OPEN ACCESS

International
Journal
Of Modern Engineering Research (IJMER)

Security of Data in Cloud Environment Using DPaaS

Prabhleen Singh[1], Ketki Arora[2]
[1]*Student Lovely Professional University India*
[2]*Department of Computer Science, Lovely Professional University India*

ABSTRACT: *The rapid development of cloud computing is giving way to more cloud services, due to which security of services of cloud especially data confidentiality protection, becomes more critical. Cloud computing is an emerging computing style which provides dynamic services, scalable and pay-per-use. Although cloud computing provides numerous advantages, a key challenge is how to ensure and build confidence that the cloud can handle user data securely. This paper highlights some major security issues that exist in current cloud computing environments. The status of the development of cloud computing security, the data privacy analysis, security audit, information check and another challenges that the cloud computing security faces have been explored. The recent researches on data protection regarding security and privacy issues in cloud computing have partially addressed some issues. The best option is to build data-protection solutions at the platform layer. The growing appeal of data protection as a service is that it enables to access just the resources you need at minimal upfront expense while providing the benefits of enterprise-class data protection capabilities. The paper proposes a solution to make existing developed applications for simple cloud Systems compatible with DPaaS. The various security challenges have been highlighted and the various necessary metrics required for designing DPaaS have been investigated.*

Keywords: *Cloud Computing, data security, privacy protection.*

I. INTRODUCTION

Over the past few years, cloud computing has become significant research topic of the scientific and industrial communities. The Cloud computing has emerged as a new computing model which aims to provide reliable, customized, scalable, pay-per-use and dynamic computing environments for end-users. Numerous organizations have started realizing the benefits by putting their applications and data into the cloud. Cloud computing is not new to Information Technology. Unlike other computing models, cloud computing possess some additional features that make it distinguishable such as service-driven, resource pooling, and data hosting in outsourcing storage. Pooling resource makes the hardware performance be used more efficient and provides economic benefits for users to reduce the capital cost and additional expenditure. The biggest benefit is that developers no longer require the large capital outlays in hardware to deploy the innovative ideas for new Internet services service and hence cutting the human expense to operate it.

Defining cloud computing actually becomes a difficult task with many definitions. Since recent past, several efforts have been made to provide the exact definition of “cloud computing”. The definition provided by U.S. NIST (National Institute of Standards and Technology) appears to include key common elements widely used in the Cloud Computing community as it says that: "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction [3].

The cloud computing offers numerous potential advantages comparatively traditional IT model. Yet the major barrier for the adoption of cloud computing are the security concerns. Security control measures in cloud are similar to ones in traditional IT environment. Traditional security issues are still present in cloud computing environments. But as enterprise boundaries have been extended to the cloud, traditional security mechanisms are no longer able to go with applications and data in cloud. Due to the openness and multi-tenant characteristic of the cloud, cloud computing is bringing tremendous impact on information security field [4].

II. CHARACTERISTICS OF CLOUD COMPUTING

Cloud computing provides several compelling characteristics which differentiate it from other computing paradigms. Some of them are:

- **Broad network access range:** System capacities are available to customers through a network and can be accessed from different devices such as desktop computers, mobile phones, smartphones and tablet devices.

- **Pay- per use model:** Cloud computing uses a pay-as you-go-pricing model. Resources in a cloud environment can be allocated and de-allocated on demand. So a service provider does not need to invest in the infrastructure to start gaining benefit from cloud computing. It simply rents resources from the cloud according to its own needs and pay for the usage.
- **Service provisioning on demand:** Computer services such as email, applications, network or server service can be provided without requiring human interaction with each service provider. Cloud service providers providing on demand self-service include Amazon Web Services, Microsoft, Google, IBM and Salesforce.com.
- **Sharing of resources:** The computing resources are pooled together to serve multiple consumers using multiple-tenant model, with different physical and virtual resources dynamically assigned according to consumer demand. The resources include storage, processing, memory, network bandwidth, virtual machines and email services.
- **Rapid elasticity:** The cloud is flexible and scalable to suit your immediate business needs. You can quickly and easily add or remove users, software features, and other resources.

III. CLOUD SERVICES

Cloud service delivery is divided among three service models. The three fundamental classifications are often referred to as the “SPI Model” where ‘SPI’ refers to software, platform, and infrastructure as defined below:

1. Software as a Service (SaaS)
2. Platform as a Service (PaaS)
3. Infrastructure as a Service (IaaS)

1.3.1 Software as a Service (SaaS)

Unlike the traditional model of one application per desktop, Software as a Service (SaaS) makes use of a cloud computing infrastructure to deliver one application to many users, regardless of their location. It allows activities to be managed from central locations in a one-to-many model, including architecture, pricing, partnering, and management characteristics. Some examples are Google Apps (mail, docs, and etc.) and Salesforce.com

1.3.2 Platform as a Service (PaaS)

Platform as a Service (PaaS) is a software distribution model in which hosted software applications are made available to customers over the Internet. Service provider provides a specific cloud environment, some software tools and programming language to consumer for developing, testing, and hosting their applications. PaaS provides users with a high level of abstraction that allows them to focus on developing their applications without concerning about the underlying infrastructure. An example of PaaS is Google App engine.

1.3.3 Infrastructure as a Service (IaaS)

IaaS allows consumer to rent hardware include processors, storages, network, and other fundamental computing resources. In this service model, consumers do not control or manage the underlying cloud infrastructure directly. They control the computing resources through operating systems [6]. This service provides the required infrastructure as a service. The key advantage here is that customers need to pay only for the time duration they use the service. As a result customers can achieve a much faster service delivery with less cost.

IV. SECURITY OF DATA IN CLOUD

Security within cloud computing is a critical issue because the devices that provide services do not belong to the users themselves in actual. Although 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. This is a great concern in cases when users have valuable and personal information stored in a cloud computing service. It is an increasingly important problem to protect the confidentiality of information manipulated by computing systems. There is little assurance that current computing systems protect data confidentiality and integrity. New security issues are raised at the same time due to the changing system environment.

The development of new services open doors for new opportunities and difficulties. By now, almost all IT enterprises are involved in cloud storage by services provision. But while provision of services, we must take into account the problems emerging from the storage operations in cloud. When the data store on personal devices, users have the highest privilege to operate on them and ensure its security. But once the users choose to put data into cloud, they lose their control over the data [7]. The user's authentication and authorization is needed to access the data so as to prevent stealing other user's data through service failure or intrusion.

The answer to data confidentiality is data encryption. The use of both encryption algorithm and key strength are needed to be considered in order to ensure the effect of encryption,. The major issue about data encryption is key management. The major issue considered in key management is as who will be responsible for key management. Ideally, the data owners are responsible for managing the key. But at present, because the users have not enough expertise to manage the keys, they usually entrust the key management to the cloud providers. As the cloud providers need to maintain keys for a large number of users, key management become more complex and difficult [4].

V. SECURITY CHALLENGES

Data security has consistently been a major issue in IT. There are complex data security challenges in the cloud:

- The need to protect confidential business, government, or regulatory data
- Cloud service models with multiple tenants sharing the same infrastructure
- Data mobility and legal issues relative to such government rules as the EU Data Privacy Directive
- Lack of standards about how cloud service providers securely recycle disk space and erase existing data
- Auditing, reporting, and compliance concerns
- Loss of visibility to key security and operational intelligence that no longer is available to feed enterprise IT security intelligence and risk management
- A new type of insider who does not even work for your company, but may have control and visibility into your data

VI. ENCRYPTION

A feasible solution for data protection is data encryption. Encryption algorithm offers the benefit of minimum reliance on cloud provider. The user data can migrate from one provider to another provider without limiting to the specific provider. Encryption algorithm protects data without considering their physical location. Unfortunately, when performing the encryption algorithm, it often consumes a lot of system resources, such as CPU utilization, and stronger algorithm that generates more significant impact to the system performance. The trade -off between security and system performance become an important issue when applying an encryption algorithm in cloud environment.

It's very important to understand what kinds of encryption are most important for a particular need. Two types of encryption algorithms have been considered in the study: FDE and FHE.

- Full Disk Encryption- FDE: As the name reveals, FDE encrypts entire physical disks with a symmetric key for simplicity and speed. Although FDE is effective in protecting private data in certain scenarios, the concern is that it can't fulfill data protection goals in the cloud, where physical theft isn't the main threat. FDE offers excellent performance and ease of development but it does little to protect privacy at the required granularity.
- Fully Homomorphic Encryption- FHE: Here, the server does the real work, but it doesn't know the data it's computing. It offers the promise of general computation on ciphertexts. Any function in plaintext can be transformed into an equivalent function in ciphertext. This property guarantees strong privacy when computing on private data, but the question of its practicality for general cloud applications still remains. FHE removies data visibility entirely from both the server and application developer [8].

VII. DATA PROTECTION AS A SERVICE- DPAAS

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.

A cloud platform helps the developers to write maintainable applications that protect user data in the cloud, hence 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. Hence users can gain confidence that their data is being handled properly.

Cloud-delivered services allow businesses to access enterprise-class resources and infrastructures at a lower price and with very little capital expenses. Cloud- delivered services also help to free IT resources and maximize administrator productivity. Many midsize businesses have already moved costly and administratively time-consuming applications to the cloud. The adoption of data protection as a service has gained momentum due to these reasons. The growing appeal of data protection as a service is that it enable the access of resources you need at minimal upfront expense as well as providing the benefits of enterprise-class data protection capabilities. Data protection as a service removes the complexity barriers for midsize businesses to meet enterprise-level recovery point and recovery time objectives.

VIII. MOTIVATION

One of the main concerns people and organizations have about putting data in the cloud is that they don't know what happens to it. Having a clear audit of when data is accessed, who access the data contributes to strengthen the confidence that data is being handled appropriately. Cloud storage offers an on-demand data outsourcing service model, and is gaining popularity due to its elasticity and low maintenance cost. However, security concerns arise when data storage is outsourced to third-party cloud storage providers. It is desirable to enable cloud clients to verify the integrity of their outsourced data in the cloud, in case their data has been accidentally corrupted or maliciously compromised [9].

With the growing popularity of cloud computing, the importance of security show gradual upward trend, become an important factor in the development of cloud computing. Encryption in the cloud is about preventing outside hackers and external partners from accessing a company's private data. The cloud offers little platform-level support or standardization for user data protection. A new cloud computing paradigm data protection as a service DPaaS has been proposed in the work which is defined as 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.

IX. PROPOSED SCHEME

Cloud computing refers to a large number of computers connected by real-time network viz. internet. Cloud computing provides a way to execute applications on many computers at same time so it is also called as Distributed computing. Though IaaS promises cost efficient and high availability of service across the internet, there is a limitation of building a confident cloud system which can handle data securely and reliably. DPaaS provides secure cloud environment to save data. There are different techniques used for handling data security like – encryption and authentication in data access.

The major issue is that providing protection to 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 as the platform can achieve economies of scale by reducing expertise costs and distributing sophisticated security solutions across different applications and their developers.

Major problem in DPaas is to make existing developed applications for simple cloud Systems compatible with DPaaS as there are many changes in cloud implementation and security integrations. This leads to requirement of changing application architecture and also many changes will be required in application codes. We shall be listing all the necessary metrics required for designing DPaaS so that simpler cloud applications can be migrated to DPaaS with minimum cost and updates.

In our system, there is an administrator who can view data of the users, change the data in the web files and save them. In other words administrator has the control over the user data. The users can upload, view, and change the data in their created web file. They cannot view data or web files of other users. While the auditor is one who audits the overall performance of the system. He can track the transactions, upload of file, change of data and logins of users with correct time and date.

Whenever a user will upload a file and the file gets migrated onto the cloud. After that if the user make any changes to that file, those changes are made standards for further uploads. Here in our system, three types of web files are uploaded- .asp, .jsp and .php files. These formats are made standard formats for the upload. If any file other than this file format is uploaded, it will not get migrated to the cloud. Another advantage offered is that user gets the control over his data protection. If administrator or auditor has made any change to user's file, user will get to know all the details about that through a notification message. It adds a lot into the data security on cloud.

The proposed methodology is needed to be implemented in a tool. The proposed solution is to be implemented in java and CloudSim. CloudSim enables modeling, simulation, and experimenting on Cloud computing infrastructures. It is a self-contained platform used to model data centers, service brokers, scheduling and allocation policies of large scale Cloud platforms. It provides a virtualization engine with extensive features for modeling creation and life cycle management of virtual machines in a data center, including policies for provisioning of virtual machines to hosts, scheduling of resources of hosts among virtual machines, scheduling of tasks in virtual machines, and modeling of costs incurring in such operations.

X. CONCLUSION

In an emerging discipline, like cloud computing, security needs to be analyzed more frequently. With advancement in cloud technologies and increasing number of cloud users, data security dimensions will continuously increase. Cloud computing security needs consider both technology and strategy, including: audit, compliance and risk assessment. Both the Service providers and the clients must work together to ensure safety and security of cloud and data on clouds. Mutual understanding between service providers and users is extremely necessary for providing better cloud security. In our paper we are laying stress on the security issue in the cloud. In this paper, we propose an approach for applying DpaaS to the existing applications in cloud environment to secure the confidentiality of users' data without increasing system performance overhead too much.

ACKNOWLEDGMENT

The paper has been written with the kind assistance, guidance and active support of my department who have helped me in this work. I would like to thank all the individuals whose encouragement and support has made the completion of this work possible.

REFERENCES

[1] Sadie Creese, Paul Hopkins, Siani Pearson, Yun Shen, "Data Protection-Aware Design for Cloud Computing", HP Laboratories

[2] "Introduction to Cloud Computing", Dialogic Corporation

[3] Yashpalsinh Jadeja, Kirit Modi (2012), "Cloud Computing - Concepts, Architecture and Challenges", 2012 International Conference on Computing, Electronics and Electrical Technologies [ICCEET]

[4] Deyan Chen, Hong Zhao (2012), "Data Security and Privacy Protection Issues in Cloud Computing", International Conference on Computer Science and Electronics Engineering

[5] Hans-Dieter Wehle (2011), "Cloud billing service: An SOA-enabled billing service module for the cloud environment", IBM

[6] Ranjita Mishra, Sanjit Kumar Dash (2011), "A Privacy Preserving Repository for Securing Data across the Cloud", 978-1-4244-8679-3/11/2011 IEEE

[7] Ling Li Lin Xu Jing Li Changchun Zhang (2011), "Study on the Third-party Audit in Cloud Storage Service", International Conference on Cloud and Service Computing, -1-4577-1637-9/11/2011 IEEE

[8] Dawn Song, Elaine Shi, and Ian Fischer, Umesh Shankar (2012), "Cloud Data Protection for the Masses", 0018-9162/12/2012 IEEE

[9] Henry C. H. Chen and Patrick P. C. Lee (2012), "Enabling Data Integrity Protection in Regenerating-Coding-Based Cloud Storage", 2012 31st International Symposium on Reliable Distributed Systems, IEEE Computer Society

[10] Raghu Yeluri, Enrique Castro-Leon, Robert R. Harmon, James Greene (2012), "Building Trust and Compliance in the Cloud for Services", 2012 Service Research and Innovation Institute Global Conference, 978-0-7695-4770-1/12/2012 IEEE

[11] Lingfeng Chen and Doan B. Hoang (2011), "Novel data protection model in healthcare cloud", 2011 IEEE International Conference on High Performance Computing and Communications

[12] Engr: Farhan Bashir Shaikh and Sajjad Haider (2011), "Security Threats in Cloud Computing",IEEE

[13] I-Hsun Chuang, Syuan-Hao Li, Kuan-Chieh Huang, Yau-Hwang Kuo (2011), "An Effective Privacy Protection Scheme for Cloud Computing", ISBN 978-89-5519-155-4, Feb. 13~16, 2011 ICACT2011

[14] Pei-Yun Hsueh, Tyrone Grandison, Ci-Wei Lan, lenHao Hsiao, and Henry Chang (2012), "Privacy Protection for Personal Data Integration and Sharing in Care Coordination Services A Case Study on Wellness Cloud", International Journal of Scientific and Research Publications, Volume 3, Issue 6, June 2013 1ISSN 2250-3153

[15] Sunumol Cherian, Kavitha Murukezhan (2013), "Providing Data Protection as a Service in Cloud Computing", International Journal of Scientific and Research Publications, Volume 3, Issue 6, June 2013, ISSN 2250 -3153

[16] http://searchitchannel.techtarget.com/feature/Challenges-of-transitioning-to-cloud-data-protection-services

[17] http://www.applicure.com/blog/securing-cloud-data

[18] http://www.pcworld.com/article/164933/cloud_computing.html

[19] http://www.darkreading.com/services/protecting-data-in-the-cloud-withoutmak/240145260