Design and Implementation of Security Policy for Public Cloud

Thesis submitted in partial fulfillment of the requirements for the award of degree
of

Master of Engineering
in
Software Engineering

By:
Jarrar
(Roll No. 800831004)

Under the supervision
of
Dr. Inderveer Chana
Assistant Professor

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT
THAPAR UNIVERSITY
PATIALA – 147004
July 2010

Certificate

I hereby certify that the work which is being presented in the thesis titled, **"Design and Implementation of Security Policy for Public Cloud"**, in partial fulfillment of the requirements for the award of degree of Master of Engineering in Software Engineering submitted in Computer Science and Engineering Department of Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of *Dr. Inderveer Chana* and refers other researcher's works which are duly listed in the reference section.

The matter presented in this thesis has not been submitted for the award of any other degree of this or any other university.

Jarrar A. Ra

(Jarrar)

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

Inderveer

(Dr. Inderveer Chana) 12/7/2k
Assistant Professor
Computer Science and Engineering Department
Thapar University,
Patiala

Countersigned by

12/07/10

(RAJESH BHATIA)
Head
Computer Science & Engineering Department,
Thapar, University
Patiala.

RK Sharma 14.7.10

(R.K.SHARMA)
Dean (Academic Affairs)
Thapar University,
Patiala.

Acknowledgement

I wish to express my deep gratitude to Dr. Inderveer Chana, Assistant Professor, Computer Science and Engineering Department, for providing her uncanny guidance and support throughout the preparation of the thesis report.

I am also heartily thankful to Dr. Maninder Singh, Associate Professor, Computer Science and Engineering Department for the motivation and inspiration that triggered me for my thesis work.

I would also like to thank all the staff members, Thapar University, and all my friends especially Zareen, Amandeep Kaur, Divya Pandove, Gagandeep Singh, Rupinderdeep Kaur who were always there at the need of the hour and provided all the help and support, which I required for the completion of the thesis.

Last but not the least; I would like to thank God for not letting me down at the time of crisis and showing me the silver lining in the dark clouds.

Jarrar
(800831004)

Abstract

Cloud computing has become a buzzword of today. Cloud computing is not a completely new concept; it has intricate connection to the established Grid Computing paradigm, and other relevant technologies such as utility computing, cluster computing and distributed systems in general. The term “cloud” is used as a metaphor for the Internet, based on how Internet is depicted in computer network diagrams.

Cloud computing promises to cut operational and capital costs and, more importantly, let IT departments focus on strategic projects instead of keeping the datacenters running. Cloud computing is much more than the simple Internet. It is a construct that allows user to access applications that actually reside at a location other than user’s own computer or other Internet-connected devices, most often of a distant datacenter. There are numerous benefits of this construct. For instance, some other company hosts user application. This implies that they handle the cost of servers, they manage the software updates, and depending on contract, user pays less i.e. for the service only. People can simply log in and use their applications wherever they are, therefore cloud computing is convenient for telecommuters and travelling remote workers too. Cloud computing is becoming increasingly relevant, as it will enable companies involved in spreading this technology to open the doors to Web3.0.

Cloud Computing has progressed a lot but still challenges like data security, data location, regulatory compliance, privileged user access etc need to be addressed. Amongst these, security and trust issues are major issues, since the user’s data has to be released to the Cloud and thus leaves the protection sphere of the data owner. In this thesis, security issues for Clouds have been analyzed. A user security policy has been designed. Further, a Cloud environment has been setup using Hadoop & the user authentication policy has been verified in this environment.

Contents

List of Figures &Tables

Chapter 1
Introduction

This chapter introduces cloud computing. It explains the various related technologies like distributed computing and Grid computing, and also the benefits of cloud environment.

1.1 Background

The term "Grid" was coined in the mid-1990s to denote a proposed distributed computing infrastructure for advanced science and engineering. Considerable progress has since been made on the construction of such an infrastructure, but the term "Grid" has also been conflated, at least in popular perception, to embrace everything from advanced networking to artificial intelligence [5]. The growth of the Internet, along with the availability of power computers and high-speed networks as low cost commodity components, is changing the way scientists and an engineer's do computing, and is also changing how society in general manages information and information services. These new technologies have enabled the clustering of a wide variety of geographically distributed resources, such as supercomputers, storage systems, data sources, special devices and services [14].

Grid computing and the utilization of the global grid infrastructure has presented significant challenges at all levels including conceptual and implementation models, application formulation and development, programming systems infrastructures and services, and resource management.

One of the most valuable aspects of all Grid Computing systems is that they attract the business they are intended to address. In an on-demand scenario, these Grid Computing environments are the result of autonomic provisioning of a multitude of resources and capabilities, typically demonstrating increased computing resource Utilization, access to specialized computer systems, cost sharing, and improved management capabilities [10].

1.2 Cloud Computing

The term 'Cloud' first appeared in the early 1990s, referring mainly to large ATM networks. Cloud computing began in earnest at the beginning of this century, just a short eight years ago with the advent of Amazon's web-based services. Less than two years ago, Yahoo and Google announced plans to provide cloud computing services to some country's largest universities: Carnegie Mellon, University of Washington, Stanford, and MIT. The IBM quickly announced plans to offer cloud computing technologies. More recent entries into the encounter include well- known companies: Sun, Intel, Oracle, SAS, and Adobe. All of these companies invested mightily in cloud computing infrastructure to provide vendor-based cloud services to the masses [13].

Cloud computing has become a buzzword of today. Cloud computing is not a completely new concept; it has intricate connection to the established Grid Computing paradigm, and other relevant technologies such as utility computing, cluster computing, and distributed systems in general[12]. The term "cloud" is used as a metaphor for the internet, based on how internet is depicted in computer network diagrams [2]. There has been a computing paradigm shift over the last half century, as illustrated in Figure 1.1 [11]:

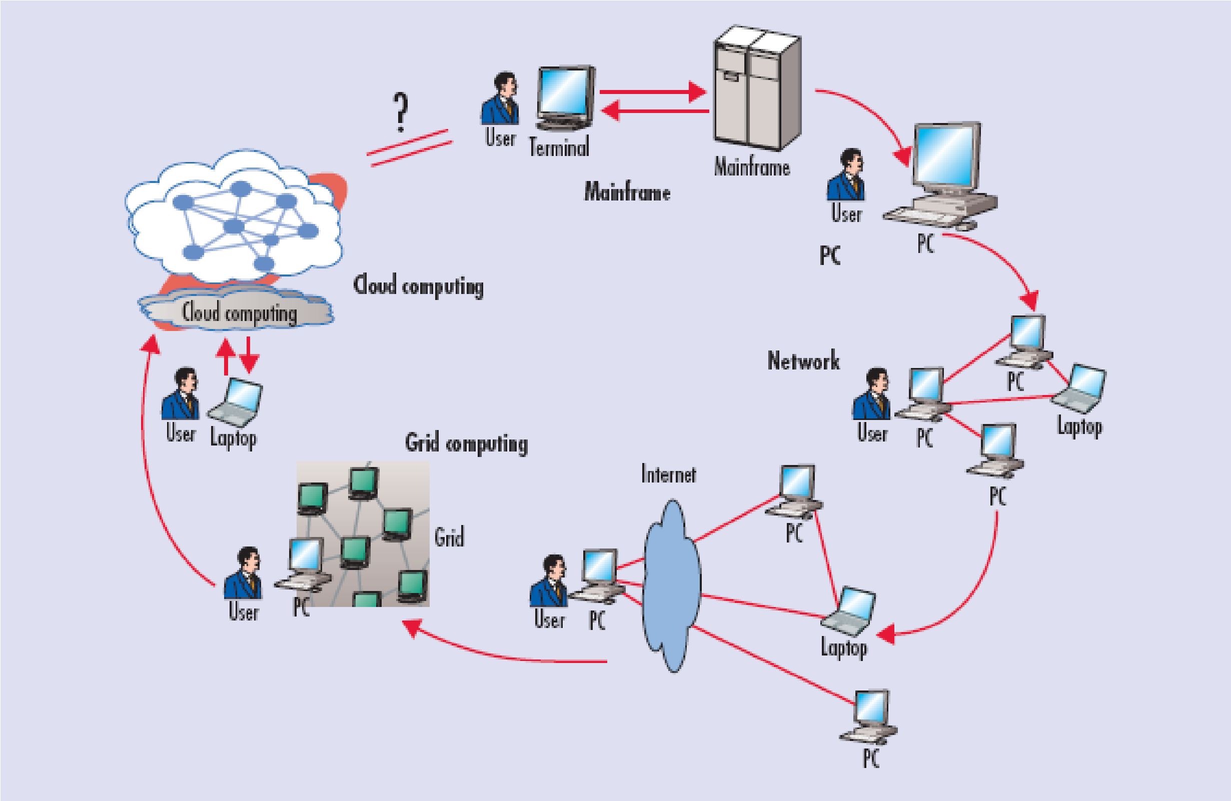


Figure 1.1: Computing paradigm shift. (Over six distinct phases, computers have evolved from dummy terminals to grids and clouds) [11].

Cloud Computing is a concept of computing in which dynamically scalable and often virtualized resources are provided as a service over the Internet. Cloud Computing consists of hardware and software resources made available on the Internet as managed by third-party services. These services typically provide access to advanced software applications and high-end networks of server computers [13].

To get Cloud Computing to work, three things are required: thin clients (or clients with a thick-thin switch), grid computing, and utility computing. Grid computing links disparate computers to form one large infrastructure, harnessing unused resources. Utility computing is paying for what users use on shared servers like consumers pay for a public utility such as electricity, gas, and so on[9].

1.3 Characteristics of Clouds

- Cloud Computing customers do not generally own the physical infrastructure serving as host to the software platform in question[9]
- Capital expenditure is reduced by renting usage from a third-party provider
- Customers consume resources as a service and pay only for resources that they use.
- Sharing "perishable and intangible" computing power can improve utilization rates, as servers are not unnecessarily left idle (which can reduce costs significantly while increasing the speed of application development).
- Agility improves with users able to rapidly and inexpensively re-provision technological infrastructure resources.
- Cost is greatly reduced and capital expenditure is converted to operational expenditure.
- This enables users to access systems using a web browser regardless of their location or what device they are using (*e.g.* PC, mobile).
- It enables sharing of resources and costs across a large pool of users.
- Reliability improves through the use of multiple redundant sites.

- Scalability via dynamic provisioning of resources on a fine-grained, self-service basis near real-time, without users having to engineer for peak.
- Security typically improves due to centralization of data.
- Sustainability comes about through improved resource utilization, and more efficient systems

1.4 Organization of Thesis

The chapters in thesis are organized as follows:

Chapter 2 This chapter describes in detail the literature survey, what is Cloud Computing is, various kinds of Clouds, based on the kind of services they provide, survey of security issues & benefits in Clouds.

Chapter 3 This Chapter describes the requirement analysis of security policy, design of security policy, UML diagrams, and comparative analysis of existing tools.

Chapter 4 describes in detail the design of the security policy, design alternatives approach in cloud.

Chapter 5 This chapter focuses on implementation of proposed design of security policy on hadoop in Cloud environment and experimental results of this approach.

Chapter 2

Literature Survey

This chapter describes in detail the literature survey, what is Cloud Computing, various kinds of Clouds, based on the kind of services they provide, survey of security issues & benefits in Clouds.

2.1 Cloud Computing Services

Cloud Computing provides different services like Software as a service (SaaS), Platform as a service (PaaS), and Infrastructure as a service (IaaS) *etc*. Each service has its security issues. The Cloud computing concept generally incorporates combinations of the following:

- Infrastructure as a Service - Traditional computing resources such as servers, storage, and other forms of low level network and hardware resources offered in a virtual, on demand fashion over the Internet. IaaS in a general sense provides the ability to call for resources in specific configurations at will and delivers value similar to what one might find in a traditional data centre. IaaS power lies in its massive on-the-fly flexibility and configurability [9].
- Platform as a Service - A runtime-system and application framework that presents itself as an execution environment and computing platform available over the Internet with the sole purpose of acting as a host to application software Generally, PaaS focuses on enabling SaaS applications, so many well-expected core concepts, such as abstracting away multi-tenancy issues, are expected of any reasonable PaaS offering. Another key concept for PaaS is that needs to run semi-arbitrary instructions [9].
- Software as a Service - Specialized software functionality delivered over the Internet to users who intend to use the set of delivered functionality to augment or replace real world processes. Generally speaking, users within the SaaS space are aggregated into tenants or bodies of one or more categorically related users [9].

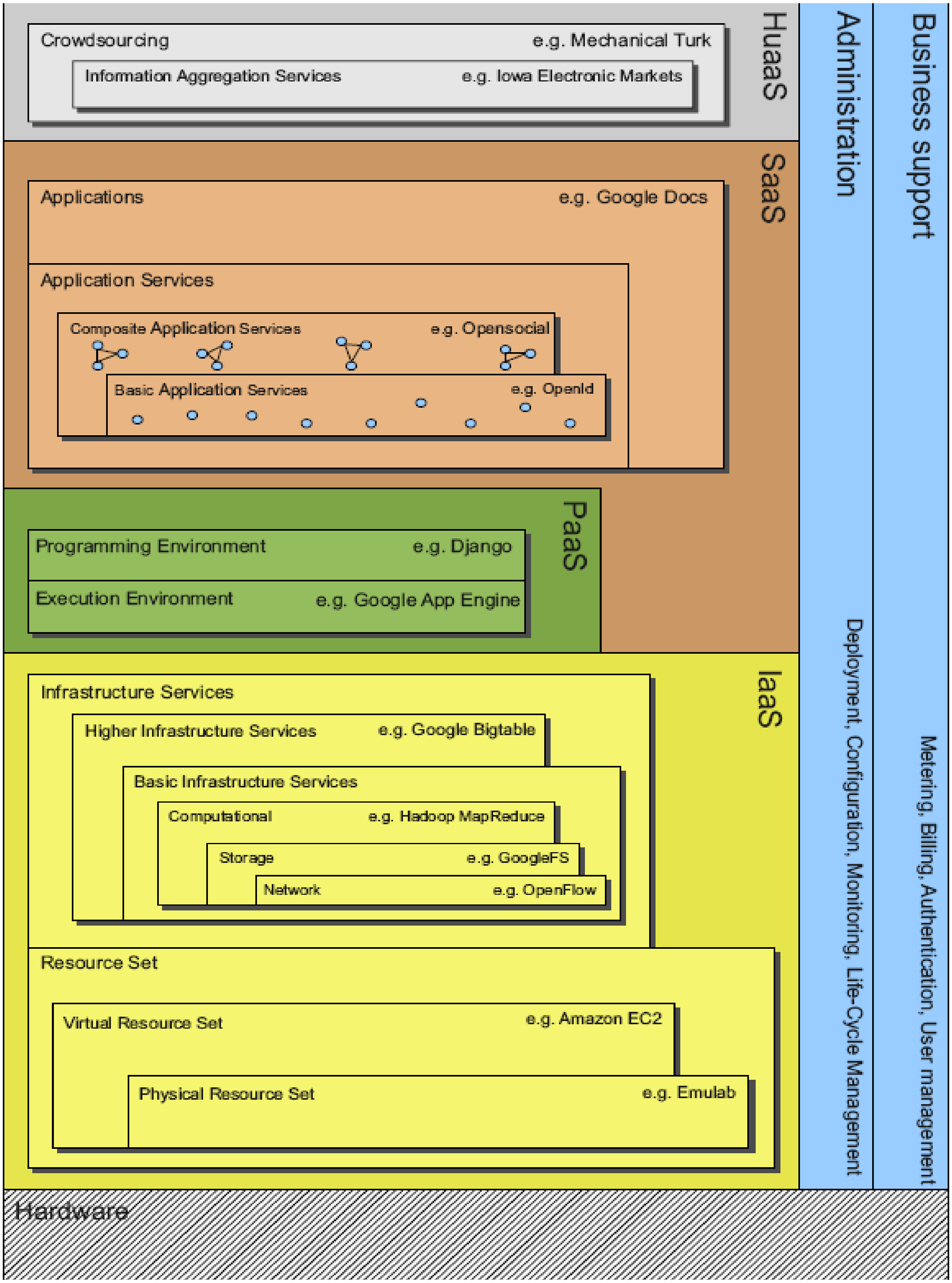


Figure 2.1: Cloud Computing Services [11]

- Infrastructure as a Service - Traditional computing resources such as servers, storage, and other forms of low level network and hardware resources offered in a virtual, on demand fashion over the Internet. IaaS in a general sense provides the ability to call for resources in specific configurations at will and delivers value similar to what one might find in a traditional data centre. IaaS power lies in its massive on-the-fly flexibility and configurability [9].
- Platform as a Service - A runtime-system and application framework that presents itself as an execution environment and computing platform available over the Internet with the sole purpose of acting as a host to application software Generally, PaaS focuses on enabling SaaS applications, so many well-expected core concepts, such as abstracting away multi-tenancy issues, are expected of any reasonable PaaS offering. Another key concept for PaaS is that needs to run semi-arbitrary instructions [9].
- Software as a Service - Specialized software functionality delivered over the Internet to users who intend to use the set of delivered functionality to augment or replace real world processes. Generally speaking, users within the SaaS space are aggregated into tenants or bodies of one or more categorically related users [9].
- Data-as-a-Service- Data-as-a-Service offering as one that facilitates the consumption and distribution of live data and business functionality over the Web. The live data feeds are available on a paid subscription basis, though there is also a free trial period, which companies such as D&B have long been in the business of providing information directly to customers [10].
- Network as a Service -Network as a Service concept seeks to deliver innovation to customers' businesses by leveraging the power of network-enabled IT utilization based on an integrated services platform comprising computers. It is networks and other IT resources, security technologies such as personal authentication, and an array of programs and interfaces for rapid business deployment. The services platform will be created through a combination of Fujitsu's dramatically enhanced FENICS value-added multi-

carrier network service and a soon-to-be-announced new SaaS (Software as a Service) platform, which will enable network delivery of advanced applications and content [10].

- Human as a Service - Some services rely on massive-scale aggregation and extraction of information from crowds of people. Each individual in the crowd may use whatever technology or tools he or she sees fit to solve the task. This top-most layer in our stack is called Human as a Service (HuaaS). In some cases human intelligence is used to contribute arbitrary services, such as newsworthy video streams, or on demand subtask solutions. Some human intelligence aggregation services are more controlled and more targeted at predicting events or promoting popular ideas [11].

2.2 Types of Clouds

Cloud Computing can be classified as suggested by Univa UD in [8] as follows -

- Public Cloud: Public Cloud or external Cloud describes Cloud Computing in the traditional mainstream sense, whereby resources are dynamically provisioned on a fine-grained, self-service basis over the Internet, via web applications/web services, from an off-site third-party provider who shares resources and bills on a fine-grained utility computing basis.
- Hybrid Cloud: Hybrid Cloud environment in which external services are leveraged to extend or supplement the internal Cloud simply put a mixture of both private and public Cloud [8].
- Community Cloud: A Community Cloud is controlled and used by a group of organizations that have shared interests, such as specific security requirements or a common mission. The members of the community share access to the data and applications in the Cloud.
- Private Cloud: Private Cloud and Internal Cloud are neologisms that some vendors have recently used to describe offerings that emulate cloud computing on private networks. These (typically virtualization automation) products claim to deliver some benefits of Cloud Computing without the

pitfalls, capitalizing on data security, corporate governance, and reliability concerns. They have been criticized on the basis that users still have to buy, build, and manage them and as such do not benefit from lower up-front capital costs and less hands-on management, essentially the economic model that makes Cloud Computing such an intriguing concept [7].

2.3 Cloud Security Issues and Benefits

Many new companies often lack the protection measures to weather off an attack on their servers due to the shortage of resources poor programming that explores software vulnerabilities (PHP, JavaScript, etc) open ports to firewalls. For this reason, new companies are encouraged to pursue cloud computing as the alternative to supporting their own hardware backbone. However, Cloud Computing does not come without its pitfalls. A cloud is a single point of failure for multiple resources. Even though network carriers such as AT&T believe a distributed cloud structure is the right implementation, it faces major challenges in finding the optimal approach for low power transmission and high network availability [1]. Some people believe that major corporations will retire away from implementing cloud solutions in the near future due to ineffective security policies. One problem comes from the fact that different cloud providers have different ways to store data, so creating a distributed cloud implies more challenges to be solved between vendors. Cloud computing has unique attributes that require risk assessment in areas such as data integrity, recovery, and privacy, and an evaluation of legal issues in areas such as e-discovery, regulatory compliance, and auditing [17].

Amazon's EC2 service and Google's Google App Engine are examples of cloud computing, which defines as a type of computing in which massively scalable IT-enabled capabilities are delivered as a service to external customers using Internet technologies .

Customers must demand transparency, avoiding vendors that refuse to provide detailed information on security programs. Ask questions related to the qualifications of policy makers, architects, coders and operators; risk-control processes and technical mechanisms; and the level of testing that's been done to verify that service and control processes are functioning as intended, and that vendors can identify unanticipated vulnerabilities.

There are seven specific security issues. Customers should rise with vendors before selecting a cloud vendor [5], while addressing these issues:

2.3.1 Privileged User Access

Sensitive data processed outside the enterprise brings with it an inherent level of risk, because outsourced services bypass the physical, logical and personnel controls IT shops exert over in-house programs. Get as much information as user can about the people who manage user data. Ask providers to supply specific information on the hiring and oversight of privileged administrators, and the controls over their access.

2.3.2 Regulatory Compliance

Customers are ultimately responsible for the security and integrity of their own data, even when it is held by a service provider. Traditional service providers are subjected to external audits and security certifications. Cloud Computing providers who refuse to undergo this scrutiny are signaling that customers can only use them for the most trivial functions [5].

2.3.3 Data Location

When user uses the cloud, User probably won't know exactly where data is hosted. In fact, User might not even know what country it will be stored in. Ask providers if they will commit to storing and processing data in specific jurisdictions, and whether they will make a contractual commitment to obey local privacy requirements on behalf of their customers [5].

2.3.4 Data Security

Security refers to confidentiality, integrity and availability, which pose major issues for cloud vendors. Confidentiality refers to who stores the encryption keys data from company A, stored in an encrypted Format at company B must be kept secure from employees of B; thus, the client company should own the encryption keys. Integrity refers to the face that no common policies exist for approved data exchanges; the industry has various protocols used to push different software images or jobs. One way to maintain data security on the client side is the use of thin clients that run with as few resources as possible and do not store any user data, so passwords cannot be stolen. The concept seems to be impervious to attacks based on capturing this data. However, companies have implemented systems with unpublished APIs, claiming that it improves security [3].

2.3.5 Data Segregation

Data in the Cloud is typically in a shared environment alongside data from other customers. Encryption is effective but isn't a cure-all. The cloud provider should provide evidence that encryption schemes were designed and tested by experienced specialists. Encryption accidents can make data totally unusable, and even normal encryption can complicate availability [5].

2.3.6 Data Recovery

Even if user doesn't know where the data is, a Cloud provider should tell user what will happen to data and service in case of a disaster. Any offering that does not replicate the data and application infrastructure across multiple sites is vulnerable to a total failure. Ask user provider if it has the ability to do a complete restoration, and how long it will take [5].

2.3.7 Investigative Support

Investigating inappropriate or illegal activity may be impossible in Cloud Computing. Cloud Services are especially difficult to investigate, because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centers. If user cannot get a contractual commitment to support specific forms of investigation, along with evidence that the vendor has already successfully supported such activities, then user is only safe assumption is that investigation and discovery requests will be impossible [5].

2.4 Cloud Security Benefits

There are definitely a lot of concerns regarding the inability to trust cloud computing due to its security issues. All kinds of security measures are cheaper when implemented on a larger scale. Therefore the same amount of investment in security buys better protection. This includes all kinds of defensive measures such as filtering; patch management, hardening of virtual machine instances and hypervisors, etc.

Other benefits of scale include: multiple locations, edge networks timeliness of response, to incidents, threat management mentioned by [2].

- Security is a priority concern for many Cloud customers; many of them will make buying choices on the basis of the reputation for confidentiality, integrity and resilience of, and the security services offered by, a provider. This is a strong driver for Cloud providers to improve security practices [12].

- Large Cloud providers can offer a standardized, open interface to managed security services providers. This creates a more open and readily available market for security services.

- The ability of the Cloud provider to dynamically reallocate resources for filtering, traffic shaping, authentication, encryption, etc to defensive measures has obvious advantages for resilience.

- Cloud Computing (when using virtualization) can provide dedicated, pay-per-use forensic images of virtual machines which are accessible without taking infrastructure off-line, leading to less down-time for forensic analysis. It can also provide more cost-effective storage for logs allowing more comprehensive logging without compromising performance.

- Default virtual machine images and software modules used by customers can be pre-hardened and updated with the latest patches and security settings according to fine-tuned processes, IaaS cloud service APIs also allow snapshots of virtual infrastructure to be taken regularly and compared with a baseline. Updates can be rolled out many times more rapidly across a homogenous platform than in traditional client-based systems that rely on the patching model [15].

This chapter presented in detailed what Cloud Computing is along with a detailed, various kinds of Clouds based on the kind of services they provide, survey of security issues & benefits in Clouds.

Next Chapter will focus on the requirement analysis of security policy, software specification requirement, U M L diagrams, and comparative analysis of existing tools.

Chapter 3

Cloud Security: Requirement Analysis

This chapter describes the requirement analysis of security policy, design of security issues policy, UML diagrams, and comparative analysis of existing tools for Cloud environment. All the requirements for setting up a secure Cloud have been gathered from literature survey & presented in SRS described in below:

3.1 Software Requirement Specification

This SRS describes functional & non-functional requirements for secure Cloud.

3.1.1 Introduction

This introduction to Virtual Public Cloud is intended to give a high-level overview Cloud security issues. This document highlights the capabilities and requirements that need to be standardized in a cloud environment to ensure interoperability, security, ease of integration and portability. Cloud Computing must evolve as an open environment, minimizing vendor lock-in and increasing customer choice.

- Purpose

  The main objective of this document is to illustrate the requirement of virtual public Cloud. This document gives the detailed description of both the functional and non-functional requirements proposed by vendor.

- Scope

  Cloud Computing technology that provides organizational abilities to access software and hardware resources from a virtual space. User can use any manner of small applications/programmers/software can be used to edit images, video, power points, excel sheets, etc. which might not be available on local machines. Cloud Computing is unlimited by the availability of internet. It is very useful for remote areas. People can use all sorts of computer applications and manage data without being shifted to metros. It can be even in a small town. This technology facilitates delivery of common business applications online that are accessed from the Internet.

- Definition:

  A compiled definition of public Cloud or internal Cloud is based on an environment which is capable of running and implementing characteristics of cloud computing like virtualization and layered services over the network but at the same time also applies stricter polices and requirements like security, latencies, SLAs and also usage of existing data enter resources. An existing cloud user may have been familiar with Amazon EC2, Amazon S3, Google APP Engine, Apache Hadoop, Cloud era and other products from companies providing cloud infrastructure or cloud-based software and service.

- References

[1] http://groups.google.com/group/cloud-computing-use-cases.

[2] Cloud Computing Use Cases Whitepaper. http://www.scribd.com/doc/17929394/ Cloud-Computing-Use-Cases-Whitepaper. Cloud Computing Use Case Discussion group 2009-08.

[3] Cloud Computing :A practical approach ,Anthony T. Velte ,Toby J. Velte ,Robert Elsenpeter ,TATA McGRAW-HILL EDITTION-2010

3.1.2 Overall Description

- Product Perspective

  The proposed Cloud model which is designed is a security aware cloud model. This model will provide security and scalability .Cloud ready services will be online that can be accessed from thin client or web browser, while the software and data are stored on the servers. These services and servers run in a collaborative environment through the combination of private and public Cloud. Security concerns the barrier for large scale adoption of cloud computing.

- Cloud Computing Interface

  There is a needed for a standard interface for dynamic infrastructure provisioning for cloud.

  - SLA-aware cloud infrastructure using SLA.
  - Service Manger to control the life cycle of Services.

- Interoperability across cloud infrastructure using open source tool.
- AJAX web front-end directly calling API.
- Single technical integration to support multiple service providers.
- Automated business Continuity and Disaster Recovery.
- Manage Cloud resources from a Centralized dashboard.
- Wrapping EC2 in CCI.

- **Hardware Requirements for Generic Public Cloud**

➢ For one user Cloud:

Memory**:** 2.0 GB

Storage**:** 160 GB

Platform: 32-bits

➢ For Four users Cloud:

Memory: 8.0 GB

Storage: 850 GB

Platform: 64-bits

➢ For eight users Cloud:

Memory: 16 GB

Storage: 1,690 GB

Platform: 64-bits

3.1.3 Functional Requirements

Virtual Machine Description**:** A means to add non-functional constraints on functional attributes. Virtual Machine should be described consistently across cloud providers using a slim set of indispensable attributes, such as:

- Memory: Amount of RAM needed by the Virtual Machine.

- CPU: Number of CPUs needed by the Virtual Machine.
- Disk: Disks that will be conform the basic file system and possibly others for the Virtual Machine.
- Virtual Machine Management**:** All parameters in the request should be monitor –able and verifiable. Full control of resources allocated required, a minimum: start, stop, suspend resume.
- DEPLOY: Launch the Virtual Machine.
- SHUTDOWN*:* Shutdown the Virtual Machine.
- CANCEL: Cancels the virtual Machine in case of failure, or destroys if it is running.
- CHECKPOINT: Creates a snapshot of the virtual machine.
- SAVE: Creates a snapshot of the virtual machine and suspends it.
- RESTORE: Resumes a virtual Machine from a previous snapshot.
- ROLL: Retrieves information about virtual machine state and consumption attributes (percentages of memory, CPU, used, bytes transferred, and so on).
- Storage Management: Simple mount points, resume storage SaaS offerings.
- Geographical Restrictions**:** Locations where the VM can / cannot be deployed.
- Migration Allowed (yes/no*):* If migration is supported by the infrastructure, this flag sets .if it is allowed for the VM.
- Error Messages**:** If a Virtual Machine cloud not be created, or an image cloud not be uploaded, etc. The platform should return an error message carrying a detailed description of the reason.
- Network Management: API should expose functionality to
- Create private Virtual Networks.
- Attach public IP to Virtual Machine.
- Identity**:** The cloud service must authenticate the end user.

3.1.3 Non –Functional Requirements

- Security*:* Transport and user level security.
- Scheduling Information: When a particular resource is to be run. Also in which order should a collection of resources be run in this case that one resource is dependent on another.
- Quality of Service: Part of services offering from infrastructure provider e.g. security QoS, isolation levels.
- Syntax: A simple JSON syntax for the API will make the AJAX interfaces much simpler to implement.
- Availability**:** Availability of service request.
- Scalability: The cloud refers to unlimited scalability to user.
- Interoperability: Because more than one enterprise is involved, interoperability between the enterprises is essential**.**
- Location awareness: A way of identifying the location of the Physical machine hosting the cloud infrastructure is an absolute requirement for many government regulations.
- Completeness**:** APIs must be containing complete set of calls to completely specify and control cloud.
- Uptake*:* Standardized IaaS API needs strong uptake in by both cloud providers and cloud ecosystem.
- Usability**:** This should be allowing to user to easily see what actions can be performed for each resources.
- Search ability*:* The ability to request lists of resources must allow an optional filter that can specify a category

3.2 U M L Diagram

Use case diagram shows the functionality provided by a system in terms of user, administrator their goals represented as use cases, and any dependencies among those use cases. In this work, focus is on security policy & specifically on user authentication. Therefore, following UML diagram have been drawn. As part of UML (as shown in Figure 3.1) are used to capture the requirements for required user authentication.

- **Use Case Diagram:** Use case diagram has been shown in fig 3.1.

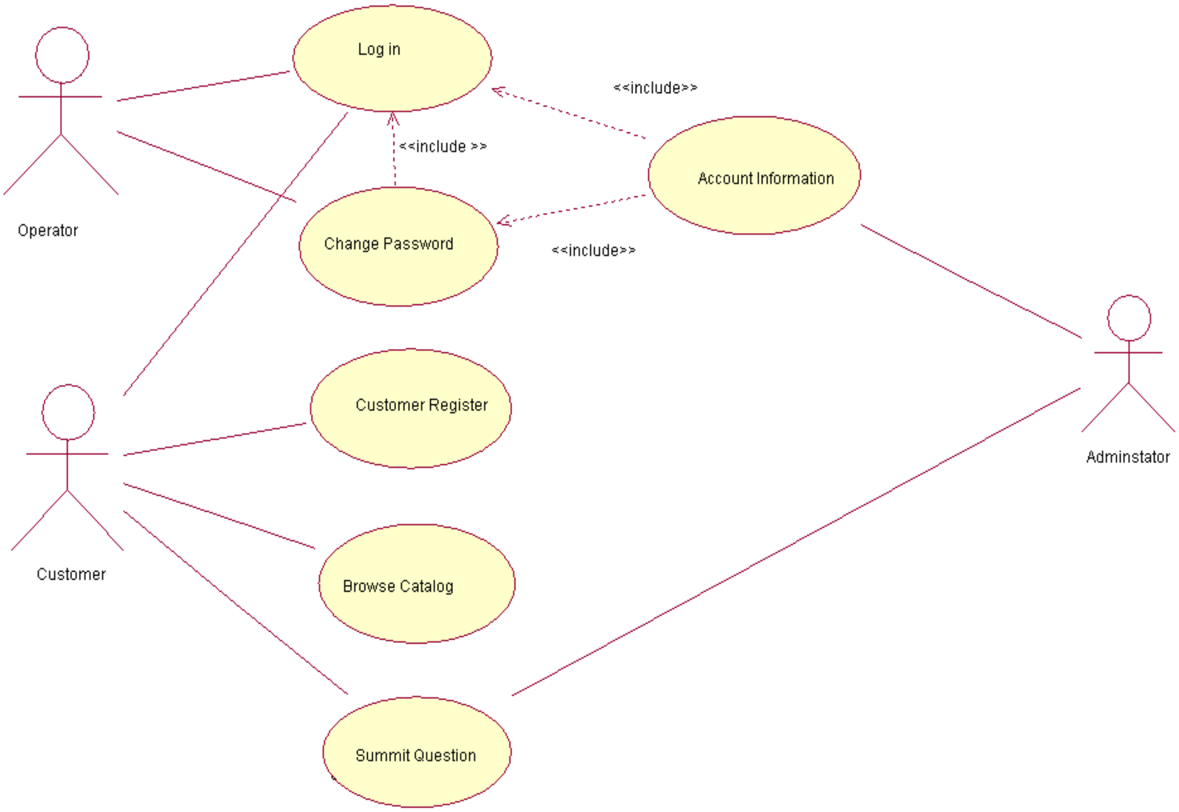


Figure 3.1: Use Case Diagram for Customer Account for Login.

- **Sequence Diagram:** sequence diagram has been shown in Fig3.2.

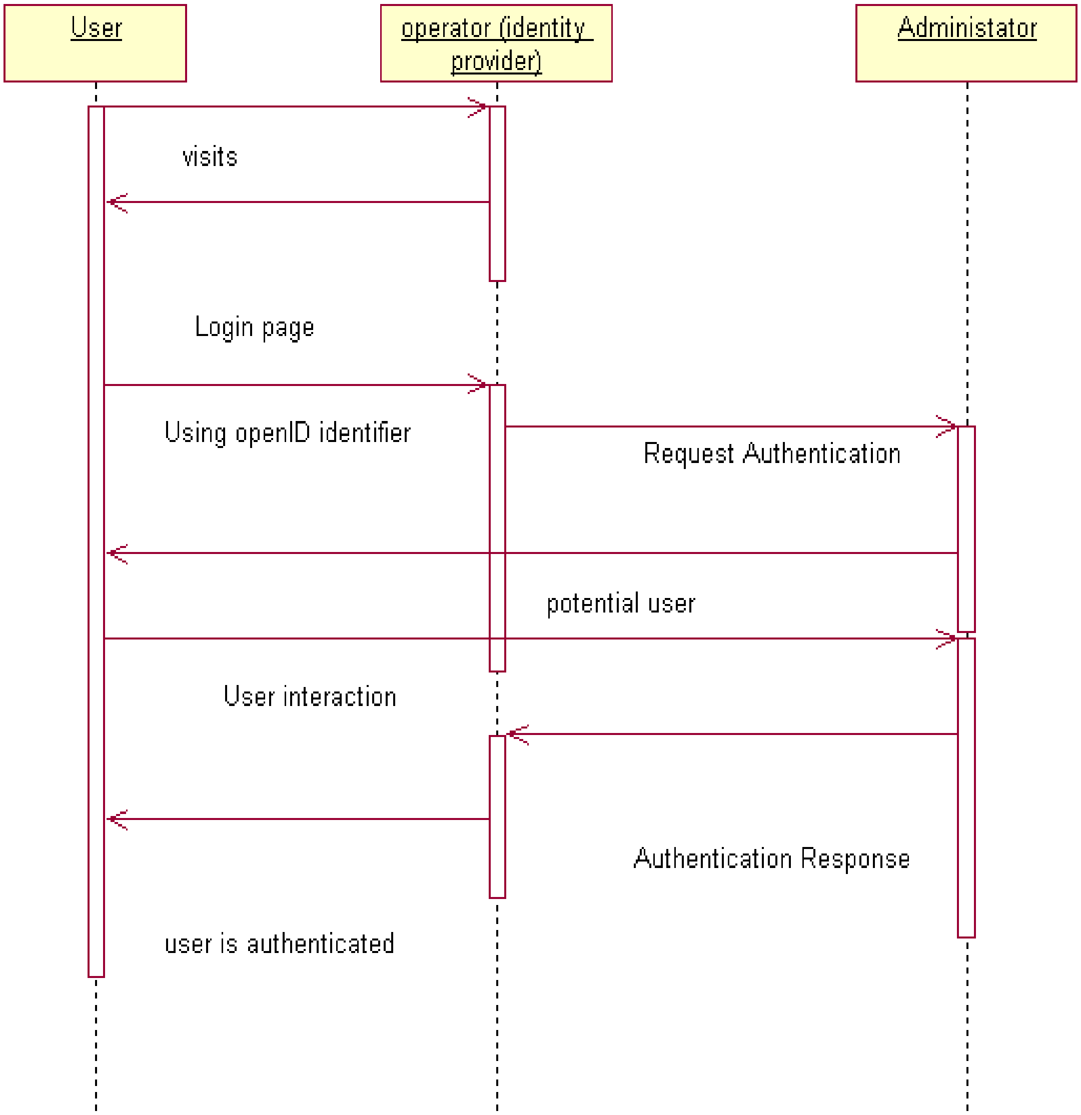


Figure 3.2: Sequence Diagram for Login

- **Activity Diagram:** Activity diagram has been shown in Fig 3.3

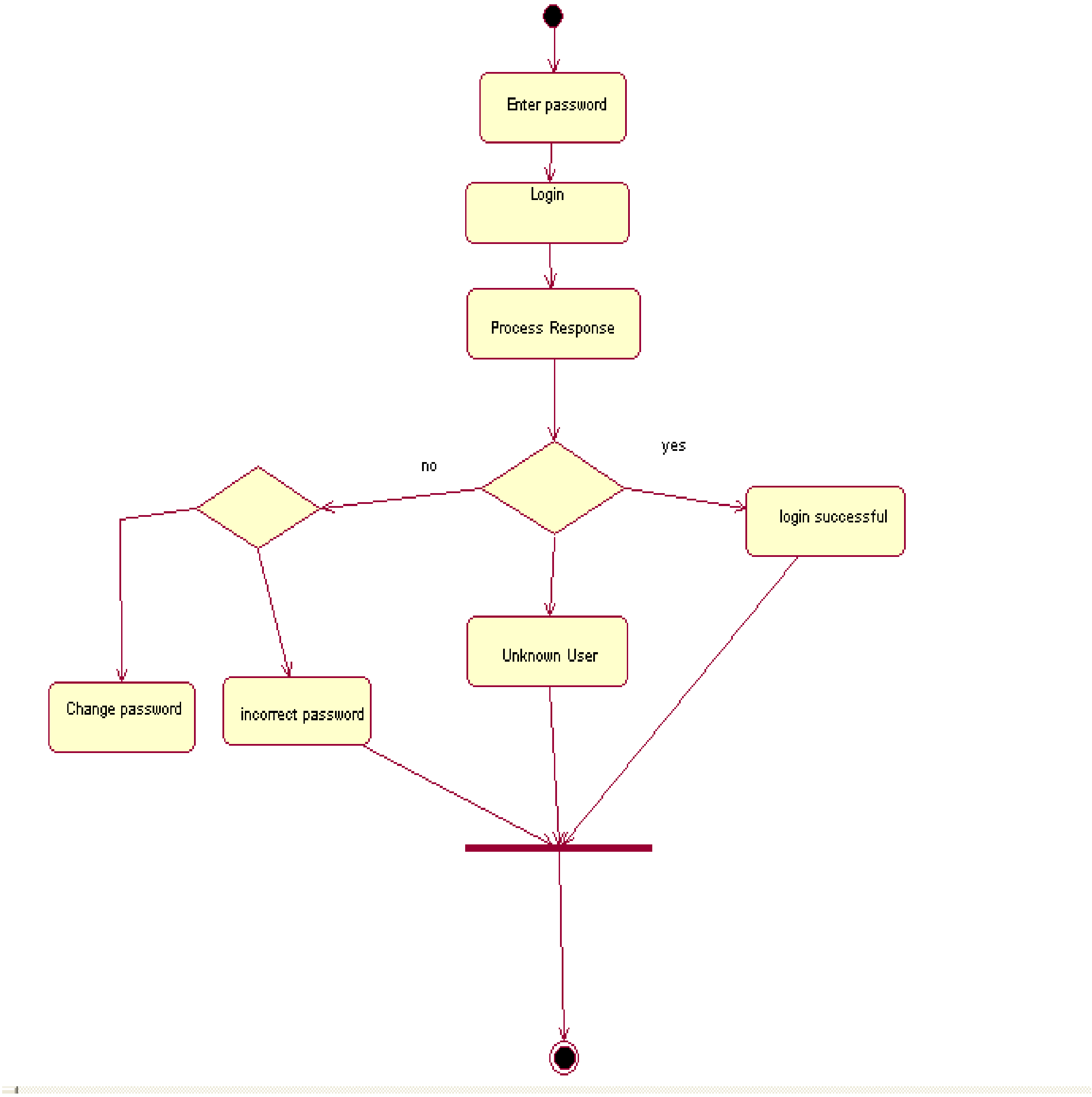


Figure 3.3 Activity Diagram for Login

3.2 Categorization of Security Issues

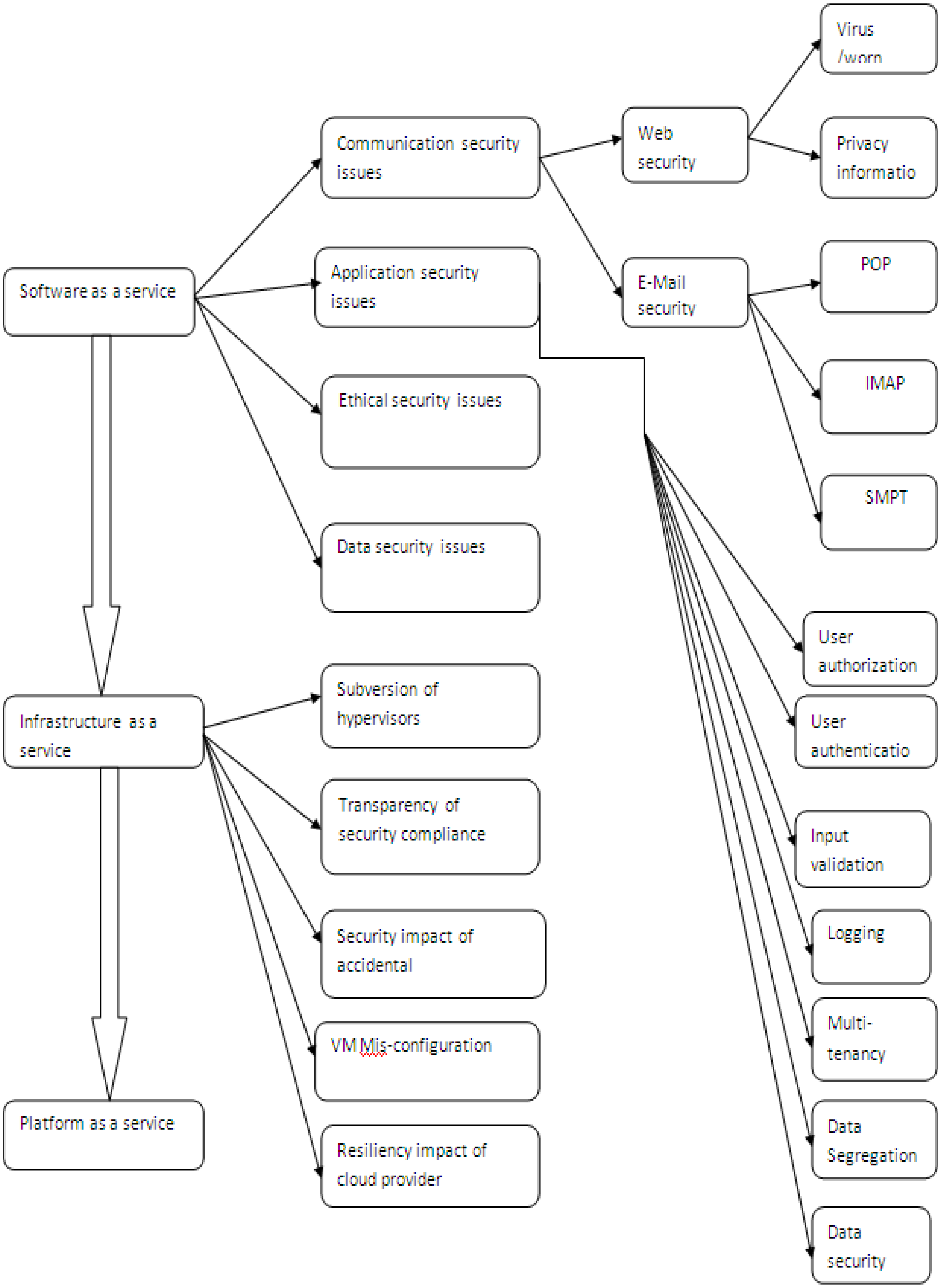


Figure 3.4: Categorization of Security Issues

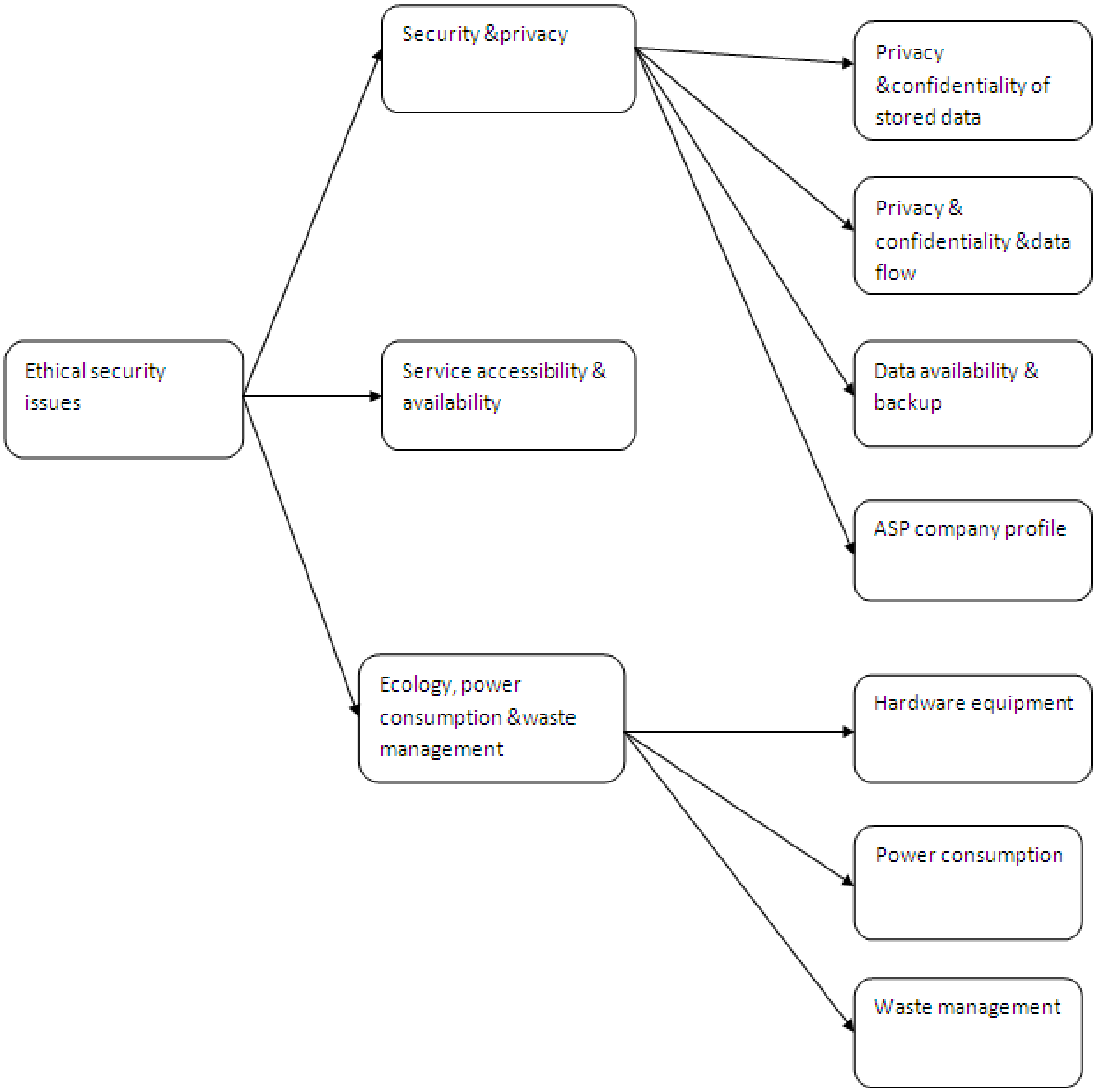
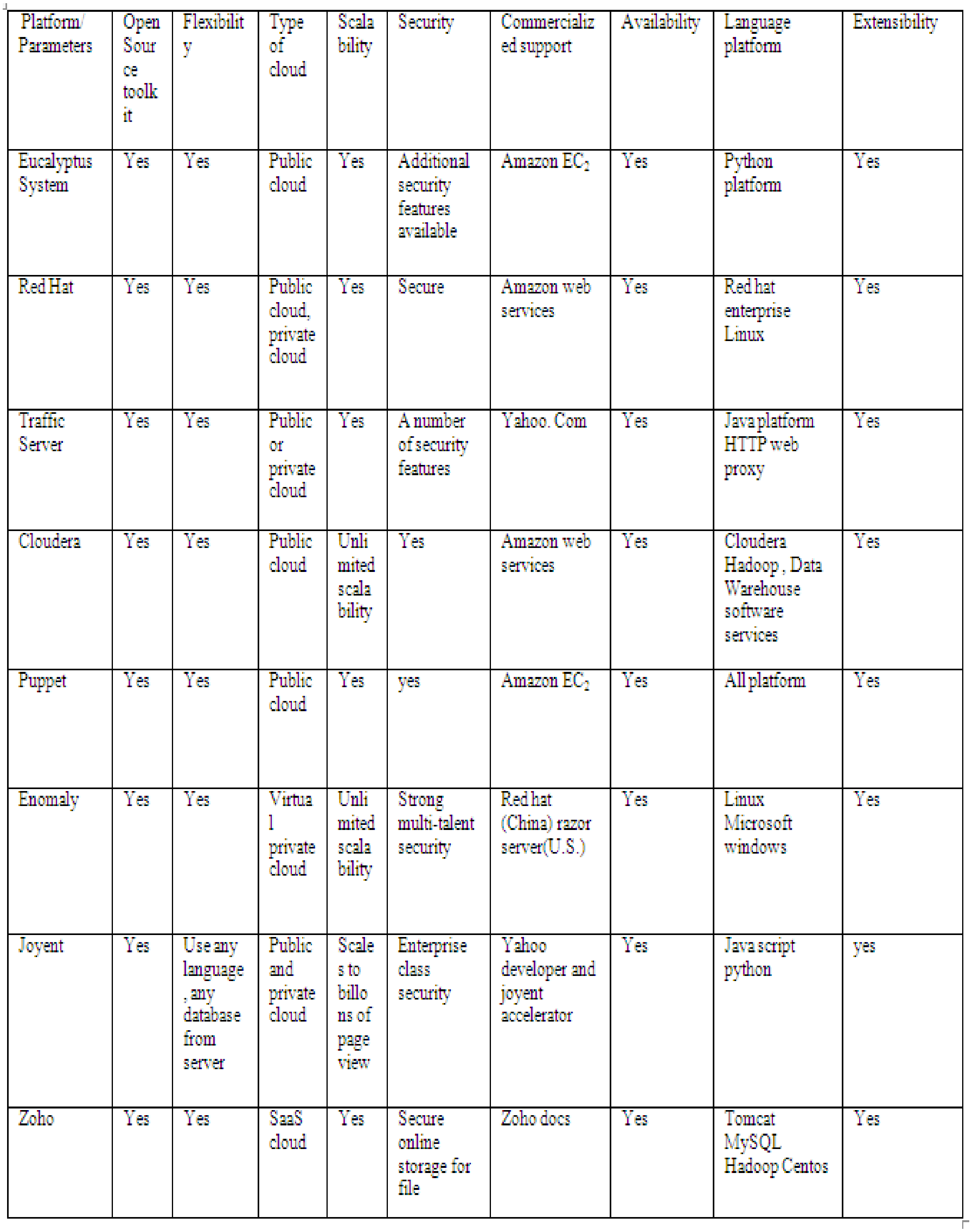

Ethical security issues
Security &privacy
Service accessibility & availability
Ecology, power consumption &waste management
Privacy &confidentiality of stored data
Privacy & confidentiality &data flow
Data availability & backup
ASP company profile
Hardware equipment
Power consumption
Waste management

Figure 3.5: Categorization of Security Issues

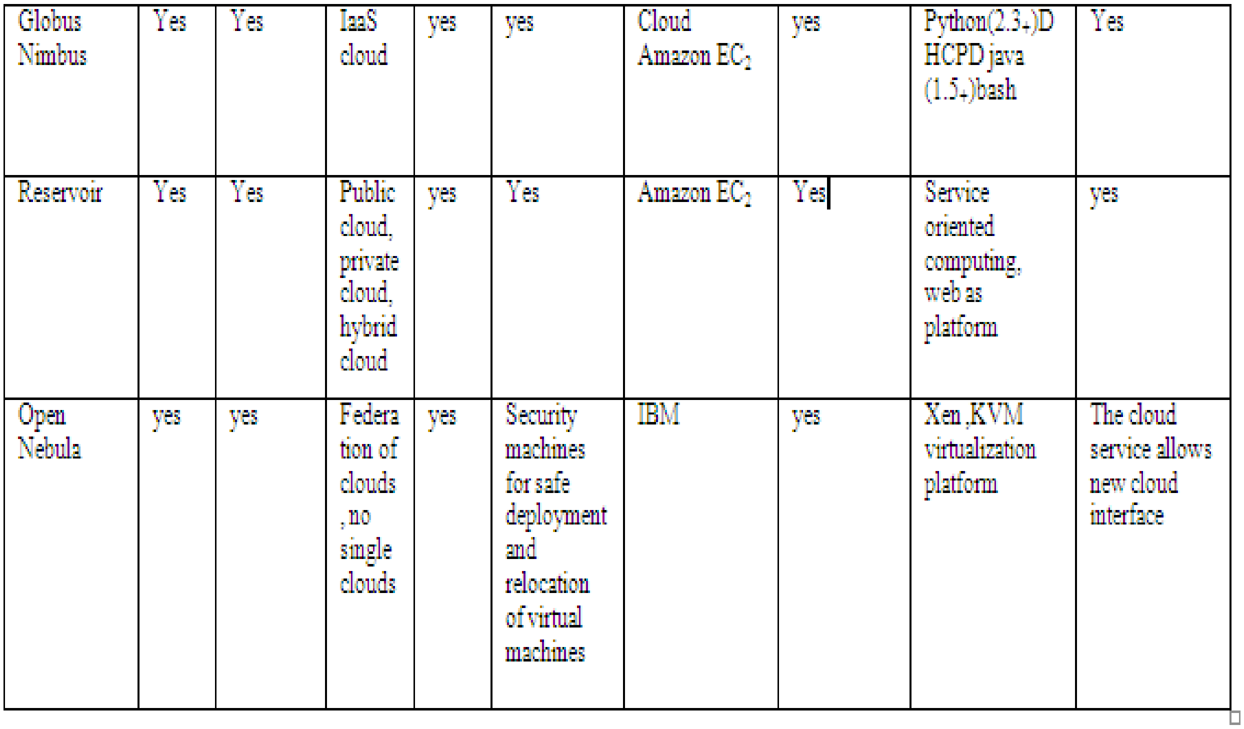
3.3 Comparative Analysis of Open Sources Tools

Numerous tools are available for Cloud Computing. The 11 popular tools available till date have been surveyed and compared on the basis of following parameters such as flexibility, scalability, security, availability, language platform, extensibility etc. This comparison has been shown in Table 1.

Table 1: Comparison top 11 Open Source Tools for Cloud Computing



Platform/ Parameters	Open Source toolkit	Flexibility	Type of cloud	Scalability	Security	Commercialized support	Availability	Language platform	Extensibility
Eucalyptus System	Yes	Yes	Public cloud	Yes	Additional security features available	Amazon EC_2	Yes	Python platform	Yes
Red Hat	Yes	Yes	Public cloud, private cloud	Yes	Secure	Amazon web services	Yes	Red hat enterprise Linux	Yes
Traffic Server	Yes	Yes	Public or private cloud	Yes	A number of security features	Yahoo. Com	Yes	Java platform HTTP web proxy	Yes
Cloudera	Yes	Yes	Public cloud	Unlimited scalability	Yes	Amazon web services	Yes	Cloudera Hadoop , Data Warehouse software services	Yes
Puppet	Yes	Yes	Public cloud	Yes	yes	Amazon EC_2	Yes	All platform	Yes
Enomaly	Yes	Yes	Virtual private cloud	Unlimited scalability	Strong multi-talent security	Red hat (China) razor server(U.S.)	Yes	Linux Microsoft windows	Yes
Joyent	Yes	Use any language , any database from server	Public and private cloud	Scales to billons of page view	Enterprise class security	Yahoo developer and joyent accelerator	Yes	Java script python	yes
Zoho	Yes	Yes	SaaS cloud	Yes	Secure online storage for file	Zoho docs	Yes	Tomcat MySQL Hadoop Centos	Yes



Globus Nimbus	Yes	Yes	IaaS cloud	yes	yes	Cloud Amazon EC_2	yes	Python(2.3+)D HCPD java (1.5+)bash	Yes
Reservoir	Yes	Yes	Public cloud, private cloud, hybrid cloud	yes	Yes	Amazon EC_2	Yes	Service oriented computing, web as platform	yes
Open Nebula	yes	yes	Federation of clouds , no single clouds	yes	Security machines for safe deployment and relocation of virtual machines	IBM	yes	Xen ,KVM virtualization platform	The cloud service allows new cloud interface

This chapter mainly discussed on requirement analysis, UML diagrams, and comparative analysis of existing tools for setting up Cloud environment.

Next chapter will focus on design of security policy, design alternatives approaches.

Chapter 4

Design of Security Policy

Security policy can be defined as rules that regulate how an organization manages and protects its information and computing resources. The policy tells the users, staff, managers what they can do, what they cannot do, what they must do. The vast majority of organizations fail to proactively safeguard sensitive business information that is being stored in the cloud. In this thesis, user recommend a policy development approach that is consistent with industry best practice standards such as ISO 177992/27001 format.

4.1 Design of security policy (ISO 17799/27001 Format)

Cloud Security Policies are the combination of objects and access rights. They are individual items that can be applied to any piece of the system - content types, pages, discussions, users, administrator, third party, and authorization & authentication policy for user. Following security policies has been design for public Cloud.

4.1.1 User Access Control Policy: An access control policy established, documented and periodically reviewed is based on business needs and external requirements. Access control policy should take account of:

- Security issues for particular data systems, given business needs, anticipated threats and vulnerabilities.
- Security issues for particular types of data, given business needs, anticipated threats and vulnerabilities.
- All relevant legislative, regulatory and certificatory requirements.
- Relevant contractual obligations or service level agreements.
- Other organizational policies for information access, use and disclosure.
- Consistency among such policies across the organization's systems and networks.

i) **User Password Management Policy:** Allocation of passwords should be control through a formal management process. It includes:

- Requiring users to sign a statement indicating they will keep their individual passwords confidential and, if applicable, any group passwords solely within the group.
- Secure methods for creating and distributing temporary, initial-use passwords.
- Forcing users to change any temporary, initial-use password.
- Development of procedures to verify a user's identity prior to providing a replacement password (password reset).
- Prohibiting loaning of passwords.
- Prohibiting storage of passwords on computer systems in unprotected form.
- Prohibiting use of default vendor passwords, where applicable.

ii) **User Access Token Management Policy:** Allocation of access tokens, such as key-cards, should be controlled through a formal management process. It includes:

- Requiring users to sign a statement indicating they will keep their access tokens secure.
- Secure methods for creating and distributing tokens.
- Use of two-factor tokens (token plus PIN) where appropriate and technically feasible.
- Development of procedures to verify a user's identity prior to providing a replacement token.

iii) **Review of User Access Rights Policy:** Each user's access rights should be periodically reviewed using a formal process. It includes:

- Review at regular intervals, and after any status change (promotion, demotion, transfer, termination).
- More frequent review of privileged (super user) access rights.

iv) **Password Use Policy:** Users should follow good security practices in the selection and use of passwords. It includes advising/requiring users to:

- Keep passwords confidential and not share them.

- Avoid keeping a paper or electronic record of passwords, unless this can be done securely.
- Change a password when there is any suspicion that it has been compromised, and report the suspicion.
- Select strong passwords that are resistant to dictionary, brute force or other standard attacks.
- Change passwords periodically.
- Change a temporary password on first log-on.
- Avoid storing passwords in automated log-on processes.
- Not use the same password for business and non-business purposes.
- Use the same password for multiple systems/services only where a reasonable level of security can be assured for each.

v) **User Identification and Authentication Policy:** All data system users should have a unique identifier (user-ID) for their personal use only. Suitable authentication technique knowledge, token should be chosen to authenticate the user. It includes:

- Shared user-IDs are employed only in exceptional circumstances, where there is a clear justification.
- Generic user-IDs are employed only where no individual-user audit is required and limited access privileges otherwise justify the practice.
- Strength of the identification and authentication method (e.g., use of multiple authentication factors) are suitable to the sensitivity of the information being accessed.
- Regular user activities are not performed from privileged accounts.

4.1.2 User Account Policy

User Account Policy is a document which outlines the requirements for requesting and maintaining an account on computer systems or networks, within an organization. It is very important for large sites where users typically have accounts on many systems. Some sites have users read and sign an Account Policy as part of the account request process. It includes following polices:

- Should state who has the authority to approve account requests.
- Should state who is allowed to use the resources (*e.g.* employees or students only).
- Should state any citizenship/resident requirements.
- Should state if users are allowed to share accounts or if users are allowed to have multiple accounts on a single host.
- Should state the user's rights and responsibilities.
- Should state when the account should be disabled and archived.
- Should state how long the account can remain inactive before it is disabled.
- Should state password construction and aging rules.

4.1.3 User Authentication Policy

The user authentication Policy requires traceability of users of the organization computing facilities in most circumstances. This will normally be achieved by them logging on before they can use the facilities, with security provided by the use of a password known only to the user concerned. It includes:

- Passwords shall be no less than 6 characters in length, and must be changed at least every 3 months.
- It is forbidden to reveal a password to anyone else. Procedures for user support shall be designed such that it is never necessary for anyone to know someone else's password after initial assignment.
- For access to highly secure systems , user authentication should use different ids and passwords to those used by the same individual for access to less secure systems
- For user who needs access to secure systems, a physical token shall be required in addition to username and password.

4.1.4 User Data Access Security policy

- Security Firewalls are installed to prevent unauthorized access to the network.
- Group policies in place for accessing PCs and workstations for authorized access.
- Access to important files and directories is given only to specific personnel.
- All email and web servers are located at an independent internet data center.
- GFS Backup policy in place. Monthly backups are stored at an off-site location and removable backups are kept safe with logs duly maintained. Daily backup are stored in fire-proof safe.
- External security audits are enforced to assess any breach with multi level security management in control.
- By default, all ports (USB, Serial, Parallel) are disabled on PCs. Enabling of the required ports is done only on specific requests by the client.
- Physical security ensures no CDs, Pen-drives; movable media goes in and out of the facility without written permission from the management.

4.1.5 Cloud Service level Agreement Policy

This Service Level Agreement is a policy governing the use of the Cloud service under the Cloud Terms of Service between On2 Technologies, Inc. The SLA is subject to the terms of the Cloud Agreement. Terms not otherwise defined herein will have the meaning given to them in the Flix Cloud Agreement.

- **Term and Termination:** This Agreement is effective when user accepts the terms and conditions of the Agreement and will continue in effect until terminated by user. Either You or On2 may terminate this agreement effective immediately upon written notice to the other for any reason.
- **Ownership:** All data that user submits to administrator and all output files that user creates in its use of the Services remain user data. On2 makes no claim of ownership in user Data.
- **Redundancy:** Data backup and recovery best practices dictate that you should always keep a second copy of your backup's offsite. Outsourcing data backup

does not change that basic rule even though the backups are actually stored elsewhere; user SLA should include a clear description of how your backup data is protected from hardware failure or media loss.

- **Response Time:** Response time must be clearly articulated in a service-level agreement. This should include not only the time it takes to acknowledge a request for restore but also the time to process initiation.
- **Disaster Recovery and Cloud Data Backup**
- User service provider must clearly demonstrate their ability to completely recover and in a timely fashion should disaster strike their facility. The service-level agreement must also be associated with user own disaster recovery requirements. The service levels must meet user recovery time objectives and recovery point objectives.
- **Client's Responsibilities**

  Client shall be responsible for:

  - all of their users' compliance with this Agreement,
  - Be solely responsible for the accuracy, quality, integrity and legality of Client's data and of the means by which Client acquired the data.
  - Use commercially reasonable efforts to prevent unauthorized access to or use of the purchase services, and notify Cyber View promptly of any such unauthorized access or use.
  - Use of Cyber View services only in accordance with the User Guide and applicable laws and government regulations.

4.2 Selection of Cloud Environment

Various open source software for cloud computing were explored and compared as mentioned in see Table 1. Following is a brief description of the popular tools commonly utilized for creating Cloud environment.

4.2.1 Globus Nimbus

Globus Nimbus is an open source toolkit that allows us to turn our cluster into an Infrastructure-as-a-Service (IaaS) cloud.

Feature highlights include:

- Two sets of Web Service interfaces: Amazon *EC2 WSDL***s** and Grid community *WSRF*
- Implementation based on the *Xen* hypervisor (*KVM* coming soon)
- Can be configured to *use familiar schedulers like PBS or SGE* to schedule virtual machines
- Launches self-configuring *virtual clusters with one click*
- Defines an *extensible architecture* that allows us to customize the software to the needs of our project

Science Clouds

- Science Clouds provide compute cycles in the cloud for scientific communities using Nimbus.
- The Nimbus cloud client allows us to provision customized compute nodes (that we call "workspaces") that we have full control over using a leasing model based on the Amazon's EC2 service.
- The Science Clouds have two objectives:
- To make it easy for scientific and educational projects to experiment with cloud
- To enable us to learn how to make cloud computing a useful tool for the scientific community.

Available Science clouds

- Nimbus @ University of Chicago
- Stratus @ University of Florida
- Wispy @ Purdue University
- Kupa @ Masaryk University

4.2.2 Eucalyptus

"EUCALYPTUS - Elastic Utility Computing Architecture for Linking Your Programs To Useful Systems is an open-source software infrastructure for implementing Cloud Computing' on clusters.

The current interface to EUCALYPTUS is compatible with Amazon's EC2 interface, but the infrastructure is designed to support multiple client-side interfaces.

EUCALYPTUS is implemented using commonly-available Linux tools and basic Web-service technologies making it easy to install and maintain."

Some of the key features of Eucalyptus are:

- It installs automatically as part of a Rocks 5 installation.
- It is modular and extensible, implemented entirely using open-source web service tools.
- It is interface-compatible with Amazon EC2 and uses the EC2 tools directly.
- Version 1.0 implements the EC2 features with the exception of static IPs address (planned for a later release).

At the moment, Eucalyptus depends on an open source cluster management software package called Rocks. Rocks are to clusters what Debian, Red Hat, Ubuntu, etc. are to individual Linux machines.

It's a packaging and deployment tool. So to use it (or at least to use it according to our documentation) we need to be using Rocks to manage the software on our clusters.

- Version 1.0 of Eucalyptus, downloadable now, is a feature-limited binary-only beta at this point.
- Eucalyptus was publicly demonstrated at the Open Source Grid and Cluster conference on May 14th.

4.2.3 Hadoop

- The Apache Hadoop project develops open-source software for reliable, scalable, distributed computing.
- Hadoop Distributed File System (HDFS) is the primary storage system used by Hadoop applications. HDFS creates multiple replicas of data blocks and

distributes them on compute nodes throughout a cluster to enable reliable, extremely rapid computations.

- It is available both for Linux & Windows platform.
- For Cloud setup Hadoop for windows has been selected.

This chapter mainly described design of security issues policy, design alternatives approaches based on this study, Hadoop has been chosen setting up cloud environment.

Next chapter will discuss the technology and implementation details for the thesis work.

Chapter 5

Experimental Results

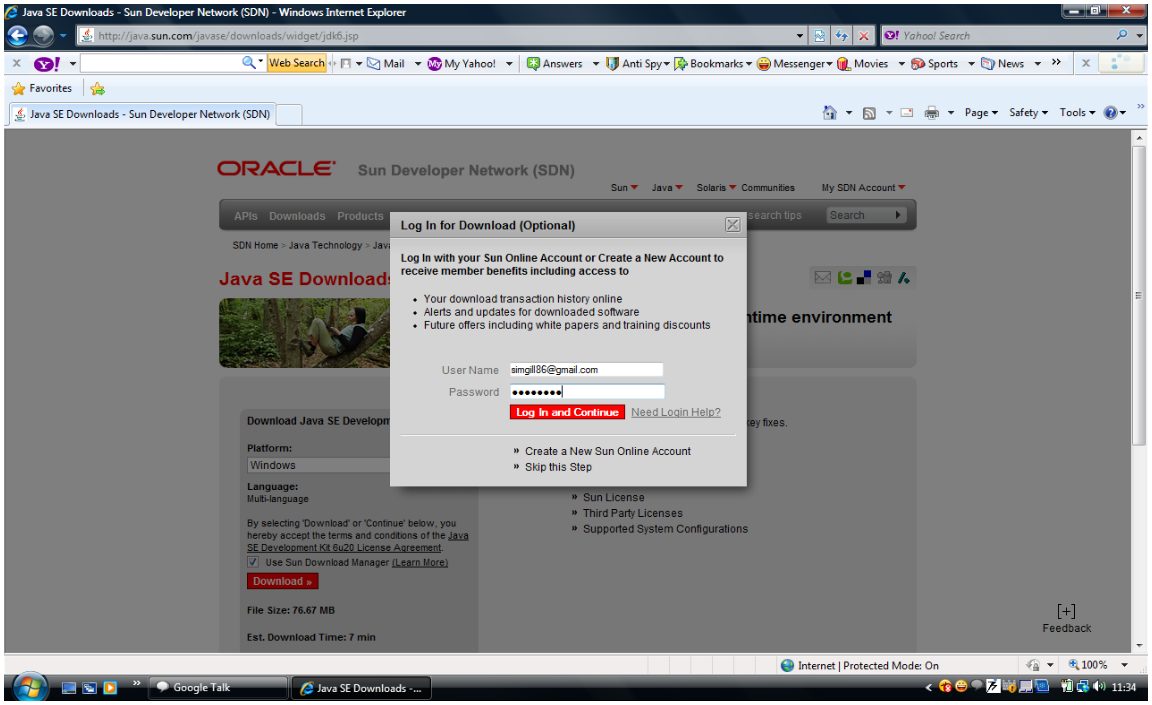
This chapter focuses on implementation of proposed design of security policy on hadoop in Cloud environment and experimental results of this approach.

5.1 Installation of Hadoop on Windows

The aim was to make a simplified version of Hadoop cluster that would run locally on the developer's machine. The first step was to install java 1.6 and Eclipse Europa 3.3.2 on the system as these are the pre-requisites for the Hadoop installation.

5.1.1Installation of java 1.6

Java was downloaded from *http://java.sun.com/* and installed on the system. The screenshots for java installation are as follows: We need to login as a user to download java using sun download manager.



Log In for Download (Optional)

Log In with your Sun Online Account or Create a New Account to receive member benefits including access to

- Your download transaction history online
- Alerts and updates for downloaded software
- Future offers including white papers and training discounts

User Name simgill86@gmail.com

Password ••••••••

Download Java SE Developm

Platform: Windows

Language: Multi-language

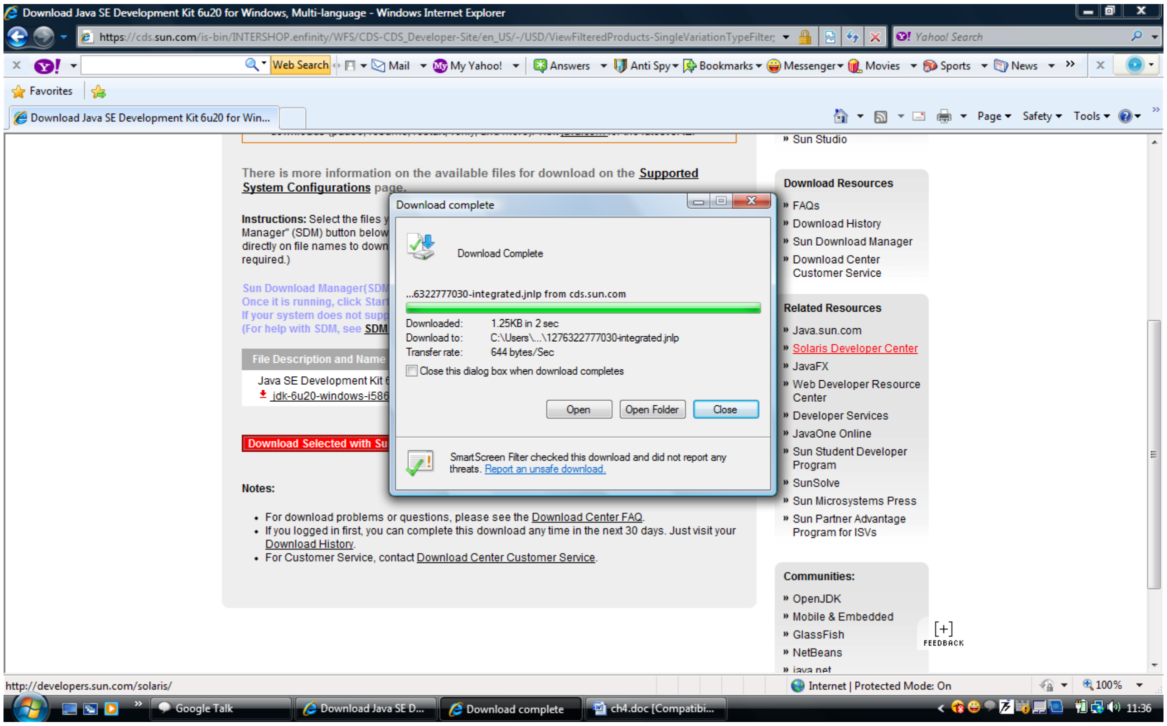
By selecting 'Download' or 'Continue' below, you hereby accept the terms and conditions of the Java SE Development Kit 6u20 License Agreement.

☑ Use Sun Download Manager (Learn More)

File Size: 76.67 MB

Est. Download Time: 7 min

Figure 5.1: Log in page for Downloading Java



Download Java SE Development Kit 6u20 for Windows, Multi-language - Windows Internet Explorer

https://cds.sun.com/is-bin/INTERSHOP.enfinity/WFS/CDS-CDS_Developer-Site/en_US/-/USD/ViewFilteredProducts-SingleVariationTypeFilter;

There is more information on the available files for download on the **Supported System Configurations** page.

Instructions: Select the files y
Manager" (SDM) button below
directly on file names to down
required.)

Sun Download Manager(SDM
Once it is running, click Start
If your system does not supp
(For help with SDM, see SDM

File Description and Name
Java SE Development Kit 6
jdk-6u20-windows-i586

Download Selected with Su

Notes:

- For download problems or questions, please see the Download Center FAQ.
- If you logged in first, you can complete this download any time in the next 30 days. Just visit your Download History.
- For Customer Service, contact Download Center Customer Service.

» Sun Studio

Download Resources

» FAQs
» Download History
» Sun Download Manager
» Download Center Customer Service

Related Resources

» Java.sun.com
» Solaris Developer Center
» JavaFX
» Web Developer Resource Center
» Developer Services
» JavaOne Online
» Sun Student Developer Program
» SunSolve
» Sun Microsystems Press
» Sun Partner Advantage Program for ISVs

Communities:

» OpenJDK
» Mobile & Embedded
» GlassFish
» NetBeans
» java.net

Download complete

Download Complete

...6322777030-integrated.jnlp from cds.sun.com

Downloaded: 1.25KB in 2 sec
Download to: C:\Users\...\1276322777030-integrated.jnlp
Transfer rate: 644 bytes/Sec

□ Close this dialog box when download completes

SmartScreen Filter checked this download and did not report any threats. Report an unsafe download.

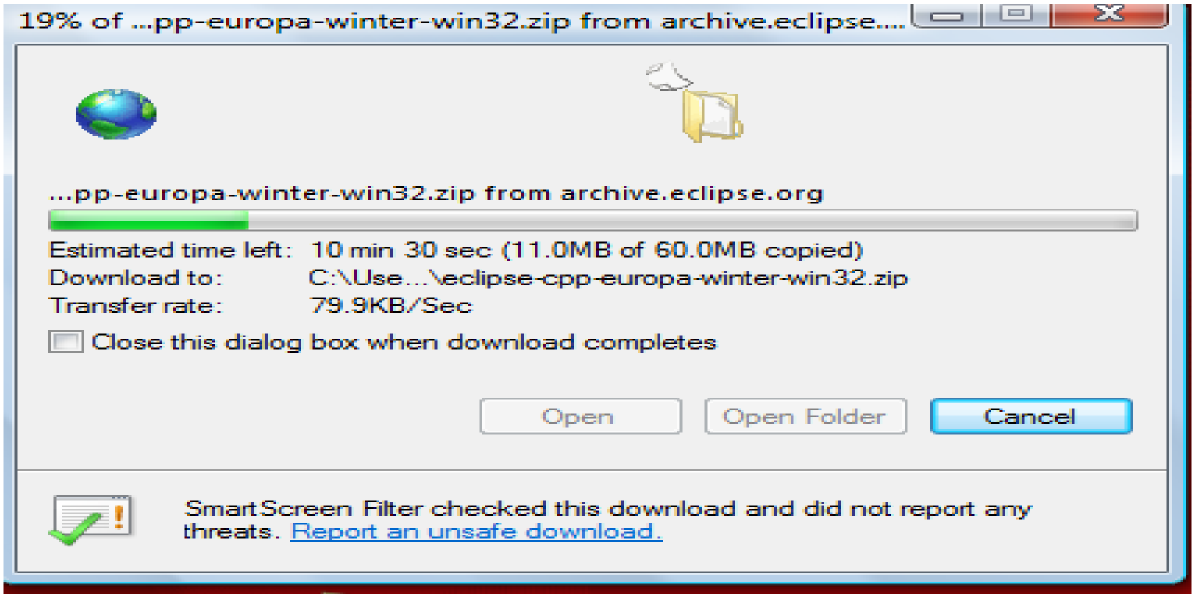
http://developers.sun.com/solaris/

Internet | Protected Mode: On

Figure 5.2 Download of Java in progress

5.1.2 Installing Eclipse Europa 3.3.2

Eclipse was downloaded from *www.eclipse.org* as shown in Fig 5.3



19% of ...pp-europa-winter-win32.zip from archive.eclipse....

...pp-europa-winter-win32.zip from archive.eclipse.org

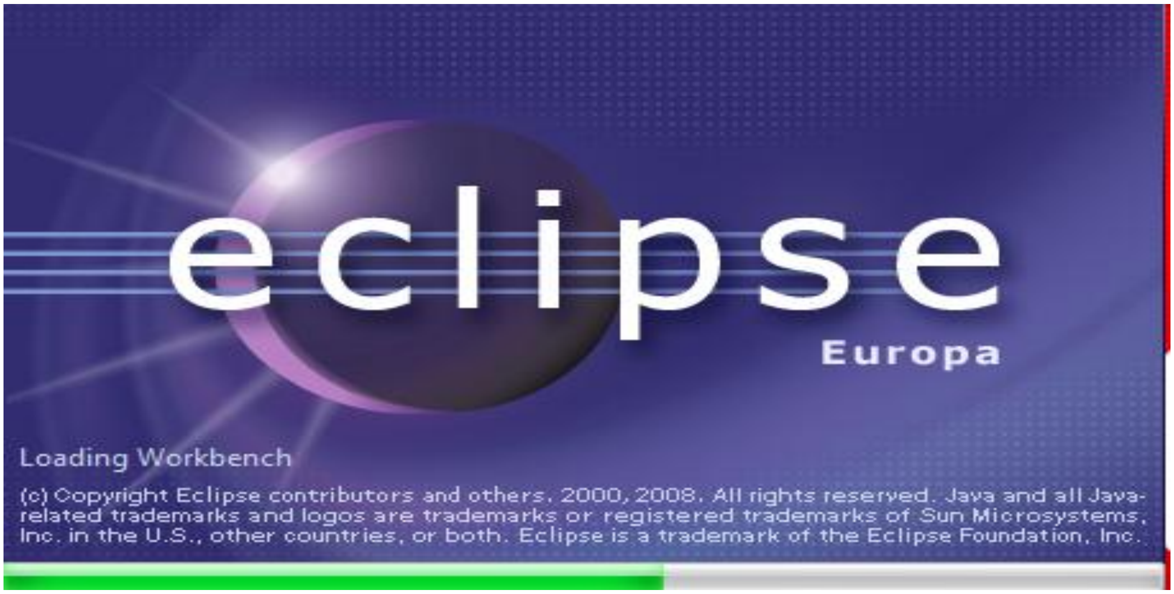
Estimated time left: 10 min 30 sec (11.0MB of 60.0MB copied)
Download to: C:\Use...\eclipse-cpp-europa-winter-win32.zip
Transfer rate: 79.9KB/Sec

□ Close this dialog box when download completes

SmartScreen Filter checked this download and did not report any threats. Report an unsafe download.

Figure 5.3: Download in Progress

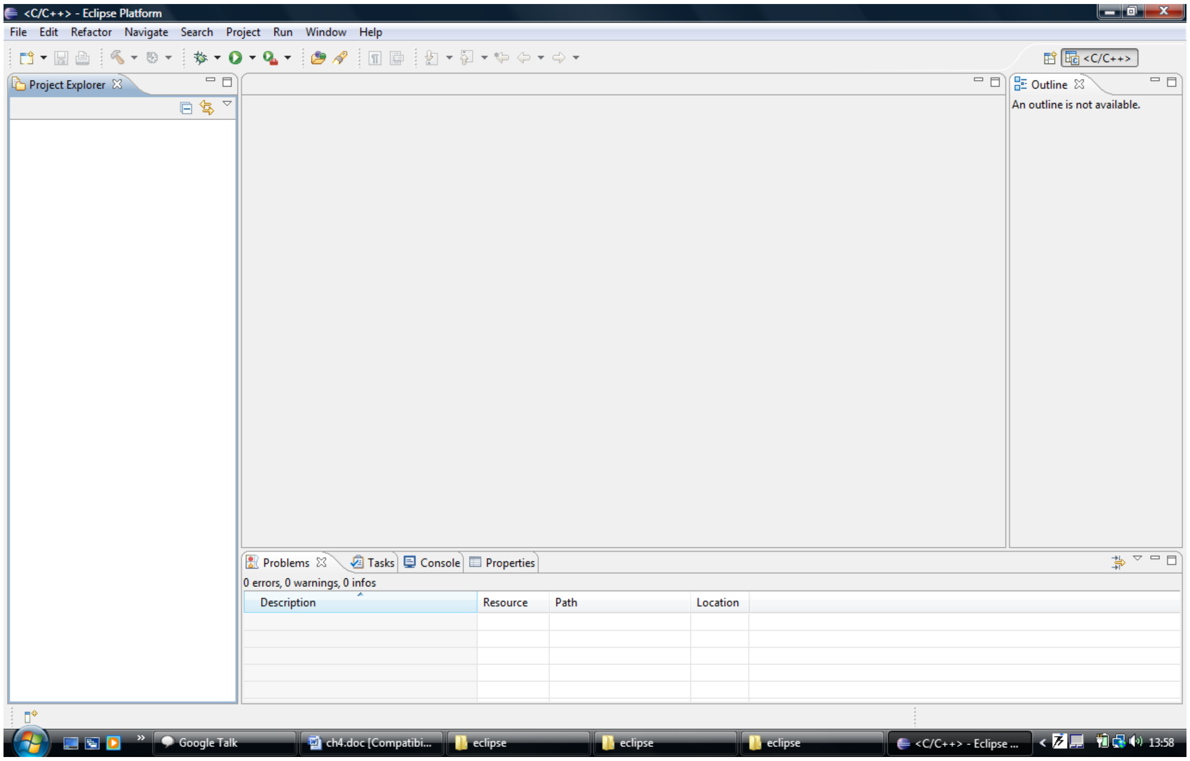
We need to uncompress the downloaded eclipse-cpp-europa-winter-win32.zip and then run the eclipse.exe file.



Loading Workbench

(c) Copyright Eclipse contributors and others, 2000, 2008. All rights reserved. Java and all Java-related trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S., other countries, or both. Eclipse is a trademark of the Eclipse Foundation, Inc.

Figure 5.4: Workspace Launcher for Eclipse



An outline is not available.

0 errors, 0 warnings, 0 infos

Figure 5.5: Eclipse Worksheet

Eclipse worksheet is opened after running the launcher.

5.1.3 Installing Cygwin:

After installing the prerequisite software, the next step is to install the Cygwin environment.

Cygwin is a set of UNIX packages ported to Microsoft Windows. It is needed to run the scripts supplied with Hadoop because they are all written for the UNIX platform.

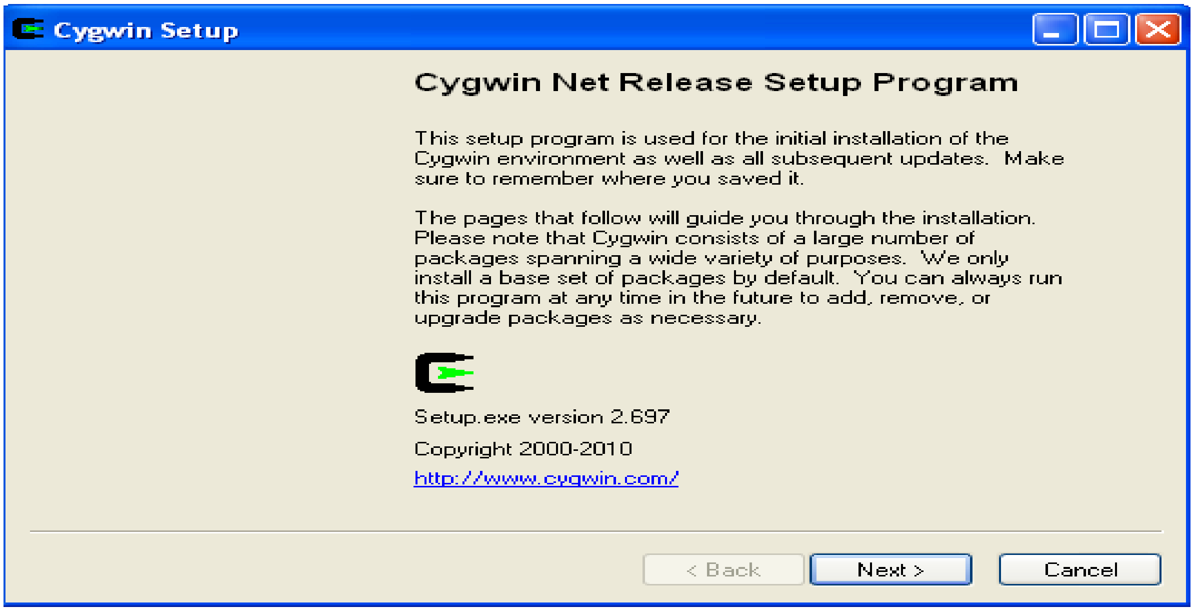
To install the Cygwin environment following steps used:

1. Download Cygwin installer from *http://www.cygwin.com*.
2. Run the downloaded file.

- **Running the Cygwin installer**

1. Click on the "Install Cygwin now" icon at right. Save the link (setup.exe) to your desktop, and then double-click on the saved icon.

2. A window titled *Cygwin Net Release Setup Program* appears. Click *Next* to get started.



Cygwin Net Release Setup Program

This setup program is used for the initial installation of the Cygwin environment as well as all subsequent updates. Make sure to remember where you saved it.

The pages that follow will guide you through the installation. Please note that Cygwin consists of a large number of packages spanning a wide variety of purposes. We only install a base set of packages by default. You can always run this program at any time in the future to add, remove, or upgrade packages as necessary.

Setup.exe version 2.697

Copyright 2000-2010

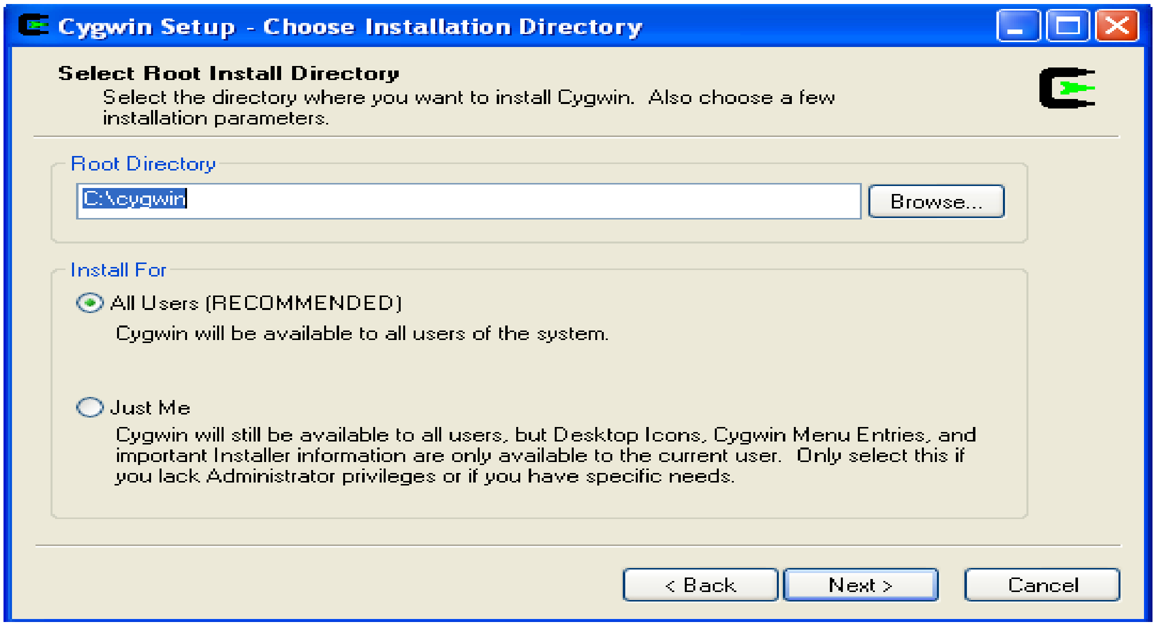
http://www.cygwin.com/

Figure 5.6: Cygwin Net Release Setup Program

- **Choose A Download Source**: Accept the default ("Install from Internet") and click *next.*

  Choosing the default "Install from Internet" causes the files you will choose in a later step to be downloaded first and then validated and installed. The other choices allow you to perform this procedure in two steps.

- **Select Root Install Directory**: Accept the defaults ("C:/cygwin", All Users, and UNIX) and click *next.*



Cygwin Setup - Choose Installation Directory

Select Root Install Directory

Select the directory where you want to install Cygwin. Also choose a few installation parameters.

Root Directory

C:\cygwin

Install For

● All Users (RECOMMENDED)

Cygwin will be available to all users of the system.

○ Just Me

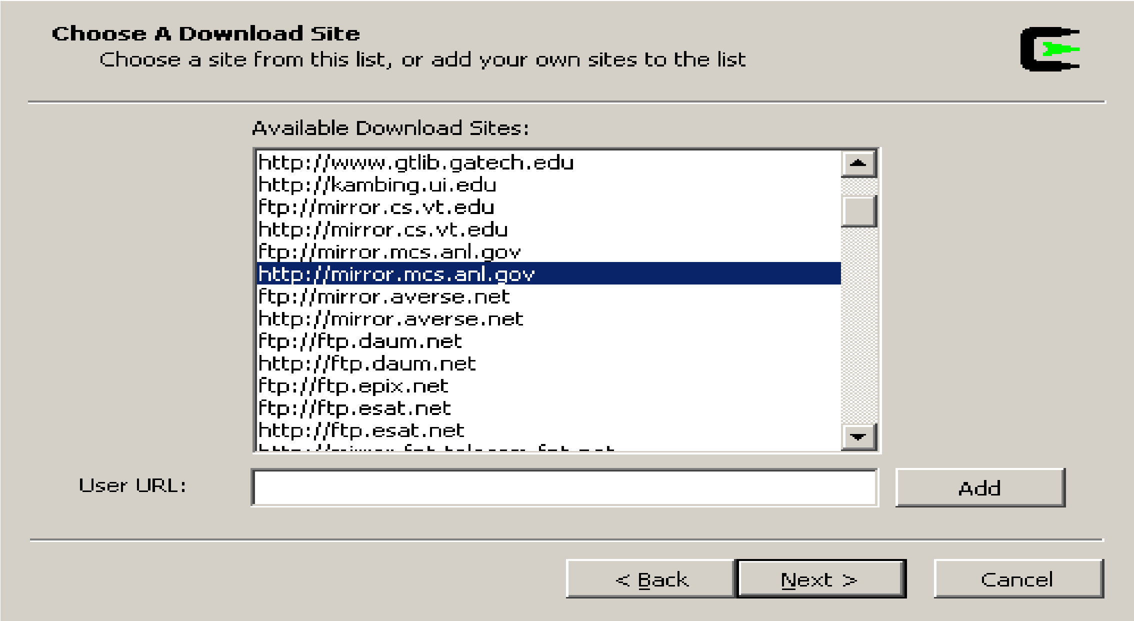
Cygwin will still be available to all users, but Desktop Icons, Cygwin Menu Entries, and important Installer information are only available to the current user. Only select this if you lack Administrator privileges or if you have specific needs.

Figure 5.7: Choose Installation Directory

- **Select Local Package Directory**: Accept the default or change it to any temporary directory of your choice, but make a note of it.

- **Select Your Internet Connection:** The default should be correct for most users. Change it only if you encounter problems.

- **Choose A Download Site**: Select a nearby mirror site from which to download the Cygwin packages. Speeds may vary considerably from site to site.



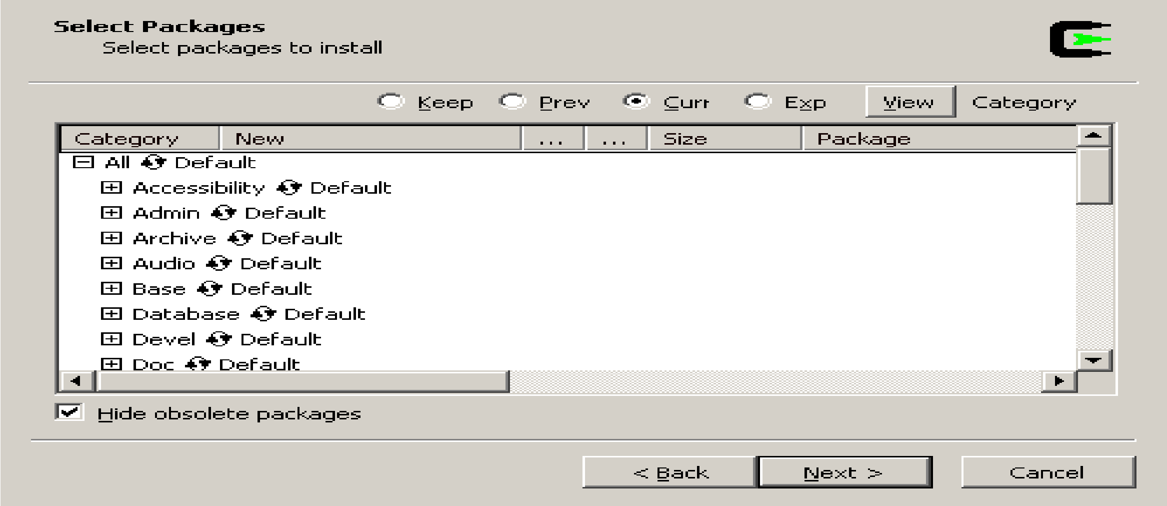
Choose A Download Site
Choose a site from this list, or add your own sites to the list

Available Download Sites:

```
http://www.gtlib.gatech.edu
http://kambing.ui.edu
ftp://mirror.cs.vt.edu
http://mirror.cs.vt.edu
ftp://mirror.mcs.anl.gov
http://mirror.mcs.anl.gov
ftp://mirror.averse.net
http://mirror.averse.net
ftp://ftp.daum.net
http://ftp.daum.net
ftp://ftp.epix.net
ftp://ftp.esat.net
http://ftp.esat.net
```

Figure 5.8 Choose a Download Site

- **Select Packages**: If we wish to do a *full installation*, click on the rotating selector next to "All" (at the top of the Category list) so that the indicator to its right changes from "Default" to "Install". Click *Next.*



Select Packages
Select packages to install

○ Keep ○ Prev ● Curr ○ Exp View Category

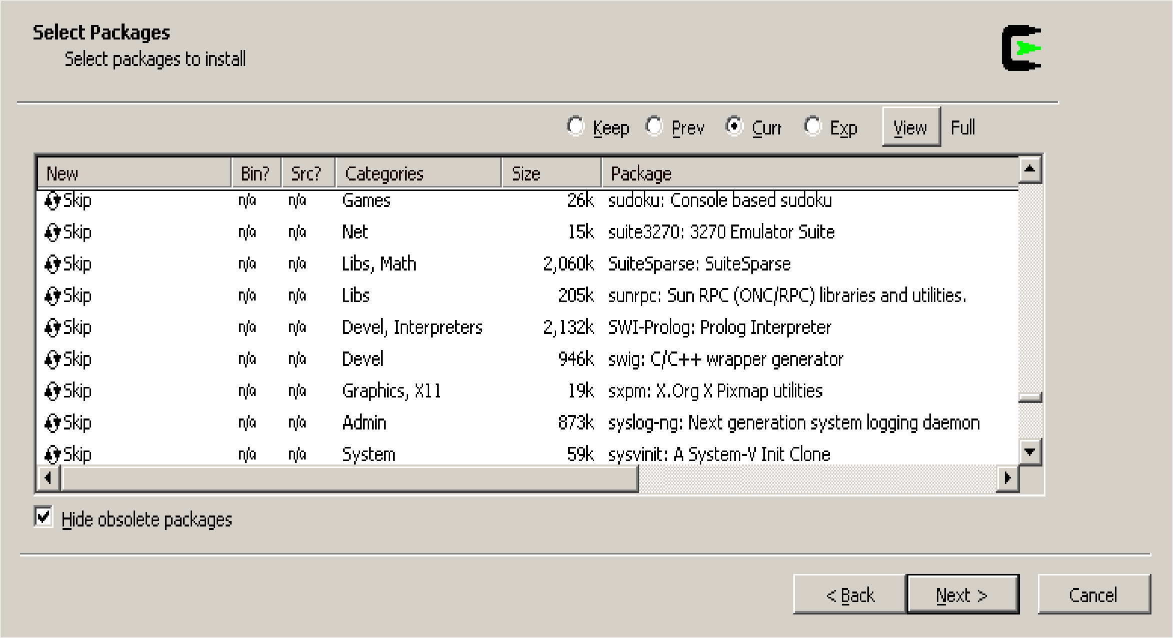
Category	New	...	...	Size	Package

```
⊟ All ⟳ Default
  ⊞ Accessibility ⟳ Default
  ⊞ Admin ⟳ Default
  ⊞ Archive ⟳ Default
  ⊞ Audio ⟳ Default
  ⊞ Base ⟳ Default
  ⊞ Database ⟳ Default
  ⊞ Devel ⟳ Default
  ⊞ Doc ⟳ Default
```

☑ Hide obsolete packages

Figure 5.9: Select Packages to Install

1. If we wish to do a *custom installation*, click the *View* button so that the indicator to its right changes from "Category" to Full.
2. We may resize the dialog box as needed until the package names are visible.
3. To select a package for installation, click on its rotating selector (in the **New** column) to cycle through the available choices until a version number appears. Usually the first alternative offered.



Select Packages

Select packages to install

○ Keep ○ Prev ● Curr ○ Exp View Full

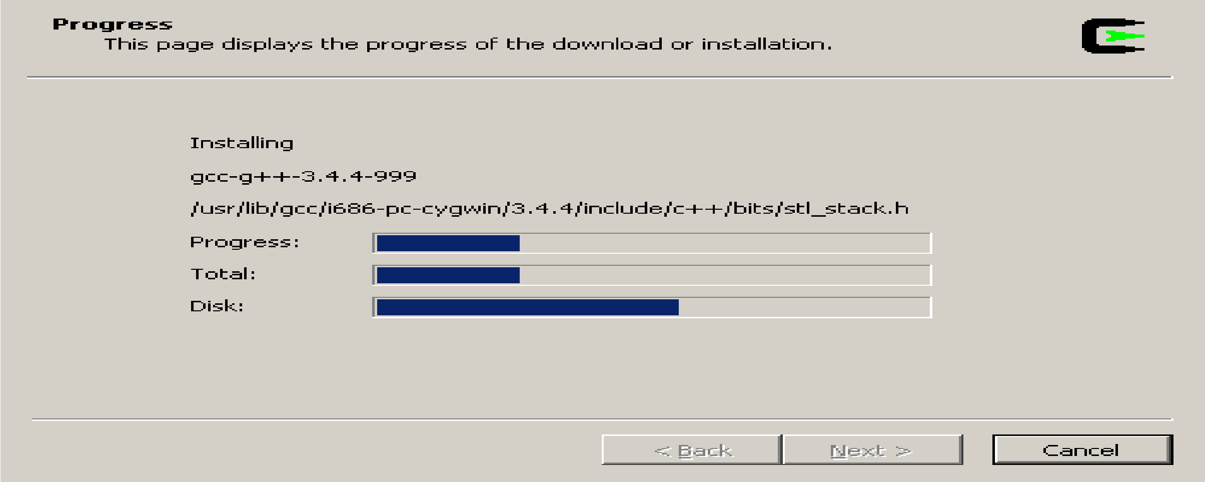
New	Bin?	Src?	Categories	Size	Package
Skip	n/a	n/a	Games	26k	sudoku: Console based sudoku
Skip	n/a	n/a	Net	15k	suite3270: 3270 Emulator Suite
Skip	n/a	n/a	Libs, Math	2,060k	SuiteSparse: SuiteSparse
Skip	n/a	n/a	Libs	205k	sunrpc: Sun RPC (ONC/RPC) libraries and utilities.
Skip	n/a	n/a	Devel, Interpreters	2,132k	SWI-Prolog: Prolog Interpreter
Skip	n/a	n/a	Devel	946k	swig: C/C++ wrapper generator
Skip	n/a	n/a	Graphics, X11	19k	sxpm: X.Org X Pixmap utilities
Skip	n/a	n/a	Admin	873k	syslog-ng: Next generation system logging daemon
Skip	n/a	n/a	System	59k	sysvinit: A System-V Init Clone

☑ Hide obsolete packages

Figure 5.10: Select Packages

The Cygwin installer will automatically download any additional packages needed to satisfy dependencies of those you select. When you have completed your selections, click *next.* The downloading process begins once the packages have been selected. The installer indicates its progress.

Once all selected package files have been downloaded and checked, they are unpacked into the Cygwin root install directory.



Progress

This page displays the progress of the download or installation.

Installing

gcc-g++-3.4.4-999

/usr/lib/gcc/i686-pc-cygwin/3.4.4/include/c++/bits/stl_stack.h

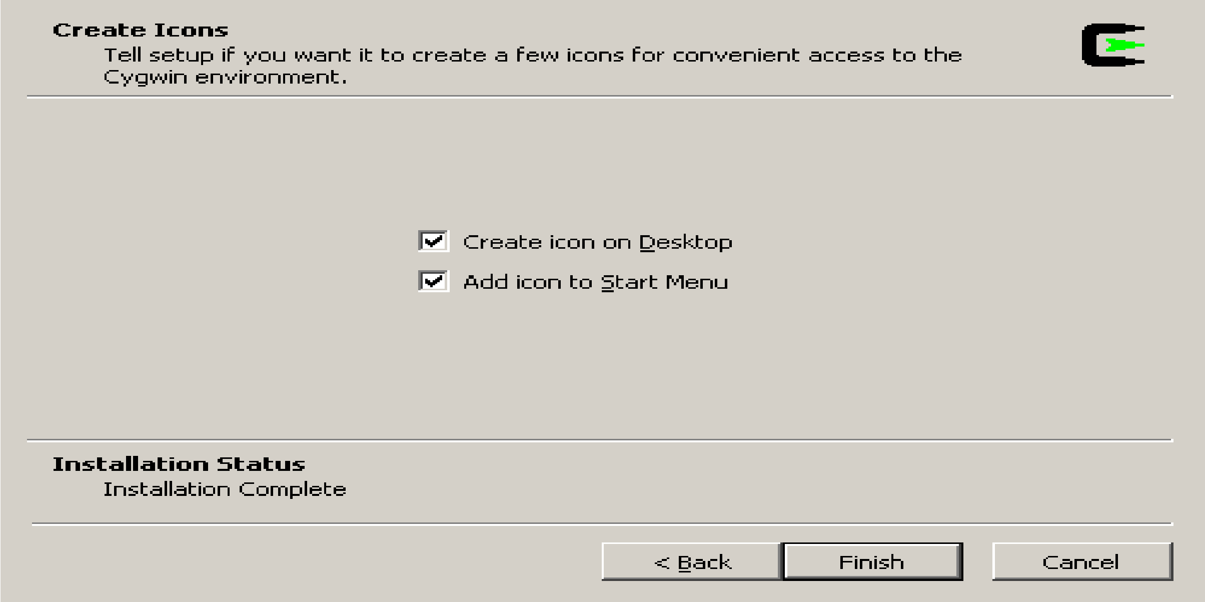
Progress:

Total:

Disk:

Figure 5.11: Installing Progress of gcc-g++3.4.4-999

- **Create Icons**: Unless these icons already exist from a previous Cygwin installation, make sure the boxes are checked and click *Finish.*



Create Icons

Tell setup if you want it to create a few icons for convenient access to the Cygwin environment.

☑ Create icon on Desktop

☑ Add icon to Start Menu

Installation Status

Installation Complete

Fig 5.12: Installation Status

5.2 Set Environment Variables

The next step is to set up the PATH environment variables, so that eclipse IDE could access Cygwin commands.

To set environment variables follow these steps.

1. Find "*My Computer*" icon either on the desktop or in the start menu, right click on it, and select Properties item from the menu.

2. When you see the properties dialog box, click on the *Environment Variables* button as shown below.
3. When Environment Variables dialog shows up, click on the *Path* variable located in the *System Variables* box and click the *Edit* button.
4. When *Edit* dialog appears append the following text to the end of variable value field:
5. *L:\cygwin\bin;L:\cygwin\usr\bin*

Close all three dialog boxes by pressing OK button of each dialog box.

5.4 Setup SSH Daemon

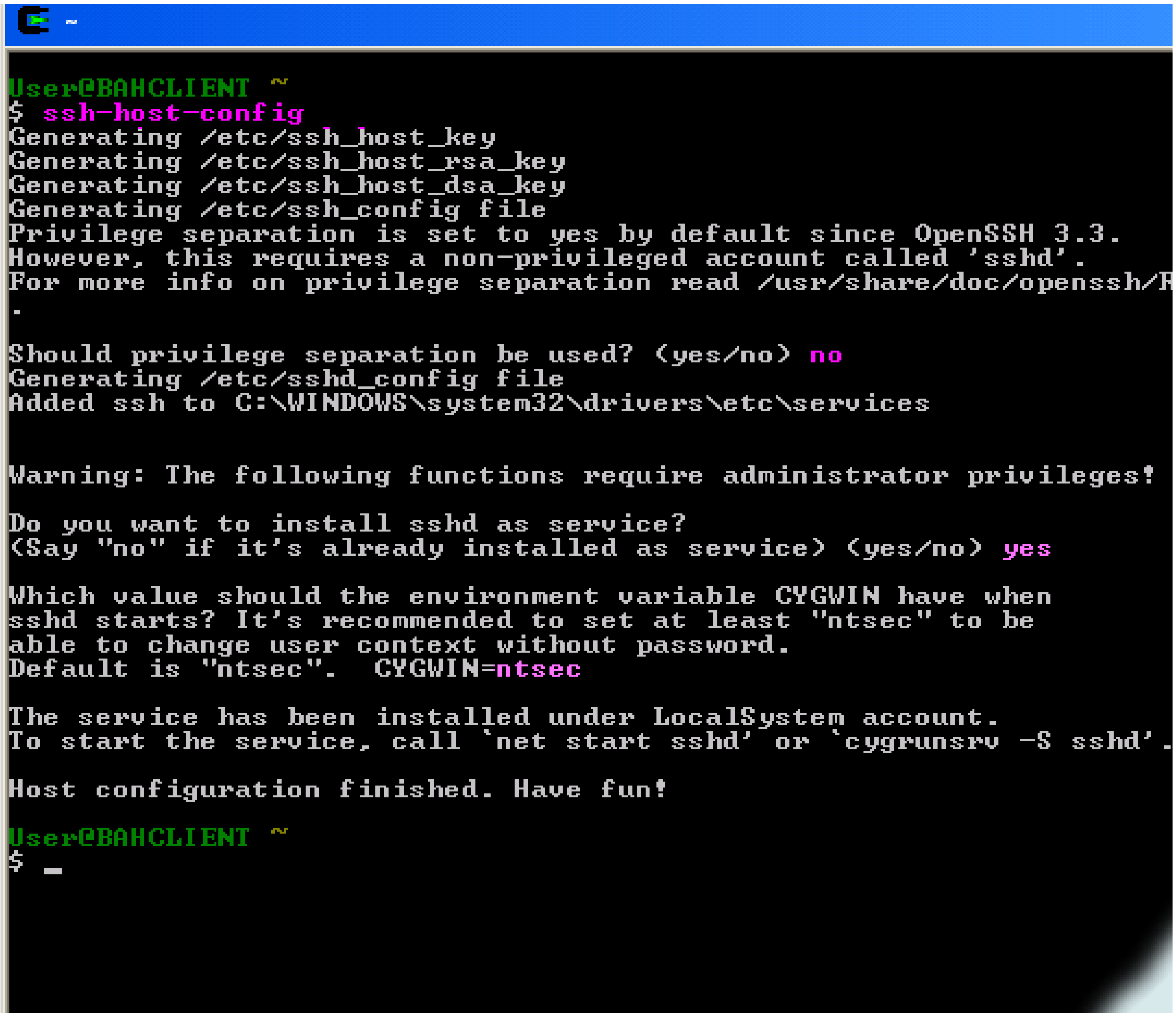
Both hadoop scripts and eclipse plug-in need password less ssh to operate. This section describes how to set it up in the Cygwin environment.

5.4.1 Configure SSh Daemon:

1. Open Cygwin command prompt.
2. Execute the following command.

```
ssh-host-config
```

1. When asked if privilege separation should be used, answer ***no***.
2. When asked if sshd should be installed as a service, answer ***yes.***
3. When asked about the value of CYGWIN environment variable enter ***ntsec***.
4. Here is the example session of this command, note that the input typed by the user is shown in pink and output from the system is shown in gray.



```
User@BAHCLIENT ~
$ ssh-host-config
Generating /etc/ssh_host_key
Generating /etc/ssh_host_rsa_key
Generating /etc/ssh_host_dsa_key
Generating /etc/ssh_config file
Privilege separation is set to yes by default since OpenSSH 3.3.
However, this requires a non-privileged account called 'sshd'.
For more info on privilege separation read /usr/share/doc/openssh/R
.

Should privilege separation be used? (yes/no) no
Generating /etc/sshd_config file
Added ssh to C:\WINDOWS\system32\drivers\etc\services


Warning: The following functions require administrator privileges!

Do you want to install sshd as service?
(Say "no" if it's already installed as service) (yes/no) yes

Which value should the environment variable CYGWIN have when
sshd starts? It's recommended to set at least "ntsec" to be
able to change user context without password.
Default is "ntsec".  CYGWIN=ntsec

The service has been installed under LocalSystem account.
To start the service, call `net start sshd' or `cygrunsrv -S sshd'.

Host configuration finished. Have fun!

User@BAHCLIENT ~
$ _
```

Figure 5.13: Configure ssh daemon

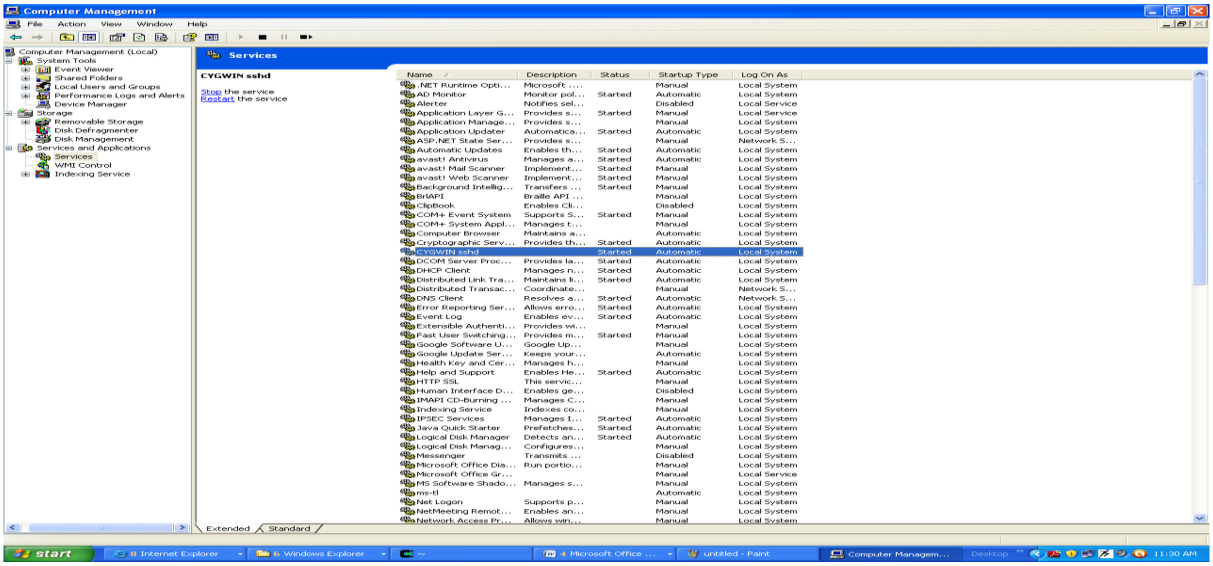
5.4.2 Start SSH Daemon

1. Find my computer icon either on your desktop or in the start-up menu, right-click on it and select Manage from the context menu.

2. Open Services and Applications in the left-hand panel then select the *Services* item.

3 Find the *CYGWIN sshd* item in the main section and right-click on it.

4 Select *Start* from the context menu.



CYGWIN sshd

Stop the service
Restart the service

Name	Description	Status	Startup Type	Log On As
.NET Runtime Opti...	Microsoft		Manual	Local System
AD Monitor	Monitor pol...	Started	Automatic	Local System
Alerter	Notifies sel...		Disabled	Local Service
Application Layer G...	Provides s...	Started	Manual	Local Service
Application Manage...	Provides s...		Manual	Local System
Application Updater	Automatica...	Started	Automatic	Local System
ASP.NET State Ser...	Provides s...		Manual	Network S...
Automatic Updates	Enables th...	Started	Automatic	Local System
avast! Antivirus	Manages a...	Started	Automatic	Local System
avast! Mail Scanner	Implement...	Started	Manual	Local System
avast! Web Scanner	Implement...	Started	Manual	Local System
Background Intellig...	Transfers ...	Started	Manual	Local System
BrlAPI	Braille API ...		Manual	Local System
ClipBook	Enables Cli...		Disabled	Local System
COM+ Event System	Supports S...	Started	Manual	Local System
COM+ System Appl...	Manages t...		Manual	Local System
Computer Browser	Maintains a...		Automatic	Local System
Cryptographic Serv...	Provides th...	Started	Automatic	Local System
CYGWIN sshd		Started	Automatic	Local System
DCOM Server Proc...	Provides la...	Started	Automatic	Local System
DHCP Client	Manages n...	Started	Automatic	Local System
Distributed Link Tra...	Maintains li...	Started	Automatic	Local System
Distributed Transac...	Coordinate...		Manual	Network S...
DNS Client	Resolves a...	Started	Automatic	Network S...
Error Reporting Ser...	Allows erro...	Started	Automatic	Local System
Event Log	Enables ev...	Started	Automatic	Local System
Extensible Authenti...	Provides wi...		Manual	Local System
Fast User Switching...	Provides m...	Started	Manual	Local System
Google Software U...	Google Up...		Manual	Local System
Google Update Ser...	Keeps your...		Automatic	Local System
Health Key and Cer...	Manages h...		Manual	Local System
Help and Support	Enables He...	Started	Automatic	Local System
HTTP SSL	This servic...		Manual	Local System
Human Interface D...	Enables ge...		Disabled	Local System
IMAPI CD-Burning ...	Manages C...		Manual	Local System
Indexing Service	Indexes co...		Manual	Local System
IPSEC Services	Manages I...	Started	Automatic	Local System
Java Quick Starter	Prefetches...	Started	Automatic	Local System
Logical Disk Manager	Detects an...	Started	Automatic	Local System
Logical Disk Manag...	Configures...		Manual	Local System
Messenger	Transmits ...		Disabled	Local System
Microsoft Office Dia...	Run portio...		Manual	Local System
Microsoft Office Gr...			Manual	Local Service
MS Software Shado...	Manages s...		Manual	Local System
ms-tl			Automatic	Local System
Net Logon	Supports p...		Manual	Local System
NetMeeting Remot...	Enables an...		Manual	Local System
Network Access Pr...	Allows win...		Manual	Local System

Figure 5.14: Start ssh daemon

3. A small window should pop-up indicating the progress of the service start-up. After that window disappears the status of CYGWIN sshd service should change to *Started*.

5.4.3 Setup Authorization keys

Eclipse plug-in and hadoop scripts require ssh authentication to be performed through authorization keys rather than through passwords. To enable key based authorization you have to setup authorization keys. The following steps describe how to do it.

1. Open cygwin command prompt.

2. Execute the following command to generate keys.

```
ssh-keygen
```

3. When prompted for filenames and pass phrases press ENTER to accept default values.

4. After command has finished generating they key, enter the following command to change into your .ssh directory.

```
cd  .ssh
```

5. Check if the keys where indeed generated by executing the following command.

```
ls  -l
```

You should see two file ***id_rsa.pub*** and ***id_rsa*** with the recent creation dates. These files contain authorization keys.

6. To register the new authorization keys enter the following command. Note that double brackets, they are very important.

```
cat id_rsa.pub >> authorized_keys
```

7. Now check if the keys where set-up correctly by executing the following command.

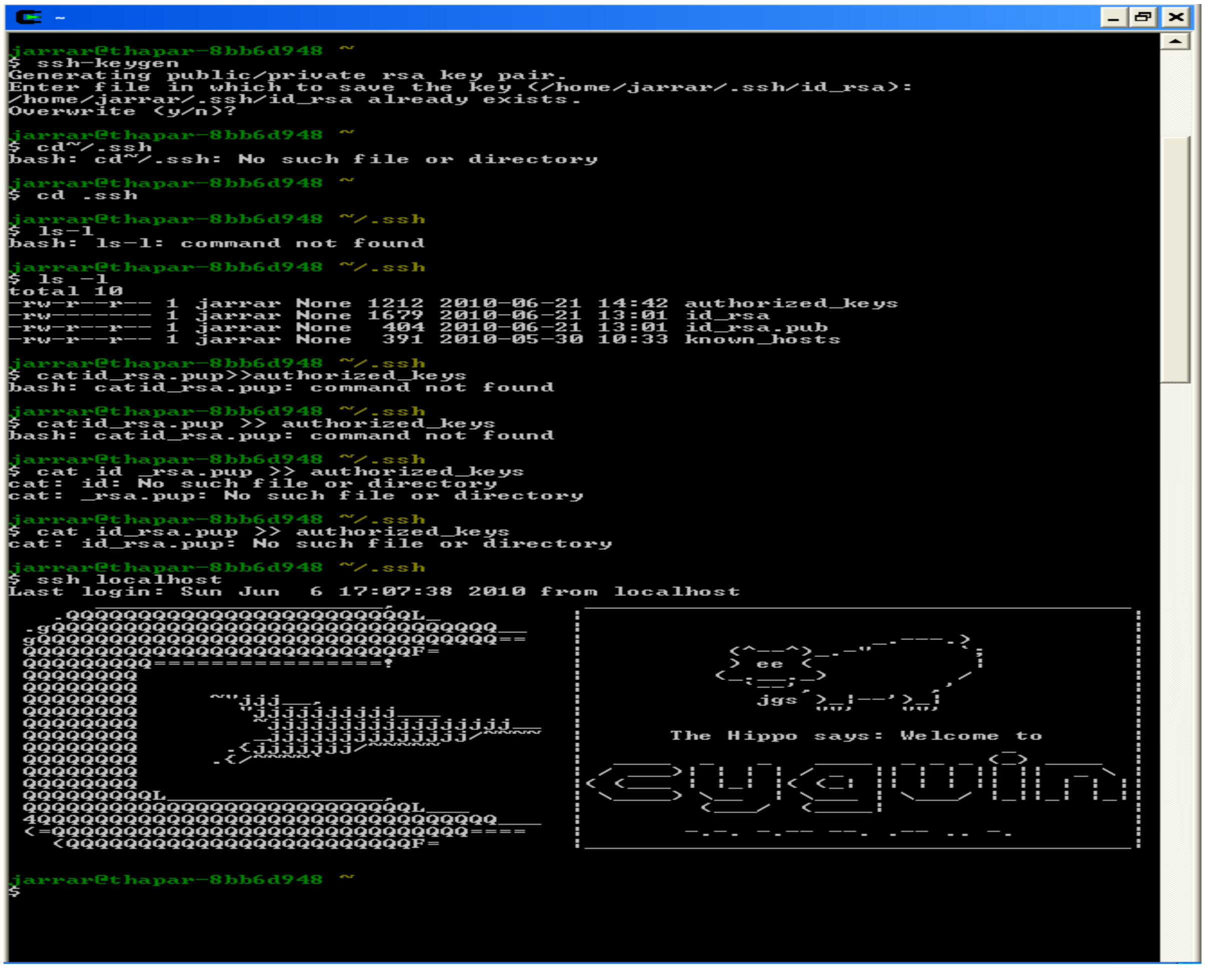
```
ssh localhost
```

Since it is a new ssh installation you warned that authenticity of the host could not be established and will be prompted whether you really want to connect, answer ***yes*** and press ENTER. You should see the cygwin prompt again, which means that you have successfully connected.

8. Now execute the command again.

```
ssh localhost
```

This time you should not be prompted for anything.



```
jarrar@thapar-8bb6d948 ~
$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/jarrar/.ssh/id_rsa):
/home/jarrar/.ssh/id_rsa already exists.
Overwrite (y/n)?

jarrar@thapar-8bb6d948 ~
$ cd~/.ssh
bash: cd~/.ssh: No such file or directory

jarrar@thapar-8bb6d948 ~
$ cd .ssh

jarrar@thapar-8bb6d948 ~/.ssh
$ ls-l
bash: ls-l: command not found

jarrar@thapar-8bb6d948 ~/.ssh
$ ls -l
total 10
-rw-r--r-- 1 jarrar None 1212 2010-06-21 14:42 authorized_keys
-rw------- 1 jarrar None 1679 2010-06-21 13:01 id_rsa
-rw-r--r-- 1 jarrar None  404 2010-06-21 13:01 id_rsa.pub
-rw-r--r-- 1 jarrar None  391 2010-05-30 10:33 known_hosts

jarrar@thapar-8bb6d948 ~/.ssh
$ catid_rsa.pup>>authorized_keys
bash: catid_rsa.pup: command not found

jarrar@thapar-8bb6d948 ~/.ssh
$ catid_rsa.pup >> authorized_keys
bash: catid_rsa.pup: command not found

jarrar@thapar-8bb6d948 ~/.ssh
$ cat id _rsa.pup >> authorized_keys
cat: id: No such file or directory
cat: _rsa.pup: No such file or directory

jarrar@thapar-8bb6d948 ~/.ssh
$ cat id_rsa.pup >> authorized_keys
cat: id_rsa.pup: No such file or directory

jarrar@thapar-8bb6d948 ~/.ssh
$ ssh localhost
Last login: Sun Jun  6 17:07:38 2010 from localhost

                                        The Hippo says: Welcome to

jarrar@thapar-8bb6d948 ~
$
```

Fig 5.15: Setting up Authorization keys

5.5 Download, Copy and Unpack:

The next step is to download and unpack the hadoop distribution.

1. Download hadoop 0.19.2 and place in some folder on your computer such as ***L:\Java***.

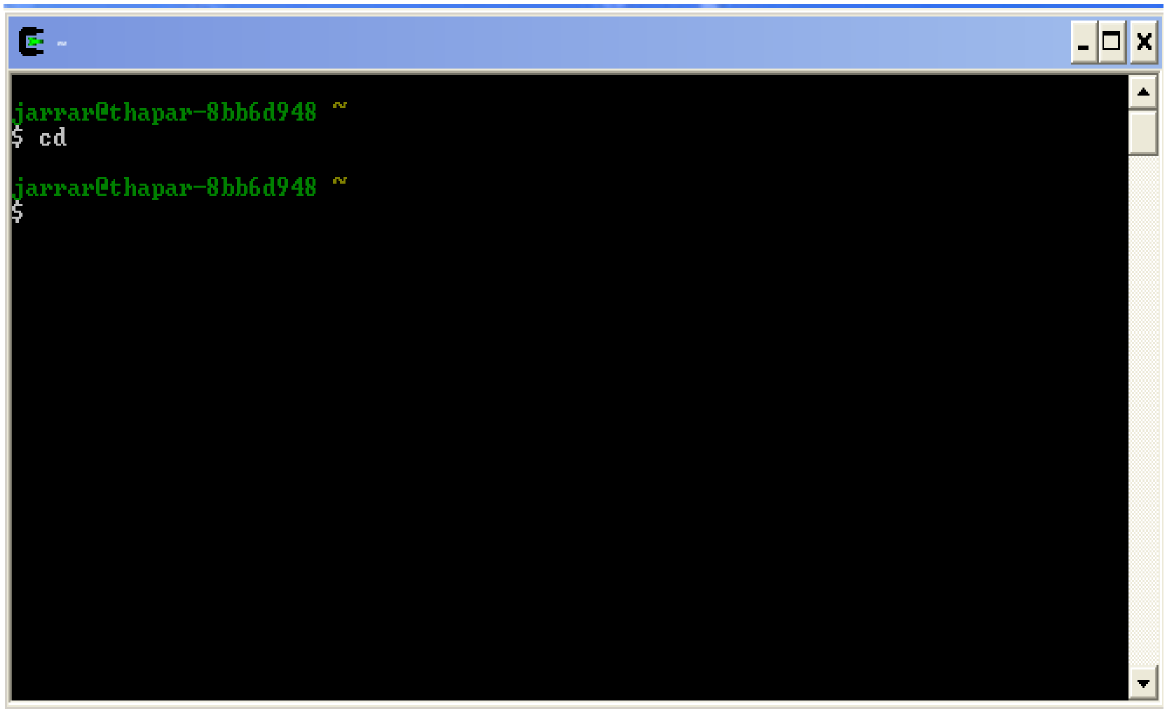
2. Open Cygwin command prompt.

3. Execute the following command.

```
cd .
```

4. Then execute the following command to get your home directory folder shown in the Windows Explorer window.

```
explorer .
```



```
jarrar@thapar-8bb6d948 ~
$ cd

jarrar@thapar-8bb6d948 ~
$
```

Figure 5.16: Unpack Hadoop

5.6 Unpack Hadoop Installation

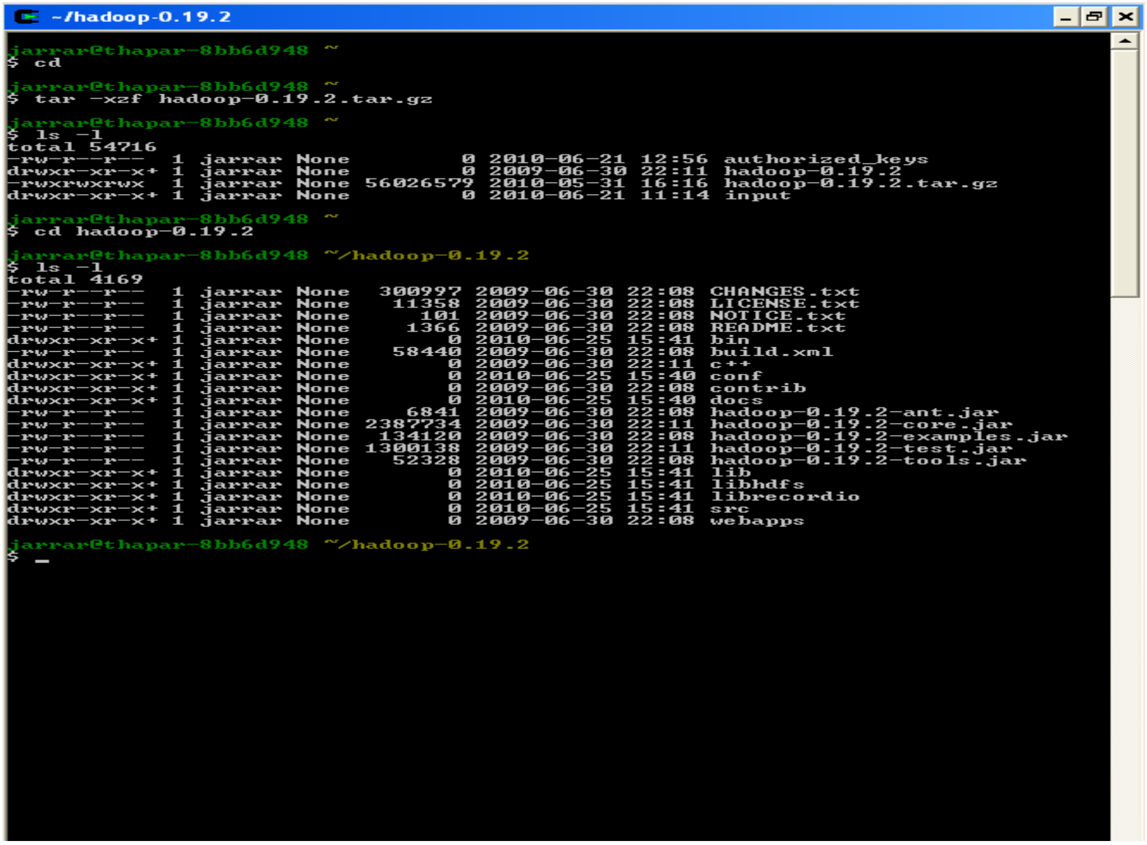
The next step is to unpack the downloaded and copied package

1. Open the new cygwin window.

2. After new cygwin window appears, execute the following command:

```
3. tar -xzf hadoop-0.19.1.tar.gz
```

This will start the process of unpacking the Hadoop distribution. After several minutes you should see a new CYGWIN prompt again. As shown on the screenshot below.



```
jarrar@thapar-8bb6d948 ~
$ cd

jarrar@thapar-8bb6d948 ~
$ tar -xzf hadoop-0.19.2.tar.gz

jarrar@thapar-8bb6d948 ~
$ ls -l
total 54716
-rw-r--r--   1 jarrar None        0 2010-06-21 12:56 authorized_keys
drwxr-xr-x+ 1 jarrar None        0 2009-06-30 22:11 hadoop-0.19.2
-rwxrwxrwx   1 jarrar None 56026579 2010-05-31 16:16 hadoop-0.19.2.tar.gz
drwxr-xr-x+ 1 jarrar None        0 2010-06-21 11:14 input

jarrar@thapar-8bb6d948 ~
$ cd hadoop-0.19.2

jarrar@thapar-8bb6d948 ~/hadoop-0.19.2
$ ls -l
total 4169
-rw-r--r--   1 jarrar None  300997 2009-06-30 22:08 CHANGES.txt
-rw-r--r--   1 jarrar None   11358 2009-06-30 22:08 LICENSE.txt
-rw-r--r--   1 jarrar None     101 2009-06-30 22:08 NOTICE.txt
-rw-r--r--   1 jarrar None    1366 2009-06-30 22:08 README.txt
drwxr-xr-x+ 1 jarrar None       0 2010-06-25 15:41 bin
-rw-r--r--   1 jarrar None   58440 2009-06-30 22:08 build.xml
drwxr-xr-x+ 1 jarrar None       0 2009-06-30 22:11 c++
drwxr-xr-x+ 1 jarrar None       0 2010-06-25 15:40 conf
drwxr-xr-x+ 1 jarrar None       0 2009-06-30 22:08 contrib
drwxr-xr-x+ 1 jarrar None       0 2010-06-25 15:40 docs
-rw-r--r--   1 jarrar None    6841 2009-06-30 22:08 hadoop-0.19.2-ant.jar
-rw-r--r--   1 jarrar None 2387734 2009-06-30 22:11 hadoop-0.19.2-core.jar
-rw-r--r--   1 jarrar None  134120 2009-06-30 22:08 hadoop-0.19.2-examples.jar
-rw-r--r--   1 jarrar None 1300138 2009-06-30 22:11 hadoop-0.19.2-test.jar
-rw-r--r--   1 jarrar None   52328 2009-06-30 22:08 hadoop-0.19.2-tools.jar
drwxr-xr-x+ 1 jarrar None       0 2010-06-25 15:41 lib
drwxr-xr-x+ 1 jarrar None       0 2010-06-25 15:41 libhdfs
drwxr-xr-x+ 1 jarrar None       0 2010-06-25 15:41 librecordio
drwxr-xr-x+ 1 jarrar None       0 2010-06-25 15:41 src
drwxr-xr-x+ 1 jarrar None       0 2009-06-30 22:08 webapps

jarrar@thapar-8bb6d948 ~/hadoop-0.19.2
$ _
```

Figure 5.17: Unpack Hadoop Installation Commands

3. When you see the new prompt execute the following command:

```
ls -l
```

This command will list the contents of your home directory. You should see a newly created directory called ***hadoop-0.19.2.***

4. Next execute the following commands.

```
cd hadoop-0.19.2
ls -l
```

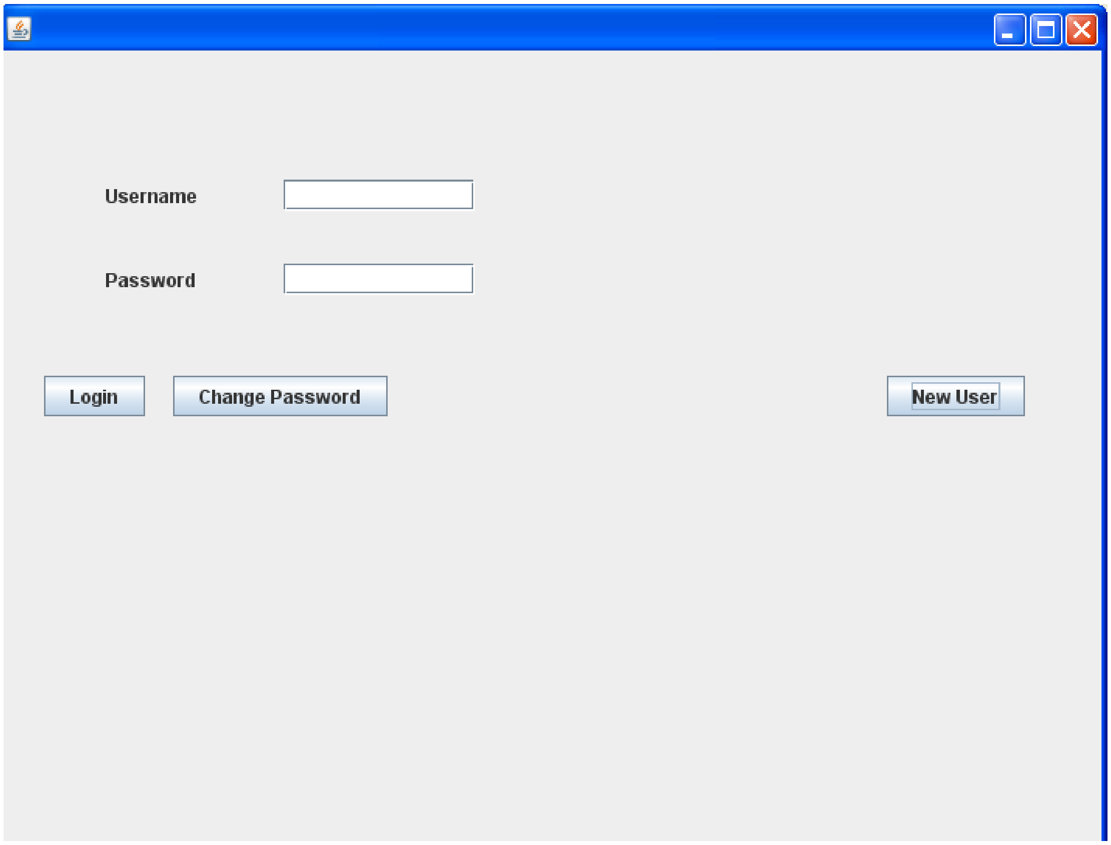
5.7 Implementation and working of the system

We have developed the database in MS Access, and Graphical User Interface with Net Beans platform. For providing the output in Java application, we have used Unicode driver in MS Access and stored data in Java application itself. Here, we describe the functionalities of the designed system in three parts [27].

i) Login

ii) Change password

iii) New user



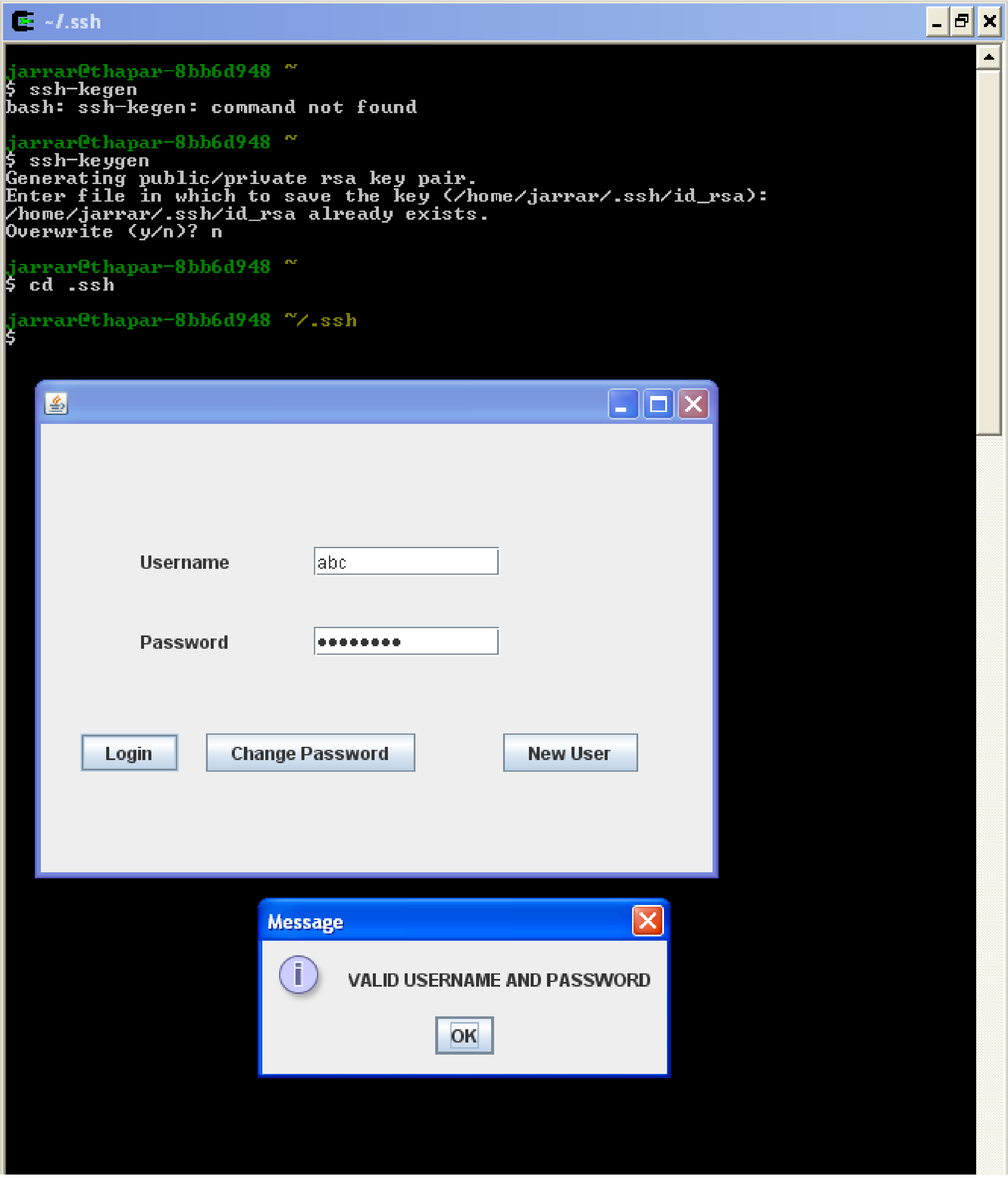
Username

Password

Figure 5.18: User interface of Java Application on hadoop.

i) Login

- User provides input in the form of username & password.
- For authentication, password should be more than 6 words.



```
jarrar@thapar-8bb6d948 ~
$ ssh-kegen
bash: ssh-kegen: command not found

jarrar@thapar-8bb6d948 ~
$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/jarrar/.ssh/id_rsa):
/home/jarrar/.ssh/id_rsa already exists.
Overwrite (y/n)? n

jarrar@thapar-8bb6d948 ~
$ cd .ssh

jarrar@thapar-8bb6d948 ~/.ssh
$
```

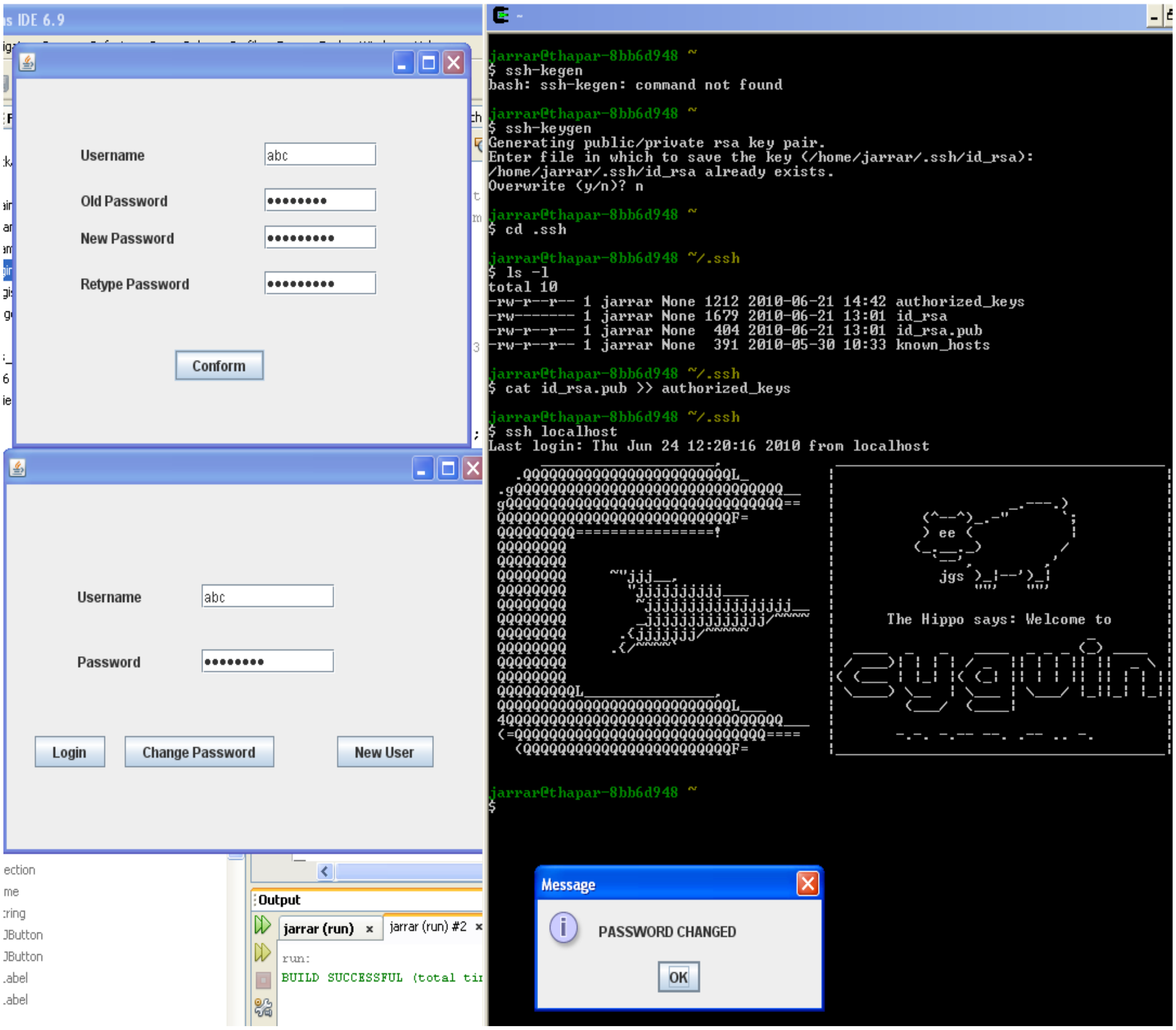
Username: abc

Password: ●●●●●●●●●

Message: VALID USERNAME AND PASSWORD

Figure 5.19: User Authentication page in Java Application

- **Change Password:** User can change username and password.



Username: abc

Old Password: ••••••••

New Password: •••••••••

Retype Password: •••••••••

Username: abc

Password: ••••••••

```
run:
BUILD SUCCESSFUL (total ti
```

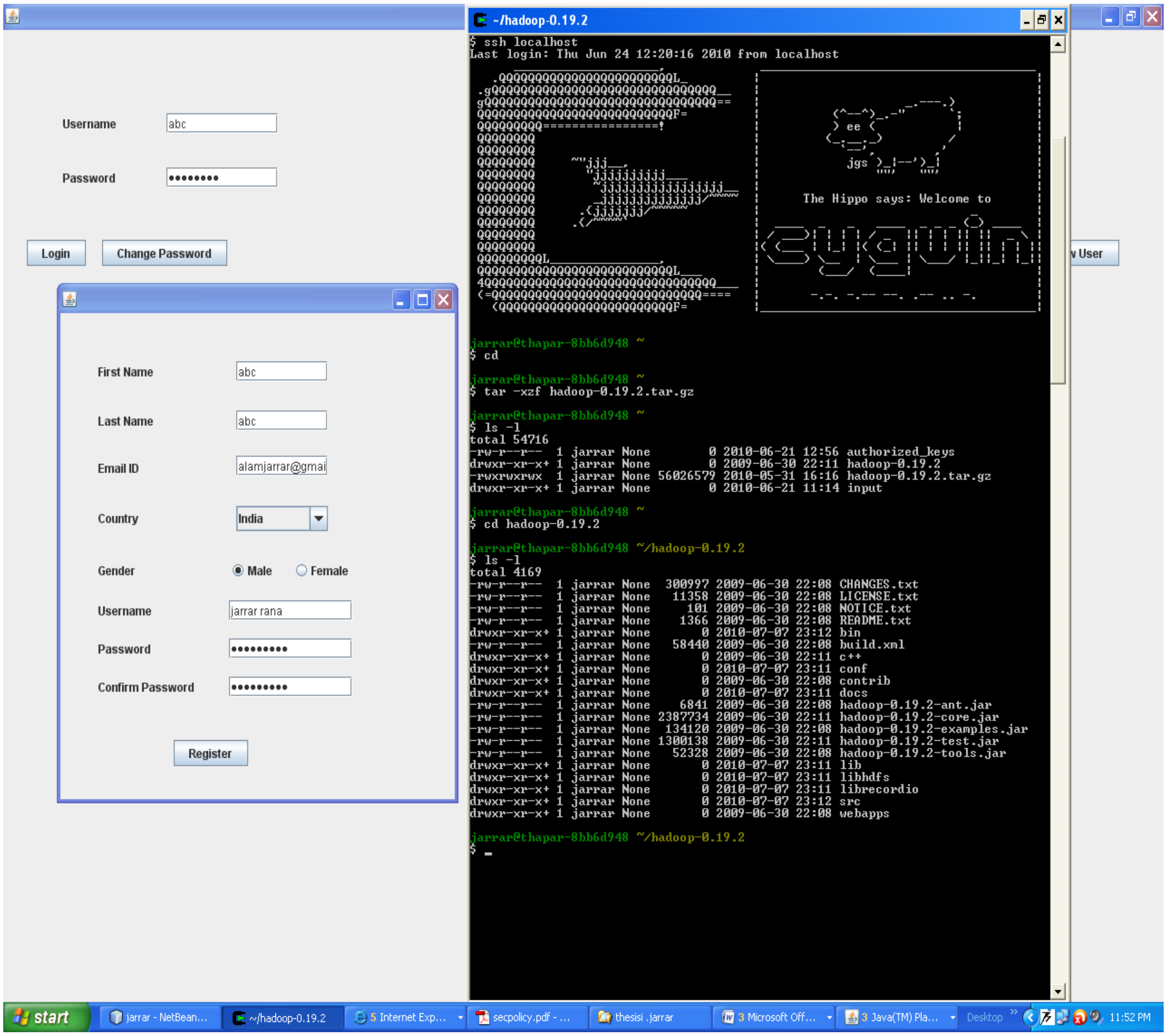
```
jarrar@thapar-8bb6d948 ~
$ ssh-kegen
bash: ssh-kegen: command not found

jarrar@thapar-8bb6d948 ~
$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/jarrar/.ssh/id_rsa):
/home/jarrar/.ssh/id_rsa already exists.
Overwrite (y/n)? n

jarrar@thapar-8bb6d948 ~
$ cd .ssh

jarrar@thapar-8bb6d948 ~/.ssh
$ ls -l
total 10
-rw-r--r-- 1 jarrar None 1212 2010-06-21 14:42 authorized_keys
-rw------- 1 jarrar None 1679 2010-06-21 13:01 id_rsa
-rw-r--r-- 1 jarrar None  404 2010-06-21 13:01 id_rsa.pub
-rw-r--r-- 1 jarrar None  391 2010-05-30 10:33 known_hosts

jarrar@thapar-8bb6d948 ~/.ssh
$ cat id_rsa.pub >> authorized_keys

jarrar@thapar-8bb6d948 ~/.ssh
$ ssh localhost
Last login: Thu Jun 24 12:20:16 2010 from localhost

The Hippo says: Welcome to

jarrar@thapar-8bb6d948 ~
$
```

Message

PASSWORD CHANGED

Figure 5.20: Change password page in Java Application

- **New user:** When user click on new user button, system generate a new user form for user. User Password allowed is as per security policy only as shown in Fig 5.17.



Username abc

Password ••••••••

First Name abc

Last Name abc

Email ID alamjarrar@gmai

Country India

Gender ● Male ○ Female

Username jarrar rana

Password •••••••••

Confirm Password •••••••••

```
$ ssh localhost
Last login: Thu Jun 24 12:20:16 2010 from localhost

                                        The Hippo says: Welcome to

jarrar@thapar-8bb6d948 ~
$ cd

jarrar@thapar-8bb6d948 ~
$ tar -xzf hadoop-0.19.2.tar.gz

jarrar@thapar-8bb6d948 ~
$ ls -l
total 54716
-rw-r--r--  1 jarrar None        0 2010-06-21 12:56 authorized_keys
drwxr-xr-x+ 1 jarrar None        0 2009-06-30 22:11 hadoop-0.19.2
-rwxrwxrwx  1 jarrar None 56026579 2010-05-31 16:16 hadoop-0.19.2.tar.gz
drwxr-xr-x+ 1 jarrar None        0 2010-06-21 11:14 input

jarrar@thapar-8bb6d948 ~
$ cd hadoop-0.19.2

jarrar@thapar-8bb6d948 ~/hadoop-0.19.2
$ ls -l
total 4169
-rw-r--r--  1 jarrar None  300997 2009-06-30 22:08 CHANGES.txt
-rw-r--r--  1 jarrar None   11358 2009-06-30 22:08 LICENSE.txt
-rw-r--r--  1 jarrar None     101 2009-06-30 22:08 NOTICE.txt
-rw-r--r--  1 jarrar None    1366 2009-06-30 22:08 README.txt
drwxr-xr-x+ 1 jarrar None       0 2010-07-07 23:12 bin
-rw-r--r--  1 jarrar None   58440 2009-06-30 22:08 build.xml
drwxr-xr-x+ 1 jarrar None       0 2009-06-30 22:11 c++
drwxr-xr-x+ 1 jarrar None       0 2010-07-07 23:11 conf
drwxr-xr-x+ 1 jarrar None       0 2009-06-30 22:08 contrib
drwxr-xr-x+ 1 jarrar None       0 2010-07-07 23:11 docs
-rw-r--r--  1 jarrar None    6841 2009-06-30 22:08 hadoop-0.19.2-ant.jar
-rw-r--r--  1 jarrar None 2387734 2009-06-30 22:11 hadoop-0.19.2-core.jar
-rw-r--r--  1 jarrar None  134120 2009-06-30 22:08 hadoop-0.19.2-examples.jar
-rw-r--r--  1 jarrar None 1300138 2009-06-30 22:11 hadoop-0.19.2-test.jar
-rw-r--r--  1 jarrar None   52328 2009-06-30 22:08 hadoop-0.19.2-tools.jar
drwxr-xr-x+ 1 jarrar None       0 2010-07-07 23:11 lib
drwxr-xr-x+ 1 jarrar None       0 2010-07-07 23:11 libhdfs
drwxr-xr-x+ 1 jarrar None       0 2010-07-07 23:11 librecordio
drwxr-xr-x+ 1 jarrar None       0 2010-07-07 23:12 src
drwxr-xr-x+ 1 jarrar None       0 2009-06-30 22:08 webapps

jarrar@thapar-8bb6d948 ~/hadoop-0.19.2
$ _
```

Figure 5.21: New User Registration Page

This chapter focused on implementation of design of security issues policy on Hadoop in cloud environment.

The next chapter summarizes this thesis work and suggests features that can be incorporated in future for in enhanced security issues policy in cloud environment.

Chapter 6
Conclusions and Future Scope

This chapter discusses the conclusions of work presented in this thesis. The chapter ends with a discussion of the future direction which thesis work will take.

6.1 Conclusions

In this thesis, security issues and challenges involved in cloud computing have been addressed. In this work requirements analysis, design of security policy for user, categorization of security issues, comparison of open source tools for implementation in Cloud in environment have been done & presented in thesis. A Cloud environment has been setup using Hadoop.

By developing Java applications on Hadoop in Cloud environment, there is no need to brother about setting up of any servers. The cloud vendor takes care of all the data storage. The user doesn't have to bother about data security. The provider takes care of everything. In this thesis, GUI has been developed for user authentication. Further, Hadoop generates an authentication key for user to login in Java application.

6.2 Thesis Contributions

a) Open source tools have been compared.

b) Merits of Cloud environment have been discussed.

c) Security policy has been designed for Public Cloud.

d) Cloud environment has been setup.

e) Use of Cloud through user authentication policy has been demonstrated.

6.3 Future Research

a) Cloud is a new technology. It can be explored further by developing more complex applications.

b) Applications can be developed to explore areas like cloud security issues.

c) Applications can be developed to explore web page in cloud environment.

d) User can even set up their own private Cloud environment by using Hadoop.

e) Entire security policy can be implemented and validated in Cloud environment.

References

[1] Alistair Croll, "Why Cloud Computing Needs Security", 2008 http://gigaom.com/2008/06/10/the-amazon-outage-fortresses-in-the clouds/

[2] Jonothan Erickson, "Best Practices for Protecting Data in the Cloud", 2008 http://www.ddj.com/security/210602698

[3] Jon Bodkin, "Seven Cloud-Computing Security Risks", 2008 http://www.networkworld.com/news/2008/070208-cloud.html

[4] Elinor Mills, "Cloud Computing Security Forecast: Clear Skies", 2009 http://news.zdnet.com/2100-9595_22-264312.html

[5] Jon Brondkin, cloud computing security issues, http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853 , 2July 2008

[6]http://peeyes.spaces.live.com/blog/cns!9D867CC7936D3E20!1004.ent

[7]http://en.wikipedia.org/wiki/Cloud_computing

[8] Univa UD, Hybrid Cloud ,http://www.univaud.com/about-cloud/internal-private.php

[9] Cloud computing: A practical approach, Anthony T. Velte, Toby J. Velte, Robert Elsenpeter, TATA McGRAW-HILL EDITTION-2010.

[10] Jeffrey Voas, Jia Zhang. “Cloud Computing, New Wine or Just a New Bottle? “ . IT Pro, March/April.2009.

[11] Francesco Maria Agmerich, Gianni Fenu, Simone Surcis. “An Approach to Cloud Computing Network”.2008.

[12] Ian Foster, Yong Zhao, Ioan Raicu, Shiyong Lu. “Cloud Computing and Grid Computing 360-Degree Compared”, 2009.

[13] Jeffrey Voas, Jia Zhang. “Cloud Computing, New Wine or Just a New Bottle? “ . IT Pro, March/April.2009.

[14] Alexander Lenk, Markus Klems, Jens Nimis, Stefan Tai, Thomas Sandholm. "What's Inside the Cloud? An Architectural Map of the Cloud Landscape",Vancouver, Canada, CLOUD'09, May.2009, ICSE Workshop, 2009.

[15] http://www.infoworld.com/d/cloud-computing/what-cloud-computing-really-means-031.

[16] http://knowledge.wpcarey.asu.edu/article.cfm?articleid=1614.

[17] Jeffrey Voas, Jia Zhang. "Cloud Computing, New Wine or Just a New Bottle? " . IT Pro, March/April.2009.

[18] Anthony T.Velte, Joby J.Velte, Robert Elsenpeter. "Cloud Computing". Tata McGraw-Hill.

[19] Francesco Maria Agmerich, Gianni Fenu, Simone Surcis. "An Approach to Cloud Computing Network",2008.

[20] Robert W. Lucky. "Cloud Computing", IEEE Spectrum, May.2009.

[21] http://www.kk.org/thetechnium/archives/2007/11/a_cloudbook_for.php.

[22] Alexander Lenk, Markus Klems, Jens Nimis, Stefan Tai, Thomas Sandholm. "What's Inside the Cloud? An Architectural Map of the Cloud Landscape",Vancouver, Canada, CLOUD'09, May.2009, ICSE Workshop, 2009.

[23]http://www.informationweek.com/news/services/business/showArticle.jhtml?articleID=209904474.

[24] Liang-Jie Zhang and Qun Zhou, "CCOA: Cloud Computing Open Architecture". IEEE Computing society, 2009.

[25] Luis Ferreira, Viktors Bersti, Jonathan Armstrong, Mike Kendzierski, AndreasNeukoetter, MasanobuTakagi, Richard Bing-Wo, Adeeb Amir, Ryo Murakawa, Olegario Hernandez, James Magowan, Norbert Bieberstein".IBM Red Books.

[26] Ian Foster, Yong Zhao, Ioan Raicu, Shiyong Lu. “Cloud Computing and Grid Computing 360-Degree Compared”, 2009.

[27] Borje Ohlman, Anders, Eriksson, Rene Rembarz. “What Networking of Information Can Do for Cloud Computing”. IEEE computer society, 2009.

[28] Roger Halbheer, Chief Security Advisor, Public Sector, EMEA Doug Cavit, Principal Security Strategist Lead, Trustworthy Computing, USA ,January 2010.

[29] Dustin Amrhein, Joe Armstrong, Ezhil Arasan B, “Cloud Computing Use Cases” A white paper produced by the Cloud Computing Use Case Discussion Group, 31 July.

[30] Sadie Creese, Paul Hopkins, Siani Pearson, Yun Shen “Data Protection-Aware design for Cloud Computing” HP Laboratories, Dec-2009.

List of Publications

1. Dr Inderveer Chana, Jarrar, “Cloud computing security Issues” published in National Conference Emerging Trends in IT and Computing (ETIC- 2010), 16 march, 2010.