cloud computing is an import factor in modern businesses because it can cut costs drastically and gives small companies the possibility to enter large markets without high, risky start-up costs. The significance of cloud computing will only grow in the future, the International Data Corporation (IDC) forecasts that 85% of new commercial enterprise apps will be deployed on cloud platforms1 and one can state that cloud computing services are essential for the internet as we know it. The European Commission acknowledges the importance of cloud computing and has the objective to "unleash the potential of cloud computing in Europe" on its digital agenda. It has the ambition to have the European Union at the forefront of the development of cloud computing to have the benefits on the demand as well as on the supply side. This is not without a proper reason; predictions are

ISSN: 2320-1363

that a cloud-friendly approach will generate 250 billion Euros in GDP in 2020, which is 162 billion Euros more than the case without this approach. Extra cumulative impacts from 2015 to 2020 are estimated at 600 billion Euros. Moreover an enormous growth in jobs is predicted, the number of cloud-related jobs could rise above 3.8 million, which is in huge contrast with the predicted 1.3 million in the case of non-intervention.

2. Related Work

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 service's 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 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.

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.

3. Usage of System modules

Cloud Computing

Cloud computing is the provision of dynamically scalable and often virtualized

ISSN: 2320-1363

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 user's 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.

4. 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.

ISSN: 2320-1363

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" 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 hardware based full disk encryption systems that can truly encrypt the entire boot disk, including the MBR**.**

4.1 Design space and a sample architecture

Figure 4.1.1 illustrates example architecture for exploring the DPaaS design space. Here, each server contains a Trusted Platform Module (TPM) to provide secure and verifiable boot and dynamic root of trust. This example architecture demonstrates at a high level how it's potentially possible to combine various technologies such as application confinement, encryption, logging, code attestation, and information flow checking to realize DPaaS.

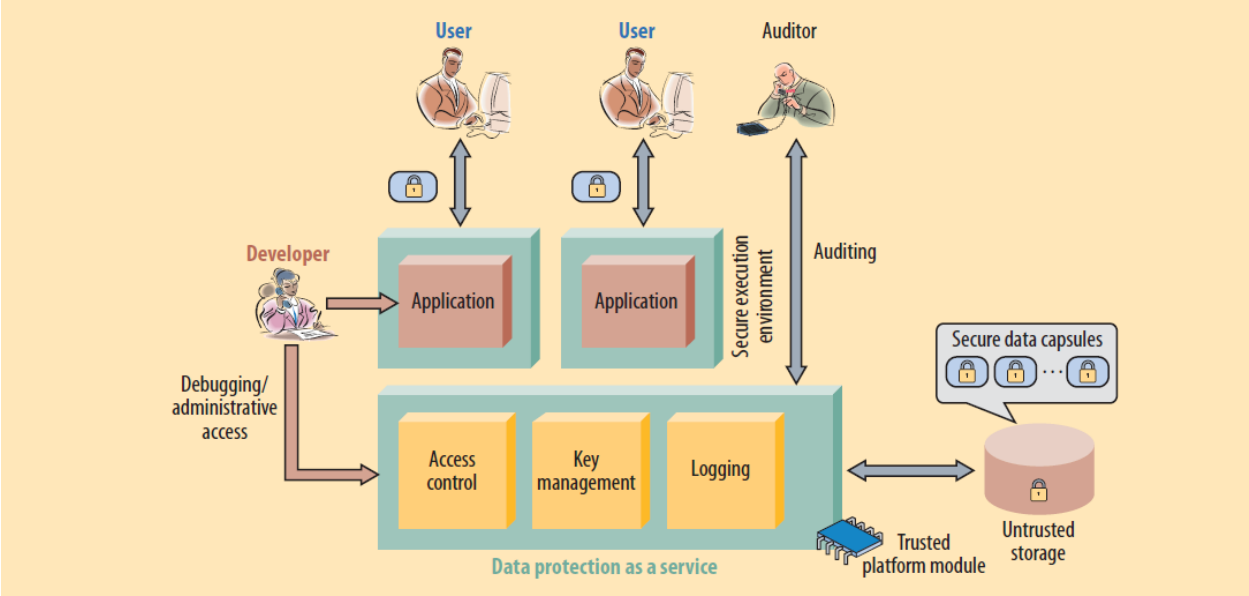

Figure 4.1.1 sample architecture for data protection as a service illustrates how it's possible to integrate various technologies, such as application confinement, encryption, logging, code attestation, and information flow checking to realize DPaaS.

Because our target applications have a basic requirement of sharable data units, DPaaS supports ACLs on SDCs. The key to enforcing those ACLs is to control the I/O channels available to the SEEs. To confine data, the platform decrypts the SDC's data

ISSN: 2320-1363

only in a SEE in compliance with the SDC's security policy. A SEE can funnel the output either directly to the user or to another SEE that provides a service; in either case, the platform mediates the channel. A buggy SEE only exposes a single SDC, an improvement over systems in which malicious input triggers a bug that allows access to all data. The platform also mediates ACL modifications, otherwise known as sharing or un-sharing. A simple policy that the platform can enforce without having to know too much about the application is transitive: only currently authorized users can modify the ACL. For example, the creator is the first owner of a data unit, and at any time, any user with the owner status can add or revoke other authorized users. The support of anonymous sharing, in which possession of, say a secret URL grants access to data, is also straightforward.

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.

References

1. C. Dwork, "The Differential Privacy Frontier Extended 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, 13 July 2009; www.forbes.com/forbes/2009/0713/ breakthroughs-privacy-super-secret-encryption.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.

ISSN: 2320-1363

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.