Abstract

Cloud computing is emerging field because of its performance, high availability, least cost and many others. In cloud computing, the data will be stored in storage provided by service providers. But still many business companies are not willing to adopt cloud computing technology due to lack of proper security control policy and weakness in safeguard which lead to many vulnerability in cloud computing. This paper has been written to focus on the problem of data security. Service providers must have a viable way to protect their clients’ data, especially to prevent the data from disclosure by unauthorized insiders. To ensure the security of users’ data in the cloud, we propose an effective and flexible scheme with two different algorithms. A user can access cloud services as a utility service and begin to use them almost instantly. These features that make cloud computing so flexible with the fact that services are accessible anywhere any time lead to several potential risks. The key intent of this research work is to investigate the existing security schemes and to ensure data confidentiality, integrity and authentication. In model RSA algorithm and DES algorithm cryptographic algorithms are adopted for the optimization of data security in cloud computing. These days encryption techniques which use large keys is seldom used for data encryption due to computational overhead. Their usage is restricted to transport of keys for symmetric key encryption and in signature schemes where data size is generally small. In the first section of the paper analysis the cloud computing Techniques and fundamental concept of multimedia cloud computing. In the second section of the paper analysis the related work of security terms of cloud computing. In the third section are discussed about proposed work of Security method of RSA and DES. In the fourth section described characteristics of multimedia cloud computing and in the fifth section analysis the RSA Algorithm & DES Algorithm. Finally present the Conclusion & future works with the references.

Keywords- Cloud Computing, RSA, DES, cryptography, encryption, decryption

1. INTRODUCTION

Cloud computing multimedia database is based on the current of database development, object-oriented technology and object-oriented fields in the database, which increasing display its vitality [1]. Cloud computing provides a computer user access to Information Technology (IT) services which contains applications, servers, data storage, without requiring an understanding of the technology. An analogy to an electricity computing grid is to be useful for cloud computing. To enabling convenient and on-demand network access to a shared pool of configurable computing resources are used for as a model of cloud computing. Cloud computing can be expressed as a combination of Software-as-a-Service which refers to a service delivery model to enabling used for business services of software interface and can be combined creating new business services delivered via flexible networks and Platform as a Service in which Cloud systems offering an additional abstraction level which supplying a virtualized infrastructure that can provide the software platform where systems should be run on and Infrastructure as a Service which Providers manage a large set of computing resources which is used for storing and processing capacity. Through Virtualization, they are able to split, assign and dynamically re-size these resources to build ad-hoc systems as demanded by customers [2].
Cloud computing is that emerging technology which is used for providing various computing and storage services over the Internet [3]. It generally incorporates infrastructure, platform, and software as services. These service providers rent data-center hardware and software to deliver storage and computing services through the Internet. Internet users can receive services from a cloud as if they were employing a super computer which is using cloud computing. To storing data in the cloud instead of on their own devices and it making ubiquitous data access possible. They can run their applications on much more powerful cloud computing platforms with software deployed in the cloud which mitigating the users’ burden of full software installation and continual upgrade on their local devices. Internet multimedia is emerging as a service with the development of Web 2.0. Multimedia computing has emerged as a noteworthy technology to generate, edit, process, and search media contents, such as images, video, audio, graphics, and so on which provide rich media services. For multimedia applications and services over the Internet and mobile wireless networks, there are strong demands for cloud computing because of the significant amount of computation required for serving millions of Internet or mobile users at the same time [4]. In new cloud-based multimedia-computing paradigm the users store and process their multimedia application data in the cloud in a distributed manner, eliminating full installation of the media application software on the users’ computer or device and thus alleviating the burden of multimedia software maintenance and upgrade as well as sparing the computation of user devices and saving the battery of mobile phones.

**Fig: 1 – Fundamental Concept of Multimedia Cloud Computing**

Multimedia processing in a cloud imposes great challenges. Several fundamental challenges for multimedia computing in the cloud are highlighted as follows[5].

1) **Multimedia and service heterogeneity:** The types of multimedia and services, such as voice over IP (VoIP), video conferencing, photo sharing and editing, multimedia streaming, image search, image-based rendering, video transcoding and adaptation, and multimedia content delivery, the cloud shall support different types of multimedia and multimedia services.

2) **QoS heterogeneity:** For different multimedia services different QoS requirements should be include and the cloud shall provide QoS provisioning which support for various types of multimedia services to meet different multimedia QoS requirements.

3) **Network heterogeneity:** The cloud shall adapt multimedia contents for optimal delivery to various types of devices with different network bandwidths and latencies which providing different networks, such as Internet, wireless local area network (LAN), and third generation wireless network, have different network characteristics, such as bandwidth, delay, and jitter.
4) Device heterogeneity: As different types of devices, such as TVs, personal computers (PCs), and mobile phones, have different capabilities for multimedia processing, the cloud shall have multimedia adaptation capability to fit different types of devices, including CPU, GPU, display, memory, storage, and power.

2. RELATED WORK
Multimedia file storage in cloud computing required the security. Multimedia cloud computing is termed as multimedia computing over grids, content delivery network (it is used for reduce the latency and increase the bandwidth of data), server-based computing, and P2P multimedia computing. It gives infrastructure of high-performance computing (HPC) aspect [6]. Desktop computing is Server-based multimedia computing addresses in which all multimedia computing is done in a set of servers, and the client interacts only with the servers [7]. Wenwu Zhu [8] is described the overview of multimedia cloud computing and it gives addressed multimedia cloud computing from multimedia-aware cloud. Multimedia-aware cloud presented how a cloud can provide QoS support, distributed parallel processing, storage, and load balancing for various multimedia applications and services. It proposed an MEC-computing architecture that can achieve high cloud QoS support for various multimedia services. On cloud aware multimedia, we addressed how multimedia services and applications, such as storage and sharing, authoring and mash up, adaptation and delivery, and rendering and retrieval, can optimally utilize cloud-computing resources. Jiann-Liang Chen [9] it proposed a novel IP Multimedia Subsystem (IMS) framework with cloud computing architecture for use in high quality multimedia applications. The IMS supports heterogeneous networking with Quality-of-Service (QoS) policy. Tamleek Ali [10] proposed a framework for the use of cloud computing for secure dissemination of protected multimedia content as well as documents and rich media. They have leveraged the UCON model for enforcing fine-grained continuous usage control constraints on objects residing in the cloud. Hang Yuan [11] provides a comprehensive overview of the techniques and approaches in the fields of energy efficiency for data centers and large-scale multimedia services. The paper also highlights important challenges in designing and maintaining green data centers and identifies some of the opportunities in offering green streaming service in cloud computing frameworks. Zhang Mian [12] presented the study that describes the cloud computing-based multimedia database and the different traditional database, object-oriented database model of the concept, discusses the cloud-based object-oriented multimedia database of two ways, and summarized the characteristics of such multimedia database model, superiority and development. Chun-Ting Huang [13] conduct a depth survey on recent multimedia storage security research activities in association with cloud computing. Neha Jain [14] presented a data security system in cloud computing using DES algorithm. This Cipher Block Chaining system is to be secure for clients and server. The security architecture of the system is designed by using DES cipher block chaining, which eliminates the fraud that occurs today with stolen data. Results in order to be secure the system the communication between modules is encrypted using symmetric key.

3 PROPOSED WORK
This is proposes a reference ontology framework for access control in a cloud to facilitate the design of security system and reduce the complexity of system design and implementation. This is exploits the possibility of RSA to support public-key cryptosystem and digital signatures. On the other hand, RSA and DES well defined as well as policy template in his specific domain is provided for reference [15]. To design an encryption algorithm based on combination on RSA and DES to have better security than RSA or DES alone to encrypt the data files before storage on cloud. It enhanced security and prevent replay attacks and then, the result of this security service can be delivered to the service model, and perform actions according to this security checking process. QoS provisioning and support for various types of multimedia services with different QoS requirements. The distributed parallel multimedia processing, and multimedia QoS adaptation to fit various types of devices and network bandwidth. In this section, we first present the architecture of the media cloud. Then we discuss the distributed parallel multimedia processing in the media cloud and how the cloud can provide QoS support for multimedia applications and services.

4. CHARACTERISTICS OF MULTIMEDIA CLOUD COMPUTING [16]
4.1 Large-Scability
The scale of cloud is very large and the cloud of Google has owned more than one million servers and service is given to infinite users. Even in Amazon, IBM, Microsoft, Yahoo, they have more than hundreds of thousands servers and they provide much good services.
4.2 Virtualization of cloud computing
Through any kind of interface the cloud computing makes user to get service anywhere and anytime. To complete all you want through net service using a computer or a mobile phone. Users can a use or share it safely through an easy way, anytime, anywhere. Users can complete a task quickly that can’t be completed in a single computer.

4.3 Good reliability
Cloud uses data with multiplicity, it has good fault tolerant, and the computation of cloud has very ability so it has high reliability of the service. The use of cloud computing is more reliable than local computer.

4.4 Versatility
Cloud computing can produce different applications which running it at the same time with accuracy and good productivity.

4.5 Extendibility
The scale of cloud can extend dynamically to meet the users to increasingly requirement and suggestions.

4.6. Service on demand
Cloud is a big resource pool that you can buy according to your requirement and specification. Cloud is just like running water, gas, and electric that can be charged by the amount which you used.

5. RSA ALGORIHM & DES ALGORITHM
The RSA algorithm implements a public-key cryptosystem and digital signatures. RSA is a block cipher in which every message is mapped to an integer. RSA consists of public-key and private-key [17]. In Cloud environment the Public-Key is known to all whereas private-key is known only to the user who originally owns the data. Thus, encryption is done by the Cloud service provider and decryption is done by the Cloud user or consumer. Once the data is encrypted with the Public-Key, it can be decrypted with the corresponding Private-Key only.

RSA algorithm involves three steps [18].
(i) First, in Key generation before the data is encrypted, Key generation should be done. This process is done between the Cloud service provider and the user.
(ii) Second, in Encryption is the process of converting original plain text (data) into cipher text (data).
(iii) Third, Decryption is the process of converting the cipher text (data) to the original plain text(data).

In the DES Algorithm there are two main types of cryptography.
(i) Symmetric key or secret key cryptography is the oldest type whereas asymmetric or public key cryptography is only being used publicly since the late 1970’s [19].
(ii) Asymmetric cryptography was a major milestone in the search for a perfect encryption scheme. Secret key cryptography goes back to at least Egyptian times and is of concern here. It involves the use of only one key which is used for both encryption and decryption.

Figure 2 depicts this idea. It is necessary for security purposes that the secret key never be revealed.

Secret Key (k) Secret Key (k)

Plaintext(P) → E_{p,k} → Ciphertext(C) → D_{c,k} → Plaintext(P)

Fig: 2Secret Key Encryption
To accomplish encryption the most secret key algorithms use two main techniques known as substitution and permutation. Substitution is simply a mapping of one value to another whereas permutation is a reordering of the bit positions for each of the inputs. These techniques are used a number of times in iterations called rounds. Generally, the more rounds there are, the more secure the algorithm. A non-linearity is also introduced into the encryption so that decryption will be computationally infeasible without the secret key. This is achieved with the use of S-boxes which are basically non-linear substitution tables where either the output is smaller than the input or vice versa. The DES algorithm is a basic building block for providing data security [20].

6. METHODOLOGY
When designing a solution to protect the data security and privacy, one needs to take into account the following three dimensions describe how data is used in subsection where data is located in subsection and how data is protected in distributed environments in subsection.

**STEP-1** First, pick any text file, audio or video and upload these in cloud computing work.  
**STEP-2** To encrypt text file, audio or video the cryptography RSA and DES algorithms to be used.  
**STEP-3** Create architecture categories for system process.  
**STEP-4** Image, file or video is shown at Azure Cloud Computing.

### 7. WINDOWS AZURE

#### 7.1 Windows Azure

Windows Azure is a foundation for running applications and storing data in the cloud [21]. Rather than providing software that Microsoft customers can install and run themselves on their own computers, Windows Azure today is a service that include customers use it to run applications and store data on Internet accessible machines owned by Microsoft. Those applications might provide services to businesses and to consumers or both [22]. Microsoft’s Windows Azure Platform is used for internet-scale cloud platform. Azure’s flexible and interoperable platform can be used to build new applications to run from the cloud or enhance existing applications with cloud based capabilities [23].

Windows Azure is a cloud service of operating system that serves as the development, service hosting and service management environment for the Windows Azure Platform. For example, physical hardware resources are abstracted away and exposed as compute resources ready to be consumed by cloud applications. Physical storage is abstracted with storage resources and exposed through well-defined storage interfaces.

#### 7.2 WINDOWS AZURE COMPONENTS

Windows Azure has five main parts: Compute, Storage, the Fabric Controller, the CDN, and Connect.

(i) **Compute:** Windows Azure compute can run many different kinds of applications. Whatever an application implemented as one or more roles. Windows Azure then typically runs multiple instances of each role, using built-in load balancing to spread requests across them [21].

(ii) **Storage:** The second component in Windows Azure is the storage that states how to store the different applications. We have three types that are Blobs which are like files, Tables, which are key-value-pair type storage, and Queue which let Web Roles and Worker Roles communicate to each other [22].

(iii) **Fabric Controller:** The third component in Windows Azure is the Fabric controller or Application Fabric. This component handles authentication and transport not only between Windows Azure applications, but even from servers [23].

(iv) **Content Delivery Network:** The CDN stores copies at sites closer to the clients that use it. The Windows Azure CDN actually has many more global caching locations than it shows, but the concept is correct.

(v) **Connect:** Running applications in the Microsoft cloud is useful but connecting to the on-premises environments with Windows Azure is important. Windows Azure Connect is designed to help do this. By providing IP-level connectivity between a Windows Azure application and machines running outside the Microsoft cloud, it can make this combination easier to use.

The following sections outline the documentation available for Windows Azure.

#### Local development environment

The Windows Azure SDKs for .NET, Node.js, Java, and PHP provide common tools and resources that you use to package, test and deploy your application. The following learning resources are available:

- Windows Azure SDK Tools
Windows Azure Tools for Visual Studio

Management Portal
- To learn more about the portal, see The Management Portal.
- To learn about managing hosted services, see Managing Hosted Services in Windows Azure.

Applications
Cloud Services, Web Sites, and Virtual Machines
You can run applications on Windows Azure using Windows Azure Web Sites, Cloud Services (formerly hosted services), and Virtual Machines (which support IaaS)
- Web Sites
- Cloud Services
- Virtual Machines

8. RESULT
This paper proposes a more effective and flexible distributed verification scheme to address the data storage security issue in cloud computing. As it rely on the cryptography algorithms [RSA] and [DES] to be used. These algorithms are used for protecting user data include encryption prior to storage, user authentication procedures prior to storage or retrieval and building secure channels for data transmission. This method achieves the availability, reliability and integrity of erasure coded data and simultaneously identifies misbehaving servers. There is a strong industry consensus that security, along with regulatory compliance is the barrier to the adoption of cloud computing. The needed breakthrough should mean customer’s data is always encrypted, and the master encryption keys are themselves encrypted, even when in use. The combination on RSA and DES of secret Key encryption and homomorphism technologies are the secret sauce. To encrypt large messages a hybrid approach is used in which the messages are actually encrypted using symmetric schemes (RSA, DES etc.) and the key is transported using asymmetric schemes (RSA). In the algorithm that has been proposed here the effort has been in the direction of faster public key encryption without compromising the security of the system.

References


