ISSN 2348 – 8034
Impact Factor- 3.155

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

SECURE CLOUD STORAGE SYSTEM BY USING OF ENCRYPTION AND DECRYPTION

Royyuru Srikanth[*1] & Dr S M Tiwari[2]
[*1]Research Scholar, Department Of CSE, University of C S M Kanpur
[2]Professor in CSE Department Of CSE, University of C S M Kanpur

ABSTRACT

As these days business data that needs to be stored and used (e-mail, personal health records, photo albums, tax documents, financial transactions, etc.) increases rapidly, data owners are encouraged. With cloud storage, consumers and businesses can use applications without installing them and access their personal files on any computer with internet access. In cloud storage, the stored data is stored by a cloud service provider (CSP). Cloud service providers need a viable way to protect their customer data, especially data against unauthorized access. However, protecting features for data backup and restoration is the most difficult and challenging task of cloud computing. In addition, the service provider must provide authentication to a valid user and the cloud system can fall. This document focuses primarily on centralized cloud storage services, such as Cryptography to provide cryptographic techniques for backing up and processing data in a cloud environment. Cryptography is a new security service in cloud computing for security and privacy in the cloud.

Keywords: *Network Security, Cloud Computing, Saas, Iaas, Paas, Encryption, Decryption.*

I. INTRODUCTION

PC computing is the biggest paradigm shift in IT life. These services are generally used in some computer enclosures. Technology has recently developed a technology for complex systems with many large-scale services for different users. Therefore, the authentication and integration of users and services for the trust and security of the unique cloud computing platform that reflects new security issues is a major problem. In fact, cloud computing is the management and delivery of applications, information and data as a service. These services are offered on the internet, often according to a model that is based on payment by you. Cloud computing is a convenient way to access IT services, regardless of the hardware you use or your physical location. This reduces the need to store information on your computer, mobile device or gadget, if you can access this information quickly and easily via the Internet. Cloud computing offers customers a virtual computer infrastructure with which they can store data and run applications. Cloud computing brings with it new security challenges because the customer of a cloud provider can be completely reliable. Cryptography depends on cloud computing on a secure cloud architecture shown in fig 1 The cluster computer is a computer model that is driven by economies of scale and distributed on a large scale. Cloud architectures are developed according to the most recent and urgent requests. In other words, the resources are made available dynamically to a user according to his request and are resumed upon completion of the work. The cloud computer is a service, including hardware and operating system, installation of system management software, systems and virtualisation platforms and components.

There are three main types of cloud services:

A. Software as a service (SaaS)
B. Service Platform (PaaS)
C. Infrastructure as a service (IaaS)

ISSN 2348 – 8034
Impact Factor- 3.155

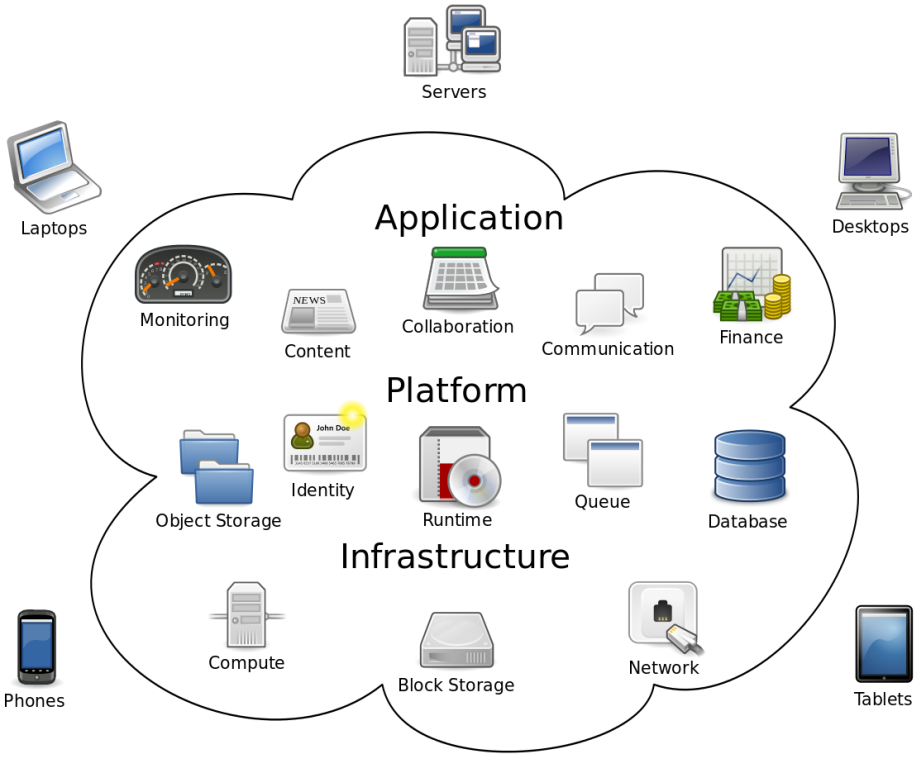

Fig:1 Cloud Computing

Software as a service (SaaS)

In the business model that uses software as a service (SaaS), users are placed on application software and databases in figure 2. Cloud service providers provide access to the infrastructure and platforms on which applications are running. SaaS is also called "software on demand" and the costs are usually paid for an affordable price and as a separate subscription. A software deployment model that allows a client application provider to be used as an on-demand service. Applications for different client devices are accessible via a thin client and a cloud interface, such as a web browser (for example, a web-based e-mail). SaaS stores the connection between machines and solutions so that customers can authorize those who need them. Business functions that require a high degree of integration with other institutional systems can lead to more interoperability problems. With SaaS, potential companies can reduce IT operating costs through outsourcing and software maintenance and cloud provider support. This allows the company to transfer the high costs of IT activities from hardware and software costs and staff costs to other important targets. Because applications are hosted centrally, updates can also be provided without them must install new software users. SaaS is that user data is stored on the server of the cloud provider. As a result, the data may have unauthorized access. For this reason, users use an intelligent and reliable third-party key management system to secure their data.

ISSN 2348 – 8034
Impact Factor- 3.155

Fig:2. Software as a Service [SaaS] Architecture

Platform as a Service (PaaS)

In the PaaS models, the 'cloud providers' computer platform, including the operating system, the runtime environment of the programming language, the web server and the database. In this model, the consumer develops applications for the cloud infrastructure using the programming languages and tools offered by the cloud provider in Fig 3.Application developers can develop and run their software on a cloud platform without having to purchase and manage the cost and complexity of the hardware and software layers behind the software. With some PaaS, the Windows Azure user, computer resources, and default storage must be automatically associated with the application so that the cloud user allocates resources manually. The architecture also recommended the second to enable real-time operations in cloud environments. The consumer does not apply to the management or control of the basic infrastructure of the cloud, including the network, servers, operating systems or storage. Users have complete control over the applications that have been implemented and can apply to environment configurations.

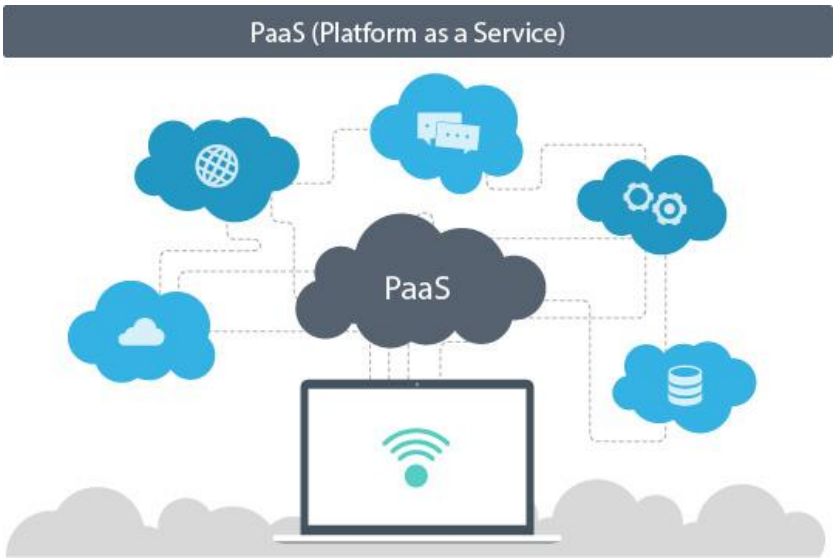

Fig:3. Paas Architecture

Infrastructure as a service (IaaS)

In this service model, the institution wants to use cloud services for the provision of all its infrastructure, including servers, storage, networks, etc shown in fig 4. With an external provider. This category of model is sometimes referred to as Hardware as a Service. In the most basic scam service model, IaaS providers offer users physical or virtual machines from computers and other sources. (Created hypervisor such as Hyper-V or Xen or KVM or VMware ESX / ESXi, virtual guest machines.) Supervisors of threads in the cloud support operating system can support a large number of virtual machines and the ability to scale up and down depending on the different needs of the customers.) The service provider has the equipment and is responsible for housing, operation and maintenance.

ISSN 2348 – 8034
Impact Factor- 3.155

The consumer does not have the basic cloud infrastructure to manage or control, but exercises control over operating systems, storage, implemented applications and possibly limited control is part of the network components, for example host firewalls. Cloud IaaS often include additional resources such as the actual image library, raw (block) and file-based storage device disks, chromatic memory, firewall, IP addresses, VLANs and bundles of software. Iaas cloud providers provide these resources at the request of large pools installed in data centres. For extensive connectivity, clients can use Internet clouds or an operator with special virtual networks.

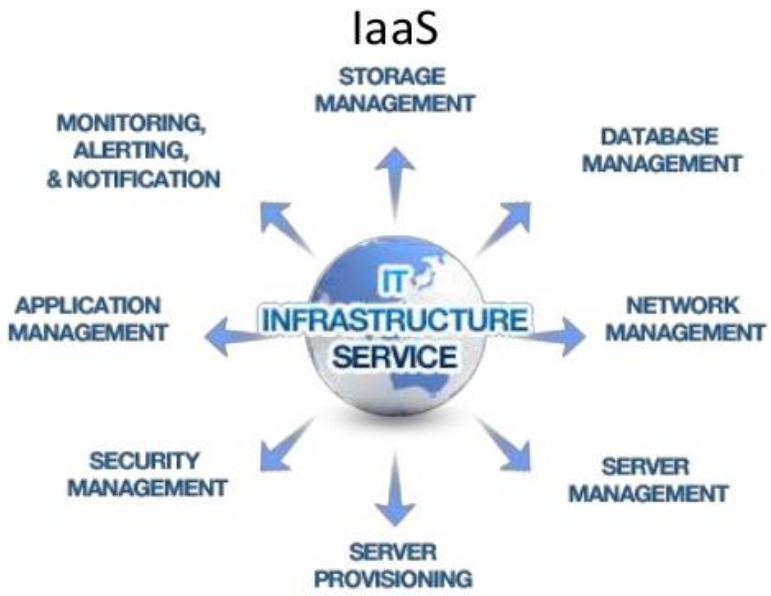

Fig:4. IAAS Architecture

II. SECURITY IN CLOUD COMPUTING

Security is still the biggest problem for IT managers when it comes to cloud computing and takes it. In two surveys conducted by IDC in 2008 and 2009 the following year, security followed the list. However, there is a combination of technologies, operating systems, storage, networks, real authentication, that address fundamental security issues shown in figure 5. For example, there have been browser attacks, Denial of Service attacks and behavioural risk networks in the life of computers. The benefits of using cloud computing are known and some of the above benefits are described. However, there is no cloud computing without a lack. Most of them are a data security centre that is stored in the cloud. There is room for a new wave of large-scale attacks on the virtualisation platform. Catted et al. Describes the 'fear of the cloud' by categorizing security problems into three traditional problems, the availability and control of data from third parties. Brunet's research firm presented seven safety risks on the data page and the separation of recovery and long-term sustainability. However, the security of customer data depends on a security service provided by cloud computing providers. However, independent operators offer the current structure of cloud computing services. The ISACA and Cloud Security Alliance organizations publish guidelines and best practices for mitigating cloud security issues [1920]. Initially, the information security of the user provides commerce and management.

ISSN 2348 – 8034
Impact Factor- 3.155

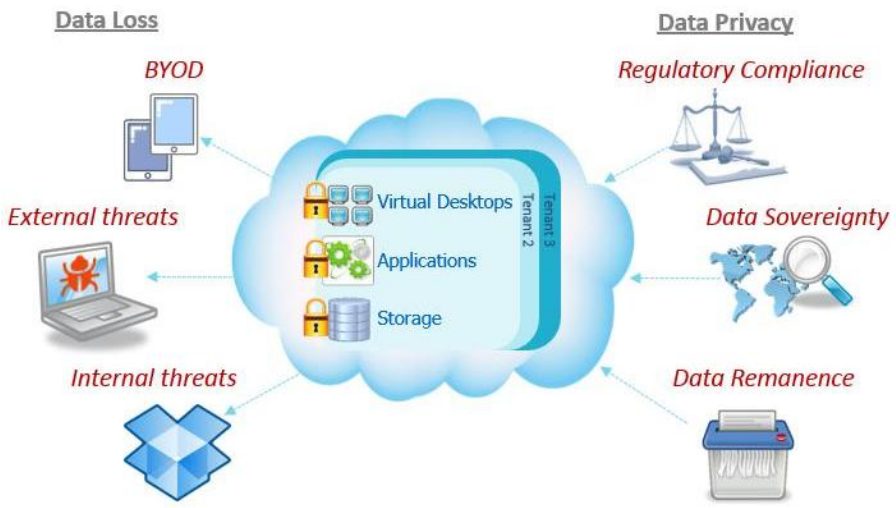

Fig:5 Security in Cloud computing

Cloud Encryption and Decryption

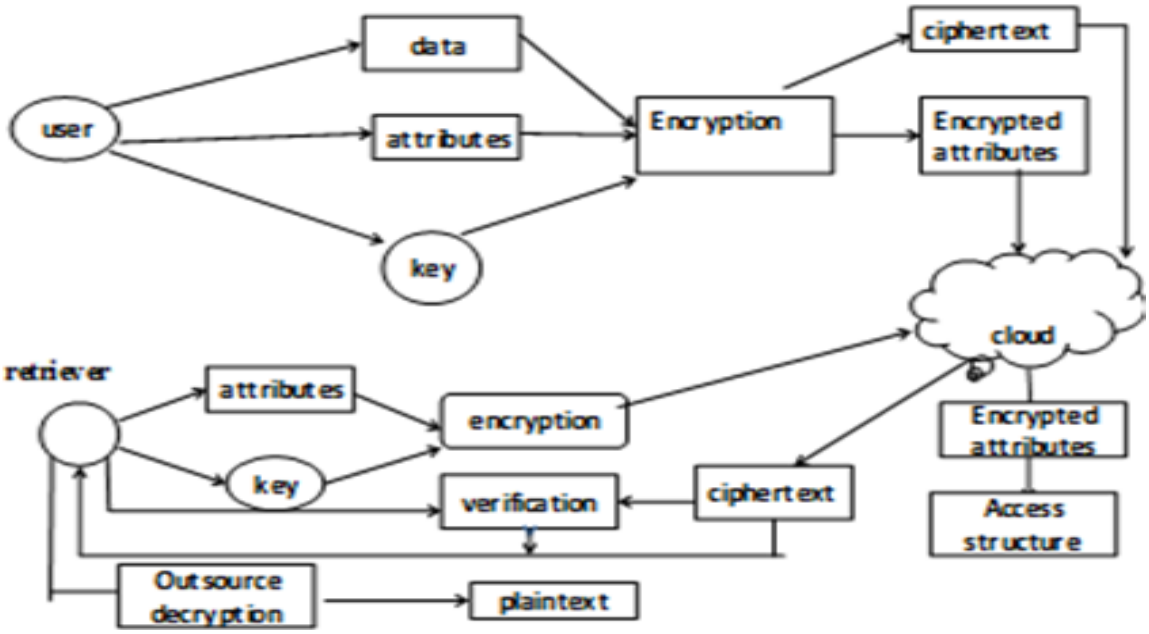

Fig:6. Cloud Encryption and Decryption Methodology

Cloud computing is a combination of IaaS, PaaS, SaaS. To secure cloud computing system to build, the security infrastructure, service platforms and application software must study levels for secure cloud computing system. Information encryption is one of the effective methods to achieve the security of cloud computing information. Traditionally, coding information focuses on specific steps and operations, such as data encryption. For cloud computing, system level design must be applied. Crypto cloud computing is a cloud computing architecture. Security of information security can be provided at system level and offers users easy and accurate access to shared services. Crypto cloud calculation protects individual connections with the outside world. Personal privacy can be protected without delay in the exchange of information. Crypto cloud computing is based on the Quantum Direct Key system. Quantum Direct Key (QDK) is a set of standard asymmetric mechanism. In this mechanism, look for all entities that are the key to public and private key based on their identity. Each entity does not have its own private key, but it has a public key generator to generate each public key. In this system, an entity with a public key can produce other entities offline, and no third-party entity (such as CA) is essential. Cloud computing enables QDK Crypto based on an overloaded network avoidance, and other disadvantages by using the existing encryption system. In the cloud computing system, all entities

ISSN 2348 – 8034
Impact Factor- 3.155

Encrypted data using its own private key. Each system has its own keys as cloud computing infrastructure, platform, virtualization tools and all related entities. While carrying out their function of information exchange and processing, the use of all elements of the public key and private key to verify the first time. The biggest events that occur in the cloud computer also get a unique key. That is why information and information security is secured thanks to a crypt cloud system.The current cloud computing structure for data and computer sharing has been developed. Security has no priority on the system. On the contrary, encryption and security are essentially integrated into cloud computing based on the QDK. The authorized functional units of QDK are bricks of cloud computing. In addition to the primary function of encryption / decryption data, encrypted cloud computing offers many security functions. For example, each data channel signals a transmission using their own keys and the receiving terminals can be avoided by verification. In addition, an accurate security leak site can be identified by analysing simulated digital data signatures. Based on the capabilities of such functions can be associated with crypts available as services in the cloud, which is called as "Crypto as a service (CAAS). Not only developments in information technology, which Crypto cloud Computation, but also the innovation of the relationship logically., in a system of cloud computing cloud, not allowed data stored and transmitted. Each data has its own key and public key offline, role identification and certification to a process of exchange of information. This way, establishes trust with the customer cloud. identification data depending on the logical trust or mutual needs and the logical relationship depends on the cloud customer.

Crypto Cloud Exporting Products

Crypto-cloud calculation is a new cyber framework based on sources. It protects security and data privacy. Well, in a cloud environment cloud computing guarantees the safety and integrity of information throughout the procedure. The cloud computing security management can be fulfilled by ownership of all aspects associated with the signatures. In addition, a user can use all of his resources to use his QDK key. There will be no personal privacy under existing cloud framework, as illustrated by Mark Zuckerberg, "The Age of Privacy is Over." [7] However, the development of cloud computing cloud, we can address the conflict between various privacy and security services It opens new perspectives for the development of technology about information sharing all of it shown in fig 7.

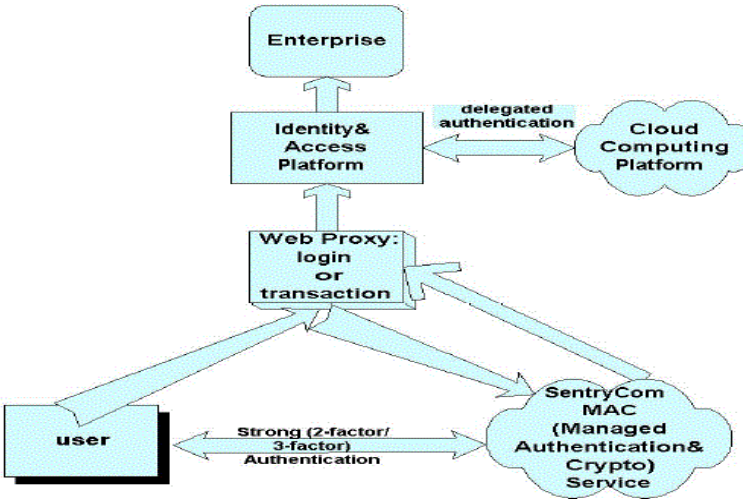

Fig:7 Cryptography in Cloud computing

III. CONCLUSION

Cloud computing technology is respected when areas such as data security are covered by the full evidence mechanism. The power of cloud computing lies in the ability to manage risks, especially with security problems. Our proposed model sketch will represent the architecture of architects involved in the application of cloud computing. The security algorithms mentioned for encryption and decryption and the resources available for accessing the multimedia content can be implemented in the future to improve the security framework on the network. In the future, we will investigate our research by providing an algorithm and achieving results for calculating our security concepts for cloud computing.In order to use this approach in the desired manner, the cloud service provider must work with the user to implement the solution. Some cloud service providers define their business models when they sell user data to advertisers. These providers are not willing to allow the user to use his applications in a way that protects the privacy of users.