I J C T A, 9(20), 2016, pp. 317-325

Designing Hybrid Security Architecture in Multi Cloud System

Bijeta Seth* and Surjeet Dalal**

ABSTRACT

Cloud computing has emerged as the latest trend in world of computers due to its cost effectiveness and flexible nature. Cloud computing is considered to be the future of internet and is an emerging technology these days. It provides services to the user on pay per use basis. However security and privacy risks have restricted its widespread use. This paper aims to mention challenges and issues existing in single clouds and promotes the use of multiclouds. It mentions need of multicouds because of its capability to reduce security risks affecting the cloud. Different multicloud models and approaches are explained. The paper aims to suggest innovative architecture for multicloud environment which will facilitate in reducing the security threats. The system is aimed to provide a framework to set up a protected cloud database that will provide guarantee to evade security risks faced by the cloud computing community

Keywords: Clouds - Cloud computing - Security –Single cloud-Multiclouds

1. INTRODUCTION

Cloud computing is the interconnection of computers over internet providing a distributed environment which provides online access anywhere and at any time. Five foundation technologies played a significant role in the comprehension of Cloud computing. These are: Distributed systems, Virtualization, Web 2.0, Service-oriented computing and Utility computing. NIST defined cloud computing as [6]:

> "*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"*.

Advantages of cloud computing are online access from anywhere at any time, lowered costs, increase in speed and scalability of cloud services, unlimited storage and easy backup and recovery feature. Loss of physical control over data, security and privacy threats, vendor lock-in problem and unpredictable costs are some of its major disadvantages. It has three deployment models namely Public Cloud which provides the interface between the unrestricted customers & owner group (third party). Examples are Google, Amazon and Microsoft. Cost effectiveness, high reliable, scalable and flexible nature, location Independent are its major advantages. However, low Security provision is its major drawback. Private cloud offers the services merely for an organization in exclusively manner. OracleGrid, IBM CloudBurst, IBM LotusLive Inotes, etc. are its examples. It can occur in two ways: On-site and Outsourced private clouds. Some of the advantages of deploying cloud as private cloud model are high Security and Privacy with more control over data. Disadvantages of using private cloud model are Restricted area of Operation, high cost and limited scalability. Community Cloud provides the services for the specific groups instead of whole public groups. They all work together for common concerns. Example: Government or G-Cloud, IBM's Federal community cloud.

* Department of Computer Science & Engineering SRM University, Sonepat, Haryana

** Department of Computer Science & Engineering SRM University, Sonepat, Haryana

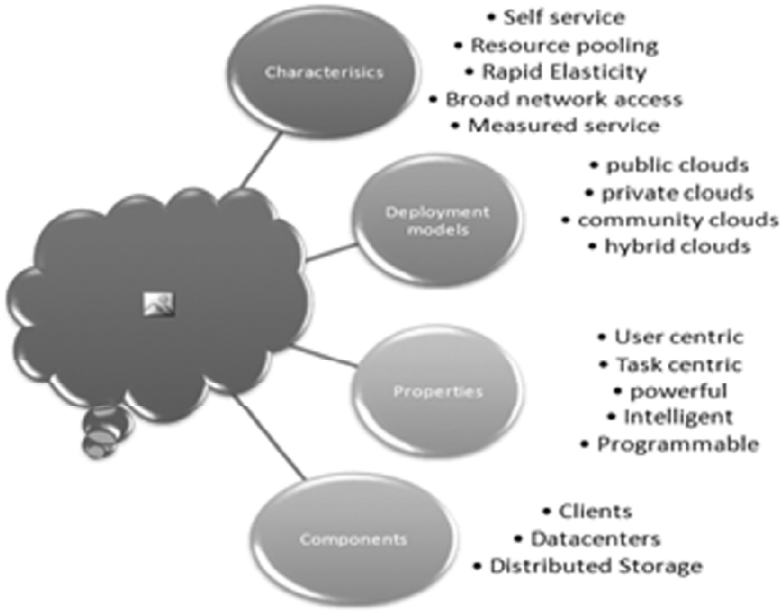

Figure 1: Description of a Cloud

It can occur in two ways: On-site and Outsourced community clouds. Benefits of deploying cloud as community cloud model are high Cost Effectiveness and security. A hybrid cloud is formed by combining any of the public, private or community clouds. Some of the benefits of hybrid clouds are high Scalability, Flexibility, Cost Efficient and security. Its drawbacks include Networking Issues, Security Compliance and Infrastructure Dependency. Cloud Computing stack has three layers namely Software as a Service which allows the client to have an application on lease from cloud service provider instead of buying, installing and running software. Example: Gmail Docs. Platform as a Service (PaaS) which provides a platform to the users upon which applications can be made and executed in the cloud. Example: Google App Engine, Microsoft Azure Services. Infrastructure as a Service which provides the resources on-demand from their huge pools installed in data centers to the users. For example, Elastic cloud Compute. Clients, the datacenter, and distributed servers are the three core components of cloud computing solutions. Clients are the devices with which end users communicate with the cloud. Datacenter are used to store subscribed applications. Distributed Servers are geographically distributed.

The rest of this document is structured as follows. Section II discusses the biggest threat in cloud computing,

Security; its concern, challenges and issues. Section III discusses types of clouds. Section IV analyzes the novel generation of cloud computing, that is, multi-clouds and modern techniques to tackle security in the Cloud Computing theory. It includes importance of multiclouds and its related work, multiclouds models and approaches used. Furthermore, Section V presents Homomorphic Encryption technique which will be used in our proposed model, depicting the basic principle and the generic multidataflow. Section VI describes the proposed model with a thorough data flow explanation and, in the end; in Section VII we present our conclusions and future scope.

2. SECURITY IN CLOUD COMPUTING

Security challenges are the prevalent barrier when taking into consideration the implementation of cloud services. This section mentions the troubles linked to cloud computing and their proposed solutions.

2.1. Security Concerns

Storing user information in the cloud has following aspects:

1. Data: The data is stored in the cloud so the cloud provider should agree to provide security to the data.
2. Access: It tells who is overseeing the data and what types of controls are applied.
3. Training to Employees: Employees need to be trained to maintain security of data.
4. Data Classification: Different users can store their data, so the data needs to be classified.
5. Service level agreement (SLA): SLA defines the conditions and regulations need to be obeyed between cloud provider and consumer.
6. Security breach: How cloud provider will help in case of any incident.

2.2. Challenges

Following are the main challenges that occur in cloud computing:

1. Outsourcing: Privacy violations can occur as the customers actually lose control on their data and tasks.
2. Multi-tenancy: New vulnerabilities and security issues can occur because of shared nature of clouds between multiple customers.
3. Massive data and intense computation: Traditional security mechanisms can't be applied to clouds due to large computation or communication overhead.
4. Political Issues Due to Global Boundaries: Laws made by major international technological and political powers are creating a negative impact on the expansion of the global cloud.

2.3. Data Security Issues in Cloud Computing

There are numerous security issues for cloud computing. Some of them are:

1. Privacy and Confidentiality: Only authorized users should be allowed to access the data.
2. Data Integrity: Truthfulness of data must be maintained.
3. Data Location and Relocation: Contractual agreement in terms of SLA needs to be set between Cloud provider and the consumer so that location of data is known.
4. Data Availability: becomes an issue because data is stored at different locations or clouds.
5. Storage, Backup and Recovery: RAID (Redundant Array of Independent Disks) storage systems can be used by cloud providers that will store many copies of data in some independent servers. Backup services in the occasion of hardware failure are provided to roll back to a previous state.
6. Trust: The cloud service provider is required to provide sufficient security policy to reduce the risk to the data when a user outsources the data to the cloud.
7. Authentication and authorization-To prevent unauthorized access, software is hosted outside of the organization firewall.

3. TYPES OF CLOUDS

1. Single Cloud: Customers would not like to lose their sensitive information due to malicious insiders and hackers in the cloud. In addition, threats like data intrusion, data loss, lack of confidentiality and integrity, availability issues has caused many problems for single cloud providers. They all should be defeated to provide better services to the customers. They need high cost for cloud maintenance process.

2. Interclouds: are interrelated global "clouds of clouds" and seen as an expansion of "networks of networks". They intend to minimize the drawbacks of single cloud. They resolve limited physical resource limitation of clouds and provide profits like high application resilience, diverse geographical location and avoid vendor lock-in to cloud client. There are two types of interclouds:
    1. Federation clouds: cloud infrastructures are shared for better resource utilization willingly by the cloud providers. Example government clouds. It is of two types namely peer to peer and centralized clouds.
    2. Multicouds: client themselves manage resource provisioning and scheduling. Example private cloud portfolios. It is of two types' services and libraries.

4. MULTICLOUDS

4.1. Introduction

Multi-cloud approach makes use of two or more clouds and thus avoids reliance on any one indivual cloud. According to Vukolic, multiclouds have increased trust, security and distributed reliability among multiple cloud providers. Abu Libdeh prefers multiclouds so as to evade "vendor lock-in" by distributing user's data between multiple clouds. Multi-cloud strategy has ability to reduce the risk of service availability failure, Loss and corruption of data, loss of privacy and the possibility of malicious insiders in the single cloud. It has included various aspects of security like confidentiality, integrity, availability, efficient retrieval and data sharing.

4.2. Related work

Jens Matthias Bohli et al. [2013] considered security as the biggest threat in cloud computing and mentioned why multiclouds architecture should be used. Also the paper included architectures, techniques and approaches used in multiclouds. Low Tang Jung et al. [2013] described a Hybrid MultiCloud Data Security (HMCDS) model based on concepts of multiclouds, clusters and data classification techniques and provided data confidentiality. Data is categorized into more sensitive, sensitive and less sensitive classes. The author defined layering concept of three layers namely cloud user login, data management layer and database layer. Mandar Kadam et al. [2015] mentioned that single cloud doesn't present a strong protection layer against the malicious attacks thereby increasing the risk of data unavailability. So, multiclouds are preferred and implemented using Shamir's secret sharing algorithm to authenticate a unique user and to access a particular file from the cloud storage. Balasaraswathi et al. [2014] discussed and presented the cryptographic data splitting approach with dynamic approach of securing information. The author mentioned that the approach prevented unauthorized data retrieval and addressed security factors in cloud computing. Also, proposed secure multiclouds architecture is implemented in OpenStack. Mohammad A.Alzain et al. [2013] compared their Multi- Cloud DataBase Model (MCDB)with Amazon cloud for data retrieval and concluded that their model provided several benefits of efficient data storage and retrieval. The model provided protection against service availability and data integrity but the data intrusion still remained as a security threat. Nupoor M. Yawale et al. [2014] used Third party auditor to resolve the conflicts between the cloud service provider and the client. RC5 Encryption Algorithm was used for storing data in cloud. The method is claimed to be secure and easy to use and verified the data integrity. Passent M. El-Kafrawy et al. [2015] focussed on discussion on security functions and comparison being made on some cloud models. Different security measures were also discussed. Maha Teeba et al. [2014] presented security restrictions in single cloud and mentioned the usefulness of adopting multiclouds to reduce risks by using Depsky and ensured availability and confidentiality of data. M Sulochana [2015] mentioned security as the biggest threat. Also mentioned to grant integrity and confidentiality application logic and data are splitted into two different clouds. The administrator performed encryption and segmentation tasks providing both confidentiality and

availability. Lino Abraham Varghese et al. [2013] implemented a scheme supporting homomorphic verifiable response and hash index hierarchy to maintain dynamic scalability on multiple storage servers. The paper provided data integrity for outsourced data storage systems. Sowmiya et al. [2014] proposed a secure cloud storage model providing anonymous authentication using digital signatures. Homomorphic encryption was used to perform encryption and storing the data. Kamal Benzeki et al. [2016] mentioned how homomorphic encryption is considered to be appropriate for storing data onto a cloud and mentioned several issues related to it.

4.3. Multicloud models

Following are the main multiclouds models:

1. DepSky: It was proposed by Bessani et al. as a virtual storage system which consists of arrangement of four dissimilar clouds namely Amazon S3, Windows Azure, Nirvanix and Rackspace to build clouds-of-clouds. It is considered to be the best model as it provides all the security issues like availability, integrity and confidentiality and avoids vendor lock-in problem by combining Byzantine Quorum System protocols, cryptographic secret sharing and erasure codes. It comprises of three parts readers, writers and four storage providers. DepSky consists of two algorithms namely DepSky-A providing only availability and DepSky-CA providing both confidentiality and availability as shown in figure 2(a) and 2(b).
2. HAIL is High Availability and Integrity Layer which provides a software layer by combining cryptographic protocols with erasure codes to provide integrity and confidentiality. It deals with static data.
3. RACS is a Redundant Array of Independent Disks (RAID) like technique and deals with monetary failures and vendor lock-in problems but it fails to provide confidentiality and security issues.
4. InterCloud Storage (ICStore): It implements all client side functionalities as a library and has three layers which provide confidentiality, integrity and reliability and consistency.
5. MultiCloud DataBase (MCDB): It is considered to be advance version of DepSky and uses distributed technique to provide privacy with database management systems. Data is aimed to be made secure using substitution and polynomial functions.

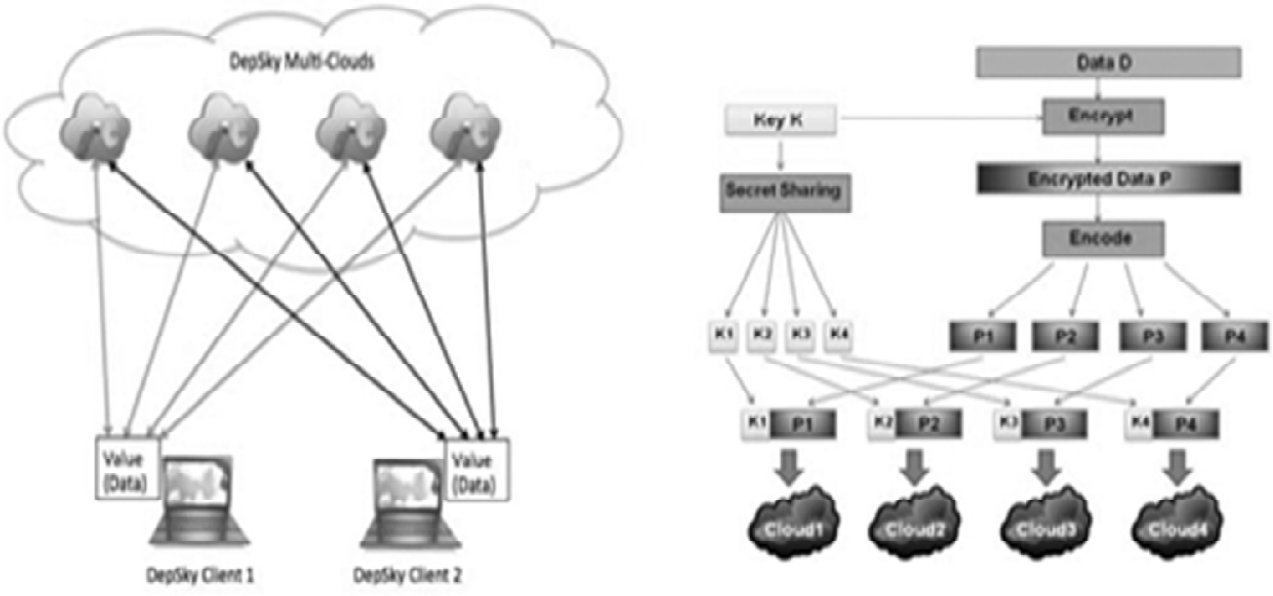

Figure 2: (a) Architecture of DepSky (b) Architecture of DepSky-CA

5. SECURITY ASPECTS AND PROPOSED METHODOLOGY IN MULTICLOUD ARCHITECTURE

The fundamental inspiration to bring into play multiple distinct clouds is to eradicate or rise above the risks of malicious data manipulation and disruptions. By integrating many different clouds, security issues can be resolved to a great extent. In multi cloud, for encryption various mechanisms like cryptographic methods, homomorphic encryption and key management are used. Multi-Cloud Database Model is a method for data splitting to guarantee the integrity and availability of data. In this manne, r the security is incredibly improved as the information is stored and replicated in multiple clouds and there is lesser probability of the intruders to attack. The clouds can distribute their data using secret sharing algorithm and TMR technique.

Four different approaches are used to store and process data in a multicloud environment namely:

1. Replication of Applications: As shown in figure 3(a) it allows several diverse clouds to execute multiple copies of the same data, thus eliminating the need of cloud user to trust one cloud service provider completely. It can be implemented by dual execution and n cloud approach.
2. Partition of Application System into tiers: It is shown in figure 3(b) and protects against undesired data leakage by separating the data and logic to distinct clouds. It can be used in email, documents, spreadsheets etc.
3. Separation of Application System into fragments: As shown in figure 4(a), it enhances confidentiality by dividing the application logic to diverse clouds. It can be implemented by using Obfuscating

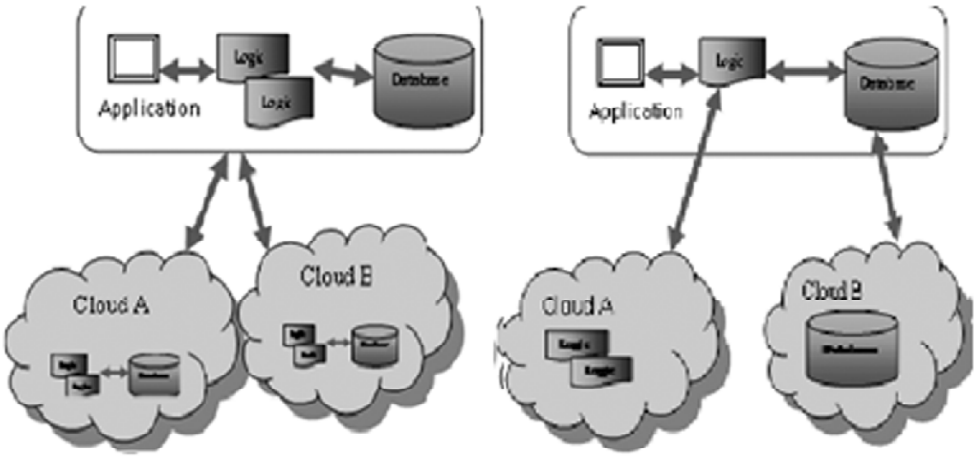

Figure 3: (a) Replication of Application Systems (b) Partition of Application Systems into tiers

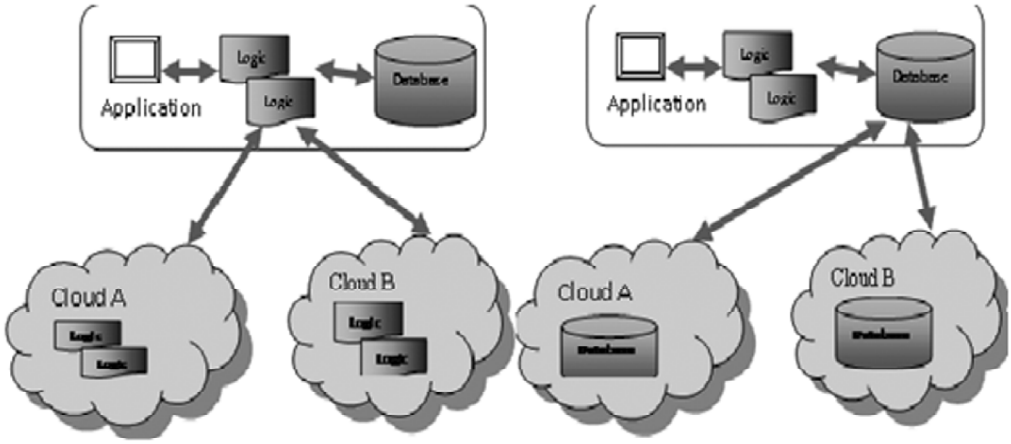

Figure 4: (a) Separation of Application logic into fragments (b) Division of Application data into fragments

splitting, Homomorphic Encryption and Secure Multiparty Computation. Example of SMC in real world is sugar beet auction.

4. Division of Application data into fragments: Shown in figure 4(b) allows storing of structured data like files and unstructured data like images by dividing fine-grained fragments of the data to distinct clouds. It can be implemented by using cryptographic data splitting and database splitting.

In this paper, we aim to design a framework which allows users to upload files to cloud server and a function to split the files into multiple parts by using the concept of cryptodatabase splitting. The security is provided using Homomorphic encryption algorithm which helps to protect data when it is outsourced to cloud database. It is a kind of encryption which allows functions to be computed on encrypted data without decrypting it first. So even if the cloud is untrustworthy the data is secured in two ways as the data is split into multiple parts so it is not readable and the data is encrypted using Homomorphic encryption algorithm making it difficult to decipher it without key. Figure 5 shows generic flow of data in the proposed scheme.

6. PROPOSED SYSTEM ARCHITECTURE

In this section we are going to analyze our projected system model, which will allow information to be stored on multiple clouds transparently to the user. The system will consist of three major components:

- Trusted Authority
- MultiCloud
- Data users

In the proposed system Architecture, the data users are the entity which uploads data and participates in learning in the Cloud. Trusted Authority (TA) is responsible for user registration and authentication and stores user information on cloud data store. After login authentication when user wants to upload any file he requests to cloud to upload a specified file .The Cloud performs key generation and distributes the keys

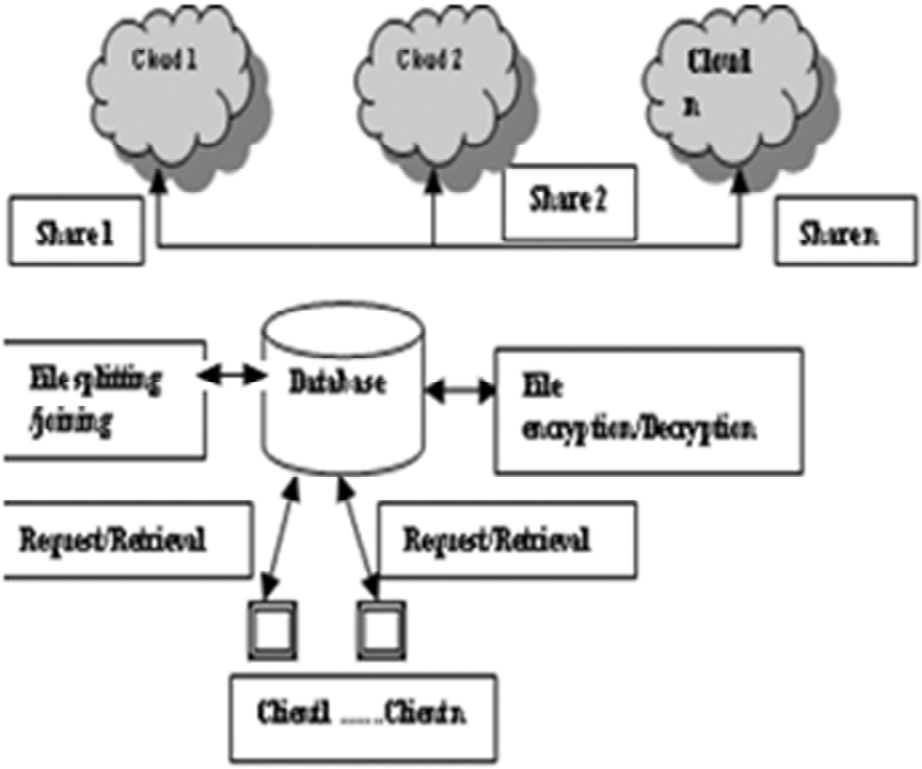

Figure 5: Generic Multicloud Data Flow

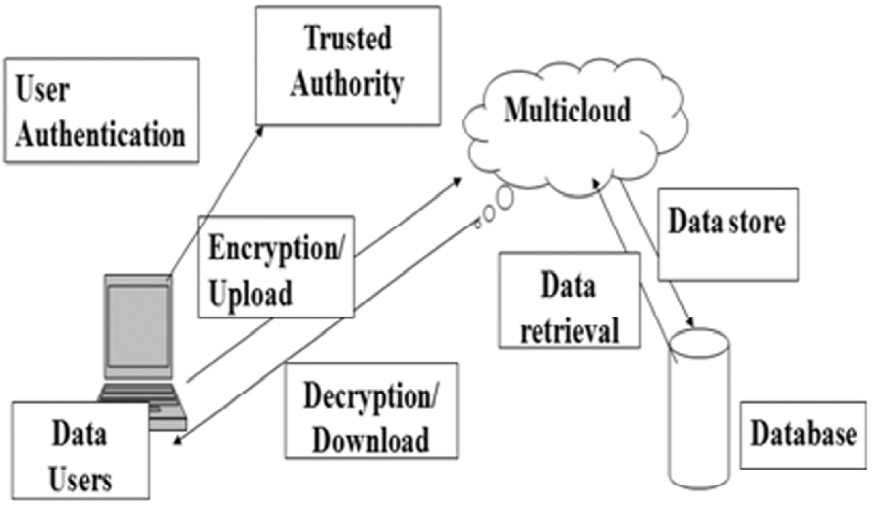

Figure 6: Proposed system Architecture

to the Owners. The datasets are arbitrarily partitioned using horizontal and vertical partitioning. The partitioning of data is done to improve scalability of learning and availability of the system. Then the partitioned dataset is encrypted using the encryption algorithm. Encrypted file and generated key are stored in the database. For encryption and decryption of data, basic homomorphic encryption scheme can be used along with database splitting. A key is sent to the user as an acknowledgement which is further used for downloading a file. When user wants to download his file, again he needs to specify a file name and key which is obtained in response while uploading a file. Artificial Intelligence technique verifies a key and corresponding file in database if it is validated. The cloud again decrypts the desired file with the help of key and sends back a decrypted file i.e. original file. Owner performs Artificial Intelligence technique Learning. After the learning, the output weights are updated in the Database. Figure 6 below shows the overall concept of the framework.

7. CONCLUSION AND FUTURE WORK

Cloud computing is the most recent development in online computing. Our research indicated that Security is considered to be major issue needed to be countered. This paper has addressed single cloud and multiclouds and mentioned why multicloud architecture has emerged as a solution to overcome the security issues in cloud computing. Multicloud model and approaches are explained using four relevant scenarios where the single cloud approach fails. Thus multiclouds are more efficient for storage as compared to single clouds. The proposed architecture aims to prevent the illegal data retrieval by hackers and intruders. For future use, the results and execution for the innovative projected representation shall be analyzed, in relation to addressing the security factors in cloud computing.

REFERENCES

[1] Low Tang Jung, “Hybrid Multi-Cloud data security(HMCDS) Model and Data Classification”,International Conference on Advanced Computer Science Applications and Technologies,DOI 10.1109/ACSAT.2013 IEEE

[2] Mandar Kadam, “Security Approach for Multiclouds Data Storage”, International Journal of Computer Applications”,Vol. 126 ,Issue 4 ,September 2015

[3] Jens-Matthias Bohli, Meiko Jensen, “Security and Privacy-Enhancing Multicloud Architecture”, IEEE Transactions on Dependable and secure Computing, Vol. 10, No. 4 July/August 2013.

[4] Passent M. El-Kafrawy,AzzaA Abdo, “Security issues over some Cloud Models”, International Conference on Communication, Management and Information Technology(ICCMIT), ScienceDirect, ELSEVIER, Procedia Computer Science 65, pp. 853-858 2015.

[5] Maha Tebaa, Said El Hajji, "Seure Cloud Computing through Homomorphic Encryption", International Conference on future Information Engineering, IERI procedia 10 pp,112-118 2014.

[6] P.Mell,T. Grance, "NIST Definition of Cloud Computing Version 15",National Institute of Standards and Technology,Information Technology Laboratory, p. 50.

[7] M Sulochana, "Preserving Data confidentiality using Multiclouds Architecture ",2nd International Symposium on Big data and Cloud computing(ISBCC'15),ELSEVIER, Procedia Computer Science 50 pp. 357-362 2015 .

[8] Lino Abraham Varghese, "Integrity verification in Muticloud Storage", Fifth International Conference on Advanced Computing, 978-1-4799-3448-5/13 IEEE 2013.

[9] Kiran baby, "Multicloud Architecture for Augmenting Security in Clouds", Global Conference on Communication Technologies, 978-1-4799-8533-1/15/$31.00 2015 IEEE.

[10] Gajendrasingh Chandel, "An Efficient and Secure Architecture for Data storage in Multiclouds", International Journal of Advance Foundation and Research in Computer (IJAFRC), Vol. 2 Issue 9 ISSN 2348-4853 September 2015.

[11] Neha Thakur, "A Secure Data Sharing in Public cloud using DES,RC4 and Diffie Hellman Algorithm", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 5 Issue 9 pp.281-284 September 2015.

[12] Isha Chawla, "Threeway Mechanism to enhance Data Security on Cloud", International Journal of Current Engineering and Scientific Research(IJCESR) ISSN 2393-8374 Vol.2 Issue 6 2015.

[13] Kamal Benzeki, "A Secure Cloud Computing Architecture using Homomorphic Encryption", International Journal of Advanced Computer Science and Applications (IJACSA) Vol. 7 Issue 2 2016 pp. 293-298.

[14] Hussain Aljafer, "A brief Overview and an experimental evaluation of data confidentiality measures on the cloud", Journal of Innovation in digital ecosystems,ELSEVIER pp:1-11 2014.

[15] Sowmiya Murthy, "Cryptograpic Secure Cloud Storage model with Anonymous Authentication and Automaticfile recovery", ICTACT Journal on Soft Computing,special Issue on Distributed Intelligent Systems and Applications,Vol. 5 Issue 1,ISSN:2229-6956 pp.844-849 Oct 2014.

[16] Tulsi Snehi, "Digital Signature to secure Data in cloud using Homomorphic Encryption technique", International Journal of Advance Engineering and Research development(IJAERD) ,ISSN:2348-4470 Vol. 3 Issue 5 pp. 429-433 May 2016.

[17] Rittinghouse John W., F. Ransome James: Cloud Computing: Implementation, Management, and Security. ISBN 9781439806807. CRC Press pp.154 (2009).

[18] Farrukh Shahzad, "State-of-the-art Survey on Cloud Computing Security Challenges,Approaches and Solutions",The 6th International Symposium on Applications of Adhoc and Sensor Networks(AASNET'14) doi:10.1016/j.procs.2014.08.053 Procedia Computer Science 37 ELSEVIER pp.357-362 2014.

[19] Keiko Hashizume, "An analysis of security issues for cloud computing", Journal of Internet Services and Applications,http://www.jisajournal.com/content/4/1/5 2013 SPRINGER.

[20] Antonio Celesti, "Adding long term availability,obfuscation, and encryption to multiclouds storage systems", Journal of Network and Computer Applications,http://dx.doi.org/10.1016/j.jnca.2014.09.021 ELSEVIER September 2014.