International Journal of Computer Sciences
July'2016 Issue
ISSN Number: 4142 3453

Cloud Computing Environment for Secure Data Storage

A. Aparna[1], G.Surya Narayana[2], Dr. A. Subramanyam[3]

[1]M.Tech.,Pg Scholar, Annamacharya Institute Of Technology & Sciences, Rajampet, Kadapa

[2]Assistant Professor, Annamacharya Institute Of Technology & Sciences, Rajampet, Kadapa

[3]Professor,HOD,Dept of CSE,Annamacharya Institute Of Technology & Sciences,Rajampet, Kadapa

ABSTRACT: Cloud computing is an innovative computing paradigm that offers amazing advantages in economical aspects such as reducing time, improved performance, flexible computing capabilities, and advantageous computing power. Cloud computing offers a prominent service for data storage known as cloud storage. The flow and storage of data on the cloud environment in plain text format may be main security threat. In early days generation of large amount of data and the rise of cloud computing have introduced new aspects for data management. In this paper we reviewed integrated set of models, algorithms and tools pointing at relieving developers' goal for developing, deploying and migrating multi data stores applications in cloud atmosphere. An approach focuses mainly on First, a unifying data model followed by applications developers to communicate with heterogeneous relational and NoSQL data stores. Depending on that, queries are expressed using OPEN-PaaS-Data Base API (ODBAPI), unique REST API granting programmers to write their code independently of the target data stores. Second, virtual data stores act as a mediator and communicate with integrated data stores covered by ODBAPI. This paper gives the basics of cloud computing with its history, architecture, features along with pros and cons. The paper also gives two ideas for secure data storage in cloud environment. It helps to store data without confidentiality leakage and also helps to retrieve only accurate files.

KEYWORDS: Cloud computing, Data security as a Service, availability, privacy, Integrity, Confidentiality, PerspecSys.

I.INTRODUCTION

Cloud computing has recently risen as a new computing paradigm which empower on-demand and it has scalable provision of resources. It also has platforms and software as services. Cloud computing is divided into three levels [1]: 1. Infrastructure as a Service (IaaS) provides access to the abstracted view on the hardware, 2, the Platform-as-a-Service (PaaS) supplies programming and execution environments to the developers, and 3, the Software as a Service (SaaS) enabling software applications to be used by cloud's end users. Cloud computing adds execution environments for some emerging applications like big data management due to its elasticity property. In this paper the variety property [2] of big data is mainly focused and more precisely on multiple data store based applications in the cloud. To satisfy variety of storage requirements, cloud applications requires accessing and interacting with several relational and NoSQL data stores having heterogeneous APIs of the data stores which induces problems while constructing, deploying and migrating multiple data store applications. Main four problems are:

Pb1: Elephantine workload on the developer: These days data stores have heterogeneous and variety of APIs. Developers of multiple data store based applications need to be known all these APIs while coding their applications Pb2: No declarative way to execute complex queries: Heterogeneity of the data models has any declarative way to define and execute complex queries over several data stores. This is mainly due to the absence of a global schema of heterogeneous data stores. In addition, NoSQL data stores are scheme less. It means developers should have to manage with the implementation of such complex queries. Pb3: Code adaptation: Application developers need to re-adapt the application source code to interact with new data stores when applications are migrating from one cloud environment to another. Developers should have potential to learn and use new APIs. Pb4: Tedious and non-standard processes of discovery and deployment: Once an application is developed or migrated, developers need to spread it into cloud provider. Discovering the most appropriate cloud and deploying the application on it are tedious and meticulous provider-specific process. In this paper an integrated set of models, algorithms and tools objecting at reducing developers' tasks to develop, deploy and migrate multiple data stores based applications in cloud environment are discussed. First, a unifying data model which is used by applications developers to communicate with different data stores is defined. This model deals with queries of heterogeneity within data models and the nonappearance of the schemes in NoSQL data stores. Based on this model, all types of queries using OPEN-PaaS-DataBase API (ODBAPI) may express and executed by developers. This API is a assembled and a unified REST-based API [3] for executing queries over relational and NoSQL data store. The main features of ODBAPI are twofold: (i) seperating cloud applications from data stores to promote the migration process, and (ii) smoothing the developers' task by reducing the

burden of managing dissimilar APIs. Second, virtual data stores (VDS) to calculate and optimize the execution of queries are proposed - especially complex queries over different data stores. In order to define and the execution of queries over A data model which abstracts from the fundamental (explicit/implicit) integrated data store models, and supplies a unified view so that developers can explain their queries on heterogeneous data stores is heterogeneous data models, the unifying data model has been used to attain with correspondence rules. The solution is based on algebraic trees composed of data sources and algebraic operators and algebraic trees annotation. Third, a clear approach for discovering proper cloud environments and redistributing applications on them in the time letting developers simply focuses on specifying their storage and computing requirements is presented.

II.RELATED WORK

Dr Elaine Shi **[4]** described several enabling technologies towards this vision. Specifically, she told about 1) how to safeguard users' data against potentially compromised applications; 2) how to safeguard users' data against a potentially compromised computation provider; and 3) how to safeguard users' data against a potentially compromised storage provider. She told about our ongoing effort at integrating these technologies to provide a cloud infrastructure which offers data security at the platform level. In this way, users can benefit from the rich cloud applications without worrying about the privacy of their data; and application developers can focus on developing functionality while offloading the burden of providing security and privacy to the cloud platform. Performance According to a recent survey, 49% of users abandon a site or switch to a competitor after
experiencing performance issues**.[5]** And the need for speed is only increasing: in 2000, a typical user was willing to wait 8 sec for a webpage to load before navigating away; by 2009, that number dropped to 3 sec. Platform verifiability**:** The DSaaS approach provides logging and auditing at the platform level, sharing the benefits with all cloud computing applications running on top.

Offline, the cloud auditor can verify that the platform implements each data protection feature as promised. At runtime, the cloud platform provider can use *trusted computing* (TC) technologies to attest to the particular software that's running. TC uses the tamper proof TPM as well as the virtualization and isolation features of modern processors, such as Intel VT-x or AMD-V.
TC also allows for a dynamic root of trust—while the system runs, the Central Processing Unit can enter a clean state, and the Trusted Platform Module (TPM) can verify, load, and execute a *trusted computing base* (TCB), TCB is responsible for security-critical functionalities such as access control, isolation enforcement, key management, and logging. Moreover, a third-party cloud auditor can verify the code of the *trusted computing base* that has been loaded on to the cloud computing platform. In this way, users and developers can gain confidence that the applications are indeed running on the correct *trusted computing base* and consequently trust the security guarantees and the audit logs the *trusted computing base* provides. One challenge in code attestation is how to establish a set of acceptable binaries in the presence of rapid software updates such as bug fixes and latest features. One potential way is to log the history of software updates and perform verification a posteriori. For the application itself, getting from verifiable to verified isn't easy; in a system with a lot of cloud users, doing all cloud pairs verification is prohibitively expensive. This is where cloud auditors come in. Certifications such as Statement on ASN70 (Auditing Standards Number 70) and others serve the important function of reducing the verification burden on both clients and service providers compared to pair wise examinations. Since applications have the data-security piece in common from the platforms, the application verifications in turn can be simpler than they otherwise would have been.

OVERVIEW OF THE SYSTEM Figure 1 show the main constitutes of the system and how these constituents intervene during the development, discovery and deployment and execution steps. Solution show in particular how below four elements enable overcoming the problems (Pb1 - Pb4) listed in introduction. The solution relies on the following four elements:

A) Unifying data model
B) REST API/services
C) Virtual data stores
D) Dedicated components for discovery and deployment

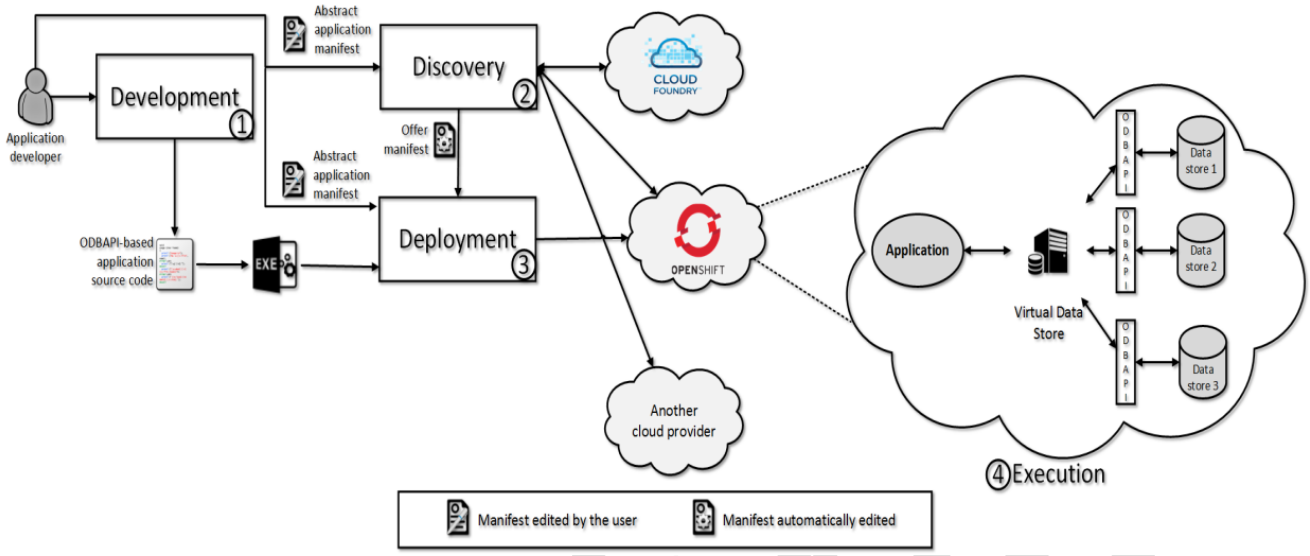


Figure 1: Overview of the solution

defined. The developers' stand of a global data model signified according to unifying model and which accomodate local data store models during the development phase. Unifying data model separates query definitions from the data stores unique languages. (Contributing to resolving Pb1 and Pb2). For manipulating complex objects, more complex algebra can be used, notably N1NF algebra [4]. **B) REST API/services:** Based on unifying data model, a resource model upon which a REST API is developed, called ODBAPI, which enables to communicate with involved data stores in a specific and uniform way. Each data store will be then covered behind a REST service applying ODBAPI. Implemented API separates the intercommunication with data stores through their specific drivers. With the help of unifying data model to define the queries and ODBAPI to communicate with the data stores, developers need not to deal with different languages and APIs and need not to adapt their code when migrating their applications (resolving thereafter Pb1 and Pb3).

III.METHODOLOGY

Cloud storage [13] is a model of data storage where the digital data is stored in logical pools, the physical storage spans multiple servers (and often locations), and the physical environment is typically owned and managed by a hosting company. These cloud storage providers are responsible for keeping the data available and accessible. People and organizations buy or lease storage capacity from the providers to store user, organization, or application data. Cloud storage is based on highly virtualized infrastructure and is like broader cloud computing in terms of accessible interfaces, near-instant elasticity and scalability, multi-tenancy, and metered resources.

Figure 2: Cloud Storage

Cloud storage is made up of many distributed resources, but acts as one – often referred to as federated storage clouds. It is highly fault tolerant through redundancy and distribution of data. It is efficient and cost effective. i.e., through cloud storage, companies need only pay for the storage and service they actually use. Cloud storage provides users with immediate access to a broad range of resources and applications hosted in the infrastructure of another organization via a

web service interface. The service provider handles the storage capacity so the user need not worry about the capacity and capability of storage. It also provides mechanism for creating, accessing and updating the outsourced data. The examples of cloud storage are Amazon S3, Microsoft Azure, etc. In cloud environment, the sensitive data of data owners are stored in the cloud storage and can be accessed from anywhere, everywhere and at any time. To protect data privacy, some cryptographic techniques like encryption can be introduced [14]. Thus the sensitive data is encrypted before uploading to the cloud storage. Mass storage and low expense provided by the cloud storage invites more and more enterprises and organizations to store their private data in cloud with effective security. A virtual private storage service is designed by taking the advantages of both public and private clouds. A public cloud provides scalable and dynamic storage and provides availability and reliability of data where as private clouds provide security and privacy for the data. Thus the virtual private storage service based on cryptographic techniques achieves both the security of a private cloud and functionality and cost savings of a public cloud. Other advantages of cryptographic cloud storage are the control of data is in the hands of customer and security properties are taken from cryptography.

IV. COMPANIES IN THE CLOUD

Some companies offered cloud services are [12]

A. Google: - Google offers a powerful collection of web based applications served through cloud architecture. Cloud base word processing – Google Docs, presentation software – Google Presentation, email – Gmail, Calendar Google Calendar etc.

B. Microsoft: - It offers Windows Live suite of web based applications.

C. Amazon: - It has its Elastic Compute Cloud (EC2), a web service which provides cloud based resizable computing capacity for application developers.

D. IBM: - It provides open source workload scheduling software called Hadoop, based on the MapReduce software used by Google in its offering. Following are some applications [12] using the features of cloud computing.

A. For the Family

Computing in the clod can help a family to communicate and collaborate. It brings the family members closer together.

- Centralized Email Communication (Gmail, Yahoo etc.)
- Collaborating with Schedules (Google Calendar Yahoo Calendar etc.)
- Collaborating on Grocery List (Google Docs)
- Collaborating on To-Do Lists (Ta-da List)
- Collaborating on Contact List (My Events)
- Sharing Family Photos

B. For the Community

Any time any group of people in the community can communicate and collaborate.

- Collaborating on Schedules – Sports team schedules, School Schedules, Event Schedules etc.
- Collaborating on Group projects and Events
- Collaborating on Budgets
- Collaborating on Event Marketing

C. For the Corporation

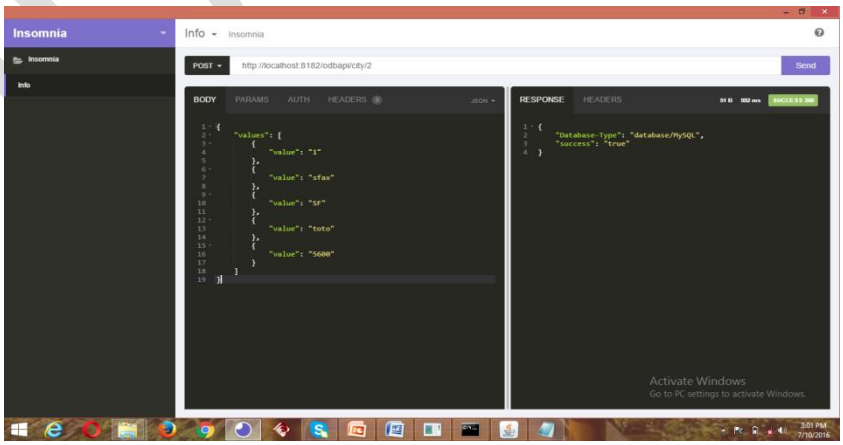
The cost savings and productivity enhancement are done through the cloud. Companies can do more with limited budgets.

- Managing Schedules (AppoinmentQuest)
- Managing Contact List (BigContacts)
- Managing Projects (AceProjects)
- Collaborating on Reports (Google Docs)
- Collaborating on Marketing Materials
- Collaborating on Presentations
- Presentation on the Road (WebEx)
- Collaborating on Budgets (HostBudgets)

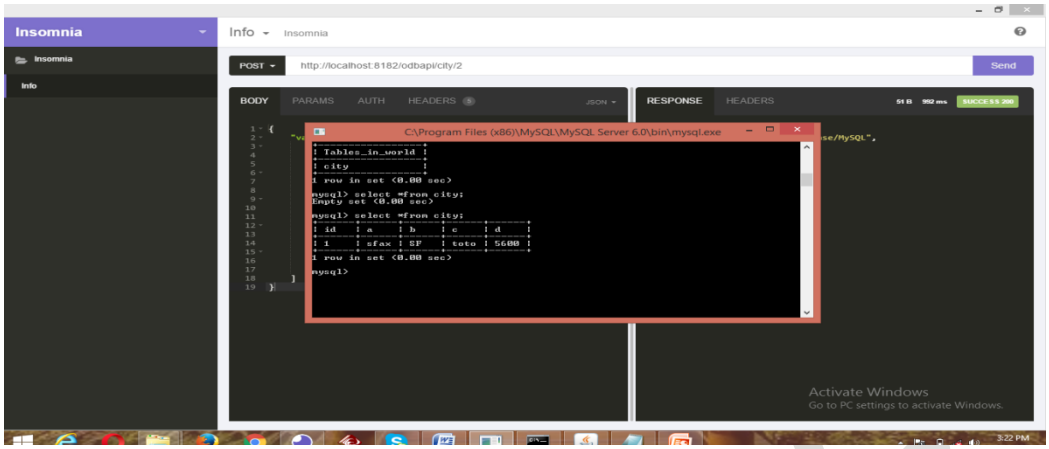
Cloud computing is an innovative technology to store and share the data publically with the assurance of data security. The various features and characteristics of cloud described above have proved its significance. Also cloud has got numerous applications in every point of human life. However, this new computing paradigm exhibits serious privacy challenges on users' data stored on remote servers which belong to a different trust domain. Here comes the need for data encryption in cloud. i.e., for data security, cryptographic techniques are used and thus the cloud storage is modified as cryptographic cloud storage. Two schemes for secure data storage in cloud premises is also mentioned along with graphs. The awesome applications of cloud inspire more and more companies to offer cloud facility in future.

V.RESULTS

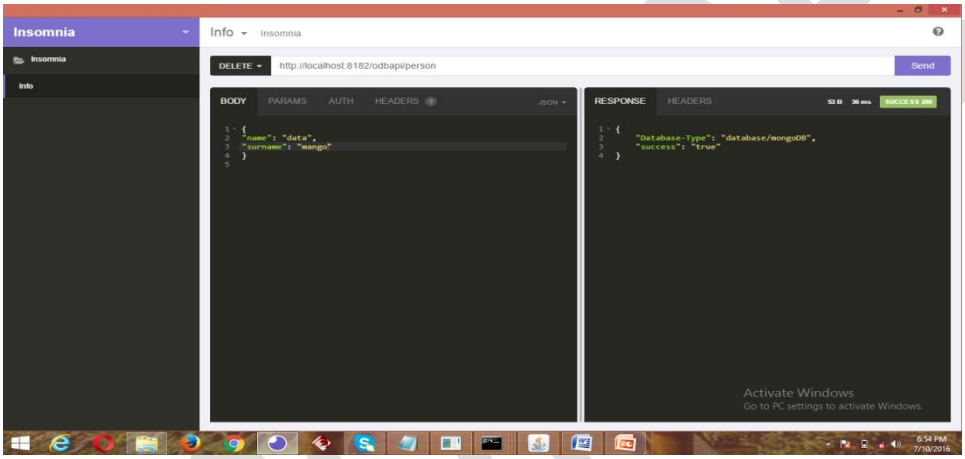
Home Page



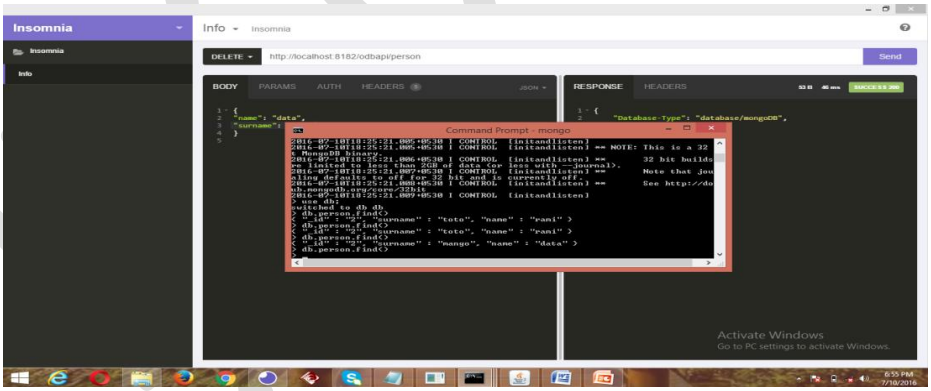
Data Set Upload Page



User Query Screen



User Query Upload Screen



User Query Result

VI.CONCLUSION AND FUTURE WORK

In this paper, we have analyzed a generic approach is explained to facilitate the developer task and enable the development of applications using multiple data stores while remaining agnostic to these latter. There is no need to write different APIs to interact with heterogeneous data. Three solutions are explained in this paper: i) Open-PaaS-Database API for CRUD operations. ii) Virtual data stores for complex queries execution. iii) Manifest for data stores discovery and automatic application deployment. Those users who have less resources and limited computing capability, they can use this service and it is most efficient service for them. Our service is also secured at the time of Dynamic Data operation like insertion deletion and updating. Based on this work anybody can implement key management system algorithms, and face challenges in key management and improve effectiveness in key management. This work may focus on how you can face new challenges in cloud computing environment

REFERENCES

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

[2] Mell, P. and Grance, T. (September 2011). "The NIST Definition of Cloud Computing. NIST Special Publication 800-145 (September 2011). National Institute of Standards and Technology, U.S. Department of Commerce" Retrieved 2012-05-20.

[3] Krutz, Ronald L., and Russell Dean Vines. "Cloud Computing Security Architecture." Cloud Security: A Comprehensive Guide to Secure Cloud Computing. Indianapolis, IN: Wiley, 179-80. Print., 2010.

[4] Richard Chow, Philippe Golle, Markus Jakobsson, Elaine Shi, Jessica Staddon, "Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control" PARC Fujitsu Laboratories of America

[5] E. Naone, "The Slow-Motion Internet," Technology Rev., www.technologyreview.com/files/54902/ GoogleSpeed_charts.pdf. Mar./Apr. 2011;

[6] Kartik Sharma, Renuka Sharma, Gitesh Dalal International Journal of Scientific & Engineering Research, Volume 4, Issue 6, June-2013 2348 ISSN 2229-5518 IJSER © http://www.ijser.org "A Secure Protocol for Data storage Security in cloud computing, 2013

[7] C. Gentry, "Fully Homomorphic Encryption Using Ideal Lattices," Proc. 41st Ann. ACM Symp. Theory Computing (STOC 09), ACM, pp. 169-178. 2009.

[8] "Security Policy and Key Management: Centrally Manage Encryption Key". Slideshare.net. 2012-08-13. Retrieved 2013-08-06.

[9] E. Bertino, F. Paci, and R. Ferrini, "Privacy-Preserving Digital Identity Management for Cloud Computing," IEEE Computer Society Data Engineering Bulletin, Mar. 2009, pp. 1–4.

[10] M. Ko, G.-J. Ahn, and M. Shehab "Privacy-Enhanced User-Centric Identity Management," Proc. IEEE Int'l Conf. Communications, IEEE Press, 2009, pp. 998–1002