IMPLEMENTATION OF STORAGE AS A SERVICE IN CLOUD INFRASTRUCTURE

Project Report submitted in partial fulfillment of the requirement for the degree of

Bachelor of Technology

In

Computer Science & Engineering

under the Supervision of

Prof. S.P. Ghrera

By

Pushpanjali Chauhan

To

Jaypee University of Information and Technology

Waknaghat, Solan – 173234, Himachal Pradesh

CERTIFICATE

This is to certify that project report entitled “Cloud Based Files and Document Management System”, submitted by Pushpanjali Chauhan in partial fulfillment for the award of degree of Bachelor of Technology in Computer Science & Engineering to Jaypee University of Information Technology, Waknaghat, Solan has been carried out under my supervision.

This work has not been submitted partially or fully to any other University or Institute for the award of this or any other degree or diploma.

Date:08/05/15 Prof. S.P. Ghrera

Head of Department

ACKNOWLEDGEMENT

This project work would not have been possible without the guidance and the help of several individuals who in one way or another contributed and extended their valuable assistance in the preparation and completion of this study.

First and foremost I offer my sincerest gratitude to my supervisor, Prof. S.P. Ghrera, who has supported me throughout my project work with his patience and knowledge whilst allowing me the room to work in my own way. I attribute the level of my Masters degree to his encouragement and effort and without him this thesis, too, would not have been completed or written. One simply could not wish for a better or friendlier supervisor.

The work was performed at Department of Computer Science and Engineering at the University, and I would like to thank all the people there for their hospitality and support.

I would also like to thank Mr. Hemraj Saini- for his unselfish and unfailing support as our course coordinator.

Last, but not the least, my family and the one above all of us, the omnipresent God.

Date:08/05/14 Pushpanjali Chauhan

TABLE OF CONTENT

LIST OF FIGURES

S.No. **Title** **Page No.**

LIST OF TABLES

ABSTRACT

Cloud computing is model that makes orientation to the two essential concepts: ‘abstraction’ and ‘virtualization’ to amplify the capacity and competence of IT by providing on demand network access to shared pool of computing resources without investing in new infrastructure. Cloud storage 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, and the physical environment protected and running. People and organizations buy or lease storage capacity from the providers to store user, organization, or application data. But as more and more information about enterprises are placed in cloud, concerns about how to secure the cloud environment to keep the data secure are also beginning to grow. In this work, study and implementation of cloud based on the service model storage as a service along with the security using multiple hash techniques is presented. File sharing is the digital process or automation of distributing or providing access to digital media, such as computer programs, multimedia (audio, images and video), documents or electronic books. File sharing may be achieved in a number of ways. Common methods of storage, transmission and dispersion include manual sharing utilizing removable media, centralized servers on computer networks, World Wide Web-based hyperlinked documents, and the use of distributed peer-to-peer networking. A file hosting service, cloud storage service, online file storage provider, or cyberlocker is an Internet hosting service specifically designed to host user files. It allows users to upload files that could then be accessed over the internet from a different computer, tablet, smart phone or other networked device, by the same user or possibly by other users, after a password or other authentication is provided. Typically, the services allow HTTP access, and sometimes FTP access. Related services are content-displaying hosting services (i.e. video & image), virtual storage, and remote backup. File syncing and sharing services are file hosting services which allow users to create special folders on each of their computers or mobile devices, which the service then synchronizes so that it appears to be the same folder regardless of which computer is used to view it. Files placed in this folder also are typically accessible through a website and online apps, and can be easily shared

with other users for viewing or collaboration. This work also concerned with the comparative study of attacks and different security issues arises due to the nature of cloud computing. In this work, we have developed the cloud based storage as a service scenario using which the files in multiple formats can be storage on remote cloud based server. The online collaboration system is developed and integrated for the sharing and distribution of cloud documents.

CHAPTER 1
INTRODUCTION

1.1 Cloud Computing

Cloud Computing has become one of the most talked about technologies in recent times and has got lots of attention from media as well as analysts because of the opportunities it is offering. The market research and analysis firm IDC suggests that the market for Cloud Computing services was $16billion in 2008 and will rise to $42billion/year by 2012. It has been estimated that the cost advantages of Cloud Computing to be three to five times for business applications and more than five times for consumer applications. According to a Gartner press release from June 2008, Cloud Computing will be “no less influential than e-business”.

“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, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”

Cloud computing is the collective term for a group of IT technologies which in collaboration are changing the landscape of how IT services are provided, accessed and paid for. Some of the supporting technologies have already been available for quite some time, but it is the combination of several technologies which enables a whole new way of using IT.

Cloud Computing is a term used to describe both a platform and type of application. As a platform it supplies, configures and reconfigures servers, while the servers can be physical machines or virtual machines. On the other hand, Cloud Computing describes applications that are extended to be accessible through the internet and for this purpose large data centers and powerful servers are used to host the web applications and web services.

The cloud is a metaphor for the Internet and is an abstraction for the complex infrastructure it conceals. There are some important points in the definition to be discussed regarding Cloud Computing. Cloud Computing differs from traditional computing paradigms as it is scalable, can be encapsulated as an abstract entity which provides different level of services to the clients, driven by economies of scale and the services are dynamically configurable.

To explain the definition in short, “convenient on-demand network access”, together with “minimal management effort or service provider interaction,” stands for easy and fast network access to resources that are ready to use. With a “shared pool of resources,” the available computing resources of a cloud provider are combined as one big collection, to serve all users. The “rapid provisioning and releasing” of computing resources is used to quickly match available resources, with the need for those resources. This rapid provisioning prevents a lack of computing power when the need increases, while rapid release of assigned resources prevents that resources are idle while they may be required elsewhere.

1.2 Evolution of Cloud Computing

The above definition is by no means exhaustive and it is very hard to find two experts having the same definition of cloud computing. Cloud computing is still an evolving paradigm. But to understand what cloud computing is and is not, it is important to understand that how this model of computing has evolved from previous computing paradigms, weather its’ really different or just progressive step in computing to solve the problems that are left unsolved from last three decades. According to historical perspective there are different phases in computing paradigms shift. Figure 1.1 shows the seven phases of computing paradigms, in phase 1 various users shared the powerful mainframe by using the terminal as an interface. In phase 2 stand- alone PCs become enough to fulfill the requirements of users without sharing the mainframe with any once else. In phase 3, computer network is used to share the resources by allowing the multiple computers, PCs, laptops and servers to connect to each other. Phase 4 allow the various local networks to connect with each other to form the global network called internet for remote application and resource sharing. As in computer networks the (CN), multiple computers are connected in two ways: wired and wireless network, in phase 5 wireless network give birth to mobile wireless computing which provide mobile users with ubiquitous communication capability and resource access regardless of its location. Phase 6 brought us the grid computing which provides the shared computing power and storage resources through distributed computing system. In phase seven, cloud computing exploits all available resources on the Internet in a scalable and simple way.

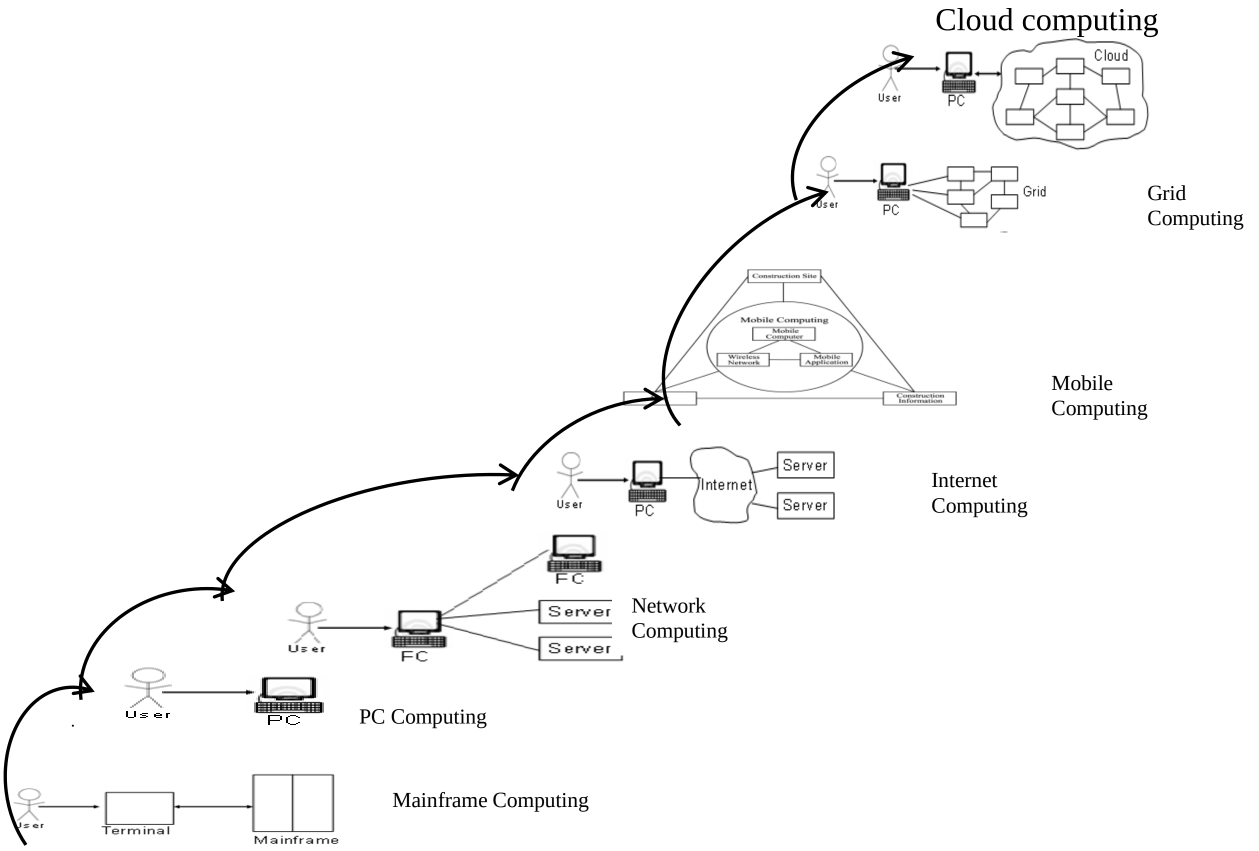


Figure 1.1: Seven computing paradigm shifts.

As with most new technologies and paradigms, one tends to look for the functionality first and only later on, one looks after the security of such functionality. However, cloud computing raises such an amount of questions concerning security guarantees that potential users are waiting for clear answers before moving into the cloud. Cloud computing users work with data and applications that are often located off-premise. Many organizations are uncomfortable with the idea of having their data and applications on systems they do not control. There is a lack of knowledge on how cloud computing impacts the confidentiality of data stored, processed and transmitted in cloud computing environments.

These definitions are based on five attributes that can be used to describe a cloud-based system. They are:

Multitenancy (shared resources): Unlike previous computing models, which assumed dedicated resources (i.e., computing facilities dedicated to a single user or owner), cloud computing is based on a business model in which resources are shared (i.e., multiple users use the same resource) at the network level, host level, and application level.
Scalability: cloud computing have property to scale to tens of thousands of system with bandwidth and storage also.

Elasticity: It is the property of increasing and decreasing the resources according to the users' need, as well as release the resources when they are no longer needed.
Pay as you go: One of the advantage of cloud computing is to pay according to the need or consumption like for one hour, two hour or cost per gigabyte and so on which has large impact on cost or economics. So cloud computing model provides a cheaper way for business to acquire and use the IT – capabilities.

Self provisioning of resources: Users self- provision resources like additional system and network resources.

Taking these features into account this thesis provides an encompassing definition of the Cloud. Obviously, the Cloud concept is still changing and these definitions show how the Cloud is conceived today:

"Cloud computing is model that makes reference to the two essential concepts: 'abstraction' and 'virtualization' to increase the capacity and capability of IT by providing on demand network access to shared pool of computing resources without investing in new infrastructure."

1.3 Cloud Computing Architecture

NIST (National Institute of Standards and Technology) is a well accepted institution all over the world for their work in the field of Information Technology. This thesis presents the working definition provided by NIST of Cloud Computing. NIST defines the Cloud Computing architecture by describing five essential characteristics, three cloud services models and four cloud deployment models.

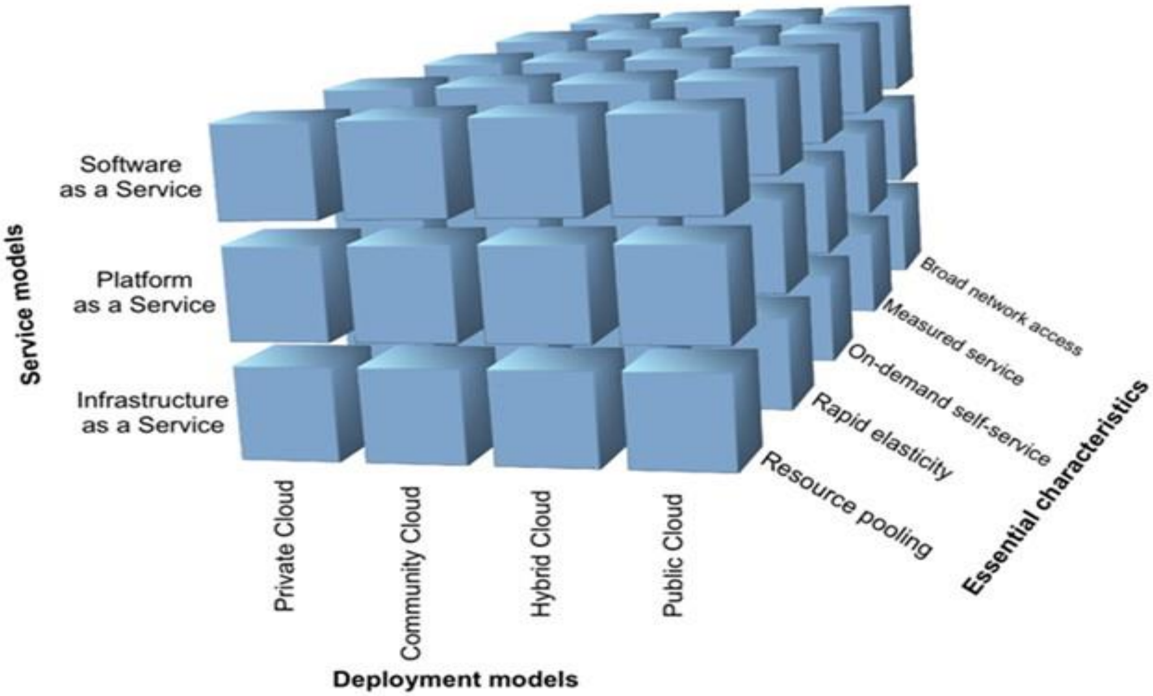


Figure 1.2 : Visual model of NIST Working Definition of Cloud Computing

1.4 Computing Service

One of the main tenets of Cloud Computing is the `as-a-Service' paradigm in which `some' service is offered by a Service Provider (also known as a Cloud Service Provider) to a User (consumer) for use. This service can also be categorised according to the application domain of its deployment. Examples of application domains that offer services are: Financial e.g. Mint.com, Managerial e.g. Ever Note and Analytical e.g. Google Analytics. The agreed terms of use, indicating the actions that must be taken by both the provider and consumer, are described in a contract that is agreed upon before service provision. Failure to honor this agreement can lead to denial of service for the consumer or legal liability for the service provider. This contract is often described as a Terms of Service or Service Level Agreement. Moreover, as part of this agreement the service provider will provide a Privacy Policy which outlines how the user's data will be stored, managed, used and protected.

1.5 Cloud Service Delivery Models

The services offered are often categorized using the SPI Service Model. This model represents the different layers/levels of service that can be offered to users by service providers over the different application domains and types of cloud available. Clouds can be used to provide as-a-Service: software to use, a platform to develop on, or an infrastructure to utilize.

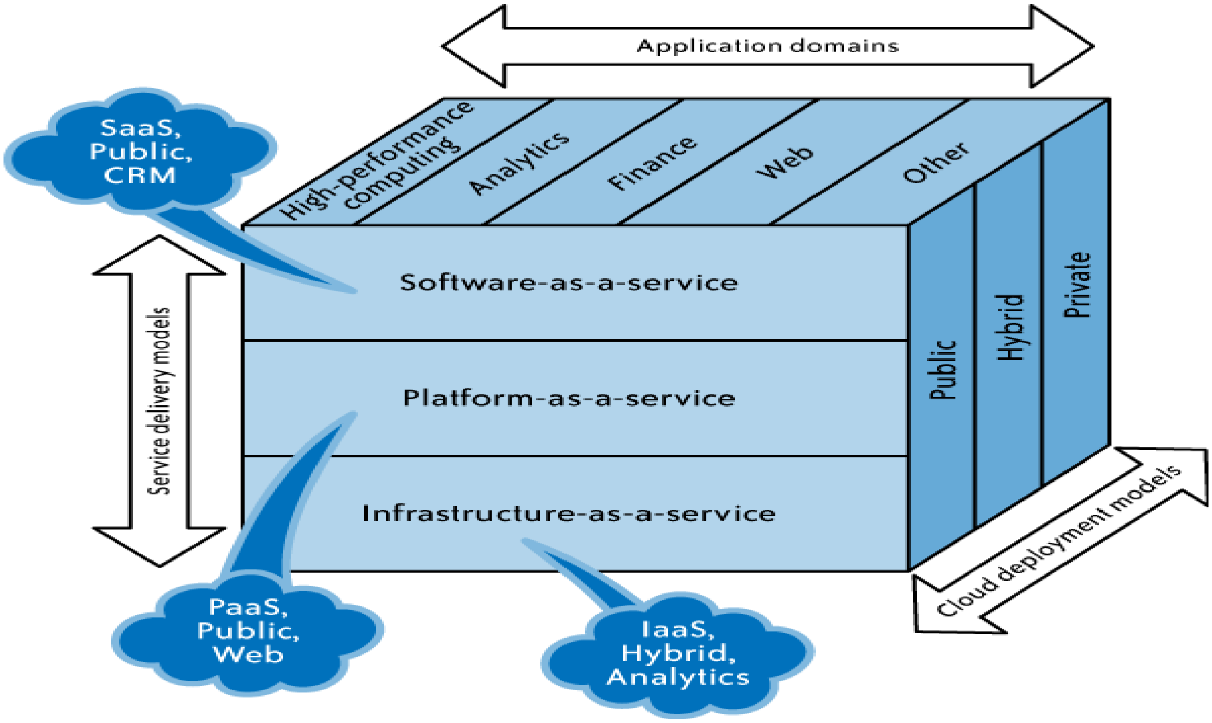
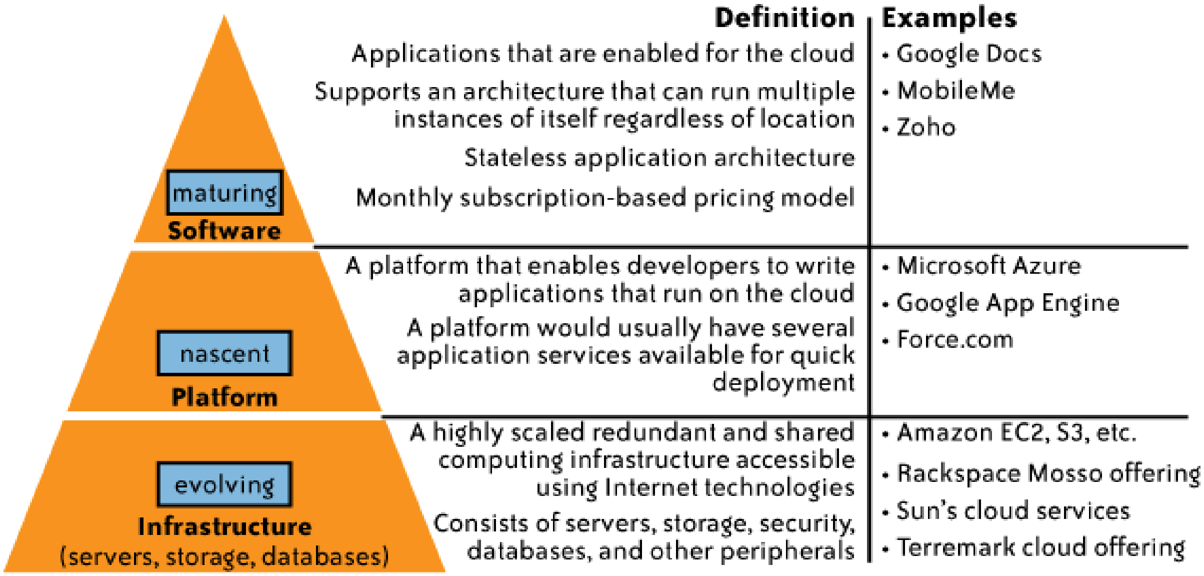


Figure 1.3: SPI service model

A cloud services delivery model is commonly referred to as an SPI and falls into three generally accepted services.


Definition
Examples
Applications that are enabled for the cloud
Supports an architecture that can run multiple instances of itself regardless of location
Stateless application architecture
Monthly subscription-based pricing model
• Google Docs
• MobileMe
• Zoho
maturing
Software
A platform that enables developers to write applications that run on the cloud
A platform would usually have several application services available for quick deployment
• Microsoft Azure
• Google App Engine
• Force.com
nascent
Platform
A highly scaled redundant and shared computing infrastructure accessible using Internet technologies
Consists of servers, storage, security, databases, and other peripherals
• Amazon EC2, S3, etc.
• Rackspace Mosso offering
• Sun's cloud services
• Terremark cloud offering
evolving
Infrastructure
(servers, storage, databases)

While cloud-based software services are maturing, cloud platform and infrastructure offerings are still in their early stages

Figure 1.4 Cloud services delivery model

1.6 The Software- As- a- Service Model

Conventional way of utilizing software involved the customer loading the software onto his own hardware after paying license fee (a capital expense, known as CapEx). For other support services the customer could also purchase a maintenance agreement. The customer was afraid with the compatibility of operational systems, patch installations, and compliance with license agreements.

In a SaaS model, there is no requirement for purchase software, but rather rents it for use on a pay as you grow model (an operational expense, known as OpEx). In some cases, the service is free for limited use. Typically, the purchased service is complete from a hardware, software, and support perspective. The user accesses the service through any authorized device

1.7 The Platform- As- a- Service Model

Pass is also a variation of SaaS model where the development environment is offered as a service. In PaaS solution the development tool is hosted in cloud which is accessed via browser and can built web applications without installing any tool on their own system and can then deploy those applications without any administrative skills.

1.8 The Infrastructure- As- a- Service Model

In the traditional hosted application model, the vendor provides the entire infrastructure for a customer to run his applications. Often, this entails housing dedicated hardware that is purchased or leased for that specific application where as IaaS model offers the various computing services as provided in utility computing. In this model we pay for the processing power, disk space and so on which is actually consumed by us. IaaS typical a service associated with cloud computing including physical computing resources, location, data partitioning, scaling, security, backup and so on. Examples are Amazon EC2, S3, suns' cloud services etc. Various features that should be available for IaaS system includes:

- Scalability: The ability to scale infrastructure requirement.
- Pay as you go: The ability to purchase the infrastructure required at any specific time.
- Best- of- breed technology: Ability to access the best suitable service and solutions for a fraction of cost

1.9 Cloud Deployment Models

In cloud computing environment, the most fundamental aspect is how services are delivered? Which mainly dependent on cloud deployment models (provides hosting environment). There are three primary types of cloud computing which are available to service consumer:

Public Clouds

A public cloud is hosted, operated, and managed by third party vendor from one or more data centers. The service is offered to multiple customers over common infrastructure. In a public cloud, security management and day- to- day operations are relegated to third party vendor, who is responsible for the public cloud service offering. Hence, the customer of the public cloud service offering has a low degree of control and oversight of the physical and logical security aspects of a private cloud. There are a few challenges listed below that are preventing wide scale adoption of public clouds.

- Security: The biggest roadblock is the potential security issues due to multitenant nature of public clouds. There are security and privacy concerns with sharing same physical hardware with unknown parties that need to addressed.

- Reliability and Performance: Performance and availability of the applications are important criteria defining the success of an enterprise's business. However, the fact that organizations lose control over IT environment and important success metrics like performance and reliability, and are dependent on factors outside the control of the IT organizations makes it dangerous for some mission critical applications.

- Vendor Lock-in: Cloud computing services offered by different vendors are not governed by any standards as of today. Depending on the vendor, the applications have to undergo changes to adapt to the service.

- Leveraging Existing Investment: Most large organizations that have already invested in their own data centers would see a need to leverage those investments as an important criterion in adopting cloud computing.

- Corporate Governance and Auditing: Performing governance and auditing activities with the corporate data abstracted in the public cloud poses challenges that are yet to be addressed.

- Maturity of the Solutions: Some of the PaaS offering like AppEngine offer limited capabilities like only a subset of JDO API.

Private Clouds

To overcome all above challenges enterprises adopt the private clouds which is managed or owned by an organization to provide the high level control over cloud services and infrastructure. In other words private cloud is build specifically to provide the services within an organization for maintaining the security and privacy. As such, a variety of private cloud patterns have emerged:

- Dedicated: Private cloud hosted within a customer- owned data center or at a collection facility, and operated by internal IT departments.
- Community: Private clouds located at the premises of third party; owned, managed, and operated by a vendor who is bound by customer SLAs and contractual clauses with security and compliance requirements.
- Managed: Private cloud infrastructure owned by customer and managed by a vendor.

Hybrid clouds

This model comprised both the private and public cloud models where organization might run non- core application in a public cloud, while maintaining core applications and sensitive data in- house in a private cloud.

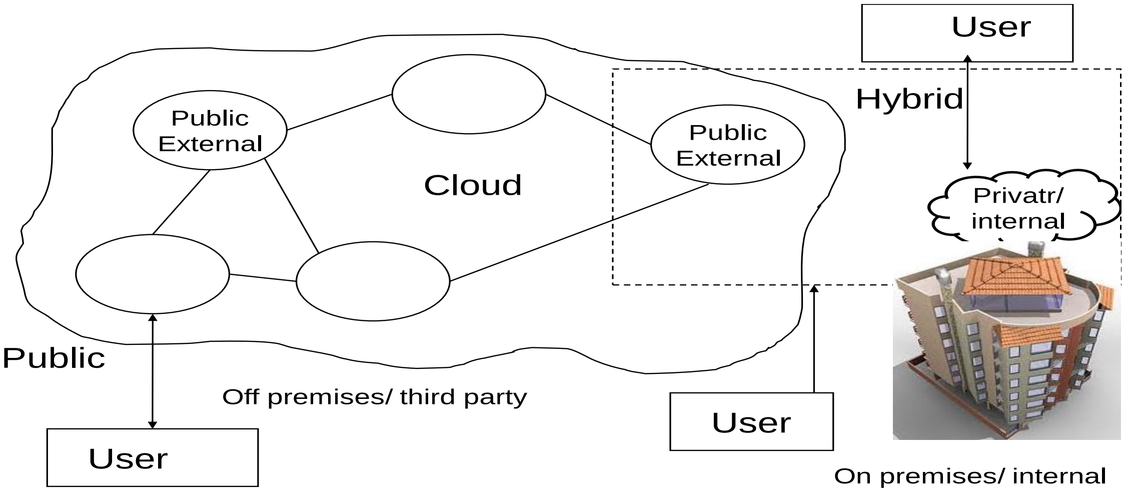


Figure 1.5: public, private, and Hybrid models of cloud

1.10 Relevant Technologies in Cloud Computing

Cloud computing isn’t so much technology as it is the combination of many pre-existing technologies. These technologies have matured at different rates and in different contexts, and were not designed as a coherent whole; however, they have come together to create a technical ecosystem for cloud computing. Key technologies that enabled cloud computing are described as follow; they include virtualization, Web service and service-oriented architecture, service flows and workflows, and Web 2.0 and mashup.

1.11 Cloud Access Devices

The range of access devices for the cloud has expanded in recent years. Home PCs, enterprise PCs, network computers, mobile phone devices, custom handheld devices, and custom static devices (including refrigerators) are all online. Interestingly, the growth of the iPhone and the Proliferation of applications available from its App Store illustrates an improvement in terms of access to the cloud. This greater access is resulting in greater use and growth of services within the cloud

1.12 Web Service and Service Oriented Architecture

Web Services and Service Oriented Architecture (SOA) are not new concepts; however they represent the base technologies for cloud computing. Cloud services are typically designed as Web services, which follow industry standards including WSDL, SOAP, and UDDI. A Service Oriented Architecture organizes and manages Web services inside clouds. A SOA also includes a set of cloud services, which are available on various distributed platforms. SOA and cloud computing are related, specifically, SOA is an architectural pattern that guides business solutions to create, organize and reuse its computing components, while cloud computing is a set of enabling technology that services a bigger, more flexible platform for enterprise to build their SOA solutions. In other words, SOA and cloud computing will coexist, complement, and support each other. There have been several initiatives at attempting bridging SOA and cloud computing but service oriented cloud computing architecture (SOCCA) is a 4-layer architecture that firstly supports both SOA and cloud computing and allow an application to run on different cloud and interoperate with each other. It supports easy application migration from one cloud to another and service redeployment to different clouds by separating the roles of service logic provider and service hosting/cloud provider. It promotes an open platform on which open standards, ontology are embraced.

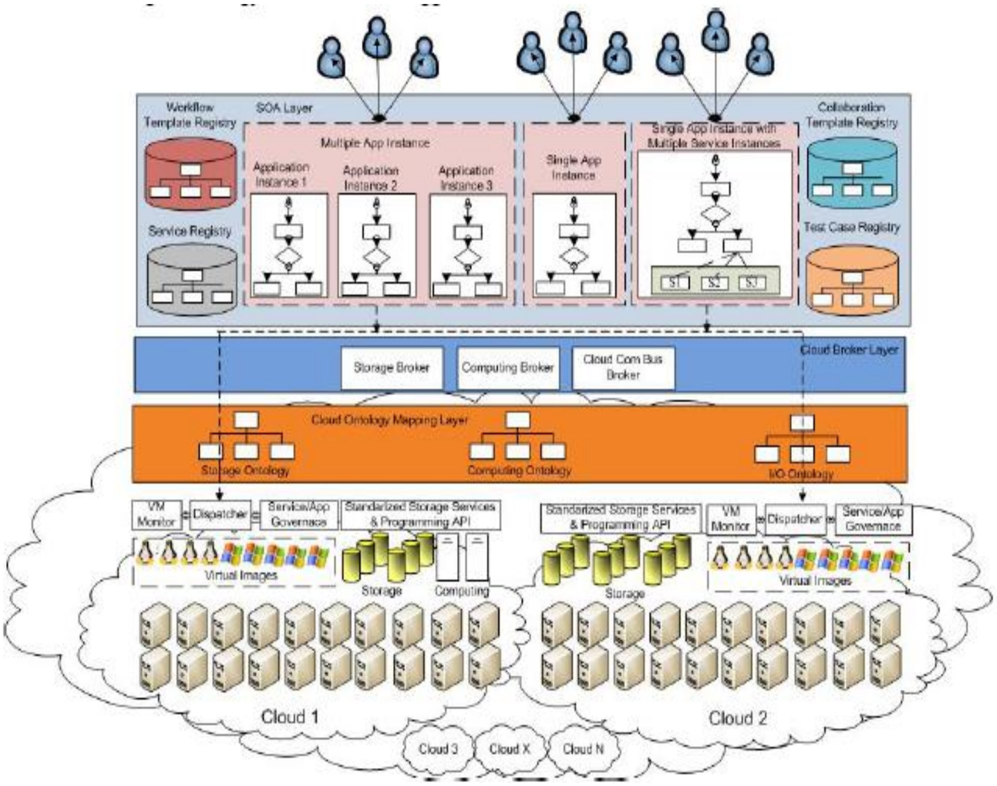


Figure 1.6 : service-oriented cloud computing architecture

1.13 Browsers and Thin Clients

Users of multiple device types can now access applications and information from wherever they can load a browser. Indeed, browsers are becoming increasingly sophisticated. Enterprise applications, such as SAP and Oracle, can be accessed through a browser interface—a change from when a client (a so-called “fat”) application needed to be loaded onto the desktop. The general population has become more familiar with the browser function and can use a discrete application, where the context is intuitive, without requiring training or user guides.

1.14 Virtualization

The advantage of cloud computing is the ability to virtualizes and share resources among different applications with the objective for better server utilization. Figure 2.6 shows an example. In non-cloud computing three independent platforms exist for three different applications running on its own server. In the cloud, servers can be shared, or virtualized, for operating systems and applications resulting in fewer servers (in specific example two servers). Virtualization technologies include virtual machine techniques such as VMware and Xen, and virtual networks, such as VPN. Virtual machines provide virtualized IT-infrastructures on-demand, while virtual networks support users with a customized network environment to access cloud resources.

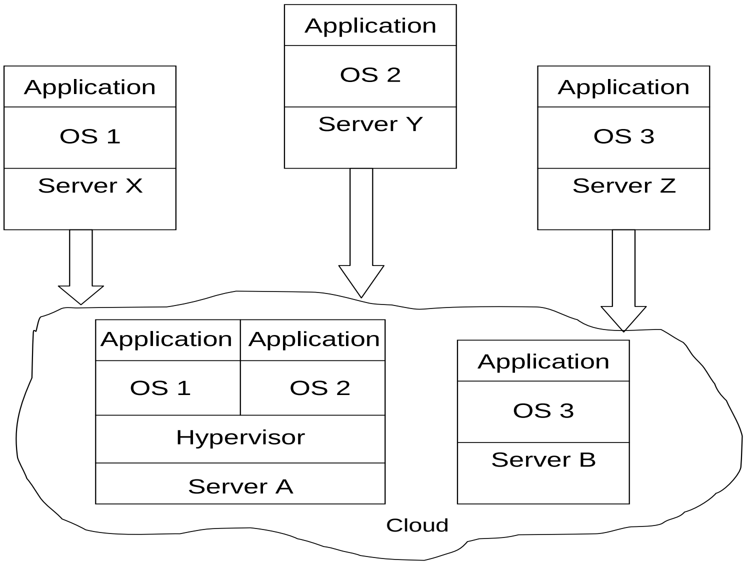


Figure 1.7 : An example of virtualization

- Service Flow and Workflows

The concept of service flow and workflow refers to an integrated view of service-based activities provided in clouds. Workflows have become one of the important areas of research in the field of database and information systems.

- Data centers and server farms

Cloud-based services require large computing capacity and are hosted in data centers and server farms. These distributed data centers and server farms span multiple locations and can be linked via internetworks providing distributed computing and service delivery capabilities. A number of examples today illustrate the flexibility and scalability of cloud computing power. For instance, Google has linked a very large number of inexpensive servers to provide tremendous flexibility and power. Amazon’s Elastic Compute Cloud (EC2) provides virtualization in the data center to create huge numbers of virtual instances for services being requested. Salesforce.com provides SaaS to its large customer base by grouping its customers into clusters to enable scalability and flexibility.

- High-speed Broadband Access

A critical component of the cloud is the broadband network, which offers the means to connect components and provides one of the substantial differences from the utility computing concept of 30 years ago. Broadband access is now widely available, especially in global metropolitan areas. Nearly pervasive wireless access (e.g., Wi-Fi, cellular, emerging WiMAX) is available, which has established mobile devices as entry points to the IT resources of the enterprise and the cloud.

- Web 2.0 and Mashup

Web 2.0 is a new concept that refers to the use of Web technology and Web design to enhance creativity, information sharing, and collaboration among users. On the other hand, Mash up is a web application that combines data from more than one source into a single integrated storage tool. Both technologies are very beneficial for cloud computing.

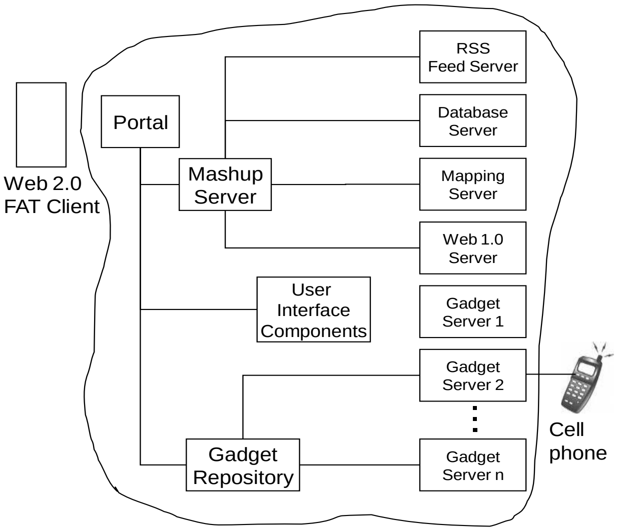


Figure 1.8: Cloud computing architecture uses various components at different levels

Figure 1.8 shows a cloud computing architecture, adapted from in which an application reuses various components. The components in this architecture are dynamic in nature, operate in a SaaS model, and leverage SOA. The components closer to the user are smaller in nature and more reusable. The components in the center contain aggregate and extend services via mash up servers and portals. Data from one service (such as addresses in a database) can be mashed up with mapping information (such as Yahoo or Google maps) to produce an aggregated view of the information

- Storage Devices

Decreasing storage costs and the flexibility with which storage can be deployed have changed the storage landscape. The fixed direct access storage device (DASD) has been replaced with storage area networks (SANs), which have reduced costs and allowed more flexibility in enterprise storage. SAN software manages integration of storage devices and can independently allocate storage space on demand across a number of devices.

1.15 Key Drivers to Adopting the Cloud

This section further articulates the cloud's impact on IT users. To compare client/server computing and cloud computing,

Table 1.2.Traditional IT v/s cloud computing: A customer's perspective

Traditional IT	Cloud Computing
High upfront IT investments for new builds	low upfront IT investments: pay- as –you grow model
High cost of reliable infrastructure	Reliable built into the cloud architecture
High complexity of IT environment	Modular IT architecture environments
Complex infrastructure	No infrastructure

The following subsection describe a number of reasons to move operations towards cloud computing.

- Economy of Scalability and on-demand services

Most development projects have a sizing phase during which one attempts to calculate the storage, processing power and memory requirements during development, testing, and production. It is often difficult to make accurate estimates; under- or overestimating these calculations is typical. The lead time for acquiring the equipment to support these estimates can sometimes be lengthy, thus adding to the time necessary to complete the project. With the flexibility that cloud computing solutions offer, companies can acquire computing and development services as needed and on demand, which means development projects are less at risk of missing deadlines and dealing with the unknown. Cloud computing provides resources and services for users on demand.

- Open standards

Some capabilities in cloud computing are based on open standards for building a modular architecture that can grow rapidly and can change when required. Open source software is defined as computer software that is governed by a software license in the public domain, or that meets the definition of open source, which allows users to use, change, and improve the software. Table 2.3 illustrates several of these open standards, which are currently used in cloud computing.

APPLICATIONS	Communications: HTTP, XMPP Security: OAuth, Open ID, SSL/TLS Syndication: Atom
CLIENT	Browsers: AJAX Offline:' HTML5
IMPLEMENTATIONS	Virtualization: OVF
PLATFORM	Solution stacks: LAMP
SERVICE	Data: XML, JSON Web services: REST

Table 1.3 - Cloud Computing Standards

- User-centric interface

Cloud interfaces are location independent and can be accesses by well established interfaces such as Web services and Internet browsers.

- Guaranteed Quality of Service (QoS)

Cloud computed can guarantee QoS for users in terms of hardware/CPU performance, bandwidth, and memory capacity.

- Autonomous system

The cloud computing systems are autonomous systems managed transparently to users. However, software and data inside clouds can be automatically reconfigured and consolidated to a simple platform depending on user's needs.

- Pricing

Cloud computing does not require up-from investment. No capital expenditure is required. Users pay for services and capacity as they need them. Pricing for cloud platforms and services is based on three key dimensions: (i) storage, (ii) bandwidth, and (iii) compute.

- Storage is typically measured as average daily amount of data stored in GB over a monthly period.

- Bandwidth is measured by calculating the total amount of data transferred in and out of platform service through transaction and batch processing. Generally, data transfer between services within the same platform is free in many platforms.

- Compute is measured as the time units needed to run an instance, or application, or machine to servicing requests. Table 2.4 compares pricing for three major cloud computing platforms.

Table 1.4: Pricing Comparison for Major Cloud Computing Platforms

RESOURCE	UNIT	Amazon	Google	Microsoft
Stored Data	GB per month	$0.10	$0.15	$0.15
Storage Transaction	Per 10K requests	$0.10	$0.10	$0.10
Outgoing Bandwidth	GB	$0.10 - $0.17	$0.12	$0.15
Incoming Bandwidth	GB	$0.10	$0.10	$0.10
Compute Time	Instance Hours	$0.10 - $1.20	$0.10	$0.12

1.16 Barriers to Cloud Computing Adoption in Enterprise

Though each cloud computing platform has its own strength, one thing should be noticed is that no matter what kind of platform there is lots unsolved issues. For example, continuously high availability, dealt mechanisms of cluster failure in cloud environment, consistency guaranty, synchronization in different clusters in cloud platform, interoperation and standardization, the security of cloud platform and data in transmission and so on are all among the issue to be better solved.

- Control

Some IT departments are concerned because cloud computing providers have a full control of the platforms. Cloud computing providers typically do not design platforms for specific companies and their business practices.

- Performance

The major issue in performance can be for some intensive transaction-oriented and other data-intensive applications, in which cloud computing may lack adequate performance. Also, users who are at a long distance from cloud providers may experience high latency and delays.

- Bandwidth Costs

With cloud computing, companies can save money on hardware and software; however they could incur higher network bandwidth charges. Bandwidth cost may be low for smaller Internet-based applications, which are not data intensive, but could significantly grow for data-intensive applications.

- Political Issues Due to Global Boundaries

In the cloud computing world, there is variability in terms of where the physical data resides, where processing takes place, and from where the data is accessed. Given this variability, different privacy rules and regulations may apply. Because of these varying rules and regulations, by definition politics becomes an element in the adoption of cloud computing, which is effectively multijurisdictional.

- Reliability

Cloud computing still does not always offer round-the-clock reliability. There were cases where cloud computing services suffered few-hours outages. In the future, we can expect more cloud computing providers, richer services, established standards, and best practices.

- Security

Because cloud computing represents a new computing model, there is a great deal of uncertainty about how security at all levels (e.g., network, host, application, and data levels) can be achieved. That uncertainty has consistently led information executives to state that security is their number one concern with cloud computing. The subsequent chapters present a detailed examination of those concerns to determine whether they are grounded.

- Privacy

The ability of cloud computing to adequately address privacy regulations has been called into question. Organizations today face numerous different requirements attempting to protect the privacy of individuals' information, and it is not clear (i.e., not yet established) whether the cloud computing model provides adequate protection of such information, or whether organizations will be found in violation of regulations because of this new model.

- Connectivity and Open Access

The full potential of cloud computing depends on the availability of high-speed access to all. Such connectivity, rather like electricity availability, globally opens the possibility for industry and a new range of consumer products. Connectivity and open access to computing power and information availability through the cloud promotes another era of industrialization and the need for more sophisticated consumer products.

- Interoperability

The interoperability and portability of information between private clouds and public clouds are critical enablers for broad adoption of cloud computing by the enterprise. Many companies have made considerable progress toward standardizing their processes, data, and systems through implementation of ERPs. This process has been enabled by scalable infrastructures to create single instances, or highly integrated connections between instances, to manage the consistency of master and transaction data and produce reliable consolidated information. Even with these improved platforms, the speed at which businesses change may still outpace the ability of IT organizations to respond to these changes. SaaS applications delivered through the cloud provide a low-capital, fast-deployment option. Depending on the application, it is critical to integrate with traditional applications that may be resident in a separate cloud or on traditional technology. The standard for interoperability is either an enabler or a barrier to interoperability, and permits maintenance of the integrity and consistency of a company's information and processes.

MOTIVATION

Cloud based document sharing systems transforms the way to share, manage and collaborate on the most valuable corporate files. Designed without compromise between security and ease-of-use, the application allows every user to securely work across teams, with customers and with partners — on any device, anywhere. The system as secure content platform to keep sensitive documents out of email and away from insecure consumer services.

The next-gen cloud-based content collaboration solution. Built for the enterprise with robust security, application integration and mobile enablement.

The cloud delivers convenience, and nothing is more convenient than synchronizing files stored on multiple computers and accessing those files from any PC, smartphone, or tablet with Internet access.

Similar Applications in Corporate Market

Box

Anyone can register an account with Box and begin using it for free, but to take advantage of its robust collaboration and security features, you must open a paid Business or Enterprise account starting at $15 per month, per user (minimum of three users). Paying unlocks a truckload of enhancements, including Google Apps integration and other tools that business users will find practical. The user-admin console, for example, lets an IT administrator add users and manage their settings in bulk.

Personal accounts of up to 5GB are free; if you need more space, Box offers 25GB for $10 per month and 50GB for $20 per month—that's the least bang for the buck among the five services in this category. With a Personal account, you can share your files with other people, with or without giving them editing privileges, and you can restrict sharing to collaborators only. Box also provides the option of restricting file previews or downloads, but you’re not allowed to set passwords or automatic expiration dates unless you have a paid account.

Dropbox

Simplicity is one of Dropbox’s greatest strengths. Install the service on your PC, and it plops a virtual folder on your desktop. The folder acts just as any other folder does, except that it automatically uploads and syncs the files that you put in it to your online account. Changes upload in real time, so you need never worry about working with an outdated file.

On a free account, you get only 2GB of storage. If you want more, you have to pony up for a paid account; prices range from $10 per month for 100GB to $50 per month for 500GB. Pestering your family and friends to open accounts will earn you a 500MB bonus per referral, up to an additional 16GB.

One great feature: Dropbox keeps a history of file changes, so you can roll back to a previous version at any time. And the tech-savvy can come up with a million and one creative ways to use Dropbox. For example, you might integrate it with a Bit Torrent client so that you can download torrent files remotely. First, set your Bit Torrent client on your home PC to monitor a folder on your Dropbox account and to automatically open any .torrent file copied to it. Then, while you’re at work or traveling, use your remote PC to copy the .torrent file to Dropbox, and your home PC will begin downloading that file the next time Dropbox syncs.

On the downside, when you share a folder, you can’t set a password or give some people permission to edit files while withholding permission from others. You also can’t upload files to your Dropbox account via email. If neither of those limitations is a deal breaker for you, Dropbox is a strong contender.

Media Fire

Unlimited storage and downloads sounds enticing—until you realize that MediaFire has little else to offer, at least to free users. If a free account becomes inactive, MediaFire will eventually delete the files associated with that account, but not before it makes several attempts to contact the user. (The $9-per-month Pro and $49-per-month Business accounts dispense with the disappearing act and hold on to files “forever.”)

The list of negatives is long. You can’t place restrictions on shared image files, no mobile apps are available, files aren’t encrypted in transit or in storage, and MediaFire doesn’t keep a history of changes. The final nail in the coffin: Users with a free account can’t upload files bigger than 200MB.

SkyDrive

Are you planning to subscribe to Microsoft’s Office 365 or buy Office 2013 when the new suites are available later this year? If so, SkyDrive is the file-sharing service for you. To use it, you must have a Windows Live account, and so must any colleagues you authorize to edit files (merely viewing shared documents does not require an account). SkyDrive allots 7GB of storage for free accounts, and you get 20GB more with either version of the Office suite. Even without that commitment, upgrades of 20GB to 100GB cost just $10 to $50 per year, not per month. That’s an incredible value.

Unfortunately, Microsoft has been paring down its service. SkyDrive’s free storage quota, for example, was once 25GB (existing customers were grandfathered into the original cap if they were using more than 4GB as of April 1, 2012, or if they took advantage of a Microsoft loyalty offer, which has since expired).

The company also zapped a feature that enabled users to publish their photos to SkyDrive through email. The iOS apps pick up the slack here (although the absence of Android support is annoying), but why take away a useful feature that’s already built?

SugarSync

As sweet as its name, SugarSync is like Dropbox with extra toppings. Rather than limiting file syncing to one virtual folder, SugarSync lets you sync any folder on your PC, including your Desktop folder. Obsessive-compulsive types will love SugarSync File

Manager’s ability to organize scattered files and folders from numerous synced devices into a single handy window on your desktop. You can also open a file stored on a remote computer, edit it, and save it back to that computer without consuming permanent storage space on the computer you’re using.

CHAPTER - 2
PRELIMINARIES AND BACKGROUND

Security and privacy are indeed interrelated because the security is provided without having privacy but the privacy is not maintained without security.

2.1 Overview

Today various small and medium size companies moved towards cloud environment because now they are capable to compete with the larger infrastructure companies by simply gaining fast access to best business application and drastically boost their infrastructure resources at negligible cost. While the cloud offers these advantages there are various issues and risks that reduce the growth of cloud computing. According to the recent IDC enterprise survey figure 3.1 shows 74% IT companies has to be taken security as a top challenge prevents the adoption of cloud services.

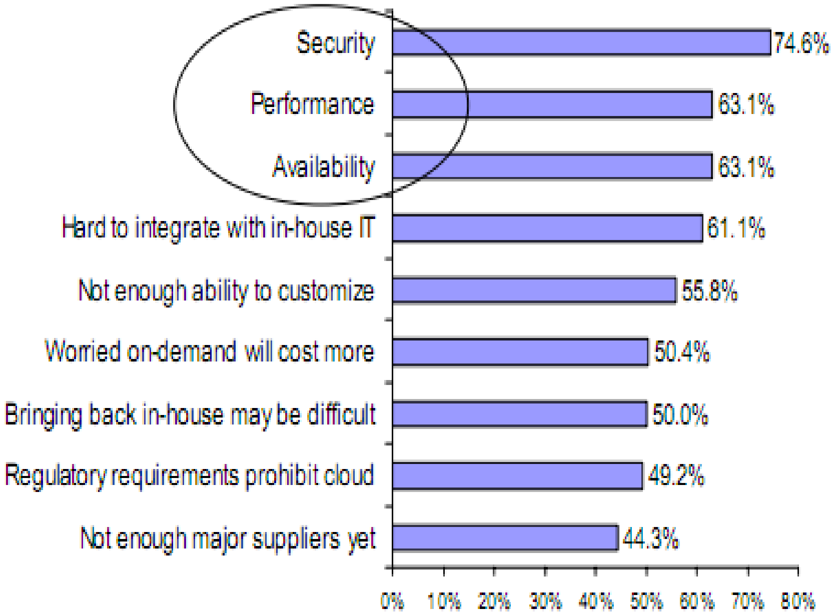
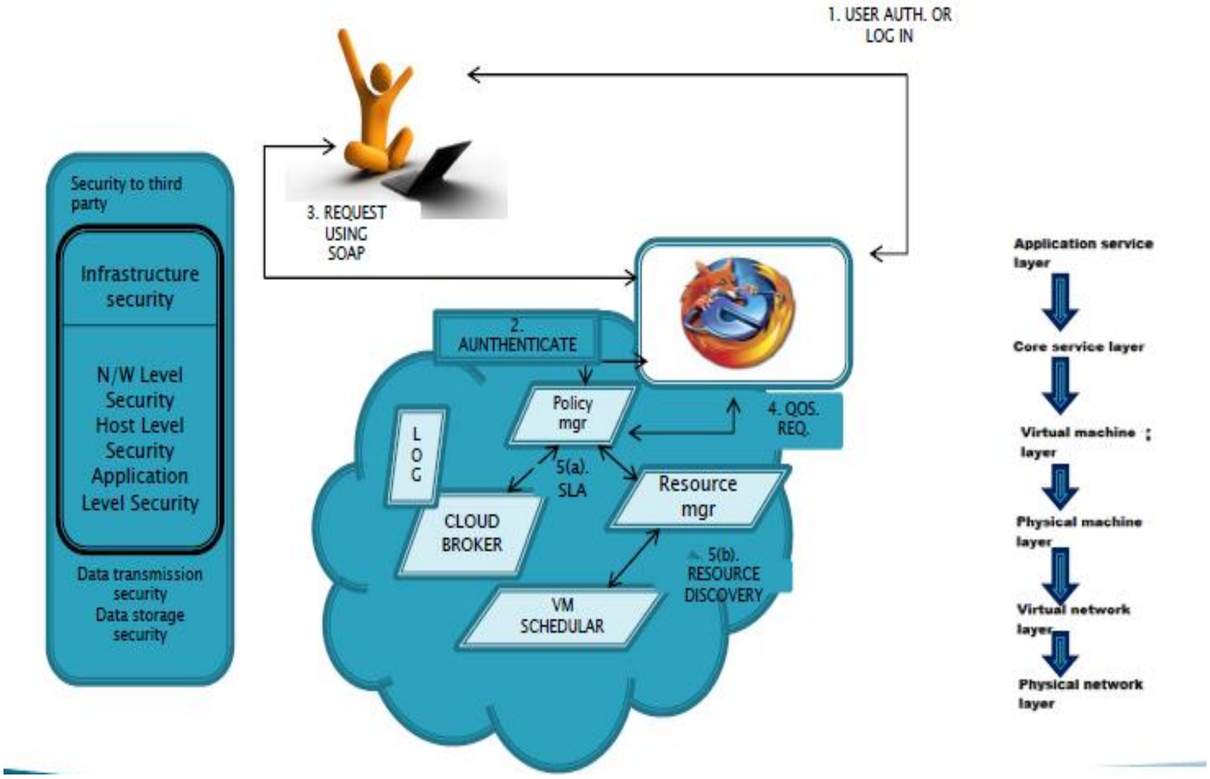


Figure 2.1 various issues/challenges to cloud model

2.2 Cloud Computing Model for Servicing to Consumers

For understanding the complexity of security aspects in cloud environment this thesis explains (figure 3.2) how the basic level communication is done between user and CSP for service providing and also describes the dependency among various layer of cloud that poses great impact on security risks.



Complexity of
dependency among security aspects
cloud layers

Figure 2.2: Cloud Computing Model for Servicing to Consumers

During communication process consumers are front end and cloud service providers are back end. For resource pooling various steps are included:

- User authentication and login process: In this web browser collects all necessary information about consumer using various security technologies/protocols like SSL/SSH/TLS.
- Web browser provides all information to policy manager which authenticate the consumer using public key infrastructure, certification authority and others.

- After that consumer request to browser for required services using Simple Object Access Protocol [XML or REST format + transfer protocols].
- Now web browser delegates the QOS requirements to policy manager, which evaluate the requirements according to service level agreement (SLA). For SLA policy manager also use cloud broker and resources engine.
- For resource discovery cloud broker collects the information about other cloud and their services and resource engine delegates the service requirement to VM schedulers which collaborates the required service from various VM / chunks provider.

Dependency among Cloud Layers - The application layer and core layer depends upon VMs layer and physical machine layer which further depend upon virtual network layer and physical network layer so damage at any layer also have great impact on other layers.

Complexity of Security Aspects - When we think about security of organization's core IT infrastructure there is need to provide security at network level, host level, application level and when we talk about data security two aspects are included 'data transmission security and data storage security'.

2.3 Cloud Security Issues

In cloud computing the Security issues deals with all the challenges associated with securing an organization's core IT infrastructure at the network, host, and application levels as well as the vulnerabilities and attacks related to the data security including: Data-in-transit, Data-at-rest, Processing of data including multitenancy, Data lineage, Data provenance. To cover all these security issues possible within the cloud, and in-depth, would be herculean task. Existing efforts look to provide a taxonomy over the issues seen. The Cloud Security Alliance is a non-profit organization that seeks to promote the best practices for providing security assurance within the cloud computing landscape. In Hubbard, Sutton et al. the Cloud Security Alliance identify seven threats to cloud computing that can be interpreted as a classification of security issues found within the cloud. They are:

- Abuse and Nefarious Use of Cloud Computing
- Insecure Application Programming Interfaces

- Malicious Insiders
- Shared Technology Vulnerabilities
- Data Loss/Leakage
- Account, Service and Traffic Hijacking
- Unknown Risk Profile

This thesis analyzed the various possible vulnerabilities and attacks that are caused because of above defined security issues found within cloud.

Analysis of Attacks and Vulnerabilities in Cloud Computing Environment

In traditional on premises deployment model the data of enterprise must resides within its boundary and follow their own access control and security policies. Whereas in cloud computing data reside at distributed data centers of cloud with the lack of control and without the knowledge of how their data resides. Due to the nature of cloud system there are many questions that arise as to weather a cloud is secure enough or not from various threats and vulnerabilities that are:

2.4 Network level attacks

During resource pooling process all data or services flow over the network needs to be secured from following attacks to prevent the leakage of sensitive information or other vulnerabilities:

- Denial of service/distributed denial of service attack

  This attack can overwhelm target's resources so that authorized user is abstained from getting the normal services of cloud. DDOS is also based on DOS attack which can be distributed for more significant effects. This attack is a cause of failure of availability.

- Eavesdropping

  Eavesdropping is an interception of network traffic to gain unauthorized access. It can results in failure of confidentiality.

- Man in the Middle attack

It is also a category of eavesdropping. The attack set up the connection with both victims that makes conversation and making them believe that they talk directly but infect the conversation between them is controlled by attack.

- Replay attack

The attacker intercepts and save the old messages and then send them later as one of participants to gain access to unauthorized resources.

- Back Door

The attacker gain access to network through bypassing the control mechanisms using "back door" such as modem and asynchronous external connections.

- Impersonation

It is vulnerability in which malicious node modify the data flow route and lure the node to wrong positions.

- Sybil attack

In Sybil attack a malicious user pretends to be distinct users after acquiring multiple identities and tries to create relationship with honest user if malicious user is successful to compromise one of the honest user then attack gain unauthorized privileges that helps in attacking process.

- Byzantine failure

It is a malicious activity which compromised a server or a set of server to degrade the performance of cloud.

2.5 Language and Malicious Program Injection Based Attack:

One of the most frequently discovered vulnerabilities in cloud are a direct result of language and programmes that are as follow.

- Buffer overflow

It is a favorite exploit for hacker which takes the advantage of programme that is waiting for user's input. But in place of user the hacker would enter the input which results to move the control to attack code.

- Trojan horses/Malware

They are the unauthorized program that are contained or injected by malicious user within legitimate program to perform unknown and unwanted function.

- XML Signature wrapping Attack

It is well known attack on protocols like SOAP that use XML format to transfer the request for services. In this, attack moves the original body of SOAP message to newly inserted wrapping element writing within SOAP header and create a new body which contains the operation that an attack wants to perform.

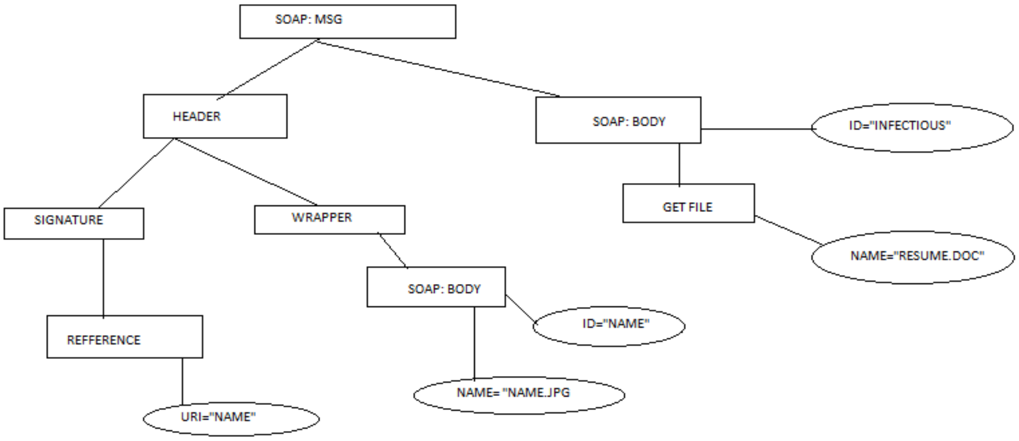


Figure 2.3 Example of SOAP message after attack

CHAPTER 3

PROPOSED WORK

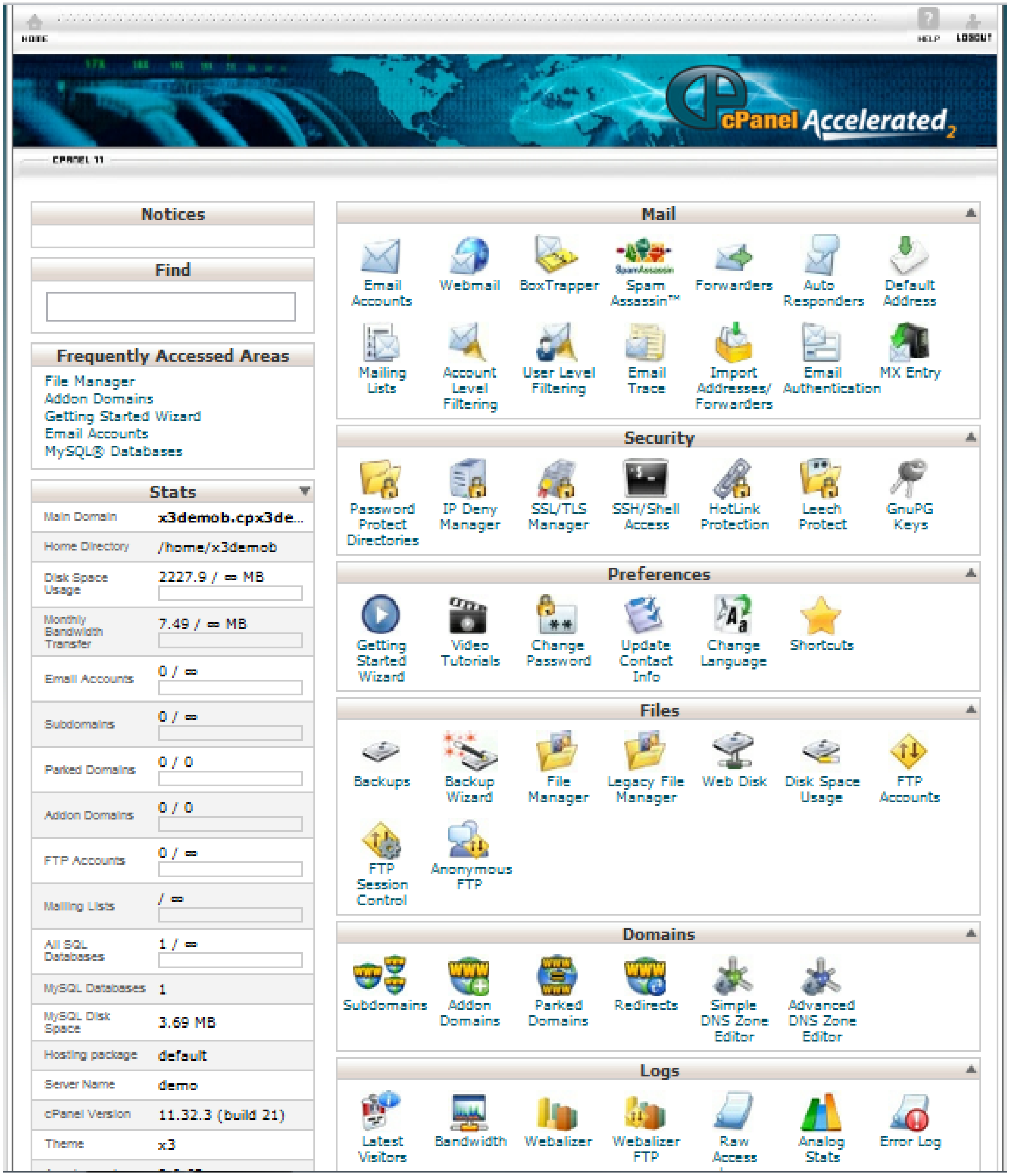
For implementation purpose, the creation of real-time cloud environment is possible only because of cloud computing service delivery models (i.e. Software as a service)

A data owner centric three-tier privacy aware cloud computing model is implemented in real-time cloud environment. Where the real time cloud environment is created using PHP enabled cloud hosting configuration. The rest of the chapter is organized as follows. Section 8.2 defines the requirements specification or tools used during implementation. In section 8.3 the design framework for implementation is described and results are evaluated. Finally section 8.4 concludes the chapter.

For implementation purpose this thesis takes the advantage of 'pay-as-you-grow' feature and 'platform-as-a-service' facility provided by cloud. The implementation of three-tier privacy aware cloud computing model is done in real-time cloud environment which is created using a website hosting platform. The cloud service provider offers the website hosting platform according to pay-per- use strategy and by using the platform as a service model. The cloud hosting platform has following configuration:

1. Apache version	2.2.17
2. PHP version	5.3.10
3. MySQL version	5.0.92-community-log
4. Architecture	x86_64
5. Operating system	Linux
6. Path to send mail	/usr/sbin/sendmail
7. Path to Perl	/usr/bin/perl
8. Perl version	5.8.8
9. Kernel version	2.6.18-194.32.1.el5
10. cPanel Pro	1.0 (RC1)

For providing all the services the Cloud service providers utilize the cPanel which is a web based control panel tool and helps to manage web hosting account through a web interface instead of a console. With cPanel it is possible to accomplish the tasks faster and even non-professionals can easily set their websites via cPanel as described in figure



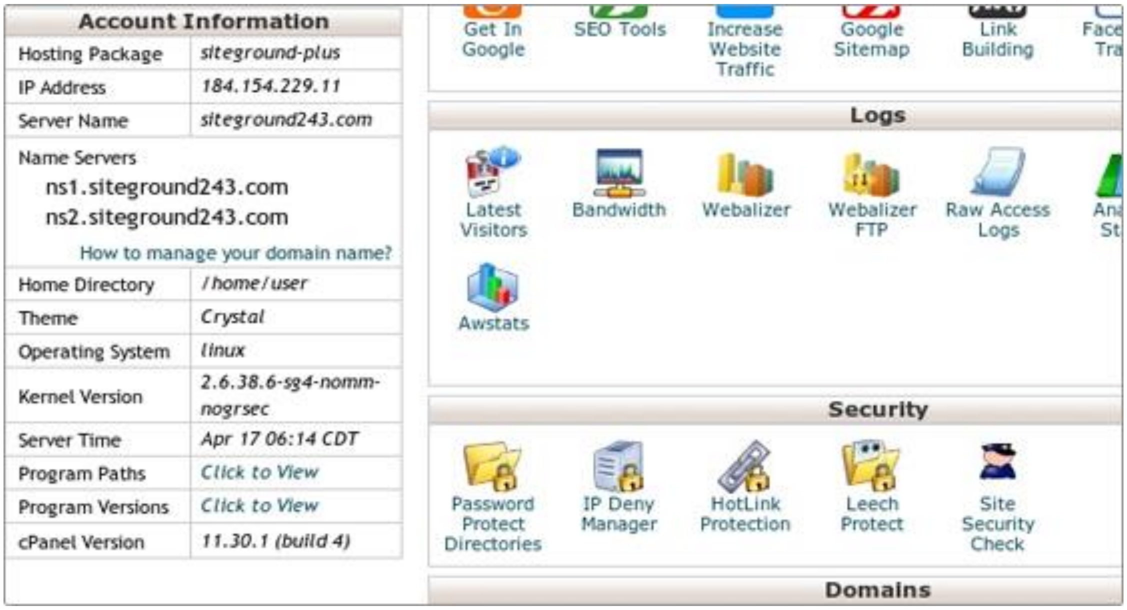
Main Domain	x3demob.cpx3de...
Home Directory	/home/x3demob
Disk Space Usage	2227.9 / ∞ MB
Monthly Bandwidth Transfer	7.49 / ∞ MB
Email Accounts	0 / ∞
Subdomains	0 / ∞
Parked Domains	0 / 0
Addon Domains	0 / 0
FTP Accounts	0 / ∞
Mailing Lists	/ ∞
All SQL Databases	1 / ∞
MySQL Databases	1
MySQL Disk Space	3.69 MB
Hosting package	default
Server Name	demo
cPanel Version	11.32.3 (build 21)
Theme	x3

Figure 3.1 General view of cPanel

For implementation of proposed model this thesis concerns only with account info or stats and file section of cPanel.

3.1 Online Web Space and Cloud Based Account Information

The Account Information section is located on the down left part of the cPanel main page.
There you can find important information about your hosting account (see figure 8.2) .

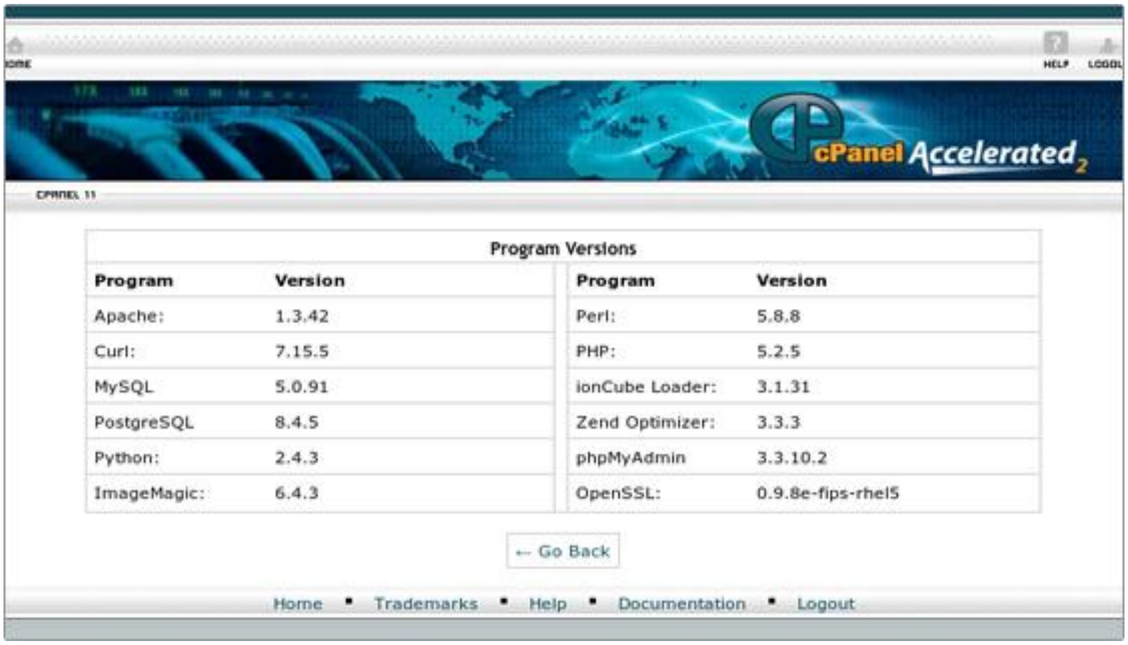


Account Information	
Hosting Package	siteground-plus
IP Address	184.154.229.11
Server Name	siteground243.com
Name Servers ns1.siteground243.com ns2.siteground243.com How to manage your domain name?	
Home Directory	/home/user
Theme	Crystal
Operating System	linux
Kernel Version	2.6.38.6-sg4-nomm-nogrsec
Server Time	Apr 17 06:14 CDT
Program Paths	Click to View
Program Versions	Click to View
cPanel Version	11.30.1 (build 4)

The details are as follows:

- Hosting Package - Shows the name of your hosting account package.
- IP Address - Shows the main IP address of the server where your account is hosted. If you have a Dedicated IP address set for your account, it will be listed in this field.
- Server Name - Shows the hostname of the server where your account is hosted.
- Name Servers - Shows the name servers (NS records) of the SiteGround server where your account is hosted.
- Home Directory - This is the absolute path to your account's home directory.
- Theme - Shows the theme for the cPanel software.
- Operating System - Shows the OS set on your hosting server.

- Server Time - Shows the server time including the corresponding time zone.
- Program Paths - Shows the paths to your home and web root folders and to programs which are essential for your web site functionality.
  ImageMagick /usr/local/bin/convert
  Perl /usr/local/bin/perl
  Python /usr/bin/python
  Sendmail /usr/sbin/sendmail
  OpenSSL /usr/bin/openssl
  Aspell /usr/bin/aspell
  curl /usr/bin/curl
- Program Versions - Shows the current versions of the most important programs installed on the server which hosts your account, as seen in figure 8.3.



Program Versions

Program	Version	Program	Version
Apache:	1.3.42	Perl:	5.8.8
Curl:	7.15.5	PHP:	5.2.5
MySQL	5.0.91	ionCube Loader:	3.1.31
PostgreSQL	8.4.5	Zend Optimizer:	3.3.3
Python:	2.4.3	phpMyAdmin	3.3.10.2
ImageMagic:	6.4.3	OpenSSL:	0.9.8e-fips-rhel5

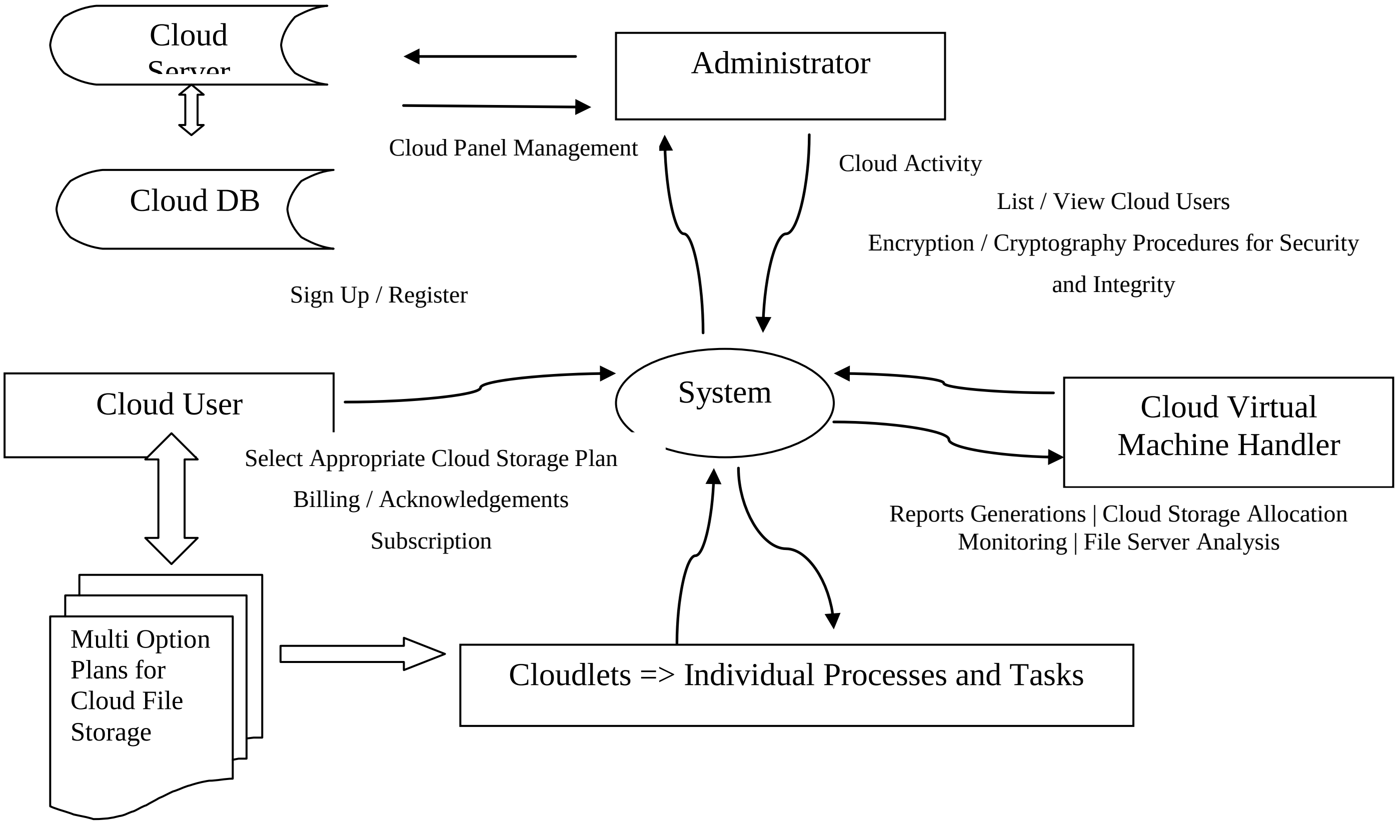
- cPanel Version - Shows the current cPanel version.

- PHP was at first created as a simple scripting platform called "Personal Home Page". Nowadays PHP (the short for Hypertext Preprocessor) is an alternative of the Microsoft's Active Server Pages (ASP) technology. PHP is an open source server-side language which is used for creating dynamic web pages. It can be embedded into HTML. PHP is usually used in conjunction with a MySQL database on Linux/UNIX web servers. It is probably the most popular scripting language.

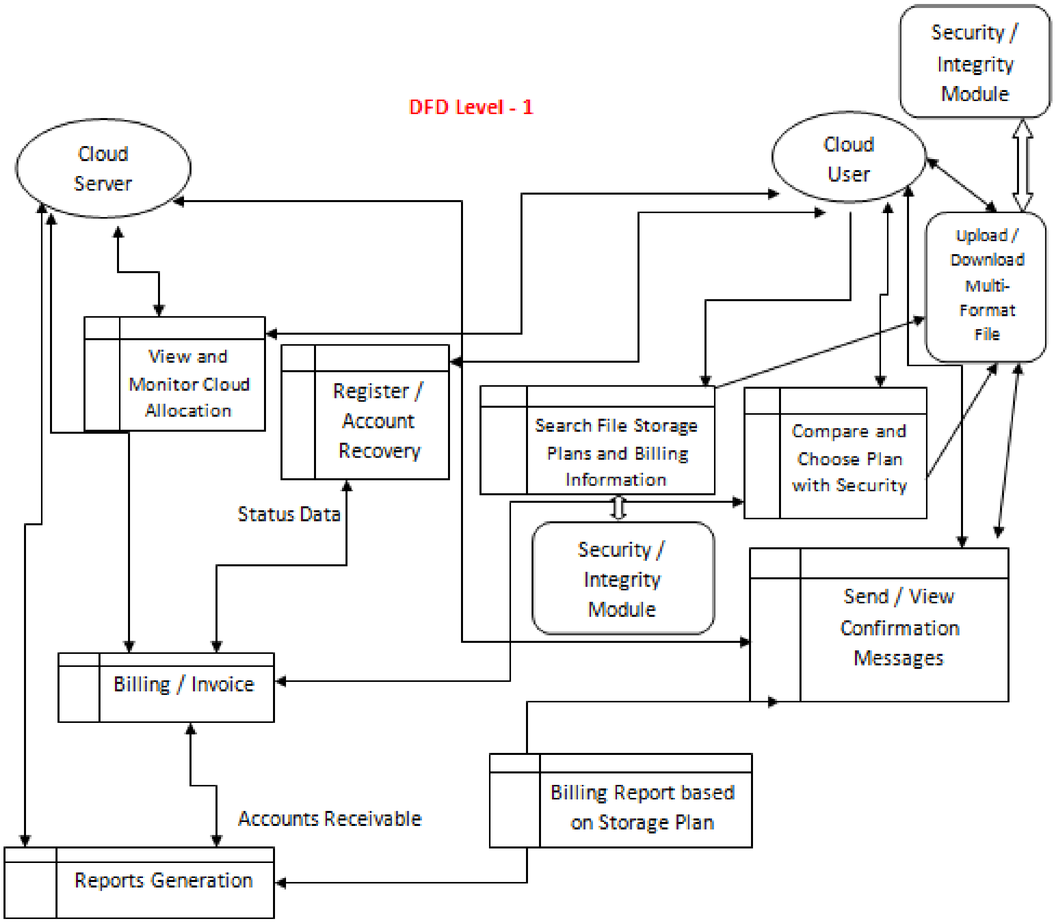
- MySQL is a freely available open source Relational Database Management System (RDBMS) that uses Structured Query Language (SQL). SQL is the most popular language for adding, accessing and managing content in a database. It is most noted for its quick processing, proven reliability, ease and flexibility of use. MySQL is an essential part of almost every open source PHP application. Good examples for PHP/MySQL-based scripts are phpBB, osCommerce and Joomla.

3.2 Data Flow Diagrams

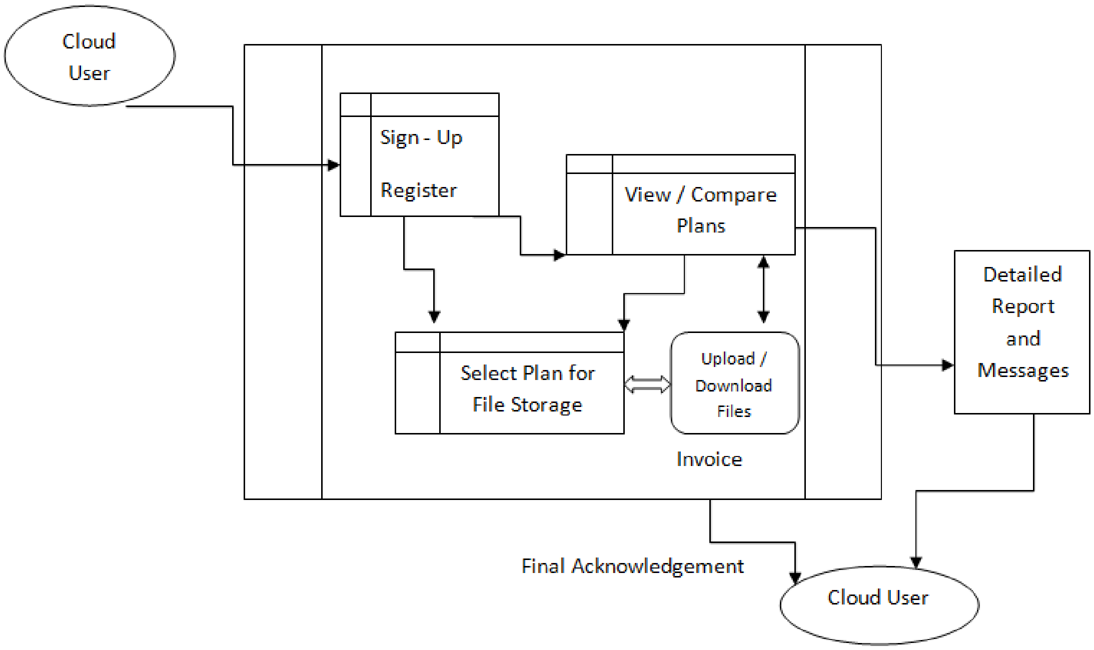
DFD Level - 0


Cloud Server
Administrator
Cloud Panel Management
Cloud Activity
Cloud DB
List / View Cloud Users
Encryption / Cryptography Procedures for Security and Integrity
Sign Up / Register
Cloud User
System
Cloud Virtual Machine Handler
Select Appropriate Cloud Storage Plan
Billing / Acknowledgements
Subscription
Reports Generations | Cloud Storage Allocation Monitoring | File Server Analysis
Multi Option Plans for Cloud File Storage
Cloudlets => Individual Processes and Tasks

DFD – 1


DFD Level - 1
Cloud Server
Cloud User
Security / Integrity Module
Upload / Download Multi-Format File
View and Monitor Cloud Allocation
Register / Account Recovery
Search File Storage Plans and Billing Information
Compare and Choose Plan with Security
Security / Integrity Module
Send / View Confirmation Messages
Status Data
Billing / Invoice
Billing Report based on Storage Plan
Accounts Receivable
Reports Generation

DFD Level - 2



3.3 CRYPTOGRAPHY TECHNIQUES AND ALGORITHMS

The MD5 message-digest algorithm is a widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed in text format as a 32 digit hexadecimal number. MD5 has been utilized in a wide variety of cryptographic applications, and is also commonly used to verify data integrity.

These hash and collision attacks have been demonstrated in the public in various situations, including colliding document files and digital certificates.

Collision vulnerabilities

In 1996, collisions were found in the compression function of MD5, and Hans Dobbertin wrote in the RSA Laboratories technical newsletter, "The presented attack does not yet threaten practical applications of MD5, but it comes rather close ... in the future MD5 should no longer be implemented...where a collision-resistant hash function is required." In 2012, according to Microsoft, the authors of the Flame malware used an MD5 collision to forge a Windows code-signing certificate.

MD5 uses the Merkle–Damgård construction, so if two prefixes with the same hash can be constructed, a common suffix can be added to both to make the collision more likely to be accepted as valid data by the application using it. Furthermore, current collision-finding techniques allow to specify an arbitrary *prefix*: an attacker can create two colliding files that both begin with the same content. All the attacker needs to generate two colliding files is a template file with a 128-byte block of data, aligned on a 64-byte boundary that can be changed freely by the collision-finding algorithm. An example MD5 collision, with the two messages differing in 6 bits, is:

```
d131dd02c5e6eec4 693d9a0698aff95c 2fcab58712467eab 4004583eb8fb7f89
55ad340609f4b302 83e488832571415a 085125e8f7cdc99f d91dbdf280373c5b
d8823e3156348f5b ae6dacd436c919c6 dd53e2b487da03fd 02396306d248cda0
e99f33420f577ee8 ce54b67080a80d1e c69821bcb6a88393 96f9652b6ff72a70
d131dd02c5e6eec4 693d9a0698aff95c 2fcab50712467eab 4004583eb8fb7f89
55ad340609f4b302 83e4888325f1415a 085125e8f7cdc99f d91dbd7280373c5b
d8823e3156348f5b ae6dacd436c919c6 dd53e23487da03fd 02396306d248cda0
e99f33420f577ee8 ce54b67080280d1e c69821bcb6a88393 96f965ab6ff72a70
```

Both produce the MD5 hash 79054025255fb1a26e4bc422aef54eb4. The difference between the two samples is the leading bit in each nibble has been flipped. For example, the 20th byte (offset 0x13) in the top sample, 0x87, is 10000111 in binary. The leading bit in the byte (also the leading bit in the first nibble) is flipped to make 00000111, which is 0x07 as shown in the lower sample.

Later it was also found to be possible to construct collisions between two files with separately chosen prefixes. This technique was used in the creation of the rogue CA certificate in 2008. A new variant of parallelized collision searching using MPI was proposed by Anton Kuznetsov in 2014 which allowed to find a collision in 11 hours on a computing cluster.

Secure Hash Algorithm

The Secure Hash Algorithm is a family of cryptographic hash functions published by the National Institute of Standards and Technology (NIST) as a U.S. Federal Information Processing Standard (FIPS), including:

- SHA-0: A retronym applied to the original version of the 160-bit hash function published in 1993 under the name "SHA". It was withdrawn shortly after publication due to an undisclosed "significant flaw" and replaced by the slightly revised version SHA-1.
- SHA-1: A 160-bit hash function which resembles the earlier MD5 algorithm. This was designed by the National Security Agency (NSA) to be part of the Digital Signature Algorithm. Cryptographic weaknesses were discovered in SHA-1, and the standard was no longer approved for most cryptographic uses after 2010.
- SHA-2: A family of two similar hash functions, with different block sizes, known as *SHA-256* and *SHA-512*. They differ in the word size; SHA-256 uses 32-bit words where SHA-512 uses 64-bit words. There are also truncated versions of each standard, known as *SHA-224*, *SHA-384*, *SHA-512/224* and *SHA-512/256*. These were also designed by the NSA.
- SHA-3: A hash function formerly called *Keccak*, chosen in 2012 after a public competition among non-NSA designers. It supports the same hash lengths as SHA-2, and its internal structure differs significantly from the rest of the SHA family.

The corresponding standards are FIPS PUB 180 (original SHA), FIPS PUB 180-1 (SHA-1), FIPS PUB 180-2 (SHA-1, SHA-256, SHA-384, and SHA-512). NIST has updated Draft FIPS Publication 202, SHA-3 Standard separate from the Secure Hash Standard (SHS).

SHA-0

At CRYPTO 98, two French researchers, Florent Chabaud and Antoine Joux, presented an attack on SHA-0 (Chabaud and Joux, 1998): collisions can be found with complexity 2^{61}, fewer than the 2^{80} for an ideal hash function of the same size.

In 2004, Biham and Chen found near-collisions for SHA-0—two messages that hash to nearly the same value; in this case, 142 out of the 160 bits are equal. They also found full collisions of SHA-0 reduced to 62 out of its 80 rounds.

Subsequently, on 12 August 2004, a collision for the full SHA-0 algorithm was announced by Joux, Carribault, Lemuet, and Jalby. This was done by using a generalization of the Chabaud and Joux attack. Finding the collision had complexity 2^{51} and took about 80,000 CPU hours on a supercomputer with 256 Itanium 2 processors. (Equivalent to 13 days of full-time use of the computer.)

On 17 August 2004, at the Rump Session of CRYPTO 2004, preliminary results were announced by Wang, Feng, Lai, and Yu, about an attack on MD5, SHA-0 and other hash functions. The complexity of their attack on SHA-0 is 2^{40}, significantly better than the attack by Joux *et al.*
In February 2005, an attack by Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu was announced which could find collisions in SHA-0 in 2^{39} operations.

Another attack in 2008 applying the boomerang attack brought the complexity of finding collisions down to $2^{33.6}$, which is estimated to take 1 hour on an average PC.

In light of the results for SHA-0, some experts suggested that plans for the use of SHA-1 in new cryptosystems should be reconsidered. After the CRYPTO 2004 results were published, NIST announced that they planned to phase out the use of SHA-1 by 2010 in favor of the SHA-2 variants.

Implementations of all FIPS-approved security functions can be officially validated through the CMVP program, jointly run by the National Institute of Standards and Technology (NIST) and the Communications Security Establishment (CSE). For informal verification, a package to generate a high number of test vectors is made available for download on the NIST site; the resulting verification however does not replace, in any way, the formal CMVP validation, which is required by law for certain applications.

As of December 2013, there are over 2000 validated implementations of SHA-1, with 14 of them capable of handling messages with a length in bits not a multiple of eight (see SHS Validation List).

Examples and pseudocode

These are examples of SHA-1 message digests in hexadecimal and in Base64 binary to ASCII text encoding.

SHA1("The quick brown fox jumps over the lazy dog")

gives hexadecimal: 2fd4e1c67a2d28fced849ee1bb76e7391b93eb12

gives Base64 binary to ASCII text encoding: L9ThxnotKPzthJ7hu3bnORuT6xI=

Even a small change in the message will, with overwhelming probability, result in a completely different hash due to the avalanche effect. For example, changing dog to cog produces a hash with different values for 81 of the 160 bits:

SHA1("The quick brown fox jumps over the lazy cog")

gives hexadecimal: de9f2c7fd25e1b3afad3e85a0bd17d9b100db4b3

gives Base64 binary to ASCII text encoding: 3p8sf9JeGzr60+haC9F9mxANtLM=

The hash of the zero-length string is:

SHA1 ("")

gives hexadecimal: da39a3ee5e6b4b0d3255bfef95601890afd80709

gives Base64 binary to ASCII text encoding: 2jmj7l5rSw0yVb/vlWAYkK/YBwk=

SHA-1 pseudocode

Pseudocode for the SHA-1 algorithm follows:

```
Note 1: All variables are unsigned 32 bits and wrap modulo $2^{32}$ when calculating, except
    ml the message length which is 64 bits, and
    hh the message digest which is 160 bits.
Note 2: All constants in this pseudo code are in big endian.
    Within each word, the most significant byte is stored in the leftmost byte position
```

```
Initialize variables:

h0 = 0x67452301
h1 = 0xEFCDAB89
h2 = 0x98BADCFE
h3 = 0x10325476
h4 = 0xC3D2E1F0

ml = message length in bits (always a multiple of the number of bits in a character).

Pre-processing:
append the bit '1' to the message i.e. by adding 0x80 if characters are 8 bits.
append 0 ≤ k < 512 bits '0', thus the resulting message length (in bits)
   is congruent to 448 (mod 512)
append ml, in a 64-bit big-endian integer. So now the message length is a multiple of 512 bits.

Process the message in successive 512-bit chunks:
break message into 512-bit chunks
for each chunk
    break chunk into sixteen 32-bit big-endian words w[i], 0 ≤ i ≤ 15

    Extend the sixteen 32-bit words into eighty 32-bit words:
    for i from 16 to 79
        w[i] = (w[i-3] xor w[i-8] xor w[i-14] xor w[i-16]) leftrotate 1

    Initialize hash value for this chunk:
    a = h0
    b = h1
    c = h2
```

```
d = h3
e = h4
```

Main loop:

```
for i from 0 to 79
    if $0 \le i \le 19$ then
        f = (b and c) or ((not b) and d)
        k = 0x5A827999
    else if $20 \le i \le 39$
        f = b xor c xor d
        k = 0x6ED9EBA1
    else if $40 \le i \le 59$
        f = (b and c) or (b and d) or (c and d)
        k = 0x8F1BBCDC
    else if $60 \le i \le 79$
        f = b xor c xor d
        k = 0xCA62C1D6

    temp = (a leftrotate 5) + f + e + k + w[i]
    e = d
    d = c
    c = b leftrotate 30
    b = a
    a = temp
```

Add this chunk's hash to result so far:

```
h0 = h0 + a
h1 = h1 + b
h2 = h2 + c
h3 = h3 + d
h4 = h4 + e
```

Produce the final hash value (big-endian) as a 160 bit number:

hh = (h0 leftshift 128) or (h1 leftshift 96) or (h2 leftshift 64) or (h3 leftshift 32) or h4

The number hh is the message digest, which can be written in hexadecimal (base 16), but is often written using Base64 binary to ASCII text encoding.

The constant values used are chosen to be nothing up my sleeve numbers: the four round constants k are 2^{30} times the square roots of 2, 3, 5 and 10. The first four starting values for h0 through h3 are the same with the MD5 algorithm, and the fifth (for h4) is similar.

Instead of the formulation from the original FIPS PUB 180-1 shown, the following equivalent expressions may be used to compute f in the main loop above:

```
(0  ≤ i ≤ 19): f = d xor (b and (c xor d))          (alternative 1)
(0  ≤ i ≤ 19): f = (b and c) xor ((not b) and d)    (alternative 2)
(0  ≤ i ≤ 19): f = (b and c) + ((not b) and d)      (alternative 3)
(0  ≤ i ≤ 19): f = vec_sel(d, c, b)                 (alternative 4)

(40 ≤ i ≤ 59): f = (b and c) or (d and (b or c))    (alternative 1)
(40 ≤ i ≤ 59): f = (b and c) or (d and (b xor c))   (alternative 2)
(40 ≤ i ≤ 59): f = (b and c) + (d and (b xor c))    (alternative 3)
(40 ≤ i ≤ 59): f = (b and c) xor (b and d) xor (c and d)  (alternative 4)
(40 ≤ i ≤ 59): f = vec_sel(c, b, c xor d)           (alternative 5)
```

Max Locktyukhin has also shown that for the rounds 32–79 the computation of:

w[i] = (w[i-3] xor w[i-8] xor w[i-14] xor w[i-16]) leftrotate 1

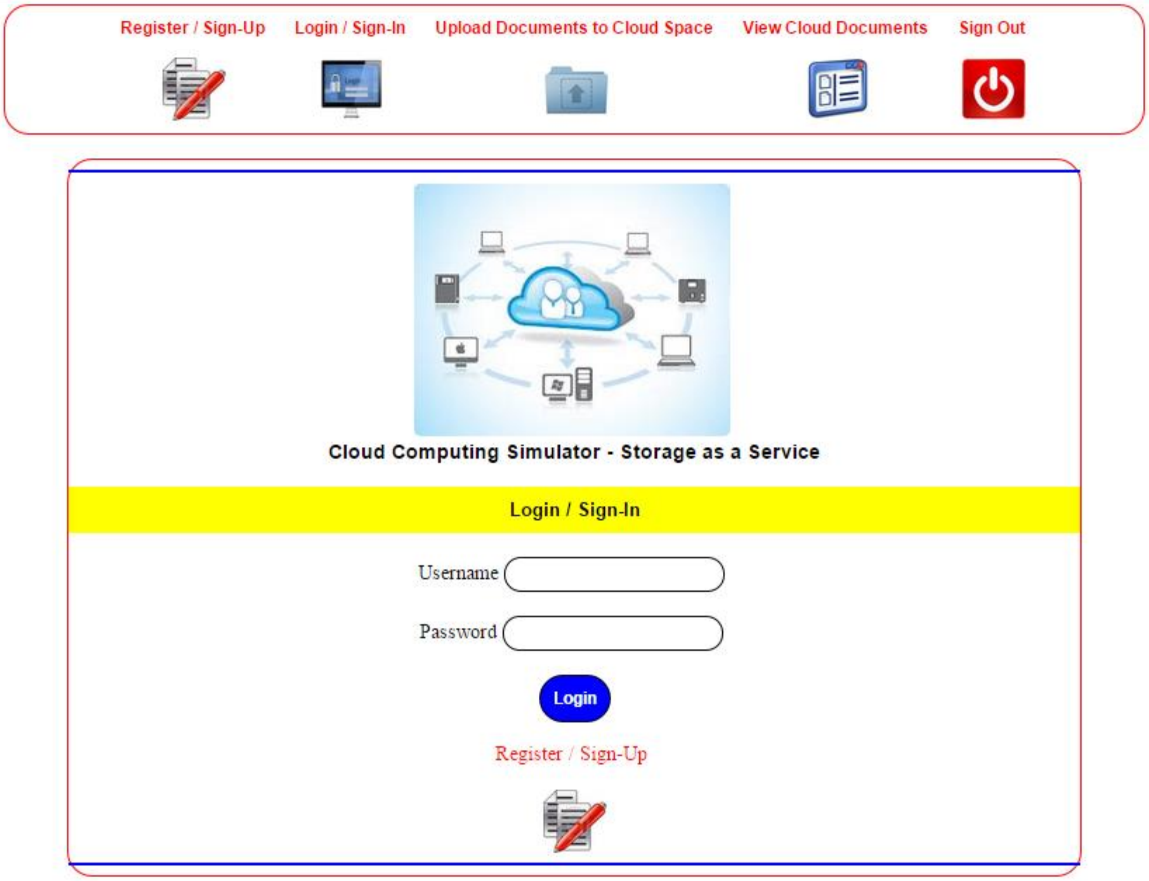
can be replaced with:

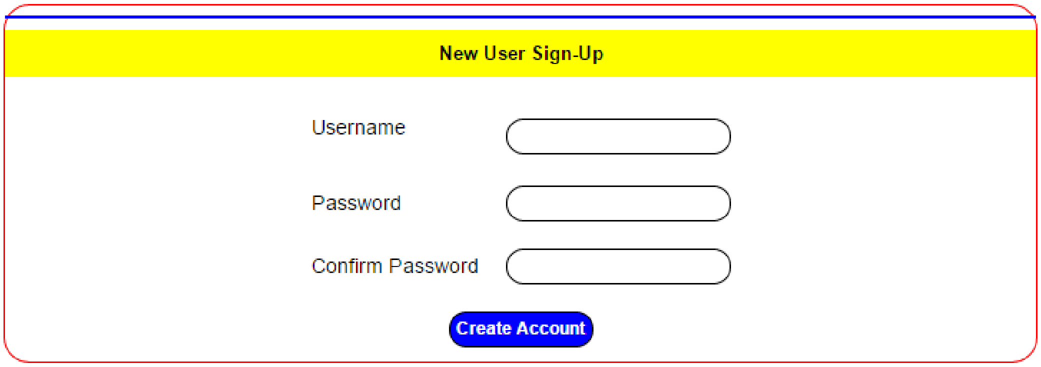
w[i] = (w[i-6] xor w[i-16] xor w[i-28] xor w[i-32]) leftrotate 2

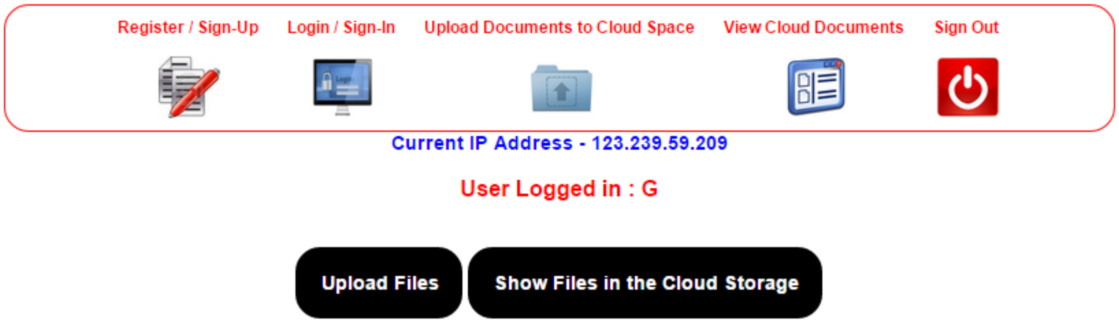
This transformation keeps all operands 64-bit aligned and, by removing the dependency of w[i] on w[i-3], allows efficient SIMD implementation with a vector length of 4 like x86 SSE instructions.

CHAPTER 4
RESULTS AND DISCUSSION

4.1 Output Screenshots

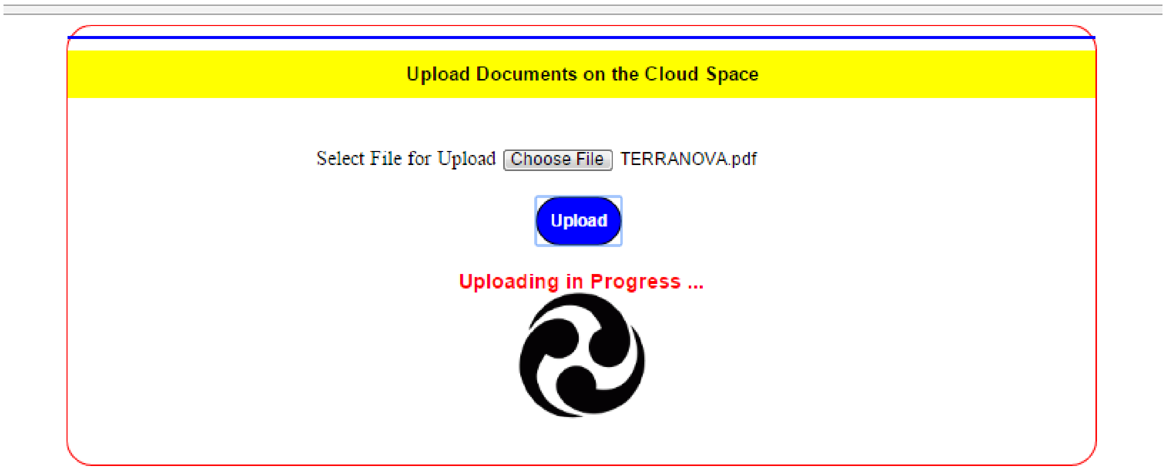






Current IP Address - 123.239.59.209

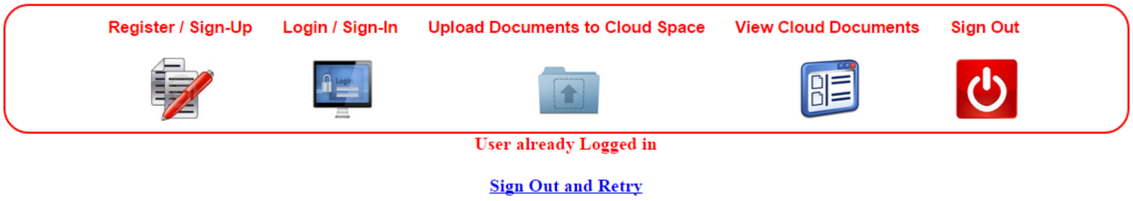
User Logged in : G



Upload Documents on the Cloud Space

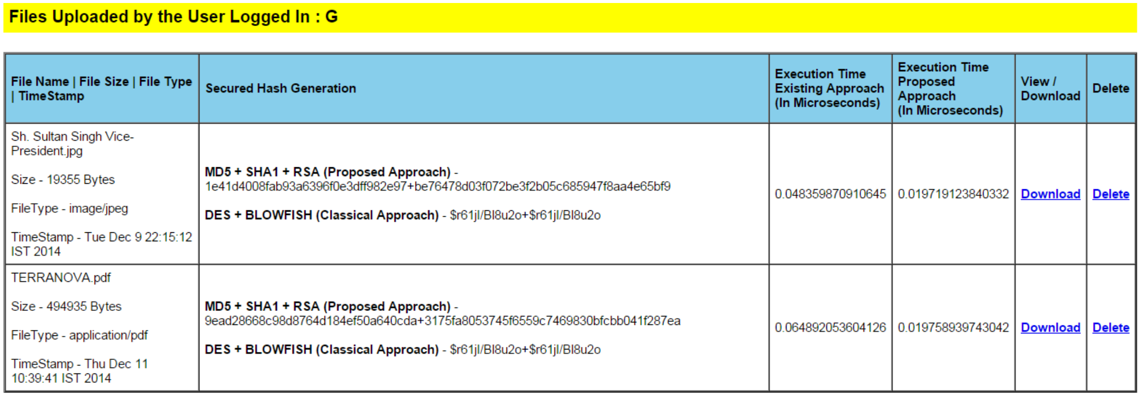
Select File for Upload TERRANOVA.pdf

Uploading in Progress ...



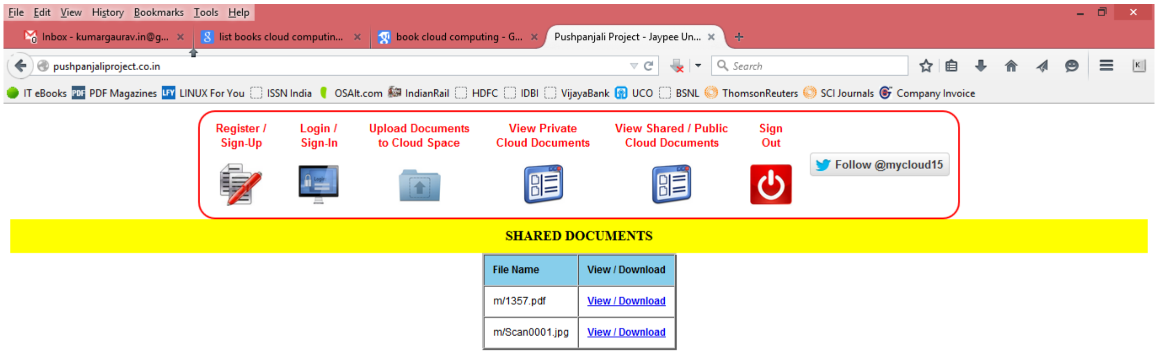
User already Logged in

Sign Out and Retry



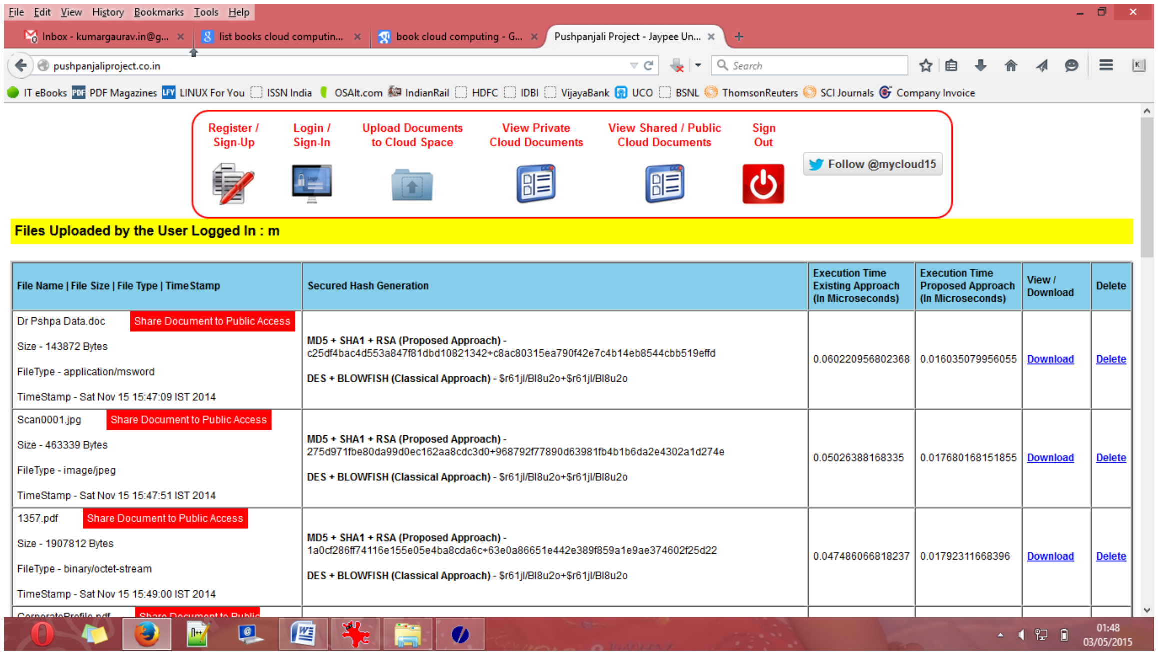
Files Uploaded by the User Logged In : G

File Name | File Size | File Type | TimeStamp	Secured Hash Generation	Execution Time Existing Approach (In Microseconds)	Execution Time Proposed Approach (In Microseconds)	View / Download	Delete
Sh. Sultan Singh Vice-President.jpg Size - 19355 Bytes FileType - image/jpeg TimeStamp - Tue Dec 9 22:15:12 IST 2014	**MD5 + SHA1 + RSA (Proposed Approach)** - 1e41d4008fab93a6396f0e3dff982e97+be76478d03f072be3f2b05c685947f8aa4e65bf9 **DES + BLOWFISH (Classical Approach)** - $r61jl/Bl8u2o+$r61jl/Bl8u2o	0.048359870910645	0.019719123840332	Download	Delete
TERRANOVA.pdf Size - 494935 Bytes FileType - application/pdf TimeStamp - Thu Dec 11 10:39:41 IST 2014	**MD5 + SHA1 + RSA (Proposed Approach)** - 9ead28668c98d8764d184ef50a640cda+3175fa8053745f6559c7469830bfcbb041f287ea **DES + BLOWFISH (Classical Approach)** - $r61jl/Bl8u2o+$r61jl/Bl8u2o	0.064892053604126	0.019758939743042	Download	Delete


File Edit View History Bookmarks Tools Help
Inbox - kumargaurav.in@g...
list books cloud computin...
book cloud computing - G...
Pushpanjali Project - Jaypee Un...
pushpanjaliproject.co.in
Search
IT eBooks
PDF Magazines
LINUX For You
ISSN India
OSAlt.com
IndianRail
HDFC
IDBI
VijayaBank
UCO
BSNL
ThomsonReuters
SCI Journals
Company Invoice
Register / Sign-Up
Login / Sign-In
Upload Documents to Cloud Space
View Private Cloud Documents
View Shared / Public Cloud Documents
Sign Out
Follow @mycloud15

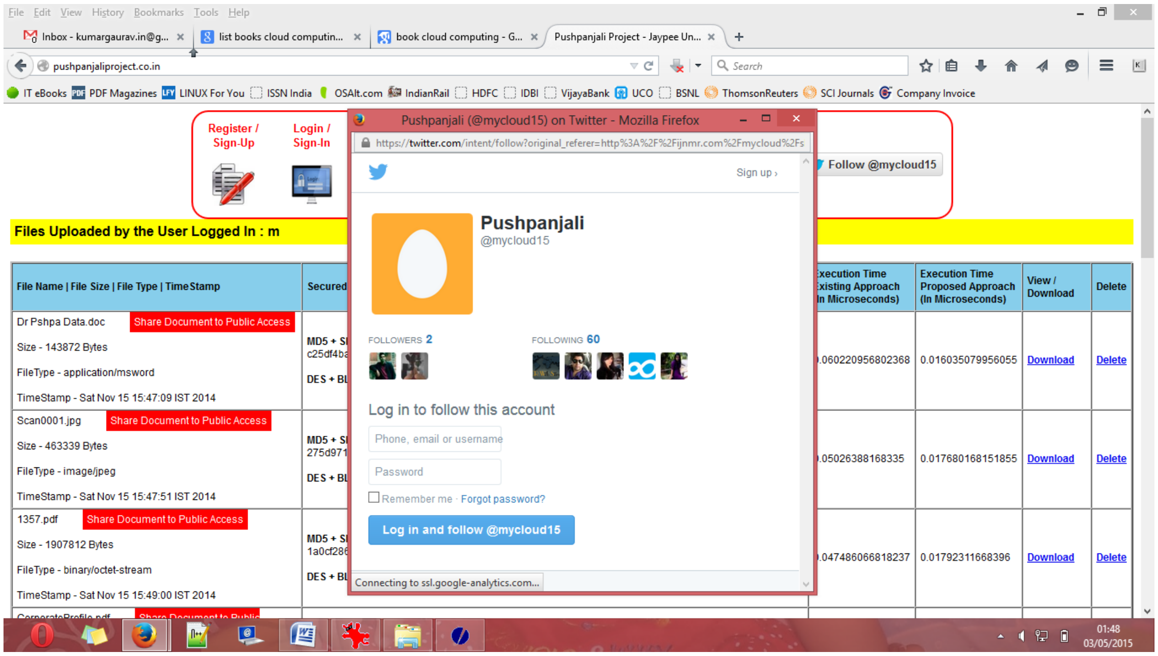
SHARED DOCUMENTS

File Name	View / Download
m/1357.pdf	View / Download
m/Scan0001.jpg	View / Download


File Edit View History Bookmarks Tools Help
Inbox - kumargaurav.in@g...
list books cloud computin...
book cloud computing - G...
Pushpanjali Project - Jaypee Un...
pushpanjaliproject.co.in
Search
IT eBooks
PDF Magazines
LINUX For You
ISSN India
OSAlt.com
IndianRail
HDFC
IDBI
VijayaBank
UCO
BSNL
ThomsonReuters
SCI Journals
Company Invoice
Register / Sign-Up
Login / Sign-In
Upload Documents to Cloud Space
View Private Cloud Documents
View Shared / Public Cloud Documents
Sign Out
Follow @mycloud15
01:48
03/05/2015

Files Uploaded by the User Logged In : m

File Name | File Size | File Type | TimeStamp	Secured Hash Generation	Execution Time Existing Approach (In Microseconds)	Execution Time Proposed Approach (In Microseconds)	View / Download	Delete
Dr Pshpa Data.doc Share Document to Public Access Size - 143872 Bytes FileType - application/msword TimeStamp - Sat Nov 15 15:47:09 IST 2014	**MD5 + SHA1 + RSA (Proposed Approach)** - c25df4bac4d553a847f81dbd10821342+c8ac80315ea790f42e7c4b14eb8544cbb519effd **DES + BLOWFISH (Classical Approach)** - $r61jl/Bl8u2o+$r61jl/Bl8u2o	0.060220956802368	0.016035079956055	Download	Delete
Scan0001.jpg Share Document to Public Access Size - 463339 Bytes FileType - image/jpeg TimeStamp - Sat Nov 15 15:47:51 IST 2014	**MD5 + SHA1 + RSA (Proposed Approach)** - 275d971fbe80da99d0ec162aa8cdc3d0+968792f77890d63981fb4b1b6da2e4302a1d274e **DES + BLOWFISH (Classical Approach)** - $r61jl/Bl8u2o+$r61jl/Bl8u2o	0.05026388168335	0.017680168151855	Download	Delete
1357.pdf Share Document to Public Access Size - 1907812 Bytes FileType - binary/octet-stream TimeStamp - Sat Nov 15 15:49:00 IST 2014	**MD5 + SHA1 + RSA (Proposed Approach)** - 1a0cf286ff74116e155e05e4ba8cda6c+63e0a86651e442e389f859a1e9ae374602f25d22 **DES + BLOWFISH (Classical Approach)** - $r61jl/Bl8u2o+$r61jl/Bl8u2o	0.047486066818237	0.01792311668396	Download	Delete
CorporateProfile.pdf Share Document to Public					



Files Uploaded by the User Logged In : m

File Name | File Size | File Type | TimeStamp	Secured	xecution Time xisting Approach n Microseconds)	Execution Time Proposed Approach (In Microseconds)	View / Download	Delete
Dr Pshpa Data.doc Share Document to Public Access Size - 143872 Bytes FileType - application/msword TimeStamp - Sat Nov 15 15:47:09 IST 2014	MD5 + SI c25df4ba DES + BL	.060220956802368	0.016035079956055	Download	Delete
Scan0001.jpg Share Document to Public Access Size - 463339 Bytes FileType - image/jpeg TimeStamp - Sat Nov 15 15:47:51 IST 2014	MD5 + SI 275d971 DES + BL	.05026388168335	0.017680168151855	Download	Delete
1357.pdf Share Document to Public Access Size - 1907812 Bytes FileType - binary/octet-stream TimeStamp - Sat Nov 15 15:49:00 IST 2014	MD5 + SI 1a0cf286 DES + BL	.047486066818237	0.01792311668396	Download	Delete

Pushpanjali (@mycloud15) on Twitter - Mozilla Firefox

https://twitter.com/intent/follow?original_referer=http%3A%2F%2Fijnmr.com%2Fmycloud%2Fs

Sign up ›

Pushpanjali
@mycloud15

FOLLOWERS 2 FOLLOWING 60

Log in to follow this account

Phone, email or username

Password

□ Remember me · Forgot password?

Log in and follow @mycloud15

Connecting to ssl.google-analytics.com...

4.2 Test Cases

A test case is a document, which has a set of test data, preconditions, expected results and post conditions, developed for a particular test scenario in order to verify compliance against a specific requirement.

Test Case acts as the starting point for the test execution, and after applying a set of input values, the application has a definitive outcome and leaves the system at some end point or also known as execution post condition.

4.2.1 Test Case - 1: Login / Sign-In Page

Test Suite ID	TS001
Test Case ID	TC001
Test Case Summary	To verify that status of Login Page
Prerequisites	• User is authorized. • Use of Special Characters not allowed
Test Procedure	• Enter the valid username

	• Enter the valid password • Click on Login
Test Data	• Values : admin, gk, m
Expected Result	• Successful Login Message • Cloud User should be redirected to the page for uploading the files on cloud storage • User should be able to view the IP Address of Login System • User should be able to view the existing documents
Actual Result	• If the specified quantity is valid, the result is as expected. • If the specified quantity is invalid, nothing happens; the expected message is not displayed • User should be able to sign out after completing the process and navigation
Status	Success
Remarks	This is a sample test case
Created By	Pushpanjali Chauhan
Executed By	Pushpanjali Chauhan
Test Environment	• OS: o Windows o Linux • Supported Browsers : o Chrome o Firefox o Opera o Safari o Internet Explorer

4.2.2 Test Case – 2: Uploading Files to the Cloud Space

Test Suite ID	TS003
Test Case ID	TC003
Test Case Summary	To Authenticate and Upload to the Cloud Space
Prerequisites	• User should be authorized. • Use of Special Characters not allowed • Use SQL Injections not allowed • Empty User can’t be created • Multiple User Login is not allowed
Test Procedure	• Enter the valid username • Enter the valid password • Click on Login • Click on Upload Documents to Cloud Space • Click on View Cloud Documents to view the documents
Test Data	• Values : admin, gk, m, iii, g
Expected Result	• Successful Message • User should be able to upload in any file format • User should be able to remove the files • Duplicate Files can’t be uploaded • Cloud User should be redirected to the Login page for uploading the files on cloud storage • User should be able to view the IP Address of Login System

	• User should be able to view the existing documents
Actual Result	• Multiple Login not allowed • Same FileName for multiple documents not allowed • Removal of documents allowed
Status	Success
Remarks	This is a sample test case
Created By	Pushpanjali Chauhan
Executed By	Pushpanjali Chauhan
Test Environment	• OS: o Windows o Linux • Supported Browsers : o Chrome o Firefox o Opera o Safari o Internet Explorer

CHAPTER 5
SCOPE OF FUTURE WORK

The cloud environment has scalable, expandable, virtualization and abstraction as basic aspects that makes cloud security become more complex. Various vulnerabilities and attacks discussed in this work are main threats for cloud that cause many enterprises which have plan to migrate to cloud prefer using cloud for less sensitive data and store important data within enterprise boundary. So as a result, moving towards cloud computing require more safe and secure environment and our further study will also focus on various security schemes or algorithm that helps in providing secure cloud environment.

An assorted stack of protocols and techniques are used for accomplishing the task of security and privacy in cloud computing. But the proposed work is implemented with a unique set of tasks and steps. There are number parameters or metrics which are required be considered for the integration and analysis of security aspects. The proposed research work consider the following parameters for development, deployment and testing -

- To analyze the security algorithms of cloud computing and their associated parameters.
- There is need to improve the existing key exchange to improve the security and authentication aspects.
- To Implement and evaluate the security based on dynamic key exchange
- To analyze the comparison and identify the best technique on the basis of their routing performance so that a network can work in an efficient manner.
- To implement the Dynamic Key Exchange to enhance the security and integrity in the network
- The existing algorithmic approach and implementation can be enhanced using metaheuristics including genetic algorithms and ant colony optimization.

For future scope of the work, following techniques can be used in hybrid approach to better and efficient results –

- Particle Swarm Optimization
- HoneyBee Algorithm
- Simulated Annealing
- Genetic Algorithmic Approaches

REFERENCES

[1] Cochavy, Baruch, Method of efficiently sending packets onto a network by eliminating an interrupt, US Patent Issued on August 18, 1998

[2] Dimitris M. Kyriazanos, Neeli R. Prasad, Charalampos Z. Patrikakis, A Security, Privacy and Trust Architecture for Wireless Sensor Networks, 50th International Symposium ELMAR-2008, 10-12 September 2008, Zadar, Croatia

[3] Donna Andert, Robin Wakefield, and Joel Weise, Professional Services Security Practice, Sun BluePrints™ OnLine - December 2002, Trust Modeling for Security Architecture Development

[4] Security, Encryption, Acceleration, http://www.networkintercept.com

[5] Youlu Zheng, Shakil Akhtar, Networks for Computer Scientists and Engineers, Oxford University Press, 2009

[6] Carl Endorf, Eugene Schultz and Jim Mellander, Intrusion Detection & Prevention, McGraw-Hill, 2004

[7] Technical Standard Risk Taxonomy ISBN 1-931624-77-1 Document Number: C081 Published by The Open Group, January 2009.

[8] "An Introduction to Factor Analysis of Information Risk (FAIR)", Risk Management Insight LLC, November 2006;

[9] Matt Bishop and Dave Bailey. A Critical Analysis of Vulnerability Taxonomies. Technical Report CSE-96-11, Department of Computer Science at the University of California at Davis, September 1996

[10] Schou, Corey (1996). Handbook of INFOSEC Terms, Version 2.0. CD-ROM (Idaho State University & Information Systems Security Organization)

[11] Wright, Joe; Jim Harmening (2009) "15" Computer and Information Security Handbook Morgan Kaufmann Publications Elsevier Inc p. 257 ISBN 978-0-12-374354-1

[12] ISACA THE RISK IT FRAMEWORK (registration required)

[13] Kakareka, Almantas (2009) "23" Computer and Information Security Handbook Morgan Kaufmann Publications Elsevier Inc p. 393 ISBN 978-0-12-374354-1

[14] Technical Report CSD-TR-97-026 Ivan Krsul The COAST Laboratory Department of Computer Sciences, Purdue University, April 15, 1997

[15] The Web Application Security Consortium Project, Web Application Security Statistics 2009

[16] Ross Anderson. Why Cryptosystems Fail. Technical report, University Computer Laboratory, Cam- bridge, January 1994.

[17] Neil Schlager. When Technology Fails: Significant Technological Disasters, Accidents, and Failures of the Twentieth Century. Gale Research Inc., 1994.

[18] Hacking: The Art of Exploitation Second Edition

[19] Kiountouzis, E. A.; Kokolakis, S. A. Information systems security: facing the information society of the 21st century London: Chapman & Hall, Ltd ISBN 0-412-78120-4

[20] Bavisi, Sanjay (2009) "22" Computer and Information Security Handbook Morgan

BOOKS

[1] Cloud Computing Explained: Implementation Handbook for Enterprises by John Rhoton

[2] Cloud Computing and SOA Convergence in Your Enterprise: A Step-by-Step Guide

[3] Cloud Application Architectures: Building Applications and Infrastructure in the

[4] Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance (Theory in Practice) by Tim Mather

[5] Host Your Web Site In The Cloud: Amazon Web Services Made Easy: Amazon EC2 Made Easy by Jeff Barr

[6] Behind the Cloud: The Untold Story of How Salesforce.com Went from Idea to

[7] Management Strategies for the Cloud Revolution : How Cloud Computing Is Transforming Business and Why You Can't Afford to Be Left Behind by Charles Babcock

[8] Enterprise Cloud Computing: A Strategy Guide for Business and Technology Leaders by Andy Mulholland

WEB REFERENCES

[1] en.wikipedia.org/wiki/Cloud_computing

[2] searchcloudcomputing.techtarget.com/definition/cloud-computing

[3] computer.howstuffworks.com/cloud-computing/cloud-computing.htm

[4] www.wikinvest.com/concept/Cloud_Computing

[5] www.ibm.com/cloud-computing/in/en/what-is-cloud-computing.html

[6] www.rackspace.com/cloud/what_is_cloud_computing

[7] www.salesforce.com/in/cloudcomputing/

[8] www.infoworld.com/category/cloud-computing

[9] https://www.coursera.org/specialization/mobilecloudcomputing2/36

[10] https://www.coursera.org/course/cloudapplications

[11] www.dell.com/learn/us/en/555/dell-cloud-computing

[12] cloud-computing.tmcnet.com/

[13] https://www.vmware.com/in/cloud-computing/overview

[14] www.microsoft.com/enterprise/it-trends/cloud-computing/

[15] www.cisco.com/web/solutions/trends/cloud/

[16] www.thecloudcomputing.org/2015/

SOURCE CODE

```
<?php // content="text/plain; charset=utf-8"
require_once ('jpgraph/jpgraph.php');
require_once ('jpgraph/jpgraph_bar.php');
include_once ("conn.php");
$q=mysql_query ("select * from uploads");

$stack1 = array();
$stack2 = array();

while ($row=mysql_fetch_object($q))
{
$classical=$row->etime;
$proposed=$row->ptime;

array_push($stack1, $classical);
array_push($stack2, $proposed);
}

$data1y=$stack1;
$data2y=$stack2;

// Create the graph. These two calls are always required
$graph = new Graph(1050,500,'auto');
$graph->SetScale("textlin");

$theme_class=new UniversalTheme;
$graph->SetTheme($theme_class);

$graph->SetBox(false);

$graph->ygrid->SetFill(false);
// $graph->xaxis->SetTickLabels(array('A','B','C','D'));
$graph->yaxis->HideLine(false);
$graph->yaxis->HideTicks(false,false);

// Create the bar plots
$b1plot = new BarPlot($data1y);
$b2plot = new BarPlot($data2y);

// Create the grouped bar plot
$gbplot = new GroupBarPlot(array($b1plot,$b2plot));
// ...and add it to the graPH
```

```
$graph->Add($gbplot);


$b1plot->SetColor("white");
$b1plot->SetFillColor("#cc1111");

$b2plot->SetColor("white");
$b2plot->SetFillColor("#11cccc");


$graph->title->Set("Bar Plots");

// Display the graph
$graph->Stroke();
?>

<div align=center>
<div style="border: 2px solid red; border-radius: 20px; width: 900px">

<table cellspacing=0 align=center cellpadding=10 style="font-family: arial; font-weight:
bold; font-size: 10pt">
<tr>

<td align=center>
<a href=linegraphwithvalues.php style="color: red; text-decoration: none"
target="_blank">Proposed Vs. Classical Approach<br><br>
<img src=graph.jpg height=50 width=50>

<td align=center>
<a href=graphslot1.php style="color: red; text-decoration: none" target="_blank">Graph
: Slot - 1 (<100 KB)<br><br>
<img src=graph.jpg height=50 width=50>

<td align=center>
<a href=graphslot2.php style="color: red; text-decoration: none" target="_blank">Graph
: Slot - 2 (100-200 KB)<br><br>
<img src=graph.jpg height=50 width=50>

<td align=center>
<a href=graphslot3.php style="color: red; text-decoration: none" target="_blank">Graph
: Slot - 3 (200-300 KB)<br><br>
<img src=graph.jpg height=50 width=50>

<td align=center>
<a href=graphslot4.php style="color: red; text-decoration: none" target="_blank">Graph
: Slot - 4 (300-400 KB)<br><br>
```

```
<img src=graph.jpg height=50 width=50>

<td align=center>
<a href=graphslot5.php style="color: red; text-decoration: none" target="_blank">Graph
: Slot - 5 (>400 KB)<br><br>
<img src=graph.jpg height=50 width=50>

<td align=center>
<a href=showtime.php style="color: red; text-decoration: none" >Comparison Table :
Classical and Proposed Approach<br><br>
<img src=table.jpg height=50 width=50>

<td align=center>
<a href=showtime2.php style="color: red; text-decoration: none" >Multiple Algorithms
Comparison Table<br><br>
<img src=table.jpg height=50 width=50>

<td align=center>
<a href=logout.php style="color: red; text-decoration: none" >Sign Out
<br><br>
<img src=logout.jpg height=50 width=50>

</table>
</div>
</div>

<?php
error_reporting(0);
$u=$_POST['u'];
$p=$_POST['p'];

session_start();

if (($u=="admin") and ($p=="amandeep"))
{
if (isset($_SESSION['u']))
{
echo "<div style='background-color: skyblue; text-align: center; font-weight:
bold'>Cloud User Already Logged In</div>";
die(" ");
}
$_SESSION['admin']=1;
echo "<div align=center style='color: red; font-weight: bold'>Administrator Login
Successful
<br><br><img src=admin.jpg>
</div>";
die(" ");
}


if (isset($_SESSION['admin']))
{
echo "<a href=javascript:history.back(-1)>Back</a>";
die("Admin Already Logged In");
}

include_once("conn.php");

$q=mysql_query("select * from users where username='$u' and password='$p'");

if (mysql_num_rows($q) <= 0)
{
include_once("login.html");
die("Login Failed");
}



$thisip=$_SERVER['REMOTE_ADDR'];

$previousip=$_SESSION['ip'];

if ($thisip == $previousip)
{
$_SESSION['login']=1;
echo "<div align=center style='color: red; font-size: 11pt; font-weight: bold'>User
already Logged in</div>";
die(" ");
}

$_SESSION['u']=$u;

$_SESSION['login']=1;


echo "Current IP Address - ".$thisip;

$_SESSION['ip']=$thisip;


echo "<font face=arial size=4 color=red><strong>User Logged in :
$u</strong></font><br><br>";
```

```
echo "<br><div align=center><a href=upload.html style='background-color: black; color: white; border-radius: 20px; padding: 20px; font-weight: bold; font-family: arial; text-decoration: none'>Upload Files</a>

<a href=showfiles.php style='background-color: black; color: white; border-radius: 20px; padding: 20px; font-weight: bold; font-family: arial; text-decoration: none'>Show Files in the Cloud Storage</a></div>";

?>

<html>
<head>
<style>
.hide {display: none}
.show {display: block}
</style>
</head>
<body>


<?php
session_start();

include_once("usermenu.php");

$loginstatus=$_SESSION['login'];

if ($loginstatus!=1)
{
echo "<div style='background-color: red; color: white; padding: 5px; font-family: arial; font-weight: bold; text-align: center'>Invalid Login ... </div>";
include_once("login.html");
die(" ");
}
?>

<div align=center>
<div style="border: 2px solid red; margin-left: 10px; margin-right: 10px; border-radius: 20px; width: 800px">
<hr color=blue>
<div style="background-color: yellow; padding: 10px; text-align: center; font-size: 11pt; font-family: arial">
<strong>Upload Documents on the Cloud Space</strong>
</div>
<br>
```

```
<br>
<div align=center>
<form action=upload.php method=post enctype="multipart/form-data">
Select File for Upload <input type=file name=f>
<br><br>
<input type=submit value=Upload style="border: 2px solid black; background-color:
blue; font-weight: bold; color: white; padding: 10px; border-radius: 20px"
onClick="loader.className='show'">
<br><br>
<div align=center id=loader class=hide>
<font size=3 face=arial color=red><strong>Uploading in Progress ...<br>
<img src=ajaxloader.gif height=100 width=100></div>
</form><br>
</div>
</div>
</div>



</div>
</div>
<?php

error_reporting(0);

include_once("conn.php");

session_start();

$_SESSION['usertype']=$u=$_POST['u'];
$p=$_POST['p'];

if ($usertype=='admin')
{
include_once("adminmenu.php");
}
else
{
include_once("usermenu.php");
}


$time1=microtime(true);

$u=$_SESSION['u'];

$fname=$_FILES['f']['name'];
```

```
$ftype=$_FILES['f']['type'];
$fsize=$_FILES['f']['size'];

$fsizekb=$fsize/(1024);

if ($fsizekb<=100)
{
$slot="1";
}
if (($fsizekb>100) and ($fsizekb<=200))
{
$slot="2";
}
if (($fsizekb>200) and ($fsizekb<=300))
{
$slot="3";
}
if (($fsizekb>300) and ($fsizekb<=400))
{
$slot="4";
}
if (($fsizekb>400))
{
$slot="5";
}


for($i=0; $i<=300000; $i++)
{echo "";}
$ftmp=$_FILES['f']['tmp_name'];
$timenow=$today=date("D M j G:i:s T Y");
$tws=microtime(true);

$timewithoutsecurity=$tws-$time1;

$md5=md5($fname);


$md5time=microtime(true)-$time1;


$sha1=sha1($fname);

$time2=microtime(true);
$ptime=$time2-$time1;
```

```
require_once("Crypt.php");
$crypt = new Crypt();
$crypt->Mode = Crypt::MODE_HEX;
$crypt->Key  = "!@#$%&*()124714812$!$^%*^@&!(_+?:)(*&^%$#@!1234567890";
echo $encrypted = $crypt->encrypt('$fname');
echo $crypt->decrypt($encrypted);
$timersa=microtime(true)-$time1;
$md5rsatime=$ptime+$timersa;

$checkupload=mysql_query("select filename from uploads where username='$u' and
filename='$fname'");
$countfile=mysql_num_rows($checkupload);

if ($countfile>0)
{
echo "<div style='background-color: red; color: white; padding: 5px; text-align: center;
font-weight: bold'>File Already Exists</div>";
include_once("uploadfile.php");
die(" ");
}
move_uploaded_file($ftmp, "$u/".$fname);
echo "File Successfully Uploaded<br>";

$time3=microtime(true);
if (CRYPT_EXT_DES == 1)
{
$rand=rand();
$des=crypt('$fname','$rand');
echo "Extended DES (Classical Approach) : ".crypt('$fname','_S4..some')."\n<br>";
$timedes=microtime(true)-$time1;
$t0=microtime(true);
}
else
{
echo "Extended DES not supported.\n<br>";
}

// Salt starting with $2a$. The two digit cost parameter: 09. 22 characters
if (CRYPT_BLOWFISH == 1)
{
$rand=rand();
$blowfish=crypt('$fname','$rand');
echo "Blowfish Encryption (Classical Approach) :
".crypt('$fname','$2a$09$anexamplestringforsalt$')."\n<br>";
}
else
```

```
{
echo "Blowfish DES not supported.\n<br>";
}


$time4=microtime(true);
$etime=$time4-$time3;
$md5f=md5($fname);

$md5des=microtime(true)-$t0;

mysql_query("insert into uploads(filename, size, type, username, timestamp, md5, sha1,
des, blowfish, etime, ptime) values('$fname', '$fsize', '$ftype', '$u', '$timenow', '$md5',
'$sha1', '$des', '$blowfish', '$etime', '$ptime')");





$timewithoutsecurity=round($timewithoutsecurity, 3);
$md5des=round($md5des, 3);
$md5rsatime=round($md5rsatime, 3);
$timersa=round($timersa, 3);
$timedes=round($timedes, 3);
$md5time=round($md5time, 3);

mysql_query("insert into executiontime(filesize, withoutsecurity, md5des, md5rsa, rsa,
des, md5, slot) values('$fsize', '$timewithoutsecurity', '$md5des', '$md5rsatime',
'$timersa', '$timedes', '$md5time', '$slot')");


include_once("showfiles.php");

?>

<?php
error_reporting(0);
session_start();

$usertype=$_SESSION['usertype'];

if ($usertype=='admin')
{
include_once("adminmenu.php");
}
else
```

```
{
include_once("usermenu.php");
}


$adminsession=$_SESSION['admin'];

if ($adminsession!=1)
{
echo "<div style='background-color: red; color: white; text-align: center; font-weight:
bold; font-family: arial'>Access Denied</div>";
include_once("login.html");
die(" ");
}


$i=1;

include_once("conn.php");

$q=mysql_query("select * from executiontime order by id desc");

echo "<table cellpadding=10 style='font-family: arial; font-size: 9pt' border=2
cellspacing=0 align=center cellpadding=5><tr bgcolor=skyblue style='font-weight:
bold'><td>Serial Number<td>File Size (In KB)<td>Without Security<td>MD5 + DES
<td>MD5 + RSA<td>RSA<td>DES<td>File Size Slot <table border cellspacing=0
cellpadding=5 style='font-size: 8pt'><tr><td><=100 KB <td> 1<tr><td>100-200 KB
<td> 2<tr><td>200-300 KB <td> 3<tr><td>300-400 KB <td> 4 <tr><td>>400 KB <td>
5</table>";
while ($r=mysql_fetch_object($q))
{
$fsizemb=$r->filesize/1024;
echo "<tr><td>$i<td>$fsizemb";
echo "<td>$r->withoutsecurity";
echo "<td>$r->md5des";
echo "<td>$r->md5rsa";
echo "<td>$r->rsa";
echo "<td>$r->des";
// echo "<td>$r->md5";
echo "<td>$r->slot";
$i++;
}


?>
```

```
<?php
error_reporting(0);


session_start();
$adminsession=$_SESSION['admin'];

$usertype=$_SESSION['usertype'];
if ($usertype=='admin')
{
include_once("adminmenu.php");
}
else
{
include_once("usermenu.php");
}


if ($adminsession!=1)
{
echo "<div style='background-color: red; color: white; text-align: center; font-weight:
bold; font-family: arial'>Access Denied</div>";
include_once("login.html");
die(" ");
}


$i=1;

include_once("conn.php");

$q=mysql_query("select * from uploads");

echo "<table cellpadding=10 style='font-family: arial; font-size: 9pt' border=2
cellspacing=0 align=center cellpadding=5><tr bgcolor=skyblue style='font-weight:
bold'><td>Serial Number<td>FileName<td>Execution Time<br>Existing
Approach<br>(In Microseconds)
<td>Execution Time<br>Proposed Approach<br>(In Microseconds)<td>Action";
while ($r=mysql_fetch_object($q))
{
echo "<tr><td>$i<td>$r->filename";
echo "<td>$r->etime";
echo "<td>$r->ptime";
echo "<td><a href=del.php?filename=$r->filename><strong>Delete</strong></a>";
$i++;
}


?>

<?php

include_once("usermenu.php");

include_once("conn.php");

$q2=mysql_query("select * from shared");

echo "<div align=center style='background-color: yellow; color: black; padding: 10px;
font-weight: bold'>SHARED DOCUMENTS</div>";
echo "<table cellpadding=10 cellspacing=0 style='font-family: arial; font-size: 9pt'
border=2 cellspacing=0 align=center cellpadding=5><tr bgcolor=skyblue style='font-
weight: bold'><td>File Name<td>View / Download";

while ($r2=mysql_fetch_object($q2))
{
echo "<tr><td>$r2->filename";
echo "<td><strong><a href='$r2->filename'>View / Download</a>";
}

echo "</table>";

?>

<?php
error_reporting(0);
session_start();

$_SESSION['usertype']=$u=$_POST['u'];
$p=$_POST['p'];

if ($usertype=='admin')
{
include_once("adminmenu.php");
}
else
{
include_once("usermenu.php");
}
```

```
$loginstatus=$_SESSION['login'];

if ($loginstatus!=1)
{
echo "<div style='background-color: red; color: white; padding: 5px; font-family: arial; font-weight: bold; text-align: center'>Invalid Login ... </div>";
include_once("login.html");
die(" ");
}
?>



<?php
include_once("conn.php");
$u=$_SESSION['u'];

echo "<div style='background-color: yellow; padding: 5px; font-weight: bold; font-family: arial'>Files Uploaded by the User Logged In : $u</div><br>";

$q=mysql_query("select * from uploads where username='$u'");

echo "<table style='font-family: arial; font-size: 9pt' border=2 cellspacing=0 align=center cellpadding=5><tr bgcolor=skyblue style='font-weight: bold'><td>File Name | File Size | File Type  | TimeStamp<td>Secured Hash Generation
<td>Execution Time<br>Existing Approach<br>(In Microseconds)
<td>Execution Time<br>Proposed Approach<br>(In Microseconds)<td>View / Download<td>Delete";
while ($r=mysql_fetch_object($q))
{
echo "<tr><td>$r->filename";


$filename=$r->filename;

echo "&nbsp; &nbsp; &nbsp; &nbsp; &nbsp; <a href='share.php?loc=$u/$filename' style='width: 200px; background-color: red; color: white; text-decoration: none; padding: 5px'>Share Document to Public Access</a>";

echo "<br><br>Size - $r->size Bytes";
echo "<br><br>FileType - $r->type";
echo "<br><br>TimeStamp - $r->timestamp";
echo "<td><strong>MD5 + SHA1 + RSA (Proposed Approach)</strong> - $r->md5"."+"."$r->sha1";

echo "<br><br><strong>DES + BLOWFISH (Classical Approach)</strong> - $r->des"."+"."$r->blowfish";
echo "<td>$r->etime";
echo "<td>$r->ptime";
echo "<td><strong><a href='$u/$filename'>Download</a>";
echo "<td><strong><a href=delete.php?id=$r->id>Delete</a>";
}
echo "</table>";


$q2=mysql_query("select * from shared");

echo "<div align=center style='background-color: yellow; color: black; padding: 10px;
font-weight: bold'>SHARED DOCUMENTS</div>";
echo "<table width=90% style='font-family: arial; font-size: 9pt' border=2 cellspacing=0
align=center cellpadding=5><tr bgcolor=skyblue style='font-weight: bold'><td>File
Name<td>View / Download";

while ($r2=mysql_fetch_object($q2))
{
echo "<tr><td>$r2->filename";
echo "<td><strong><a href='$r2->filename'>View / Download</a>";
}

echo "</table>";


?>

<?php

$loc=$_GET['loc'];

include_once("conn.php");

mysql_query("insert into shared(filename) values('$loc')");

header("location: showfiles.php");

?>

<?php
error_reporting(0);
$u=$_POST['u'];
$p=$_POST['p'];
$p2=$_POST['p2'];
```

```
if ($p!=$p2)
{
echo "<div align=center><font color=red><strong>Passwords do not Match</strong></div></div>";
include_once("register.html");
die(" ");
}

include_once("conn.php");

$q=mysql_query("select * from users where username='$u'");
if (mysql_num_rows($q) > 0)
{
include_once("register.html");
echo "<div style='background-color: red; color: white; font-family: arial; text-align: center'>Username already exist ... Choose another Username</div>";
die(" ");
}

mysql_query("insert into users(username, password) values('$u', '$p')");

echo "<div align=center><font color=red size=4><strong>Welcome $u... You are successfully registered</strong></font></div><br>";

mkdir($u);

echo "<br><div align=center><a href=login.html style='background-color: black; color: white; border-radius: 20px; padding: 20px; font-weight: bold; font-family: arial; text-decoration: none'>Click Here to Login</a></div>";

?>

<?php
error_reporting(0);
session_start();

echo $_SESSION['usertype']=$u=$_POST['u'];
$p=$_POST['p'];

if ($u=='admin')
{
include_once("adminmenu.php");
}
else
{
include_once("usermenu.php");
}

if (($u=="admin") and ($p=="admin"))
{
if (isset($_SESSION['u']))
{
echo "<div style='background-color: skyblue; text-align: center; font-weight:
bold'>Cloud User Already Logged In</div>";
die(" ");
}
$_SESSION['admin']=1;
$_SESSION['usertype']='admin';
echo "<div align=center style='color: red; font-weight: bold'>Administrator Login
Successful
<br><br><img src=admin.jpg>
</div>";
die(" ");
}
else
{
$_SESSION['usertype']='user';
}

if (isset($_SESSION['admin']))
{
echo "<a href=javascript:history.back(-1)>Back</a>";
die("Admin Already Logged In");
}

include_once("conn.php");

$q=mysql_query("select * from users where username='$u' and password='$p'");

if (mysql_num_rows($q) <= 0)
{
include_once("login.html");
die("Login Failed");
}



$thisip=$_SERVER['REMOTE_ADDR'];

$previousip=$_SESSION['ip'];

if ($thisip == $previousip)
```

```
{
$_SESSION['login']=1;
echo "<div align=center style='color: red; font-size: 11pt; font-weight: bold'>User
already Logged in<br><br><a href=logout.php>Sign Out and Retry</a></div>";
die(" ");
}

$_SESSION['u']=$u;

$_SESSION['login']=1;


echo "<div align=center><font face=arial color=blue size=3><strong>Current IP
Address - ".$thisip;

$_SESSION['ip']=$thisip;


echo "<br><br></font></strong><font face=arial size=4 color=red><strong>User
Logged in : $u</strong></font></div><br><br>";

echo "<br><div align=center><a href=upload.html style='background-color: black; color:
white; border-radius: 20px; padding: 20px; font-weight: bold; font-family: arial; text-
decoration: none'>Upload Files</a>

<a href=showfiles.php style='background-color: black; color: white; border-radius: 20px;
padding: 20px; font-weight: bold; font-family: arial; text-decoration: none'>Show Files in
the Cloud Storage</a></div>";

?>

<?php

require_once ('jpgraph/jpgraph.php');
require_once ('jpgraph/jpgraph_line.php');
include_once("conn.php");

$q=mysql_query("select * from uploads");

$stack1 = array();
$stack2 = array();

while ($row=mysql_fetch_object($q))
{
$classical=$row->etime;
$proposed=$row->ptime;
array_push($stack1, $classical);
array_push($stack2, $proposed);
}

$datay1 = $stack1;
$datay2 = $stack2;


// Setup the graph
$graph = new Graph(1000,550);
$graph->SetScale("textlin");

$theme_class=new UniversalTheme;
$graph->img->SetMargin(40,60,60,40);

$graph->SetTheme($theme_class);
$graph->img->SetAntiAliasing(false);
$graph->title->Set('Filled Y-grid');
$graph->SetBox(false);

$graph->img->SetAntiAliasing();

$graph->yaxis->HideZeroLabel();
$graph->yaxis->HideLine(false);
$graph->yaxis->HideTicks(false,false);

$graph->xgrid->Show();
$graph->xgrid->SetLineStyle("solid");
// $graph->xaxis->SetTickLabels(array('A','B','C','D'));
$graph->xgrid->SetColor('#E3E3E3');

// Create the first line
$p1 = new LinePlot($datay1);
$graph->Add($p1);
$p1->SetColor("#6495ED");
$p1->SetLegend('Line 1 - Execution Time or Overhead in Classical Approach');

$graph->xaxis->title->Set('X-Axis : Simulation Attempt of the Code | Y-Axis : Execution
Time in Microseconds');
// $graph->yaxis->title->Set('Execution Time in Microseconds');
$graph->yaxis->title->SetMargin(8);

// Create the second line
$p2 = new LinePlot($datay2);
$graph->Add($p2);
```

```
$p2->SetColor("#B22222");
$p2->SetLegend('Line 2 - Execution Time or Overhead in Proposed Approach');

$graph->legend->SetFrameWeight(1);

// Output line
$graph->Stroke();


?>

<?php
error_reporting(0);
session_start();
$usertype=$_SESSION['usertype'];

if ($usertype=='admin')
{
include_once("adminmenu.php");
}
else
{
include_once("usermenu.php");
}
?>

<br>

<div align=center>
<?php
include_once("login.html");
?>

<?php
// content="text/plain; charset=utf-8"
require_once ('jpgraph/jpgraph.php');
require_once ('jpgraph/jpgraph_line.php');

include_once("conn.php");

$q=mysql_query("select * from executiontime where slot='5'");
$stack1 = array();
$stack2 = array();
$stack3 = array();
$stack4 = array();
$stack5 = array();
```

```
$stack6 = array();

while ($row=mysql_fetch_object($q))
{
$ws=$row->ws;
$des=$row->des;
$md5des=$row->md5des;
$md5rsa=$row->md5rsa;
$rsa=$row->rsa;
$md5=$row->md5;
array_push($stack1, $ws);
array_push($stack2, $des);
array_push($stack3, $md5des);
array_push($stack4, $md5rsa);
array_push($stack5, $rsa);
array_push($stack6, $md5);
}

$datay1 = $stack1;
$datay2 = $stack2;
$datay3 = $stack3;
$datay4 = $stack4;
$datay5 = $stack5;
$datay6 = $stack6;


// Setup the graph
$graph = new Graph(1000,550);
$graph->SetScale("textlin");

$theme_class=new UniversalTheme;

$graph->SetTheme($theme_class);
$graph->img->SetAntiAliasing(false);
$graph->title->Set('Filled Y-grid');
$graph->SetBox(false);

$graph->img->SetAntiAliasing();

$graph->yaxis->HideZeroLabel();
$graph->yaxis->HideLine(false);
$graph->yaxis->HideTicks(false,false);

$graph->xgrid->Show();
$graph->xgrid->SetLineStyle("solid");
$graph->xaxis->SetTickLabels(array('1','2','3','4'));
```

```
$graph->xgrid->SetColor('#E3E3E3');

// Create the line 1
$p1 = new LinePlot($datay1);
$graph->Add($p1);
$p1->SetColor("#6495ED");
$p1->SetLegend('Without Security');

// Create the line 2
$p2 = new LinePlot($datay2);
$graph->Add($p2);
$p2->SetColor("#B22222");
$p2->SetLegend('DES');

// Create the line 3
$p3 = new LinePlot($datay3);
$graph->Add($p3);
$p3->SetColor("#006600");
$p3->SetLegend('MD5 + DES');

// Create the line 4
$p4 = new LinePlot($datay4);
$graph->Add($p4);
$p4->SetColor("#ff9900");
$p4->SetLegend('MD5 + RSA');

// Create the line 5
$p5 = new LinePlot($datay5);
$graph->Add($p5);
$p5->SetColor("#000000");
$p5->SetLegend('RSA');


// Create the line 6
$p6 = new LinePlot($datay6);
$graph->Add($p6);
$p6->SetColor("#3300CC");
$p6->SetLegend('MD5');

$graph->title->Set("Performance Analysis EXISTING APPROACH AND PROPOSED
APPROACH");
$graph->xaxis->title->Set("X-Axis Title : SIMULATION ATTEMPT | Y-Axis Title :
EXECUTION TIME");


$graph->legend->SetFrameWeight(1);
```

```
// Output line
$graph->Stroke();

?>

<?php
// content="text/plain; charset=utf-8"
require_once ('jpgraph/jpgraph.php');
require_once ('jpgraph/jpgraph_line.php');

include_once("conn.php");

$q=mysql_query("select * from executiontime where slot='1'");
$stack1 = array();
$stack2 = array();
$stack3 = array();
$stack4 = array();
$stack5 = array();
$stack6 = array();

while ($row=mysql_fetch_object($q))
{
$ws=$row->ws;
$des=$row->des;
$md5des=$row->md5des;
$md5rsa=$row->md5rsa;
$rsa=$row->rsa;
$md5=$row->md5;
array_push($stack1, $ws);
array_push($stack2, $des);
array_push($stack3, $md5des);
array_push($stack4, $md5rsa);
array_push($stack5, $rsa);
array_push($stack6, $md5);
}

$datay1 = $stack1;
$datay2 = $stack2;
$datay3 = $stack3;
$datay4 = $stack4;
$datay5 = $stack5;
$datay6 = $stack6;


// Setup the graph
```

```
$graph = new Graph(1000,550);
$graph->SetScale("textlin");

$theme_class=new UniversalTheme;

$graph->SetTheme($theme_class);
$graph->img->SetAntiAliasing(false);
$graph->title->Set('Filled Y-grid');
$graph->SetBox(false);

$graph->img->SetAntiAliasing();

$graph->yaxis->HideZeroLabel();
$graph->yaxis->HideLine(false);
$graph->yaxis->HideTicks(false,false);

$graph->xgrid->Show();
$graph->xgrid->SetLineStyle("solid");
$graph->xaxis->SetTickLabels(array('1','2','3','4'));
$graph->xgrid->SetColor('#E3E3E3');

// Create the line 1
$p1 = new LinePlot($datay1);
$graph->Add($p1);
$p1->SetColor("#6495ED");
$p1->SetLegend('Without Security');

// Create the line 2
$p2 = new LinePlot($datay2);
$graph->Add($p2);
$p2->SetColor("#B22222");
$p2->SetLegend('DES');

// Create the line 3
$p3 = new LinePlot($datay3);
$graph->Add($p3);
$p3->SetColor("#006600");
$p3->SetLegend('MD5 + DES');

// Create the line 4
$p4 = new LinePlot($datay4);
$graph->Add($p4);
$p4->SetColor("#ff9900");
$p4->SetLegend('MD5 + RSA');

// Create the line 5
```

```
$p5 = new LinePlot($datay5);
$graph->Add($p5);
$p5->SetColor("#000000");
$p5->SetLegend('RSA');


// Create the line 6
$p6 = new LinePlot($datay6);
$graph->Add($p6);
$p6->SetColor("#3300CC");
$p6->SetLegend('MD5');

$graph->title->Set("Performance Analysis EXISTING APPROACH AND PROPOSED
APPROACH");
$graph->xaxis->title->Set("X-Axis Title : SIMULATION ATTEMPT | Y-Axis Title
EXECUTION TIME");
// $graph->yaxis->title->Set("Y-title EXECUTION TIME");

$graph->legend->SetFrameWeight(1);

// Output line
$graph->Stroke();

?>
```