TECHMIND RESEARCH
ISSN: 2291-2118
International Journal of Research in Business and Technology
Volume 4 No.2 April 2014

Cloud Computing Data Security for the Masses

Omar Ali Khudhair[1], Dr. Wilson Jeberson[2]
[1]M.Tech student, Department of CS&E, SHIATS-Allahabad, India
omar.ali.khudhair@gmail.com
[2]Associate Professor, Department of Computer Science & IT, SHIATS-Allahabad, India
jeberson@rediffmail.com

Abstract-*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. Cloud computing provides many benefits in terms of low cost and accessibility of data. Ensuring the security of cloud computing is a major factor in the cloud computing environment, as users often store sensitive information with cloud storage providers but these providers may be un-trusted. This paper surveys recent research related to single and multi-cloud security and addresses possible solutions. It is found that the research into the use of multi-cloud providers to maintain security has received less attention from the research community than has the use of single clouds. The data-protection-as-a-service cloud platform architecture dramatically reduces the per-application development effortrequired to offer data protection while still allowing rapid development and maintenance.*

Keywords-*Cloud computing; cloud storage; data integrity; data intrusion; service availability*

1. INTRODUCTION

In the recent trends the 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. The use of cloud computing has increased rapidly in many organizations. Subashini and Kavitha argue that small and medium companies use cloud computing services for various reasons, including because these services provide fast access to their applications and reduce their infrastructure costs. Cloud providers should address privacy and security issues as a matter of high and urgent priority. Dealing with "single cloud" providers is becoming less popular with customers due to potential problems such as service availability failure and the possibility that there are malicious insiders in the single cloud. In recent years, there has been a move towards "multi-clouds", "inter-cloud" or "cloud-of-clouds".

This paper focuses on the issues related to the data security aspect of cloud computing. As data and information will be shared with a third party, cloud computing users want to avoid an un-trusted cloud provider. Protecting private and important information, such as credit card details or a patient's medical records from attackers or malicious insiders is of critical importance. In addition, the potential for migration from a single cloud to a multi-cloud environment is examined and research related to security issues in single and multi-clouds in cloud computing is surveyed.

2. SYSTEM DESIGN MODEL

2.1. Cloud Computing Components

The cloud computing model consists of five characteristics, three delivery models, and four deployment models. The five key characteristics of cloud computing are: location-independent resource pooling, on-demand self-service, rapid elasticity, broad network access, and measured service. These five characteristics represent the first layer in the cloud environment architecture (see Figure1).

The three key cloud delivery models are infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). In IaaS, the user can benefit from networking infrastructure facilities, data storage and computing services. In other words, it is the

delivery of computer infrastructure as a service. An example of IaaS is the Amazon web service.

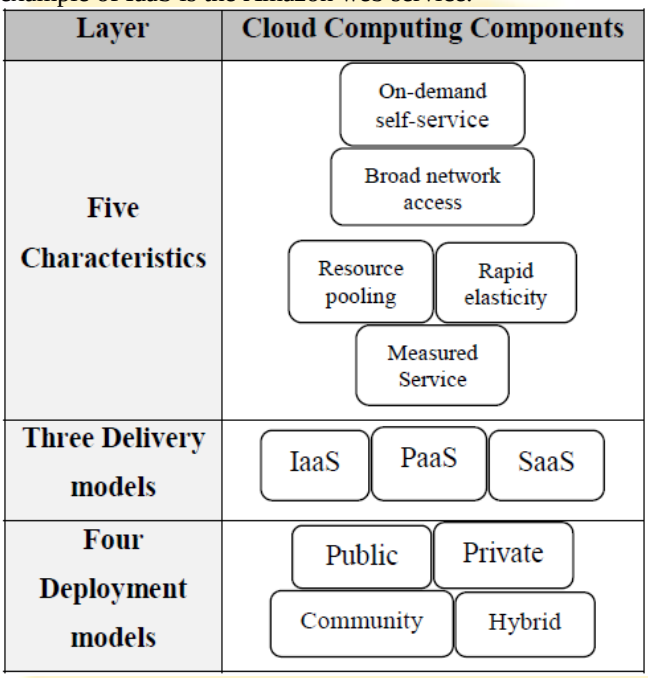

Figure 1: Cloud Environment Architecture
Source: Mohammed A. AlZain.ets (2012)

In PaaS, the user runs custom applications using the service provider's resources. It is the delivery of a computing platform and solution as a service. An example of PaaS is Google Apps. Running software on the provider's infrastructure and providing licensed applications to users to use services is known as SaaS. An example of SaaS is the Salesforce.com CRM application. This model represents the second layer in the cloud environment architecture.

2.2. Security Risks in Cloud Computing

Cloud deployment models include public, private, community, and hybrid clouds. A cloud environment that is accessible for multi-tenants and is available to the public is called a public cloud. A private cloud is available for a particular group, while a community cloud is modified for a specific group of customers. Hybrid cloud infrastructure is a composition of two or more clouds (private, community, or public cloud). This model represents the third layer in the cloud environment architecture. Kamara and Lauter present two types of cloud infrastructure only, namely private and public clouds. The infrastructure that is owned and managed by users is in the private cloud. Data that is accessed and controlled by trusted users is in a safe and secure private cloud, whereas the infrastructure that is managed and controlled by the cloud service provider is in a public cloud. In particular, this data is out of the user's control, and is managed and shared with unsafe and un-trusted servers.

In different cloud service models, the security responsibility between users and providers is different. According to Amazon, their EC2 addresses security control in relation to physical, environmental, and virtualization security, whereas, the users remain responsible for addressing security control of the IT system including the operating systems, applications and data. The way the responsibility for privacy and security in a cloud computing environment is shared between consumers and cloud service providers differs between delivery models. In SaaS, cloud providers are more responsible for the security and privacy of application services than the users. This responsibility is more relevant to the public than the private cloud environment because the clients need more strict security requirements in the public cloud. In PaaS, users are responsible for taking care of the applications that they build and run on the platform, while cloud providers are responsible for protecting one user's applications from others. In IaaS, users are responsible for protecting operating systems and applications, whereas cloud providers must provide protection for the users' data.

2.3. Security and Privacy Challenges

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:

- Integrity: the user's stored data won't be corrupted.
- 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.

2.4. Data Protection as a Service

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.

2.5. Achieving Data Protection Goals

We assume in the analysis that the platform behaves correctly with respect to code loading, authorization, and key management, and that the TPM facilitates a runtime attestation to this effect. DPaas uses a combination of encryption at rest, application confinement, information flow checking, and auditing to ensure the security and privacy of users' data. Application confinement isolates faults and compromises within each SEE, while information flow checking ensures that any information flowing among SEEs, data capsules, and users satisfies access-control policies. Controlling and auditing administrative accesses to data provides accountability. DPaaS can guarantee the integrity of the data at rest via cryptographic authentication of the data in storage and by auditing the application code at runtime. Access controls, authorization, and auditing capability are common challenges for application developers. Incorporating these features within the platform is a significant improvement in terms of ease of use, and it doesn't constrain the types of computation that can be performed within a SEE. The platform logs common maintenance and batch processing tasks to provide accountability. These tasks too often require one-off work in the development process and can benefit from standardization.

3. SIMULATION DESCRIPTION

One of the most important issues related to cloud security risks is data integrity. The data stored in the cloud may suffer from damage during transition operations from or to the cloud storage provider.

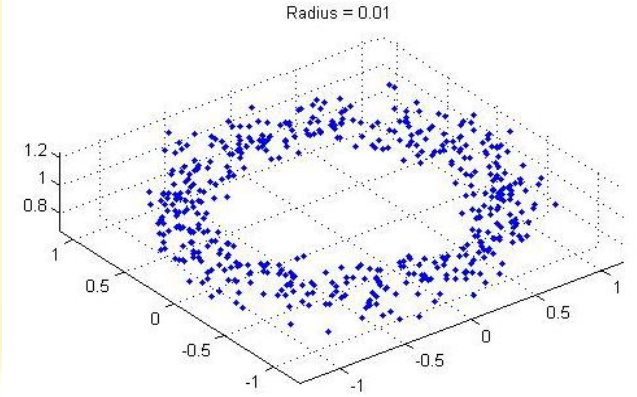

Figure 2: Cloud Node Formation

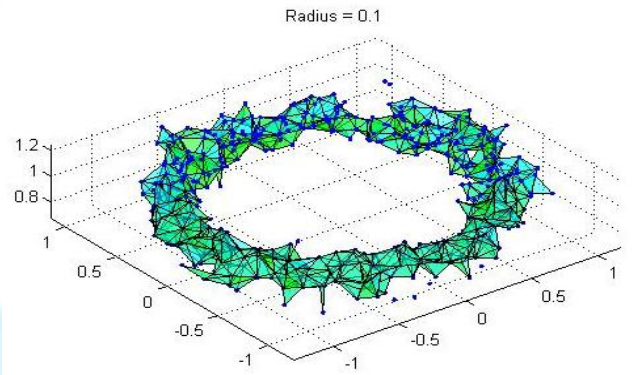

Figure 3: Cloud Node Formation of Network

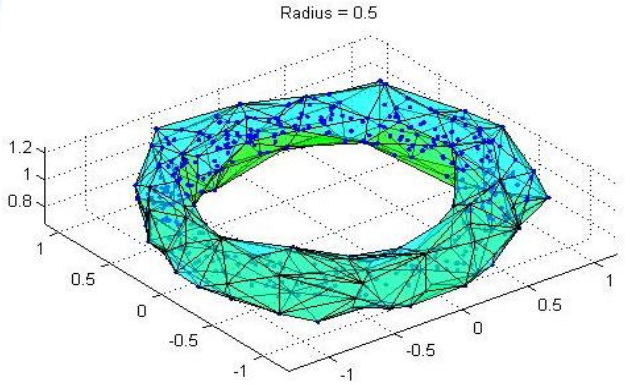

Figure 4: Cloud Node Formation Network with Cubic

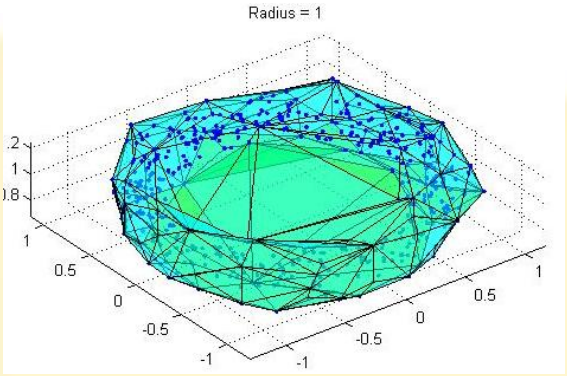

Figure 5: Cloud Node Formation Network with Data Storage

4. CONCLUSION

It is clear that although the use of cloud computing has rapidly increased; cloud computing security is still considered the major issue in the cloud computing environment. The good news is that the same forces concentrating data in enormous datacenters will also aid in using collective security expertise more effectively. We have focused here on a particular, albeit popular and privacy-sensitive, classes of applications, many other applications also need solutions. In addition, the loss of service availability has caused many problems for a large number of customers recently. The purpose of this work is to survey the recent research on single clouds and multi-clouds to address the security risks and solutions. We support the migration to multi-clouds due to its ability to decrease security risks that affect the cloud computing user.

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] S. Subashini and V. Kavitha, *"A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications,* 34(1), 2011, pp 1-11.

[3] **H. Takabi, J.B.D. Joshi and G.-J. Ahn,** *"Security and Privacy Challenges in Cloud Computing Environments", IEEE Security & Privacy*, 8(6), 2010, pp. 24-31.

[4] **(NIST),** *http://www.nist.gov/itl/cloud/.*

[5] **S. Kamara and K. Lauter,** *"Cryptographic cloud storage", FC'10: Proc. 14thIntl.Conf. on Financial cryptography and data security,* 2010, pp. 136-149.

[6] **S. Subashini and V. Kavitha,** *"A survey on security issues in service delivery models of cloud Computing", Journal of Network and Computer Applications,* 34(1), 2011, pp 1-11.

[7] **Brunette, G. and R. Mogull (ed), 2009,** *Security Guidance for Critical Areas of Focus in Cloud Computing. Cloud Security Alliance,* December 2009.

Author's Biography

Omar Ali Khudhair (Al-hadidi) is pursiung M.Tech, Department of CS & E, in Sam Higginbottom Institute of Agriculture, Technology and Sciences, Allahabad, India. He was a member of the Iraqi Engineers Union / Nineveh and Chamber of Commerce of Mosul.

Dr. Wilson Jeberson is Associate Professor, Department of Computer Science & IT, in Sam Higginbottom Institute of Agriculture, Technology and Sciences, Allahabad, India.