ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Data Protection as a Service Suite Which Offer Security and Privacy from Malicious Applications

R.A.Priyanka
B.Tech Student,
Department of CSE,
TKR College of Engineering & Technology.

Divya Shyam Swamy
B.Tech Student,
Department of CSE,
TKR College of Engineering & Technology.

N.Ujwal Reddy
B.Tech Student,
Department of CSE,
TKR College of Engineering & Technology.

T. Shashi Kumar
Assistant Professor,
Department of CSE,
TKR College of Engineering & Technology.

Abstract:

Cloud computing is computing in which large groups of remote servers are networked to allow centralized data storage and online access to computer services or resources. Cloud computing relies on sharing of resources to achieve coherence and economies of scale, similar to a utility (like the electricity grid) over a network. Due to frequent change of members in multi owner group, preserving user data and their identity privacy becomes a challenging issue in cloud. In this Paper we examine and implement a new cloud computing pattern, data protection as a service (DPASs) which is a suite of security primitives by a cloud platform, which having data security and privacy and which provide powerful proof of privacy for data owners. Despite in the presence of strongly compromised or unsecured application. Such as security of data using encryption, logging, key management. Due to this new model of security user can get the confidence that there data which store on cloud is being handle very security. The result show that user that can get notification about the security of their data which is store on the cloud platform.

Keywords:

Logging, Key management, Cloud Computing, Audito, Data integrity, Privacy.

Introduction:

Cloud computing security or, more simply, cloud security is an evolving sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing.

Security issues associated with the cloud:

Organizations use the Cloud in a variety of different service models (SaaS, PaaS, and IaaS) and deployment models (Private, Public, Hybrid, and Community). There are a number of security issues/concerns associated with cloud computing but these issues fall into two broad categories: security issues faced by cloud providers (organizations providing software-, platform-, or infrastructure-as-a-service via the cloud) and security issues faced by their customers (companies or organizations who host applications or store data on the on the cloud). The responsibility goes both ways, however: the provider must ensure that their infrastructure is secure and that their clients' data and applications are protected while the user must take measures to fortify their application and use strong passwords and authentication measures.

When an organization elects to store data or host applications on the public cloud, it loses its ability to have physical access to the servers hosting its information. As a result, potentially business sensitive and confidential data is at risk from insider attacks. According to a recent Cloud Security Alliance Report, insider attacks are the third biggest threat in cloud computing. Therefore, Cloud Service providers must ensure that thorough background checks are conducted for employees who have physical access to the servers in the data center. Additionally, data centers must be frequently monitored for suspicious activity.In order to conserve resources, cut costs, and maintain efficiency, Cloud Service Providers often store more than one customer's data on the same server. As a result there is a chance that one user's private data can by viewed by other users (possibly even competitors). To handle such sensitive situations, cloud service providers should ensure proper data isolation and logical storage segregation.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The extensive use of virtualization in implementing cloud infrastructure brings unique security concerns for customers or tenants of a public cloud service. Virtualization alters the relationship between the OS and underlying hardware - be it computing, storage or even networking.

This introduces an additional layer - virtualization - that itself must be properly configured, managed and secured. Specific concerns include the potential to compromise the virtualization software, or "hypervisor". While these concerns are largely theoretical, they do exist. For example, a breach in the administrator workstation with the management software of the virtualization software can cause the whole datacenter to go down or be reconfigured to an attacker's liking.

Some security and privacy issues that need to be considered are as follows

1) Authentication: Only authorized user can access data in the cloud

2) Correctness of data: This is the way through which user will get the confirmation that the data stored in the cloud is secure

3) Availability: The cloud data should be easily available and accessible without any burden. The user should access the cloud data as if he is accessing local data

4) No storage Overhead and easy maintenance: User doesn't have to worry about the storage requirement & maintenance of the data on a cloud

5) No data Leakage: The user data stored on a cloud can accessed by only authorize the user or owner. So all the contents are accessible by only authorize the user.

6) No Data Loss: Provider may hide data loss on a cloud for the user to maintain their reputation.

EXISTING WORK:

Cloud computing is the type of computing that realise on the sharing of resources rather than having local servers or personal devices to handle the application .

The cloud computing is the model to delivering information technology services in which the resources are retrieved from the internet through the hundreds of millions of application. In the previous cloud computing system platform is build with help of three cloud service models such as Paas(Platform as a service), Saas(Software as a service), Iaas (Infrastructure as a service).This three models deliver software application over the web build the infrastructure for the cloud & create the platform for the entire application developement environment, not only just the use of an application.

But this models having issues related with the compatibilty with hardware & operating system, also it have to do extra work to maintain the system & to maintain the integrity of the database.If the users data which is stored on cloud platform can be access by any unauthorised person then user can not get any immediate alertness about the misuse of data. Due to this more than 90 percent of public & business leaders are worried about security, availability, and privacy of their data as it rests in the cloud. Therefore the security becomes the major issue in this previous cloud computing platform.

PROPOSED WORK:

For the more security required for the cloud platform we need to build the strong security & need to protect the cloud services from large number of malicious application and avoiding unauthorised accesses. This paper proposed the new cloud computing pattern i.e the DPaas which consists of security primitives offered by cloud platform. This platform enables the verification of the cloud environment operation, so the user can get confidence about their data that is being handle securely , also DPaas is a provision of data security & privacy, that offers proof of privacy to data owners even in the presence of malicious application ,so the system have the large number of scope such as all the users are managed by the admin of the system. The uploaded data can be viewed by the auditor & user itself. Every data requires unit data key so the encryption provided in high quality. If the user data can be change by any unauthorised person or the auditor itself then the user get the security alert message & user immediately alert about their data which is stored on cloud environment.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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 dont have much in-house security expertise, because 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.Therefore the propose system build successfully by implementing security but not affecting performance.

MODULE DESCRIPTION:

1. Cloud Computing

2. Trusted Platform Module

3. Third Party Auditor

4. User Module

1. Cloud Computing:

NIST DEFINITION: Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models. 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 computer 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 solvingsecurity 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

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.

2 .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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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. 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.

4. User Module:

User store 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.

DATA PROTECTION AS A SERVICE (DPaaS):

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.

CONCLUSION AND FUTURE WORK:

Due to increasing need for secure data storage a more safe and secure DPASS module has to be proposed.in previous paper we implemented a new data protection as a service module for provide the security to the data store on the cloud.

By using the AES algorithm we provide the powerful security as compare to the previous DES algorithm. due to this new security model there is a possibilities of provision of security alert message to the user.

REFERENCES:

1. Dawn Song, Elaine Shi, and Ian Fischer "Cloud Data Protection for Masses",Published by the IEEE Computer Society, 0018-9162/12 ,JANUARY 2012.

2. SunumolCherian, KavithaMurukezhan\Providing Data ProtectionasaServiceinCloudComputing"International Journal of Scientic and Research Publications, Volume 3, Issue 6, June 2013 1 ISSN 2250-3153.

3. C.HariHar , Prof. Mrs.Varshapriya J.N. \Cloud Data Storage Protection For The Masses, ",International Journal,May- 2014 Volume 1, Issue 3.

4. P. KiranRao , V. Lakshmi Sailaja , Alfisha Khan , S. Mamatha\High level security in cloud for scalable data, International Journal of Advanced Research in Computer and Communication Engineering ,Vol. 2, Issue 3, March 2013.

5. Craig Gentry Stanford University and IBM Watson cgentry@cs.stanford.edu, Fully Homomorphic Encryption Using Ideal Lattices.

6. Andrei Sabelfeld and Andrew C. Myers, Language-Based Information-Flow Security, IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 21, NO. 1, JANUARY 2003.

[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute- Based Encryption for Fine-Grained Access Control ofEncrypted Data," Proc. ACM Conf. Computer and Comm. Security (CCS), pp. 89-98, 2006.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[8] D. Pointcheval and J. Stern, "Security Arguments for Digital Signatures and Blind Signatures," J. Cryptology, vol. 13, no. 3, pp. 361-396, 2000.

[9] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.

[10] D. Naor, M. Naor, and J.B. Lotspiech, "Revocation and Tracing Schemes for Stateless Receivers," Proc. Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-62, 2001.