Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 7, July -2017

Data Protection On Cloud With Multi-Set Partitions.

Prof. Jyoti Patil[1], Aymen Madiha[2]

[1]Computer Science and Engineering, P.D.A College of Engg, Kalaburagi.
[2]Computer Science and Engineering, P.D.A College of Engg, Kalaburagi.

Abstract — *This paper offers strong data protection to cloud users while enabling rich applications is a challenging task. We are exploring a new cloud platform architecture called Data Protection as a Service (DPaaS), which dramatically reduces the per-application development effort required to offer data protection, while still allowing rapid development and maintenance.*
This new cloud computing paradigm, data protection as a service (DPaaS). It 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 uncompromised or malicious applications. Such as secure data using encryption, logging and key management.

Keywords- *Data protection; Cloud platform architecture; DPaaS; Security primitives; Security; Privacy; Malicious; Encryption; Logging; Key management.*

I. INTRODUCTION

Cloud computing enables highly scalable services to be easily consumed over the Internet on an daily basis. A major feature of the cloud services is that users' data are usually processed remotely in unknown machines that users do not own or operate. 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.
Even though the Cloud computing is emerging in these days and the number of providers and the clients are rapidly increasing there is much more concern about the security. There is tension between user data protection and rich computation in the cloud. Users want to maintain control of their data, but also want to benefit from rich services provided by application developers using that data. At present, there is little platform-level support and standardization for verifiable data protection in the cloud. It requires specialized expertise and a lot of resources to build, which may not be readily available to most application developers. We argue that it is highly valuable to build in data protection solutions at the platform layer: The platform can be a great place to achieve economy of scale for security, by amortizing the cost of maintaining expertise and building sophisticated security solutions across different applications and their developers.

II. RELATED WORK

[1] In this paper the Author shows, cloud computing is considered as a basic infrastructure in a growing service industry. This has the advantage of the reduced cost by allowing the users to share the resources and merging with the on demand and pay as you go mechanism. This mechanism allows the users to dynamically allocate the resources and based on the payment as they pay. These kind of features in the cloud computing will have a direct impact on the information technology industry' s economy. It will also affect the traditional and trust management. The author had lot of advantages while dealing with the cloud computing environment such as its scalability, accessibility, storage of data at remote place and sharing services dynamically.

[2] In this paper the author' s shows, the existing mechanism to establish the trust between the users and the cloud providers and also the challenges and the limitation in the traditional system of trust based management. Then they show the proposed system with the new mechanism which provides the efficient results when compared with the traditional mechanisms. At last they conclude while suggesting the framework to implement different trust methods.

[3] In this paper the author's describe how cloud providers will provide the trust based policies on the service level Agreements for the services they are providing. The trust policies are different among different cloud service providers even though they provide same services to the users. This agreement will put the users in the dilemma while choosing the trustworthy cloud service providers. To help the users to decide the trustworthy cloud service provider they have proposed a trust management architecture which is based on the multi- faceted of the cloud computing market. Their proposed system will provide a way for the users to decide the cloud service provider who are trust worthy based on different features and services.

[4] In this paper the author' s focus on providing the trust based management framework which are supported and analyzed the trust related feedback given from the user and from different entities. The system also provides the flexibility to use different scoring functions to analyze the same feedback data for the evaluation of the trust. This system also provides a method to catch the recent feedbacks in the system on the recent activities. The experimental results show the efficient results when compared with previous trust management systems.

[5] In this paper the author's propose a method to detect the attack from the users which will help the users to decide the trustworthy cloud service providers out of many. This system not only provides and detects the malicious behavior but also detect the misleading feedback from the users. This identification is done using the collision attack and also identifies the Sybase attack. To analyze the feedback in the system they have collected large number of feedback given by the cloud users in the real world cloud.

III. PROPOSED WORK

We propose a new cloud computing paradigm, *data protection as a service* (DPaaS). It 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 uncompromised or malicious applications. Such as secure data using encryption, logging and key management.
The contribution in the proposed system is that we are splitting the data into three parts and storing them in three different cloud servers so the data will be more secured. Before storing the data on the cloud, the data will be encrypted and then stored and while downloading the data it will be decrypted.
While performing the search operation by the users we have implemented two searching techniques which give efficient and accurate results. The two techniques are Wild Card Technique and Gram Based Technique.
Following are the modules of the system,

3.1. Cloud Computing

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. Cloud computing exhibits the following key characteristics:

1. **Agility** improves with users' ability to re-provision technological infrastructure resources.
2. **Multi tenancy** enables sharing of resources and costs across a large pool of users thus allowing for:
3. **Utilization and efficiency** improvements for systems that are often only 10– 20% utilized.
4. **Reliability** is improved if multiple redundant sites are used, which makes well-designed cloud computing suitable for business continuity and disaster recovery.
5. **Performance** is monitored and consistent and loosely coupled architectures are constructed using web services as the system interface.
6. **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.
7. **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.

3.2. Third Party Auditor

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.

3.3. 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.
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.

3.4. User Module

User stores 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.

IV. SYSTEM ACHITECTURE

The proposed architecture is the new service model for cloud computing. This service model is meant for data protection and named as DPaaS (Data Protection as a Service). This kind of service model built into cloud computing environment can reduce the effort required by cloud service providers to have mechanisms to protect data of cloud users. This will help Increase the efficiency of cloud in terms of data protection. This will automatically encourage other people to become cloud users and thus cloud computing becomes much more reliable and popular. The architecture is built keeping many issues in mind such as trust and key management, sharing, aggregation, performance, ease of deployment and maintenance. This approach actually moves access control policies and key management into middle tier which is nothing but the computing platform that provides a common platform for masses (all users of cloud computing alike).

As seen in the figure, it is evident that the proposed data protection architecture allows developers to incorporate access control, logging and key management into their applications. It also supports auditing of data protection. It makes a secure execution environment where cloud applications can run with built in DPaaS service. There is no re-invention of wheel because the application developers have access to build in security module known as trusted platform module. This enables developers of cloud applications to have provisions for access control list, key management and logging in built. The proposed architecture is fully aware of user authentication, running binaries, based on the users and application requirements. It has auditing mechanism that ensures that the cloud data protection is in place and no discrepancies occurred in cloud computing paradigm. To realize this architecture we built a prototype application that demonstrates the usefulness of the architecture.

V. IMPLEMENTATION

5.1. Encryption

Encryption is a powerful tool. When speaking about data protection, developers often view encryption as a kind of powerful one to help achieve data protection properties. 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 disk or volume. Disk encryption prevents unauthorized access to data storage. The term full disk encryption is often used to signify that everything on a disk is encrypted, including the programs. Although FDE is effective in protecting private data in certain scenarios such as stolen laptops and backup tapes, the concern is that it can' t fulfill data protection goals in the cloud, where physical threat isn' t the main threat.

5.2. Key Management

The concept of key came from the branch called as Cryptographs. There are basically two types of keys. They are:

(i) Public key
(ii) Private key

A public key known to everyone and what a user wants to send the same message to another user, he uses public key to encrypt the message. Whereas private key or secret key known only to the recipient of the message. The same user after sending the message using public key then he can use his private key to decrypt it. In our system we encrypt the file using a key stored in the cloud. The user should enter the key to decrypt the file, so multiple protection mechanisms are used here for protecting the files in the cloud.

5.3. Wild Card Searching

Wildcard search uses character index, lexicons, and trailing wildcard indexes to speed performance. To ensure that wildcard searches are fast, one should enable at least one wildcard index (three character searches, trailing wildcard searches, two character searches, and/or one character searches) and fast element character searches (if you want fast searches within specific elements) in the Admin Interface database configuration screen.
In wild-card based technique, all the variants of keywords to be listed when an operation is performed at the same position. Based on the above approach, we use a wild card to denote the edit operations performed at the same position. This technique edits distance to solve the problems. It includes the following steps:

i) It builds an index with each keyword k. To build index data owner computes f (sk, k).
ii) Construct the secret key sk. This sk is shared among the data owner and user if he is an authorized user.
iii) Searching can be done with secret key sk , keyword k.
iv) Compare the secret key sent by the user and existed key at the data owner. If both are same, returns the requested file.

5.4. Gram Based Searching Technique

In the fields of computational linguistics and probability, an ***n*-gram** is a contiguous sequence of *n* items from a given sequence of text or speech. The items can be phonemes, syllables, letters, words or base pairs according to the application. The *n*-grams typically are collected from a text or speech corpus. When the items are words, n-grams may also be called **shingles**. An ***n*-gram model** is a type of probabilistic language model for predicting the next item in such a sequence in the form of a $(n-1)$–order Markov model. *n*-gram models are now widely used in probability, communication theory, computational linguistics (for instance, statistical natural language processing), computational biology (for instance, biological sequence analysis), and data compression. Two benefits of *n*-gram models (and algorithms that use them) are simplicity and scalability – with larger *n*, a model can store more context with a well-understood space– time trade-offs, enabling small experiments to scale up efficiently.

5.5. RSA Algorithm

RSA is an algorithm used to encrypt and decrypt the messages to provide the security to the system and the data. RSA algorithm is considered as the asymmetric cryptographic algorithm which has two keys private key and public key. The public key of this algorithm can be given to everyone which will encrypt the data. The private key is kept secret, as it is used to decrypt the data. The RSA algorithm is named after the creators of this algorithm who are Ron Rivest, Adi Shamir and Leonard Adleman, which are published in 1978.

The following steps shows how this algorithm is used in the system

Step 1: In the first, the system takes two prime number and assigns it to the variable p and q respectively. The numbers are generated by using the random function and then checked whether the number is prime. If the number is prime the values will be given to the variable.

Step 2: in the second step, the values of the variable p & q will be reduced by 1. i.e.; (p-1) and (q-1).

Step 3: in the third step, values of the variables are multiplied and stored in the new variable n.

N = (p-1) X (q-1)

Step 4: in the fourth step, the values of p and q are stored in the new variable ‘ np’ .

Np = pxq;

Step 5: in the fifth step, the common factor of the N and Np will be generated. And this common factor will be the private key which is used to encrypt the data.

Step 6: in the sixth step the text are converted into binary format and “ AND” operation is performed between the binary values and the private key. These resulting values are again converted into the character format which will be in the encrypted format.

VI. CONCLUSION AND FUTURE SCOPE

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 data entries will also aid in using collective security expertise more effectively. Accumulating security to a single platform can immediately befit hundreds of thousands of applications and by extension, hundreds of millions of clients. At the same time we have been focused on a particular, albeit popular and privacy-sensitive, class of applications, and also other application need solutions.

FUTURE SCOPE

- We can systematize or regulate technology among platforms to facilitate switching among providers.
- We can make migration to the DPaaS cloud as easy as possible for existing applications.
- We can minimize the cost of application audits.
- To block all kinds of audits are most important for building user confidence.
- We can generalize the ideas presented here to other classes of applications.

REFERENCES

[1] S. Pearson, “ Privacy, Security and Trust in Cloud Computing,” in Privacy and Security for Cloud Computing, ser. Computer Communications and Networks, 2013, pp. 3– 42.

[2] J. Huang, D. M. Nicol, “ Trust Mechanisms for Cloud Computing,” Journal of Cloud Computing, vol. 2, no. 1, pp. 1– 14, 2013.

[3] S. Habib, S. Ries, and M. Muhlhauser, “ Towards a Trust Management System for Cloud Computing,” in Proc. of TrustCom’ 11, 2011

[4] W. Conner, A. Iyengar, T. Mikalsen, I. Rouvellou, and K. Nahrstedt, “ A Trust Management Framework for Service-Oriented Environments,” in Proc. of WWW’ 09, 2009.

[5] T. H. Noor, Q. Z. Sheng, and A. Alfazi, “ Reputation Attacks Detection for Effective Trust Assessment of Cloud Services,” in Proc. of TrustCom’ 13, 2013.

[6] T. H. Noor, Q. Z. Sheng, S. Zeadally, and J. Yu, “ Trust Management of Services in Cloud Environments: Obstacles and Solutions,” ACM.

[7] Ashok Jammi, Meena.S and D V Arjun, "Design and Analysis of Data Protection as a Service (DPaaS) for Cloud Computing," Dept. Of CSE, Gurunanak Institute of Technology, Hyderabad, India.
[8] Sighakolli Ashok and Kishore Gunna, " Cloud Data Protection for the Masses," Dept of CSE, RISE Prakasam Group of Institutions, Ongole, AP, India.
[9] Sunumol Cherian and Kavitha Murukezhan, "Providing Data Protection as a Service in Cloud Computing," Department of computer Science, Vedavyasa Institute of Technology, Calicut
[10] KholeSagar R, Walunj Ajit S, Gulave Rahul K and Nikam Umesh P, " A New Cloud Paradigm: Data Protection as a Service (DPASS)," Department of Computer Engineering, Savitribai Phule Pune University, Shri Chhatrapati Shivaji College of Engineering, Shrishivajinagar, India1234
[11] K. Bhima and S. Suresh, " Privacy Data Control and Data Protection as a Service in Cloud Computing," Department of IT, Padmasri DR. B V Raju Institute of technology, Medak (Dist.), A.P, India.
[12] Jeelani and Anil Kumar .G, " Data Protection as a Service (DPaaS): A Novel Approach For Data Protection in Cloud," Department of CSE, VTU, CIT, Gubbi.
[13] Aluri Srinivas Rao, K. Rama Krishnaiah, Jupudi and Ibrahim patnam, Krishna, " Data Security for Cloud Masses Based on Data Integrity," Nova College of Engineering & Technology.

