A Novel Computing Paradigm for Data Protection in Cloud Computing

Bhagya Lakshmi Nandipati[1], G. Sridevi[2]
[1]*M. Tech, Nimra College of Engineering & Technology, Vijayawada, A.P., India*
[2]*Assoc. Professor, Dept.of CSE, Nimra College of Engineering & Technology, Vijayawada, A.P., India*

Abstract: *Cloud computing is the term given to the use of several server computers via a digital network as if they were one computer. The 'Cloud' itself is a virtualization of various resources such as networks, servers, applications, data storage and services – which the end user has on-demand access to. Cloud computing services are divided into three types, according to the abstraction level of the capability provided and the service model of providers, namely: Infrastructure as a service(IaaS), Platform as a service(PaaS) and Software as a service(SaaS). This paper proposes a novel cloud computing paradigm, data protection as a service (DPaaS). DPaaS is a suite of security primitives offered by a cloud computing 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.*

Keywords: *Auditing, Cloud, Data protection, Service.*

I. Introduction

Now minute and average business organizations are realizing that simply exchange to the cloud can get access to excellent business claims and increase up their infrastructure assets in a very low cost, Internet on an as-needed basis [1]. This new and exciting paradigm has generated significant interest in both the marketplace and the academic world [2], resulting in a number of notable commercial and individual cloud computing services, e.g., form Amazon, Google, Microsoft, Yahoo, and Sales force [3]. Also, top database vendors, like Oracle, are adding cloud environment support to their databases. The providers are enjoying the superficial opportunity in the marketplace but they should ensure that they possess the right security features. The cloud computing provide facilities like fast development, lower cost on pay-for-use, quick flexibility, quick provisioning, everywhere network contact, hypervisor defense against network vulnerability, economical failure recovery and data storage solution, on-request security checks, synchronized detection of system altering and rapid re-construction of services. The cloud environment provides this compensation, until some of the risks are better understood.

The basic concept of the cloud computing, based on the services they offer, from application service provisioning, grid and service computing, to Software as a Service [4][5]. Despite of the specific architecture, the dominant concept of this cloud computing model is that customers' data, which can be of individuals, organizations or enterprises, is processed remotely in unknown machines about which the user not aware. The ease and efficiency of this approach, however, comes with both privacy and security risks [6]. Secrecy of data is the main hurdle in implementation of cloud services. A huge data centers are established in cloud computing environment, but the deployment of data and services are not trustworthy. These create different new security challenges. These challenges are vulnerabilities in accessibility, web and virtualization, such as SQL injection, cross site scripting, physical access issues, privacy and control issues happening from third parties having physical control of data, issues related to identity and credential , data loss and theft, issues related to data confirmation, changing and privacy, issues related to integrity and IP spoofing.

II. Cloud computing service models

There are three primary classes of cloud computing service models (Figure 1):

A. *Infrastructure as a Service (IaaS)*

A cloud based virtual server providing networking and mass storage services and other infrastructure services. The user does not manage or control the data centre but may have control over the data or operating systems placed into the infrastructure. For example, Amazon web service (AWS).

B. *Platform as a Service (PaaS)*

It is the service level where a computable platform upon which the user can host and develop applications and services by using programming language and API's37 is provided. The user can control the deployed applications and sometimes the application-hosting environment as well. However, the infrastructure (servers, OS, storage) is still in the control of the cloud provider. Examples include Windows Azure and Google App engine.

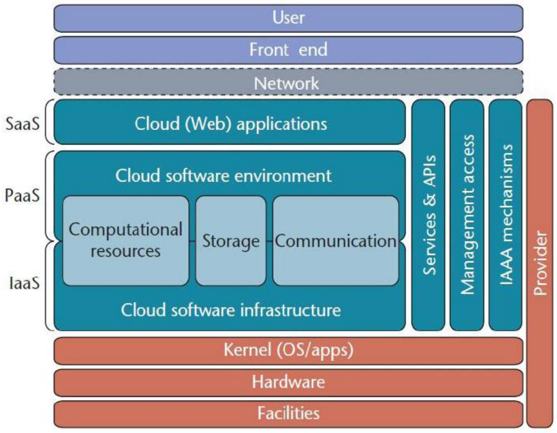

Figure 1: Cloud Computing Architecture

C. *Software as a Service (SaaS)*

In SaaS, applications are running on a cloud infrastructure or platform which is accessible via a thin client interface (browser) or program interface. The user only has the possibility to manage some user specific settings, because the provider does not accommodate cloud features; they only provide applications running 'in the cloud'. SaaS is an alternative to having the software running on local machines and good examples are online office applications (Google Docs), online CRM systems (SalesForce CRM), webmail (Google Mail) and Social Network Sites (Twitter, Facebook).

III. DATA PROTECTION AS A SERVICE

For organizations embarking on cloud computing environment, storage management is extremely important. To avoid loss, the cloud computing system must provide data protection and resiliency. If loss does occur, the computing environment must be able to recover the data quickly in order to restore access to the cloud services. This need is equally true whether the cloud computing environment is private, public or hybrid. It is possible to obtain data storage and protection services from the companies that specialize in storage, and many organizations that handle their own computing and applications choose this option for outsourcing storage. When outsourcing applications, however, an organization should never assume that the service provider includes storage management, data protection or disaster recovery among its services—not all of them do. It is therefore important to ensure from the beginning that the service provider delivers the necessary data storage and protection services, and to be familiar with the technologies and products used for storage management in the cloud environment. To ensure a practical solution, we considered the following goals relating to data protection in cloud.

- **Integrity:** The customer's stored data won't be corrupted.
- **Privacy:** Secret data won't be leaked to any unauthorized entity.
- **Access transparency:** Logs will clearly indicate who or what accessed any type of data.
- **Ease of verification:** Customers 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 cloud 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 customer demand for high performance— developers will receive both development and maintenance support.

IV. DAAS ARCHITECTURE

Figure 2 shows architecture to explore the design space of Data Protection as a Service [7].

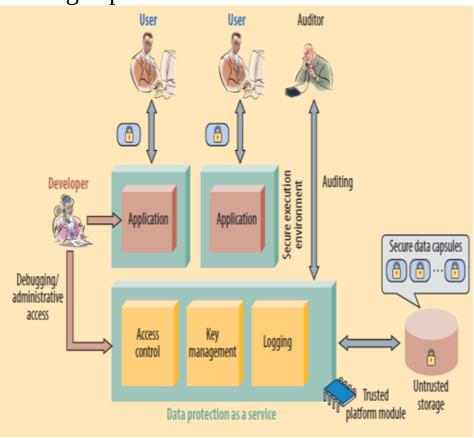

Figure 2: DPaaS Architecture

A. Lightweight Confinement

A Secure Data Capsule (SDC) is an enciphered data unit packaged with its security policy, e.g., Access Control List (ACL). To avoid unauthorized leakage of customer's data in the presence of potentially buggy or compromised applications, we confine the execution of various applications to mutually isolated environments, henceforth referred to as Secure Execution Environments (SEEs). There are different levels of inter-SEE isolation we could impose; stronger isolation in general exacts the greater performance cost due to context switching and data marshalling. At one end, a SEE could be a virtual machine with an output channel back to the requesting customer. In other words, the thread pool of the traditional server would be replaced with a pool of VMs or containers, whose data state is reset before being loaded with a new data unit.

B. Sharing and authorization

It is a basic requirement of our target applications that units of data that should be sharable; that is why SDCs are bound to a full ACL versus a particular customer. The key to enforcing those ACLs is that we can control the Input/Output channels available to SEEs. To confine data, we mandate that the data in an SDC is deciphered by the platform only for an SEE, and even then, only at an authorized user's request. The output may be funneled either directly to the customer or to another SEE which provides a service; in either case, the channel is mediated by the platform.

C. Auditor and Data Access Auditing

The auditor is one who audits the overall performance of the computing system. The auditor can track the transactions and logins of users with correct time and date. Here auditor is software component that is capable of tracking the transactions. Cloud storage offers movement of data into the cloud. It has great convenience to the customer because users can store their data in the cloud safely without the knowledge about the storage space. Since the platform mediates all access to the data, authenticates customers, and runs binaries, it knows what data is being accessed, by what user, and using which application. It can generate meaningful audit log files containing all these parameters and optionally incorporate additional information from the application layer. There are four basic types of actions we can log:

- Ordinary online data accesses occur in response to external requests from customers, and take place when a user is online and using an application.
- Access control modification by authorized customers. Knowing the provenance of these changes can be helpful for diagnosing or forensics sharing problems.
- Batch/offline access to handle requests while users are offline (e.g., e-mail delivery), to compute aggregates, or to reorganize data such as during schema changes.
- Administrative access for maintenance operations like debugging.

D. Key Management

The concept of key come from the branch of science called “cryptography”. There are basically two kinds of keys.

- Public key
- Private key

A public key known to everyone and a private or shared secret key known only to the recipient of the message. When Alice wants to send a secure message to Bob, he uses Jane's public key to encrypt the message. Bob then uses her private key to decrypt it. In our system we encrypt the file using a key and stored in the cloud. The user should enter the key in order to decrypt the file. So multiple protection schemes are used here for protecting the files in the cloud.

E. Authorization for Debugging, Maintenance, and Batch Access

While ordinary customer access is governed by the ACL on the data, administrative access needs its own separate policy. That in turn can be audited to hold developers as well as administrators accountable. Each specific invocation of the administrative policy, because it may entail user access to data for, e.g., debugging or account recovery, should be logged and made available for auditing. The same kind of mechanism would be used for batch access, with perhaps different logging granularity; and to prevent misuse, the code for the batch process can be restricted only to an approved set. That might mean requiring controlled or quantifiable information release, such as differential privacy [8] or quantitative information flow [9].

F. Verifiability of the Platform

The DPaaS paradigm provides logging and auditing at the platform level, sharing the benefits with all applications running on top. Offline, the auditor can verify that the paradigm implements each data protection feature as promised. At runtime, the platform provider can use trusted computing (TC) technologies to attest to the particular software that is running. Trusted computing uses the tamperproof TPM as well as the virtualization and isolation features of modern processors, such as Intel VT or AMDV.

V. CONCLUSION

Cloud computing environment enables highly scalable services to be easily consumed over the Internet on an as-needed basis. A major feature of the cloud computing services is that customers' data are usually processed remotely in unknown machines that users do not own or operate. Offering strong data protection to cloud customers while enabling rich applications is a challenging task. We explore a novel 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.

REFERENCES

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

[2] IEEE International Conference on Cloud Computing. 2009.

[3] P.T.Jaeger, J.Lin, and M. grimes, Cloud computing and information policy: Computing in a policy cloud? Journal of Information Technology and politics, 2009.

[4] Cloud Computing: Clash of the clouds. the economist., 2009.

[5] B.P.Rimal, E.Choi, and I.Lumb. A taxonomy and survey of Cloud Computing Systems. in Networked Computing and Advanced Information Management, International Conference. 2009.

[6] B.R. Kandukuri, R.P.V., and A. Rakshit. Cloud security issues. in IEEE International Conference on Services Computing (SCC). 2009.

[7] P. Maniatis, D. Akhawe, K. Fall, E. Shi, S. McCamant, and D. Song. Do You Know Where Your Data Are? Secure Data Capsules for Deployable Data Protection. In HotOS, 2011.

[8] C. Dwork, “The Differential Privacy Frontier Extended Abstract,” Proc. 6th Theory of Cryptography Conf. (TCC 09), LNCS 5444, Springer, 2009, pp. 496-502.

[9] S. McCamant and M. D. Ernst. Quantitative information flow as network flow capacity. In PLDI, pages 193–205, 2008.