



Sudan University of Science and
Technology
College of Graduate Studies



Cloud Computing: A Case Study of Software Implementation as a Service for Sudanese Health Organizations

الحوسبة السحابية: دراسة حالة لتنفيذ العتاد البرمجي خدمة للمنظمات الصحية السودانية

A thesis Submitted in Partial Fulfillment of the Requirement for the Degree
of M.Sc. in Electronics Engineering (Computer and Networks Engineering)

Prepared By:

Maha Abd Almageed Ibrahim Khattab

Supervisor:

Dr. Ebtihal H. G. Yousif

September 2018

الإستهلال

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

وَيَسْأَلُونَكَ عَنِ الرُّوحِ قُلِ الرُّوحُ مِنْ أَمْرِ رَبِّي وَمَا أُوتِيتُمْ مِنَ الْعِلْمِ إِلَّا قَلِيلًا ﴿٨٥﴾

سورة الإسراء

Dedication

To my mother and my father

Acknowledgments

I would like to show my greatest appreciation to Africa City of Technology. Special thanks also to my colleagues from Africa City who provided me virtual server in their cloud to host my system and gave me insightful comments and expertise that greatly assisted the research, also I am deeply grateful to my mother who gave me emotional support and raise my morale, in addition to everyone who helped me in my life.

Abstract

The development of technology has a good impact on all sciences including medicine. The use of modern technology in medicine reduces the incidence of serious medical errors; some diseases need to follow their symptoms for a long time to be discovered. There is a problem in tracking symptoms for patients at each time visiting the hospital where data cannot be saved and retrieved when needed. By using the cloud computing technology, all hospitals can be linked by the Software-as-a-Service (SaaS) model, which enables doctors to follow the patient's health throughout his life if he visits any hospital at any time. The program must be managed by the Ministry of Health, and working with this program should be imposed on all governmental and private hospitals. The program allows receptionists to create a special file for each patient by saving the basic information in a database and using national number as primary key. The doctor enters the symptoms, requests the tests and then the laboratory is responsible for adding tests results to the system, which then are sent to the doctor who will then decide the appropriate treatment. If the patient has other symptoms and visits another hospital, the new doctor can retrieve the patient's previous data. The achieved result of this program is that it facilitates the process of saving and retrieving patients' history from every hospital which leads to early detection and treatment of diseases before being serious, by this we reduce mortality due to error diagnosis.

المستخلص

التطور في التكنولوجيا له أثر جيد في كل العلوم بما في ذلك الطب، فاستخدام التكنولوجيا الحديثة في الطب يقلل من مشاكل الأخطاء الطبية فبعض الأمراض تحتاج إلى مدة زمنية طويلة لمتابعة أعراضها لكي تكتشف. هنالك مشكلة في تتبع الأعراض بالنسبة للمرضى في كل وقت يزورون فيه المستشفيات حيث يصعب حفظ البيانات واسترجاعها عند الحاجة. باستخدام الحوسبة السحابية كل المستشفيات يمكن ربطها باستخدام نموذج (البرنامج كخدمة) الذي يسمح للطبيب ويمكنه من متابعة صحة المريض طوال حياته وإذا زار أكثر من مستشفى وذلك في كل وقت. هذا البرنامج يجب أن يكون مدارا عن طريق وزارة الصحة التي تفرضه على كل المستشفيات الحكومية والخاصة، يسمح هذا البرنامج لموظفي الاستقبال بإنشاء ملفات خاصة لكل مريض وذلك بحفظ المعلومات الأساسية في قاعدة بيانات واستخدام الرقم الوطني مفتاحا رئيسا. يدخل الطبيب الأعراض ويطلب الاختبارات من التقني المسؤول من المعمل والذي يضيف نتيجة الاختبار إلى النظام ومن ثم ترسل هذه النتيجة إلى الطبيب الذي يقرر فيما بعد العلاج المناسب. إذا كان المريض لديه أعراض أخرى أو زار مستشفى آخر فإن الطبيب الجديد يمكنه استرجاع البيانات السابقة للمريض. النتائج المتحصلة عليها من هذا البرنامج هو أنه يسهل عملية حفظ واسترجاع بيانات المريض من حيث تاريخ المرض من كل مستشفى مما يؤدي إلى الاكتشاف المبكر للمرض وعلاجه قبل أن يصبح خطيرا، وبهذا نقتل من الوفيات الناجمة عن التشخيصات الخاطئة.

Table of Contents

Dedication	ii
Acknowledgments	iii
Abstract	iv
المستخلص	v
List of Figures	ix
List of Tables	xi
List of Listings	xii
List of Abbreviations	xiii
Chapter One: Introduction	1
1.1 Overview	1
1.2 Problem Statement	1
1.3 Proposed Solution	1
1.4 Objectives	2
1.5 Methodology	2
1.6 Thesis Outline	2
Chapter Two: Background and Literature Review	3
2.1 Background	3
2.1.1 Cloud History	3
2.1.2 Cloud Computing Characteristics	5
2.2 Cloud Service Models	6
2.2.1 Infrastructure as a Service (IaaS)	7
2.2.2 Platform as a Service (PaaS)	8
2.2.3 PaaS as Delivery Models for Data Solutions	10
2.2.4 Software as a Service (SaaS)	10

2.2.5	Mobile "Backend" as a Service (MBaaS)	11
2.2.6	Serverless Computing Model	11
2.3	Cloud Deployment Models	12
2.3.1	Cloud Architecture	14
2.3.2	Cloud Engineering	15
2.4	Hosting in Cloud Computing	15
2.4.1	Shared Web Hosting Vs Cloud Hosting	16
2.5	Literature Survey	18
Chapter Three: SaaS Cloud Computing		24
3.1	Introduction	24
3.2	SaaS Architecture	24
3.2.1	Service Oriented Architecture	26
3.3	Protocols and Languages in SaaS	26
3.3.1	NoSQL Database	28
3.3.2	Queuing Systems	28
3.4	Cloud Security and Privacy	30
3.5	Cloud Security Challenges	31
3.5.1	Challenges at Communication Security Level	31
3.5.2	Challenges at Architectural Level	34
3.5.2.1	Virtualization Issues	34
3.5.2.2	Data/Storage Issues	36
3.5.2.3	Web Application and Application Program- ming Interface (API) Security	37
3.5.2.4	Identity Management and Access Control	38
3.5.3	Challenges at contractual and legal levels	39
3.5.3.1	Service Level Agreements	39
3.5.3.2	Legal Issues	40
3.6	Security Solutions	40
3.7	Computing in Health Care	43
3.7.1	Healthcare Data Standards	45
3.7.2	Health Analytics Role in Predictive Modeling	46
Chapter Four: Proposed SaaS Implementation		48
4.1	Proposed SaaS Architecture	48
4.2	Proposed Security Mechanism	48
4.3	Proposed Webfront Workflow	49

4.4	DataBase Process Flow	52
Chapter Five: Cloud Model Implementation and Web Front		
	Design	55
5.1	Implementation of Cloud Hosting	55
5.1.1	Adding PHP7 Functionality	59
5.1.2	Adding Apache 2.4 Server Functionality	61
5.1.3	Adding MySQL 5.6 Functionality	62
5.1.4	Adding phpMyAdmin Functionality	64
5.2	Cloud Web Interface Design and Access	64
5.3	Web Interface Home Page	67
5.3.1	Creating Patient File	67
5.3.2	Login Page	67
5.3.3	Reception Page	68
5.3.4	Doctor Page	69
5.3.5	Receptionist Page	71
5.3.6	Medical Lab Assistant Page	72
5.3.7	Patients Database	74
Chapter Six: Conclusions and Recommendations		77
6.1	Conclusion	77
6.2	Recommendations	77
Bibliography		79

List of Figures

2.1	Cloud Computing Model [1]	4
2.2	Concept of Virtualization [2]	4
2.3	Cloud Models [5]	6
2.4	Infrastructure as a service [5]	7
2.5	PaaS Cloud Computing [7]	9
2.6	MBaaS Cloud Computing [11]	11
2.7	HPC Cloud [13]	14
2.8	Cloud Architecture [14]	15
3.1	SaaS cloud computing [33]	25
3.2	SaaS Maturity Levels [34]	25
3.3	Mango Data Base [40]	29
3.4	Queuing System [41]	30
3.5	Cloud Security Challenges [43]	31
3.6	Communication Security [43]	32
3.7	Internal Communication [43]	32
3.8	Architectural Security [46]	34
3.9	Virtulization Issue [47]	35
3.10	Data Storage Issue [52]	36
3.11	Contractual and Legal Aspect [57]	39
4.1	Proposed SaaS Architecture	48
4.2	Security Provided by Cloud	49
4.3	Webfront Workflow (Part a)	51
4.4	Webfront Workflow (Part b)	52
4.5	Data Base Flow Chart	54
5.1	Putty Page	56
5.2	Login page	56
5.3	Server Information	57
5.4	History Commands (Showing previous commands that executed before by using history command)	58

5.5	Get Update	59
5.6	Python Installation	60
5.7	Adding Repository "ppa:ondrej/php"	60
5.8	Get Update	61
5.9	Installing Apache 2.4	61
5.10	Executing Command: <code>add-apt-repository-y ppa</code>	62
5.11	Executing Command: <code>apt-get update</code>	63
5.12	Executing Command: <code>install mysql-server-5.6</code>	63
5.13	PHP Myadmin home page from browser	65
5.14	Interface (After Logging)	65
5.15	Utilizing FileZilla to upload files to virtual server	66
5.16	Home Page	67
5.17	Login Page	68
5.18	Reception Page	68
5.19	Reception Page: Control of Patients Access to Doctors	69
5.20	Doctor Page: Viewing the Patients List	69
5.21	Doctor Page: Viewing the Patients Past History	70
5.22	Doctor Page: Adding Extra Patients Information	70
5.23	Doctor Page: Patient Past History Data	71
5.24	Reception Page: Patients list	72
5.25	Reception Page: Enter-to-Lab Status	72
5.26	Medical Lab Assistant Page	73
5.27	Medical Lab Assistant Page: Patient's Personal Information	73
5.28	Doctor Page For Viewing Lab Results	74
5.29	Patient Database	75
5.30	Designer View of Patient Database	76

List of Tables

2.1	Difference between using remote servers and local server [3] . .	5
2.2	Advantages of Public and Private Cloud Models [12]	12
2.3	Disadvantages of public and private cloud models [12]	13

List of Listings

5.1.1 System Information After Logging	55
5.1.2 Command Sequence for adding PPA and PHP7	59
5.1.3 Command Sequence for adding MySQL 5.6	62

List of Abbreviations

ACPS	Advanced Cloud Prevention System
ADT	Admissions, Discharges and Transfers
API	Application Programming Interface
AWS	Amazon Web Services
BaaS	Block chain as a Service
BPM	Business Process Management
CCE	Coogole Compute Engine
CDN	Content Delivery Network
CSA	Client Server Architecture
CSP	Content Security Policy
CSRF	Cross - Site Request Forgery
DOS	Denial of Service
DPaaS	Data Platform as a Service
EC2	Elastic Compute Cloud
EHR	Electronic health records
EMR	Electronic Medical Record
GEP	Google Compute Platform
HCRM	Healthcare Customer Relationship management
HIS	Hospital Information System
IaaS	Infrastructure as a Service
IBM	International Business Machine
IDS	Intrusion Detection System
IOT	Internet of Things
IPaaS	Integration Platform as a Service
IPS	Intrusion Prevention System
IPSEC	Internet Security Protocol

JSON	Java Script Object Notation
MAC	Media Access Control
MBaaS	Mobile Backend as a Service
MDM	Master Data Management
MSMQ	Message Queuing
NASA	National Aeronautics and Space Administration
NoSQL	not only SQL
NTST	National Institute of Standards and Technologies
P2P	Peer - to - Peer
Paas	Platform as a Service
PHP	Personal Home Page
RCM	Revenue Cycle Management
RDS	Relational Database Services
S3	Simple Storage Service
SaaS	Software as a Service
SDN	Software Defined Network
SLA	Service Level Agreement
SOA	Service Orinted Architecture
SOAP	Simple Object Access Protocol
SSL	Secure Socket layer
VM	Virtual Machine
VMM	Virtual Machine Monitor
VPN	Virtual Private Network
WSDL	Web Service Description Language
XML	extensible markup language

Chapter one

Introduction

1.1 Overview

Frequent symptoms of the patient during long periods, explain the existence of diseases that is difficult to detect except after long time. Most patients visit more than one hospital every time they feel sick, that makes hard to discover the problem. Most hospitals use papers to note symptoms, diseases, required tests and treatment, this technique is difficult to track, especially when we have variable hospitals and different doctors, to help solve this problem many hospitals, health centers and clinics have developed enterprise software to collect and save patient's data so as to access the information of him whenever we need them.

This research introduces the terms of cloud computing and how we use it in the health services. The simple definition of cloud computing is using group of remote servers connected together in the Internet to save, mange, process, and retrieve information rather than local server or personal computer.

1.2 Problem Statement

The enterprise software that is used in some hospitals to save the history of patients status is only can be accessed locally and doctors could have not retrieved this information if the patient had visited another hospital.

1.3 Proposed Solution

In help solving the problem of accessing the information of the patient that is coming from different hospitals , a Healthy Software as a Service cloud computing has been introduced to implement on ministry of health for all public and private hospitals that registered in the government.

1.4 Objectives

To follow the history of all problems that faces the patient through his life from each hospital he/her likes to visit.

1.5 Methodology

In this research we will create php software for ministry of health and host it in a cloud as software as a service, the ministry of health must impose this software for all hospitals to use it even the private hospitals, Here we choose department of cardiac disease to implement this system. This system include: the receptionist , the doctor and the lab technician The receptionist creates the patient files and save them in sql database, The doctor can review the patient history data and add new data for them and ask for the appropriate test to decide right diagnosis. The lab technician identifies the result of the test which then will be visible to the doctor .The system will provide alarming notifications for critical status

The tools that used in this research are Dreamweaver version 12.0 build 5808, XAMPP Control Panel version 1.7.7 , Ubuntu 14.04.1 LTS (GNU/Linux 3.13.0-32-generic x86_64), Apache 2.4, PHP 7.0, MySQL 5.6, Putty 0.70 , Filezilla 3.37.4.

1.6 Thesis Outline

The rest of this thesis is organized as follows. Chapter two presents background of the research, information about cloud computing like definition, history, cloud goal, characteristics, models and related topics of cloud like virtualization. Chapter three identifies software as a service cloud computing in details and talk about SaaS history, architecture, programming languages, important concepts of SaaS, security and privacy of cloud computing and using computing in healthcare services including the importance of patient data collection and types of healthcare reports. Chapter four provides the techniques of cloud hosting, web hosting, implementation of healthcare system webfront, workflow scenario. Finally, conclusions and recommendations are provided in chapter five.

Chapter Two

Background and Literature Review

2.1 Background

Cloud computing, also known as on-the-line computing, it is a kind of Internet-based computing that provides shared processing resources and data to computers and other devices on demand. It is a model for enabling everywhere, on-demand access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services), which can be rapidly provisioned and released with minimal management effort [1].

2.1.1 Cloud History

The first business of cloud computing has appeared when Amazon company deployed its own Elastic Compute Cloud for customers In August 2006, after this company Google has introduced Google App Engine for test In April 2008, in the same year NASA's has initiated nebula as first open-source platform for publishing private and hybrid clouds computing then American research and advisory firm Gartner has suggested cloud computing chance "to make a relationship among customers of IT services in the mid of the year. In February 2010 Microsoft corporation has introduced Azure closed source platform cloud computing for creating, testing, deploying and managing applications. On the first of March, 2011 The International Business Machines Corporation IBM has started the IBM Smart Cloud framework to provide all cloud solutions. On the seventh of June 2012 Oracle Corporation has introduced the integrated, autonomous and secure Oracle Cloud. In May 2012 Google Compute Engine has started a preview of high performance virtual machine before deployed in December 2013. Since that time till the time being the cloud companies are developing rapidly and it is expected for this technology to be at the top of all other technologies [1].

The goal of cloud computing is to let users to enjoy features from all technologies available, without need to educate the knowledge's and have expe-



Figure 2.1: Cloud Computing Model [1]

perience with each one of them. The cloud aims to reduce costs, and helps the users focus on their core business instead of being impeded by IT obstacles. The main technique available for cloud computing is virtualization. The idea of Virtualization is enabling separation of physical computing device into more "virtual" devices, each of which can be easy to use and managed to do computing tasks. With virtualization you can create a scalable system and use resources more efficiently [2].

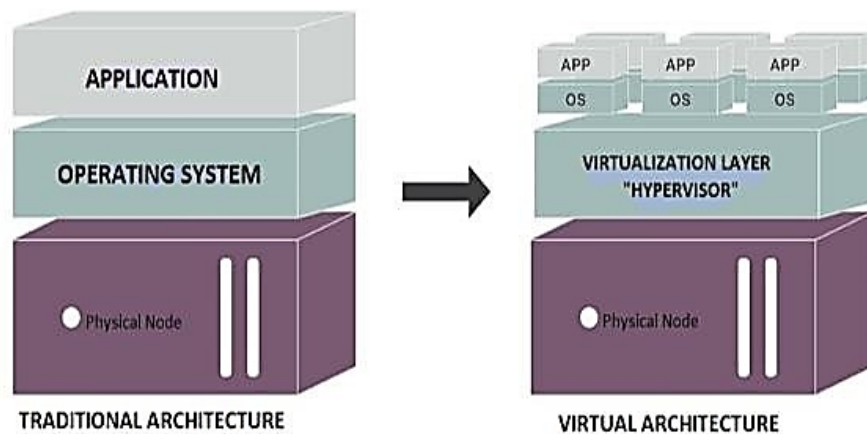


Figure 2.2: Concept of Virtualization [2]

Virtualization has pros and cons eg. It Minimizes cost by increasing infrastructure usage. Virtualization also provides the legerity to improve speed of IT operations, also it has an easy method for Recovery disaster like power outages, theft, cyber-attacks and so on. Virtualization makes recovery more

Table 2.1: Difference between using remote servers and local server [3]

Remote Servers	Local Server
requires very little infrastructure from the client Require	full infrastructure
High security	Need firewall
The scalability stronger	Low scalability
Require pay a monthly fees	You use your own resources
Depend on the internet	You can use private network
Lower cost	High cost
Easy setup and configuration	Need technical support to configure

accurate. With it also You can do full backup easily to your virtual server and ensure that your data is up to date, you can also save power because there is no local hardware or software options being utilized to consume energy. Virtualization is a major stage in transformation to cloud computing, it provides fast redeployment if any problem occurred. On other hand we need high cost to implement virtualization environment. It faces restriction in implementation because not every application is compatible to work with the environment of virtualization, it also Needs protection against hacking, sometimes with virtualization Availability and Scalability problems may occur [3]

2.1.2 Cloud Computing Characteristics

Cloud computing has many key characteristics like Increasing user's flexibility in cloud for example you can add, or expand technological infrastructure resources. Another characteristic is reducing cost, i.e., no need to have more components because infrastructure is provided and managed by a third party based on billing options. Another feature is that the Customers and data center are independent so you can access cloud applications using a web browser regardless of their location or what type of device you use. Cloud computing software is easy to fix, because it does not need to be installed on each client device and can be accessed from various locations. In cloud computing the Performance observation by IT experts in the service provider, also cloud data

centre is combined to serve many customers using a multi-tenant model with various physical resources and virtual machines. The positive impact in productivity comes when multiple end users work on the same data in the same time, we find that Cloud computing is well-designed which makes it more reliable and has ability to recover disaster. Besides this there is a Dynamic Scalability and flexibility where there is no need for engineer to identify peak load for users when the usage need is up or down [3].

Security in cloud is improved compared with traditional systems, because centralization of data makes service providers are able to introduce high security level. In addition to this the customer can request their requirements, of resources, as needed automatically without interact with human in cloud provider. Cloud platform can be accessed using different types of devices such as mobile phones, tablets, laptops, and workstations this process called broad network access [4] .

2.2 Cloud Service Models

Cloud computing has several models agreed by National Institute of Standards and Technologies (NIST). These models appear as layers, there is no need to be related you can use one layer or all layers (refer to Figure 2.3). It provides "every thing as a service" these models are: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) [5].



Figure 2.3: Cloud Models [5]

2.2.1 Infrastructure as a Service (IaaS)

IaaS is a type of cloud computing that offers online services in form of virtualized computing resources by high-level (application programming interface) APIs over the Internet. The infrastructure consists of many categories includes: physical resources, location, data partitioning, scaling, security and Backup [5].

In IaaS layer, the cloud provider hosts the infrastructure Ingredients in data center, including: servers, storage, networking hardware and Virtualization. The cloud provider also provides a range of services include: detailed billing, monitoring, log access, security, load balancing clustering, Storage resiliency, such as backup, replication and recovery.

To give Examples of IaaS vendors and products we have: Amazon Web Services (AWS) which Introduces storage services such as: Simple Storage Services (S3), Compute services and Elastic Compute Cloud (EC2). Other example we have Google Cloud Platform (GCP) which Introduces storage and compute services through Google Compute Engine (GCE), the third example is Microsoft Azure, Microsoft Azure is a cloud computing service created by Microsoft for Building, Testing, Deploying and Managing applications services through a global network of Microsoft-managed data centers [5].

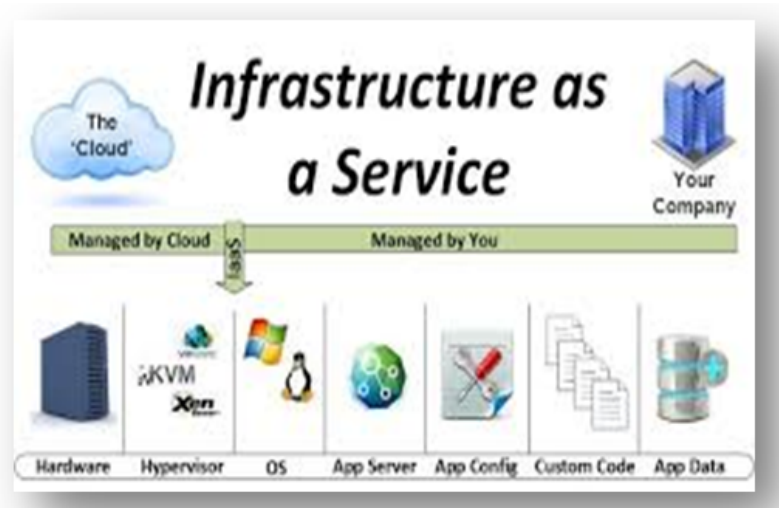


Figure 2.4: Infrastructure as a service [5]

IaaS provides customers with access to virtual resources on-demand over the Internet. You can host and manage the virtual server space, storage systems, and network security that you need. This lets you configure and control your operating systems and applications over the Internet. IaaS is different from

the other form of cloud computing, SaaS and PaaS – in which the operating systems (in the case of SaaS) manage your applications on your behalf. IaaS gives companies chance to host websites, test applications online, deploy new products and services without hosting fees, and delays times associated with their on-site data center setup [6].

IaaS pros and cons are explained as: Availability, the data is obtainable whenever you require it the thing which makes it best solution for businesses that look to test and deploy applications or services rapidly without any delay by setting up their own internal hosting infrastructure. In IaaS there is a high Flexibility and scalability because IaaS will commonly work on a pay-as-you-go base, by which it can be allowed for businesses to scale up resources, adjust expansion and increase customer demand, there is also a Cost-efficiency in which you pay only for the resources you utilize Depending on your service needed. In addition to what mentioned there is an Accessibility by which you can access your virtualized resources from any location through the internet. More over it has a high Manageability by which the cloud provider is responsible for setup and manages the hardware you require. This keep your time, money and overwork of managing and maintaining hardware.

On other hand IaaS is Most expensive, because the customer hires a resource, while the provider includes every Cycle, bit of RAM or disk space used in a bill. With IaaS the customer is responsible for all aspects of Virtual machine management. Until now the physical location of the VM can not be monitored [6].

2.2.2 Platform as a Service (PaaS)

It is The capability provided by cloud computing to the end user to deploy onto the infrastructure cloud, customer creates unique applications in runtime environments using functions, libraries, services, web service integration, information security and tools confirming by the provider Then run it, improving, testing, and managing applications without the complexity of building infrastructure. In paas there is no need for servers, databases, operating systems, development tools, etc [7].

To give examples for PaaS services we have: Heroku, the term "Heroku" is a portmanteau of "heroic" and "haiku", Google App Engine, AWS Relational Database Service (RDS), Microsoft Azure and Oracle Cloud Platform.

PaaS has many types, the first one is Public cloud PaaS, in which the client

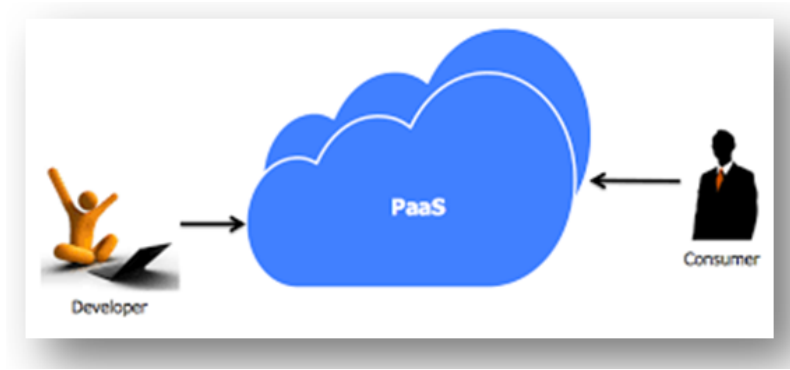


Figure 2.5: PaaS Cloud Computing [7]

controls software deployment while the cloud provider delivers all the main IT components necessary to host the implementation, including servers, storage, networks, os, and databases the second type is Private cloud PaaS this type is defined as software or an appliance built in client's firewall. The final type is the Hybrid cloud PaaS which gives a combination of the two types of cloud service. Like other types of cloud services, in PaaS customers pay per-use basis [8].

The common uses for PaaS are: API development and management, here Customers can use PaaS as end-to-end API management to create new APIs or new interfaces for existing APIs, Business analytics/intelligence, these Use PaaS tools to analyze data and behavior for better decision and more accurately predict future events, Business process management (BPM), here Customers can use PaaS to access a BPM platform which is introduced as a service with other cloud, another use is Communications by which PaaS can allow end-users to add communications features like voice, video, and messaging to the applications, other use is Databases by which A PaaS supplier can deliver services such as setting up and maintaining company database also Internet of things, IoT is another use it is predicted to be a great part of PaaS usage in future, supporting more application environments, programming languages and tools. Another use is Master data management (MDM), it covers critical data to support decision makers, the data may include reference data or information about customer transactions [10].

On other hand PaaS has pros and cons for instance developers can access an environment to create and deploy new applications without need to spend time and money to build an infrastructure, additionally there is a fast development and applications delivery, customer can use paas to test technologies

quickly such as new languages, operating systems and databases, also let it be faster to upgrade their tools. paas gives new principles and gathers more features of cloud infrastructure, also All customers's that use PaaS can manage their implementations and data so lack of control is not a big issue. Besides all these advantages we find in PaaS all cloud risks are available such as security problems, unauthorized access, attacks by hackers or other bad actors when the service provider's infrastructure downtime for whatever reason, that will affect on PaaS service like changes in its development strategy, programming languages, or in other areas, The customer only controls the deployed applications and may configure settings for the hosting environment but can not control the infrastructure [10].

2.2.3 PaaS as Delivery Models for Data Solutions

PaaS introduces many solutions for data delivery like:

- Integration Platform as a Service (iPaaS), it allow the integrations without need to setup any hardware or middleware.
- Data Platform as a Service (DPaaS). In dPaaS cloud provider introduces fully managed service for data, users keeps transparency and controls data through data-visualization tools.
- Finally, Block chain as a Service (BaaS): it is an Special type of PaaS used by some vendors like IBM Bluemix and Oracle Cloud Platform [10].

2.2.4 Software as a Service (SaaS)

Software as a service is a developed software model hosted in infrastructure cloud accessed by clients over the Internet using web browser.

The applications are accessible from different client devices using web browser, such as pc, mobile, or program interface. The customer does not manage infrastructure or platform; he has just limited user application configuration settings. The Examples of SaaS are represented in Office 365, Google Apps, Salesforce, Citrix GoToMeeting, Cisco WebEx and Netflix

SaaS has pros and cons, e.g it Reduces time IE in SaaS the software is ready for use. But in traditional model users consume time for installation and configuration, also it Lowers costs IE SaaS has low cost in hardware and software license compared with the traditional software. SaaS model

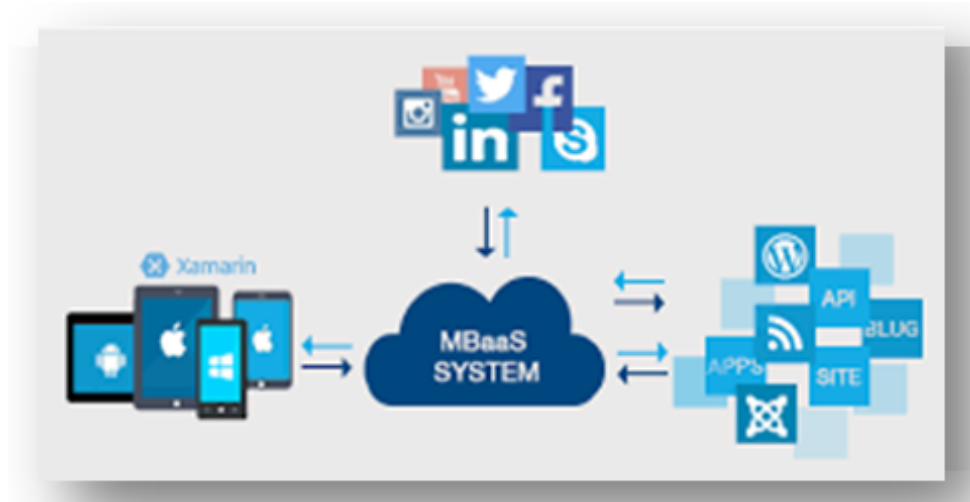


Figure 2.6: MBaaS Cloud Computing [11]

is scalable and has ability to integrate with other available SaaS. The New upgraded releases of cloud providers SaaS is ready for their clients, it reduces the cost and effort. SaaS model is easy to use because it is tested and approved by users before deployed it. If SaaS has sensitive data, this may be a problem in some functionality because the data is Stored on the Internet on third party servers IE there is a lack of security and confidentiality additionally Risk of losing data may occure in SaaS provider, also the efficiency of SaaS model is depending on the speed of the internet [11].

2.2.5 Mobile "Backend" as a Service (MBaaS)

MBaaS is a relatively modern model in cloud computing introduces integration of web app and mobile app with cloud storage and cloud computing services by application programming interfaces (API), this Services include: user administration, push notifications, Integration with other networking services, Manages data storage and Enable GPS services on mobile devices to get benefit from applications,, API management to built and control all APIs that make interaction between the front end and back end easy [11].

2.2.6 Serverless Computing Model

In server less computing, cloud computing completely controls the system uses the code implementation model, The cloud provider makes virtual machines on and off As necessary to service requests. this service model is called Server

Table 2.2: Advantages of Public and Private Cloud Models [12]

Private Cloud	Public Cloud
The infrastructure is a dedicated to one single client	the resources are shared between multiple clients and all the services are controlled by service provider
better controls for data, users and information assets	available as service in the internet, easy to deploy
initial investment for hardware is very high in case of an on-premise infrastructure	initial investment is very low or nil
high levels of security	the IT resources and services are available immediately saving time for the company
insures efficiency and good network performance	the hardware and network are maintained by the cloud service provider
the hardware and other resources can be customized easily by the company	no long term commitment with services provider
compliance achieved easily	

less computing because the customer does not need to rent servers or virtual machines to run the back-end code [12].

2.3 Cloud Deployment Models

There are many models of deployment in cloud computing, the first type is Private cloud, it is a cloud infrastructure works just for one organization, either controlled and hosted internally or externally. the second type is Public cloud, in this type the services are provided over the Internet and opened for the public use, mostly these services are free. In architecture there is no difference between public and private cloud but security consideration may be substantially different [13].

The third type is Community cloud, it shares infrastructure between different organizations from a particular community with the same business, either managed internally or externally. In this type The costs will be shared between all users.

Table 2.3: Disadvantages of public and private cloud models [12]

Private Cloud	Public Cloud
the running cost would include personnel cost and periodic hardware upgrade costs in the case of outsourced private cloud operating cost will include per resource usage	the client has no control of data or infrastructure
optimizing the utilization of all resources is a challenge	the performance of the network depends on the speed of the internet connectivity
Physical hardware are limited	Weak on security, the hardware resource is shared between multiple users IT security issues are more profound and data is vulnerable to thefts
Vendor lock it prevents the client to migrate to another vendor	customization of resources or services is not possible

The fourth type is Hybrid cloud it is a combination of some types of cloud (private, community or public) that offers the advantages of all deployment models, It allows the user to expand the ability of a cloud service, by gathering, integration or specialization with another cloud model. Hybrid cloud has an example, by which the organization may store critical data on a private cloud and connects it with another application introduced by a public cloud as a software service.

Hybrid cloud also has many factors for instance, data security, compliance requirements, level of control needed over data and applications of an organization uses.

The fifth type is Distributed cloud, it is a platform that can be distributed from an expanded set of servers in different sites, connected together to a single network. The distributed cloud divided into two kinds: Public-resource computing, This kind of distributed cloud is sub-class of cloud computing. The definition of cloud is more comprehensive . For example BOINC and Folding@Home. The second one is Volunteer cloud: in it the cloud computing infrastructure is created using volunteered resources. It can also called peer-to-peer clouds, or ad-hoc clouds [13].

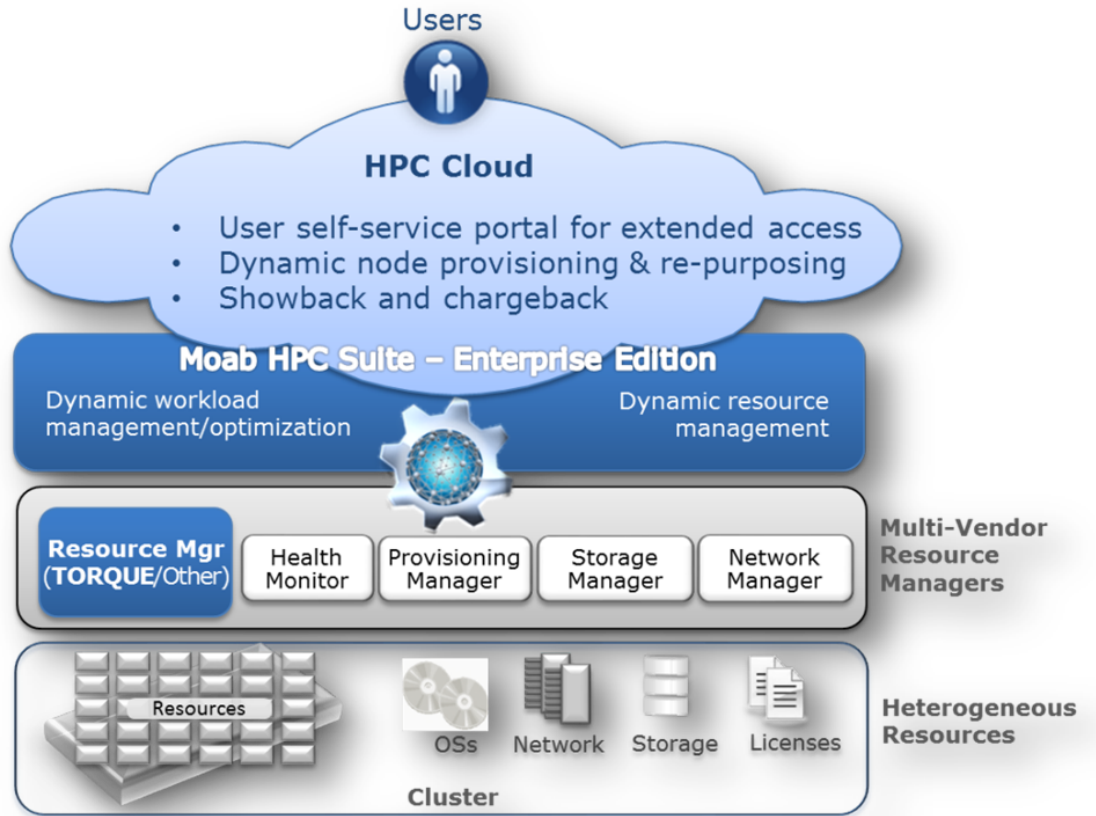


Figure 2.7: HPC Cloud [13]

The sixth type is Multi cloud, it uses combination of various public infrastructures as service environments such as Amazon Web Services and Microsoft Azure, it introduces any implementation of multiple software as a service (SaaS) or platform as a service (PaaS) cloud. The difference between hybrid and distributed cloud is that the hybrid cloud refers to multiple cloud models but distributed cloud refers to multiple cloud services.

The last type is HPC cloud, it refers to the use of cloud computing services and infrastructure to execute High Performance Computing (HPC) applications to allows experts and engineers to solve complex problems [13].

2.3.1 Cloud Architecture

Cloud computing architecture identifies the components and equipments required for cloud computing. These components typically consist of a front end platform (pc, laptop, Ipad, workstation or mobile device), back end platforms (data centre), a cloud based delivery, and a network (Internet, Intranet) [14].

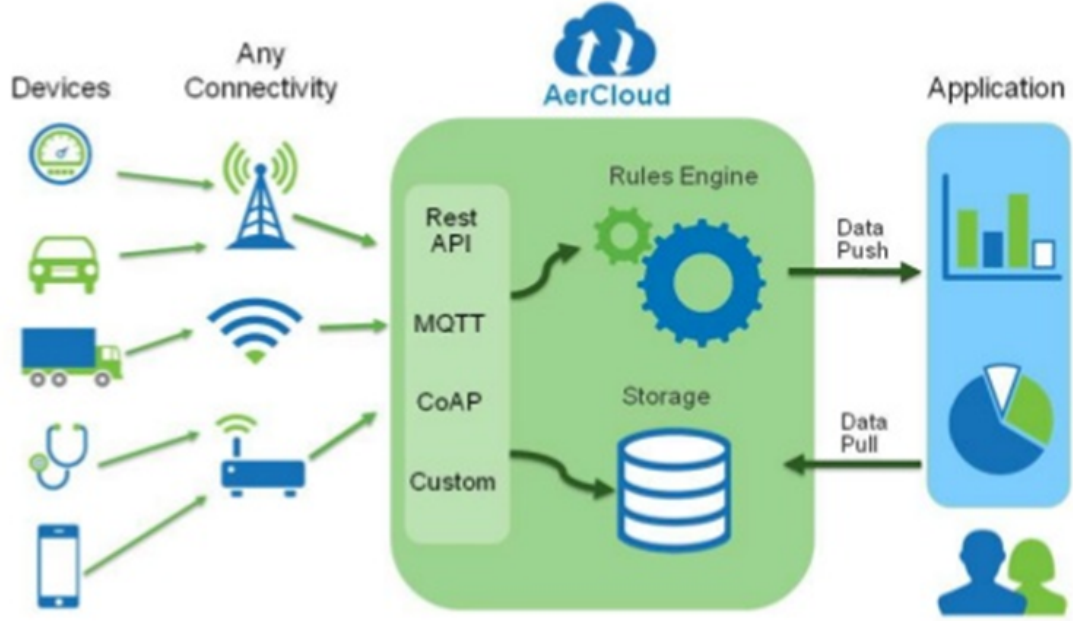


Figure 2.8: Cloud Architecture [14]

2.3.2 Cloud Engineering

Cloud engineering is a field of engineering that concentrates on cloud services, such as "software as a service", "platform as a service", and "infrastructure as a service". It is responsible for commercialization, standardization, and governance of cloud computing applications [15].

2.4 Hosting in Cloud Computing

Cloud hosting is an alternative technique for hosting websites on specific server, and can be considered as an expansion of the concept of clustered hosting where websites are hosted on infrastructure cloud.

Generally, customers can benefit from cloud hosting service as much as they request, depending on their needs. Cloud hosting also save costs because customers only pay for what they use and don't need to pay for additional capacity.

Most examples of using cloud hosting include the public cloud models where hosting will be on virtual public servers, in the public cloud, The same public networks are used to send their data; which are physically stored on the infrastructure cloud and These public clouds will contain some security mechanism to ensure that data are kept save [16].

We can also use Private clouds, which are more appropriate where safety and privacy is more of a concern. Private clouds use protected resources, such as servers and networks with high security, whether located on data centre or with the cloud provider.

Also we use Private and Hybrid Cloud which Offers the flexibility of public cloud and the security of private cloud with the ability to integrate with traditional infrastructure and other available clouds across the globe.

Cloud hosting models can be classified into, PaaS where The client is able to access software environment, on which they can go directly to install and develop their web application without need for high experience to use it . IaaS, where The virtualized hardware resources are allocated the client on which they can install their own software environment before building their own web application IaaS is More customizable and requires high experience to use it [16].

cloud hosting has many benefits, for example Cloud hosting provides virtual disk space in resource, from an overall network of underlying physical servers. If one server goes down it will have no effect on availability outcome, as the virtual servers will continue to provide resource from the remaining online servers. Instead of being hosted on one single physical server. Besides this cloud hosting has high Scalability because Resource availability in real time as you need and not limited to the physical capacity of one server. For example If a client's application has load of traffic the extra resource will be accessed easily, another benefit is a Responsive load balancing it based on the software that hosted in the infrastructure cloud, it makes the scalability for respond to changing requirement automatically. Cloud hosting also has Physical security where The physical servers are found in high secure data centers that prevent people from accessing or disrupting them on-site.

On other hand, The available resources are used on demand, pay for what actually used this introduce best utilization [16].

2.4.1 Shared Web Hosting Vs Cloud Hosting

In case of security, the security in Shared Hosting depends on databases and applications which make them susceptible to hackers. IE: if you access to a website shared on server, it will be easy to access the other websites on the same server and hack it.

Since the security threats on shared host are wide spread, most hosts

providers recommend customers to make their computers safe using new updated anti viruses with internet security like ESET or Kaspersky [17].

They also warn on using weak passwords and keeping your cPanel password on any files on your account. Also, disable unnecessary options on your programming language settings to enhance security. But in cloud hosting the security management deals with existed issues using security control, There are four major constraints behind the architecture of cloud hosting security: Deterrent controls, Preventative controls, Detective control and Corrective controls [17].

Cloud hosting is better than shared hosting for the simple reason that in cloud the users have absolute control when it comes to security the most responsibility depends on cloud In case of problems with hardware, the website will be moved to a stable server[18].

In case of Performance, the Shared Hosting resources are limited that affect on speed. However, there are corporations that work very well in this type, most host providers compete with each other to be able to give enough resources for this technique. Also the host providers compete with each other to give fixed downtimes and outages.

But in cloud hosting you have very high speed, auto scalable and customization for utilization for example if the load is over in specific period of time the site can withstand and not being down [18].

Cloud hosting is better than shared hosting because in cloud you have many resources that provide better performance.

In case of Speed the Shared Hosting always uses full capacity servers, this means if one site down all other websites will be affected with slow speed and user will wait long time to response until service provider resolve the issue, but Cloud Hosting based on distribution of resources, if hardware issue detected the websites would be moved to another clustered server.

Cloud hosting is better than shared hosting because the resources in cloud is more available and the services are highly quick.

In case of Pricing in Shared Hosting There is inverse relationship between sharing server space and hosting price because the cost of service is distributed between all shared hosting websites, the payment can be monthly, annually or every three years, but in Cloud Hosting the users pay only for what he used that means when the load became high the price increases and when the load became down the price decreases [19].

Cloud hosting is better than sharing hosting, because in cloud the payment is depending on how the utilization is. this avoid the risk of overusing resources and paying more.

The best Example of venders who introduce cloud hosting is google, it provides search engine distributed over hundreds of servers on cloud , there is no any downtime in google services, another example for cloud hosting is Enterprise Cloud Hosting which means getting help from external sources , all the providers that introduce enterprise software may also give training, backup, and upgrade services. The Hyperscale Cloud Hostingis also an example of cloud hosting, in it the storage of large amount of data in cloud is increasing in size rapidly, efficiently, and indefinitely., hyperscale storage capacity commonly runs into the petabytes. Another example is Managed Cloud Hosting, IN it the organizations share their resources, including servers, databases, hardware , software and tools, across a remote network via internet [20].

There are many web applications introduced by the cloud like: Google Documents, Google Docs is web-based office suite introduced by Google within its Google Drive service , by google docs you can create word document ,excel sheet ,powerpoint and save it for free. Also we have Quick Data Sharing, it is a technique of letting information result from researcher available to other implementer. Another example is Dropbox, it is a service where users are given 2GB memory space to save their data for free and users can purchase more space if they like, this service is more popular and users can access their data safely from anywhere [21].

2.5 Literature Survey

Cloud computing is not a new term, it has been used in many countries and a considerable amount of literature has defined cloud computing, e.g., [2–4,22]. For example, [2] introduced Cloud Computing, including a simple definition about cloud computing, service, architecture, management and importance of security and privacy. Also, the study in [3] provided an introduction about Cloud Computing, characteristics, service model, deployment and potentially privacy risks. The study in [23] discussed the cloud computing, dialogic corporation, benefits, challenges, communication in cloud, services, accessing through API and cloud scalability. The study in [4] focused on Cloud Computing and services, background, definition, flexible ICT services, Areas and

examples of applications. The study in [22] discuss more than 20 definitions of cloud computing, essential characteristics and confused with cloud technologies. The study in [24] introduced the basic principles of cloud computing. This article also introduces the application field the merit of cloud computing, cloud computing principles, cloud computing style, characteristic of cloud computing cloud computing applications and advantages.

Further defining studies can be found in [5]. The study in [5] include the difference between distributed computing, ware house – scale computing and cloud computing, cloud impact, cloud economics and risk of cloud. The study in [6] identify the relationship between cloud computing, mobile cloud computing and mobile devices, cloud computing services and models and virtualization framework. The study in [25] include the definition of cloud computing, cloud computing economics, classes of utility computing and obstacles to and opportunities for growth of cloud computing. The study in [26] introduce cloud definitions, characteristics, and trends, market-oriented cloud architecture, global cloud exchanges and markets, and emerging cloud platforms. The study in [27] introduce definition and functional aspects of cloud computing, enabling technologies behind cloud computing and virtualization technology. The study in [28] include cloud computing infrastructure, the key advantages of cloud computing, core technological concepts and terminology, cloud computing a SWOT analysis and weakness. The study in [7] include cloud computing concept, utility, architecture, cloud services, characteristic, platform, models, privacy and security. The study in [8] identify Definition of cloud computing. functional aspects of cloud, technologies behind cloud and Amazon Elastic Compute Cloud.

Cloud models has been considered in [9], along with services, deployment, management, security, threats, attacks, risk, standardization activities. The study in [29] introduce all characteristics of cloud computing and explain it in details. Privacy and the importance of it in cloud computing is discussed in [10], including types of data that needs to be protected, Privacy threats and risks for cloud Computing, challenges for cloud, Analysis for different types of scenario and Privacy risks for cloud computing. Cloud architecture is considered in [11], in addition to security, costs, hardware/software trends (commodity vs. brands, open vs. closed-source), organizational/human factors. Models in details, virtualization and future of the cloud computing market. The issue of SaaS risk analysis is introduced in [30] including evalu-

ation methods for SaaS in cloud computing. Information about cloud models can be found in [12], including a survey and comparison for open and close source in cloud computing. The study in [13] include hierarchical view of cloud computing, data centers, infrastructure as a service, platform as a service, software as a service, existing cloud computing architectures and service oriented cloud computing. The study in [31] introduce architecture of current NVMe-based VM Hypervisor, software development, virtualization overview, algorithm design of hybrid NVMe utilization approach and Parallel Queue Mode. Regarding cloud security, several studies exist, e.g., [14–20, 32]. The study in [14] includes cloud security challenges levels and security solutions in literature. The study in [15] includes cloud computing security issues and cloud security implications and remediations. The study in [32] includes cloud computing security issues and architectures. the study in [16] introduce introduction about cloud security, security issue causes and possible security approaches. The study in [17] include risk area in cloud computing, security issue in cloud services and mitigation OF of security risks. The study in [19] introduce security concerns and quick description of threats and solutions. The study in [18] introduces cloud computing security issues, risk factors and Identity, Authentication, Authorization, and Auditing Mechanisms. The study in [20] proposed a privacy aware authentication scheme for distributed mobile cloud computing services. Regarding SaaS, the study in [21] introduced the SaaS definition, models, layers, SaaS Architectural Maturity Levels, SaaS offerings and tools, Successful SaaS Architectures. SaaS architecture is considered in [33], including, common computing infrastructure considerations, SaaS in physical security today, access control, Video Surveillance, Intrusion Detection, Visitor Management, Mass notification, Current and future applications will grow in sophistication, SaaS efficiency, security and market segments for SaaS, SaaS security considerations. The importance of SaaS is considered in [34] including, architecture, functionality, efficiency, advantages and disadvantages. Further information can be found in [35], including definition of SaaS cloud computing, examples, benefits, SaaS market, drawbacks and commonly used protocols.

Security in SaaS has been considered in [36, 37]. The study in [36] introduced Security Issue in SaaS, traditional security challenges, authentication and authorization, availability, data confidentiality, virtual machine security, cloud specific security challenges, web application security and currant secu-

rity solutions. The study in [37] considered analyzing security issues in SaaS in different environments, such as SaaS in cloud Computing, SaaS in Mobile Cloud Computing, SaaS in Software Defined networking, SaaS in Internet of Things and SaaS security challenges. Finally, the study in [38] discussed SaaS system problems, role name Conflicts, cross-level management, the isomerism of tenants' access control, temporal delegation constraints.

Additional issues in SaaS are discussed in [39, 40]. Linking with PaaS can be found in [39], which discussed goals of software engineering, platform as a services and how SaaS are built in PaaS, essential requirement of SaaS applications and resources models of cloud computing. Also, [40] discussed *green It* and cloud computing, adopting SaaS cloud computing, behavior intention, subjective norms and Perceived behavior control.

The issue of access control has been considered in [41–44]. The study in [41] targeted controlling risks in the cloud, control access to resources that you don't control, Extend your internally automated processes out into the cloud, Keep workarounds at bay, report and audit. The study in [42] introduced access control, authentication and authorization, access control policies, attribute-based access control, access control requirements, access control flow. The study in [43] introduced Cloud Access Manager delivers single sign-on (SSO), benefits, and features and [44] introduced a Hierarchical Access Control Model for SaaS Systems.

Classical access models were discussed in [45] and *attribute-based access control* (ABAC). Also, [46] provided the definition of ABAC and considerations for using ABAC to improve information sharing while maintaining control of that information. The study in [47] introduce ABAC, a highly effective means of information sharing, based on the use of attributes. The study in [48] discussed attribute Based Encryption (ABE) access control techniques available to be used for cloud environments.

Regarding big data analytics, the study in [49] discussed privacy issues relating to big data analysis and investigates how emerging attribute-based access control technology can assist in protecting against the inadvertent or deliberate unauthorized access to personal data in a Big Data context. The study in [50] how to involve cloud computing in bioinformatics and big data analytics.

The concept of cloud grids and distributed systems is presented in [51], comparing between grids and cloud side by side, business models, program-

ming model, security model and application model. The study in [52] includes service oriented computing, grid computing, cloud computing and relationship between them, also identify several challenges from the cloud computing adoption perspective.

In terms of the link with IoT, the study in [53] include foundation and illustration through Internet of things, *every things as a resource* framework and categories of resources. The study in [54] present a survey of IoT and Cloud Computing with a focus on the security issues of both technologies. Specifically, the combination the two aforementioned technologies (Cloud Computing and IoT) in order to examine the common features, and discover the benefits of their integration.

Regarding the link with healthcare, several studies exist, e.g., [55–58]. The study in [55] discussed the importance of information technology in health-care, characteristic of cloud computing, cloud service models and types, cloud computing in healthcare sector, currant state of cloud computing in healthcare and cloud computing healthcare in Malaysia as an example. The study in [56] introduce Internal and external cloud based hospital supply chains, control management and load time management. The study in [57] include health care solution structure, general cloud-based solutions, cloud-based health care system architecture, applications and models, inter-operable fog-based solutions and challenges and opportunities of cloud-fog-based services. The study in [58] include problems of currant processing of patient, requirements to improve the scenario and advantages for using cloud in health care.

Example case studies can be found in [59], where Vecchiola et al. discussed two practical applications of scientific computing in the Cloud. Both the case studies have been implemented on top of the *Amazon EC2 infrastructure*. The first case study features the classification of gene expression datasets by using an *Aneka Cloud* while the second case presents the execution of an fMRI brain imaging workflow and compares its performance with the same experiment carried out on traditional Grids. In both of the two cases, a cost analysis on the usage of the Cloud is presented. The adoption of Cloud computing as a technology and a paradigm for the new era of computing has definitely become popular and appealing within the enterprise and service providers. It has also widely spread among end users, which more and more host their personal data to the cloud. For what concerns scientific computing, this trend is still at an early stage. The study in [60] introduce benefits of cloud computing in

e-learning system.

Chapter Three

SaaS Cloud Computing

3.1 Introduction

Software as a service (SaaS) is a procedure of software delivery in which a third-party provider is responsible for hosting applications and makes them available to end user over the Internet. Data can be accessed from any device using web browser. SaaS also known as pricing model, pay as you use [33].

3.2 SaaS Architecture

SaaS architecture can be classified based on their maturity levels as follows: Ad-hoc/Custom, it is the first level of maturity which is useful when changing existing client server architecture. And it doesn't require system administrator which actually helps in reducing maintenance costs. Another level is Configurability, This level of maturity is useful in giving flexibility in recognizing various users utilizing the same application or service. This is done by configuring unique metadata, which helps cloud provider in characterizing various user and their needs, So that cloud provider can maintain the main core code of the application instead of end user. it also helps cloud provider in managing the resources. The third level of maturity is Multi-Tenant Efficient, it is known as sharing of resources across hundreds of tenants or end users but can still distinguish individual users, their data and needs on demands. last level is Scalability, In this level of maturity the application resources are used efficiently by conducting best practices of IT such as optimizing locking duration, statelessness, sharing pooled resources such as threads and network connections, caching reference data and partitioning large databases [34].

Some of the important concepts in SaaS cloud computing are web services and application programming interface (API). API is a set of commands, functions, protocols, and objects used by programmers to allow two applications to talk to each other without creating new code from scratch [35].



Figure 3.1: SaaS cloud computing [33]

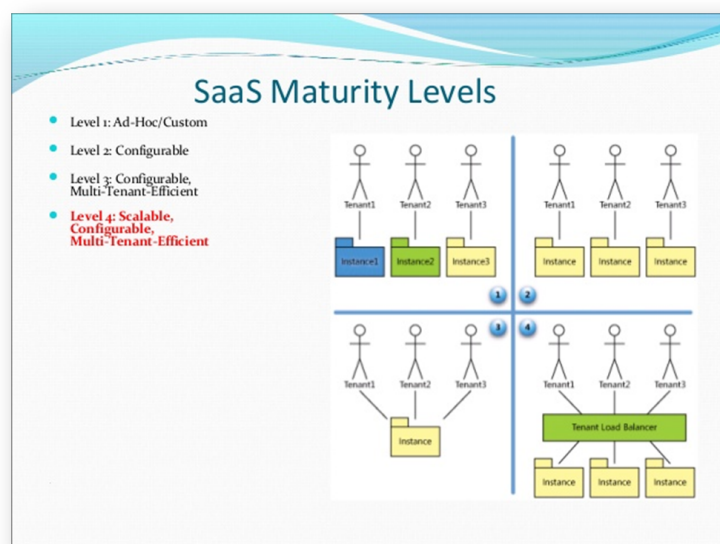


Figure 3.2: SaaS Maturity Levels [34]

3.2.1 Service Oriented Architecture

Service-oriented architecture (SOA) is a style of software expansion model where services are introduced by application components, through a communication protocol over a network that combines discovery, access control, data mapping and security features.

SOA has two major functions: the first function is that it Creates a standard architectural model that specifies the target of applications and the method that will help meet the goal. The second function is that It Identifies application specifications, usually connected to the Web Services Description Language (WSDL) format and Simple Object Access Protocol (SOAP) specifications. SOA also has three major objectives:

- The first objective aims to structure execution of software components as services. These services are intended to be loosely coupled to applications, so they are only used when needed. They are also designed to be easily utilized by software developers, who have to create applications in a consistent way.
- The second objective is to give a mechanism for publishing available services, which contains their functionality and input/output (I/O) requirements. Services are published in a way that let developers easily combine them into applications.
- The third objective of SOA is to control the utilization of these services to avoid security Obstacles. The Security in SOA is about protection of the individual components within the architecture, identity and authentication procedures related to those components, and securing the actual connections between the components of the architecture [36].

3.3 Protocols and Languages in SaaS

The first protocol is JSON, it Stands for java script object notation, which based on a subset of the JavaScript Programming Language and it is most popular because it uses Light weight data-interchange format, it is easy for humans to read and write, it is Easy for machines to parse and generate. Then we have the XML it Stands for extensible markup language that defines a set of rules readable for both human and machine to store and transport data.

Also we have SOAP which Stands for Simple Object Access Protocol, it is a messaging protocol for exchanging information if implementation is only web services. Other protocol is ATOM, it is a free opened -source platform editor for macOS, Linux, and Microsoft Windows written in Node.js, and embedded Git Control, created by GitHub. Atom is a desktop application using web technologies structure [37].

Now lets have a glance of the Most popular programming language in SaaS. The first one is Python, it is an interpreted high-level object-oriented language that carefully resembles the English language which let it a major language to learn for beginners and professionals. Python 3.6 got released in December 2016 with some awesome features.

The examples of The sites that use Python are: Instagram, YouTube, Reddit, and NASA. The Second language is Java script JS, it is a high-level, explicated programming language. It is a functional based language, easy to learn, prototype-based and multi-paradigm. The third one is Type script, it is an open-source developed by Microsoft. It includes JavaScript with some added features like amendment checks against bugs in your code. The fourth language is Java, it is a general-purpose language that supports classes, objects and special designs . java is oldie but Goldie. The fifth one is Rust, it is the most popular for programmers, it's a general-purpose language to initiate fast and secure implementations which takes benefits of the powerful features of new multi-core processors. The examples of the sites that use Rust are: Dropbox and Coursera. The sixth language is PHP, it is the lovely web development programming language. It's mostly used as general purpose language it's a powerful tool for making dynamic and interactive Web pages, php is widely-used, free, and functional. The seventh one is Elixir, it is general-purpose programming language it is functional and concurrent language built to create scalable, maintainable implementation . Concurrency is one of its main advantages. It's great for applications that handle a many tasks in the same time [39].

The sites that use Elixir are: Pinterest and Bleacher Report. The eighth one is Go, (or GOLANG) it is open source programming language created by Google, it's going to have popularity in 2017 It has an premium standard library and it compiles fast. It's considerable with concurrent tasks and programs as well.

the sites that use Go are: Netflix, YouTube and Adobe. The ninth language

is Ruby on Rails, it is a server-side web service framework that contains everything necessary to make database-backed web applications according to the Model-View-Controller, like 'jQuery for JavaScript. the businesses that use Rails are: Airbnb, Groupon, Twitter and Shopify. The tenth one is 'see-sharp', it is a multi-paradigm programming language It's not only limited to Microsoft's NET Framework. its widely-used in OS/Android Apps and Windows applications. The eleventh one is Swift, it is a general-purpose, multi-paradigm, collected programming language, it is growing faster Swift is created to work with Apple , it is also used commonly for international wire transfers [39].

3.3.1 NoSQL Database

NoSQL stands for "not only SQL," it's the most fundamental choices of non relational data NoSQL databases are especially useful for working with large amount of distributed data. It's an open source. We may find also the term Document Database it also called a document store or document-oriented database, is a subset of NoSQL used for saving, restoring, and managing semi-structured data , the data model in a document database is not constructed in a table format of rows and columns. The schema can vary, introducing more flexibility for data modeling than relational databases.also we find the term MongoDB, it is a document database that gives high performance, high availability, and easy scalability. Scalability is the most important factor for us as a international SaaS business. A lot of SaaS construct aim for scaling their business. Besides scaling your application from a business sight you shouldn't forget about the technical matters [40].

3.3.2 Queuing Systems

A message queuing system is an asynchronous communication protocol used to control queues. Between sender and receiver of a message that not interacted at the same time. Also known as Message Queuing (MSMQ) technology it enables web apps to run at different times and to communicate with various side integrations / APIs / and other services asynchronously.

RabbitMQ is a most widely deployed open source message interface broker software, that originally implemented to accept and forward messages by Queuing Protocol. Actually, we're using a single RabbitMQ server, with

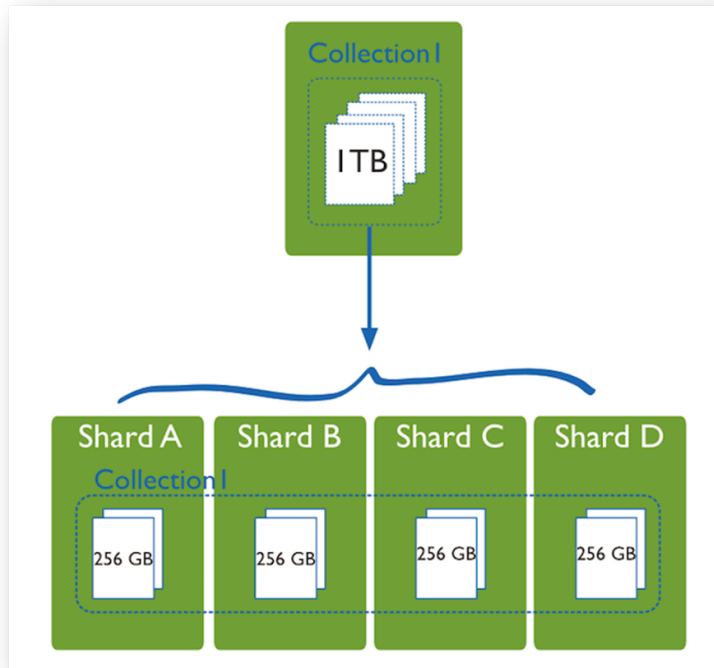


Figure 3.3: Mango Data Base [40]

multiple endpoints that feed the queue with tasks as well as endpoints that process those tasks [41].

The clearest example of SaaS is Amazon Web Services (AWS) , AWS is a global evolution of cloud computing platform provided by Amazon. It provides a combination of infrastructure as a service (IaaS), platform as a service (PaaS) and packaged software as a service (SaaS) offerings.

AWS lets you host and run your applications that contains large amount of data with high performance and spreads scalable virtual servers for every business.the AWS has many services like: Amazon Elastic Compute Cloud EC2.

EC2 is a web service that makes cloud with high security, resizable and compute capacity. It is prepared to make web-scale cloud computing easier for developers, and it provides: Simple web service interface allows you to get configuration capacity with minimal friction, Gives full control of your computing resources and lets you work on Amazon's computing environment, Minimizes the time wanted to obtain new server and authorize you to quickly scale capacity both up and down as your computing requirements change and Costs decreasing by allowing you to pay only for capacity that you actually

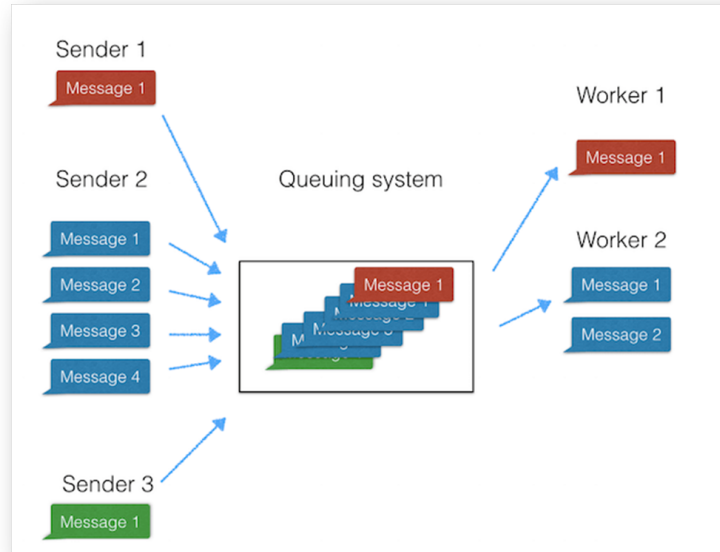


Figure 3.4: Queuing System [41]

use. Amazon EC2 gives the tools for developers to build failure resilient applications and isolates them from common failure scenarios, Another example is S3 (Simple Storage Service).

Amazon S3 is web service storage for the cloud. You can use Amazon S3 to store and retrieve any amount of data at any time, from anywhere on the world. It presented by AWS. Amazon S3 provides object storage through web services interfaces . S3 is also can be used alone or with other 3rd party storage repositories and gateways easily. And it works great together with EC2.Besides storing your data of your web app with S3, it might work great for backups, archives or big data analytics.

Another example is Content Delivery Network (CDN), simply it is a system of distributed service providers (network) that transfers Web content to a user, based on the geographic locations. With high performance and high availability. This service is operative in high speed delivery of content of websites with crowded traffic and websites that have global reach. CDNs also provide protection against large surges in traffic [42] .

3.4 Cloud Security and Privacy

Security in cloud computing refers to a wide set of policies, technologies, and controls provided to keep data, applications, and the associated infrastructure

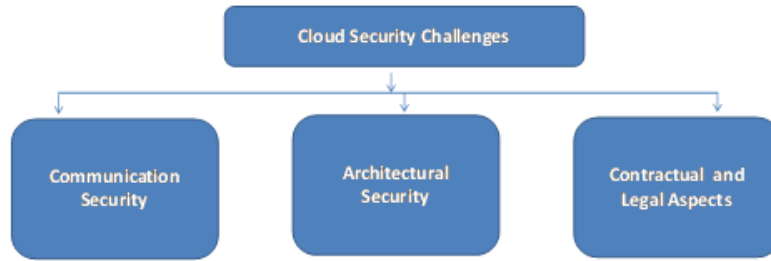


Figure 3.5: Cloud Security Challenges [43]

of cloud computing from available threats.

The threats that make cloud computing endanger are either internal or external, the external threats are similar to all threats that large data center already faced . The responsibilities of protecting the data in cloud are divided between cloud users and cloud vendors. Cloud users are responsible for security in application layer, service providers are responsible for physical security and also imposing external firewall policies. The security of intermediate layer is shared between the user and the vender. In the internal security issues cloud provider must protect data from theft and denial of service attack. There are many security issues in all aspects of cloud architecture such as network level, host level and application level [43].

3.5 Cloud Security Challenges

The security threats in cloud may vary from the risks of traditional IT infrastructure either in nature or adversity or both.

3.5.1 Challenges at Communication Security Level

The cloud services are available to the users through the public Internet, the communication between the customer and the cloud is done by default internet protocols and mechanisms, furthermore, there are communication inside cloud among VMs .there are two types of cloud communication, external communication between customers and cloud, and internal communication occurring within cloud infrastructures [44].

In External Communication There is no difference between external communication in cloud or any other communication over the internet. Therefore the challenges took place in the cloud are same as the challenges of tradi-

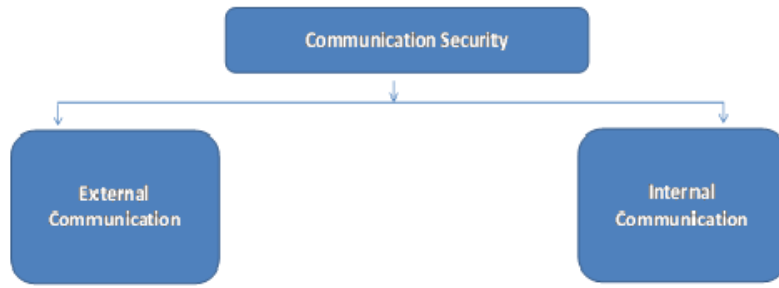


Figure 3.6: Communication Security [43]

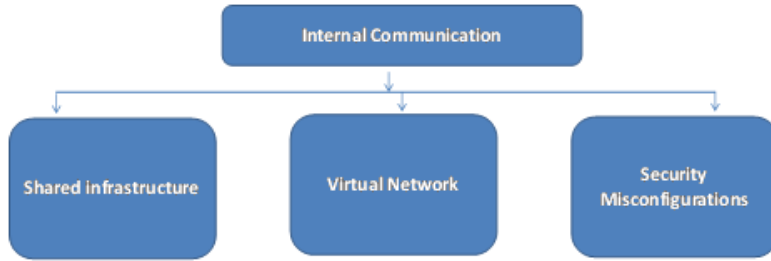


Figure 3.7: Internal Communication [43]

tional communication . These challenges are denial-of-service, man-in-the-middle, eavesdropping, IP-spoofing based flooding, and masquerading The solutions to these challenges are also the same as employed in the traditional one such as, Secure Socket Layer (SSL), Internet Security Protocol (IPSec), cryptographic algorithms, intrusion detection and prevention systems, traffic cleaning, and digital certificates.

in this section we will focus on internal cloud communication that generates cloud specific challenges because of cloud specific characteristics and technologies. There are three types of internal communication challenges include Shared communication infrastructure, Virtual network and Security misconfigurations [45].

In Shared communication infrastructure the Resource pooling is a participation of all computational resources and network infrastructure components. The sharing of network components give a chance to attacker to make cross-tenant attack , The vulnerability comes from the resource pooling property of the cloud computing and affects the IaaS model of the cloud.

It's difficult to Differentiate between a legal vulnerability scan of network and attacker activity, commonly the service providers prevent attacker scans. Similarly, the IP-based isolation of network section is not applied as statically,

it is dynamically provisioned and released; it cannot be related to particular set of users.

The customers on the cloud are usually provided with super-user access to the cloud to manage their VMs . but unfortunately this access capability authorizes the attacker to get system IP or MAC addresses and hack IaaS network interfaces. , The attacker with this super-user access to the real network infrastructure may start attacks, such as, sniffing and spoofing over the real network [46].

In Virtual network we find that in cloud computing systems the communication takes place not only on real networks but also play an important role in virtualized network Virtual network is a logical network built over a physical network, The virtual networks are responsible for communication between VMs. The software-based network components, such as bridges, routers, and software-based network configurations, support the networking of VMs over the same host. The main security challenges in virtualized networks are the Security and protection mechanisms over the physical network, these mechanisms are not able to monitor the traffic over virtualized network and become a critical challenge of attacker activities of the VMs because the attackers escape the monitoring of security tools. Intrusion detection and prevention mechanisms, usually it depends on the traffic patterns and activities to judge the anomalies and detect the possibility of the attack. The virtualized network is shared between multiple VMs that causes the potential certain attacks, such as, Denial of Service (DoS), spoofing and sniffing of virtual network. The traffic rates can be monitored for malicious goal. The cryptographic keys become vulnerable to disclose, in case of malicious sniffing and spoofing of virtual network The data users can suffer from costly breaches due to risks presented before [46].

In Security misconfigurations the service providers make Security configurations to provide secure cloud services to the user of the cloud network infrastructure , it is important to know that Misconfiguration can breach the security of the system. Misconfigurations considered as a threats to the security of customers, applications, and the whole system . The configurations need to Turn off instant translation feature. One of the widespread misconfiguration occur when manager select such configuration tool that they are known but not necessarily covers all the security requirements . The migration of VMs, data, and applications across multiple physical nodes ,cause a

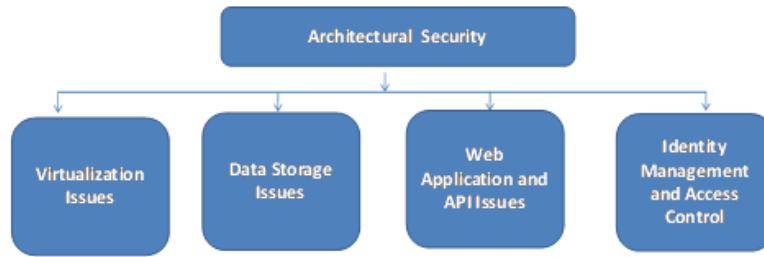


Figure 3.8: Architectural Security [46]

changes in traffic , patterns, and topology this can produce new requirement of various security policies In such scenario, the configuration of the cloud must dynamically be controlled to ensure the security of the cloud. also, any weakness in session configurations and protocol configurations can be exploited for session hijacking and to gain user sensitive data [46].

3.5.2 Challenges at Architectural Level

Security in architectural level includes many aspects such as, virtualization issues, data storage issues, web application and API issues and identity management and access control issues.

3.5.2.1 Virtualization Issues

In Virtualization issues the Virtualization allows the use of the same physical resources by multiple customers. , VMs can be mapped to the same physical resources this allowing the resource pooling in multi-tenant environment., A VM monitor (VMM) or hypervisor is the module that manages the VMs and permits various operating systems to run simultaneously on the same physical system Nevertheless, virtualization also introduces security challenges to the cloud users and infrastructure. These challenges include, VM image sharing, VM isolation, VM escape, VM migration, VM rollback and hypervisor issue [47].

A VM image sharing is used to update VMs, the user can create his own VM image or can use an existed stored image from the shared images, The users are allowed to upload and download images from the store (for example Amazons image repository).

Sharing of VM images in the image store is a common practice and can

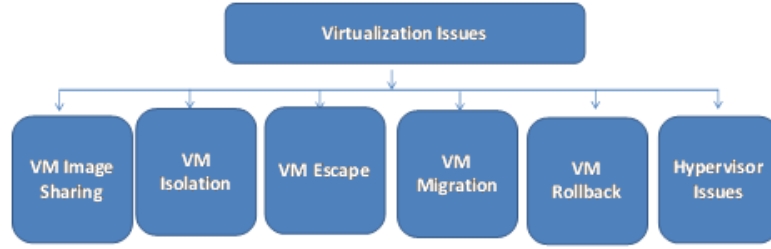


Figure 3.9: Virtualization Issue [47]

involve in a serious threat if it used in malicious manner. The attacker can investigate the code of the image to look for probable attack point.

On the other hand, the attacker can upload a similar VM image that contains a malware, this infected VM image will become a source of introducing malware in the cloud computing system. Moreover, an infected VM can be used to monitor the activities and data of other users resulting in privacy breach [48].

In the aspect of virtualization the VM is running on the same physical hardware, we need to isolate any one from each other. Although logical isolation is present between different VMS, the access to the same physical resources can lead to data breach and cross-VM attacks,. Isolation is not only needed for storage devices but also for memory and computational hardware. The VM escape is a situation where the attacker can access to other VMs or can bring the VMM down . A successful VM escape attack can provide access to the computing and storage hardware. , The IaaS model will be affected more than other service models.

The VM migration is the process of relocating a VM to another physical machine without shutting down the VM . The VM migration is carried out for a number of reasons, such as load balancing, fault tolerance, and Maintenance . During the migration phase, the contents of the VM are exposed to the network which affects data privacy and integrity concerned. during migration , the code of VM becomes vulnerable to attackers. The VM rollback is a feature provided by VM that allows the user to return to some previous point whenever needed. The rollback feature provides flexibility to the user. However, rollback also raises security concerns . For example, the rollback can enable the security credentials that were previously disabled moreover,

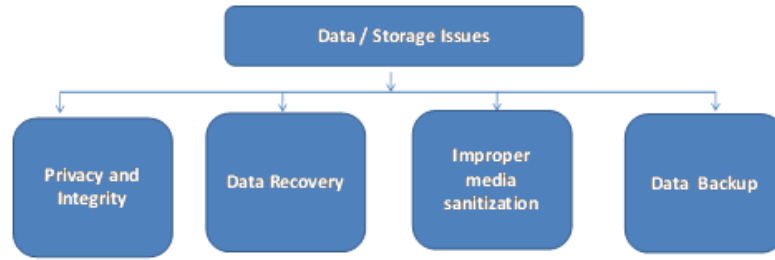


Figure 3.10: Data Storage Issue [52]

the rollback can also render the VM to a vulnerability that was previously patched Furthermore, the rollback can return the VM to the previous security policies and configuration errors [48].

in Hypervisor issues , Hypervisors are virtual machine monitor(VMM) that enables numerous virtual operating systems to simultaneously run on a computer system. These virtual machines are also referred as guest machines and they all share the hardware of the physical machine like memory, processor, storage and other related resources.

The most commonly hypervisor security threat is called “hyperjacking.” During it the hacker can exploit vulnerabilities in the operating system of the virtual machine to access and replace the hypervisor. Once the hypervisor is replaced, attackers can then access other virtual machines on the same physical server [49] .

3.5.2.2 Data/Storage Issues

The cloud computing model does not deliver users with full control over data. Unlike the conventional computing model, the cloud computing permits the service providers to exercise control to manage servers and data. The user enjoys certain level of control only over the VMs The lack of control over the data lead to greater data security risks than the conventional computing model. Moreover, the characteristics of cloud computing like multi-tenancy and virtualization also come up with the possibilities of attacks different than the conventional computing model. in the following we provide an overview of the security challenges faced by the data in cloud computing environment [52].

In Data privacy and integrity Although the cloud computing ensures the cost economy and also relieves the users from infrastructure management activities, it also entails security issues. The data in the cloud is much more

vulnerable to risks in terms of confidentiality, integrity, and availability in comparison to the conventional computing model. The growing number of users and applications leads to increase security risks in a shared environment. Violation of integrity may also result from multi-tenant nature of the cloud. Employee of SaaS providers, having access to information may also act as a potential risk. In Data recovery vulnerability Due to resource pooling and elasticity characteristics, the cloud ensures dynamic and on demand resource provisioning to the users. The resource allocated to a particular user may be assigned to the other user at some later point of time. In case of memory and storage resources, a malicious user can employ data recovery techniques to obtain the data of previous users .

In Improper media sanitization The issue is related to the destruction of physical storage media due to a number of reasons, for example, the disk needs to be changed, the data no longer needs to be there and termination of service , the data can be exposed to risks . Sometimes, the multi-tenancy also contributes to the risk of device sanitization. At the end of the device life cycle, it may not be possible to destroy it as it is in use of some tenants.

The data backup is also an important issue that needs to be dealt carefully. A regular data backup is needed at the Cotenant Security Policy CSP side to ensure the availability and recovery of data in case of intentional and accidental disasters. Moreover, the backup storage also needs to be protected against unauthorized access and tampering [52].

3.5.2.3 Web Application and Application Programming Interface (API) Security

The services and applications to the cloud users are provided through the Internet. In fact, it is one of the essential requirements for a cloud application to be utilized and managed over the Web . The application provided by the CSP is always located at the cloud with users accessing . One of the important characteristics of cloud applications is that they are not allocated to specific users,. Different users may access the same application possibly at the same time. The cloud applications inherit the same vulnerabilities as traditional Web applications and technology. However, the traditional security solutions are not adequate for the cloud computing environment because the vulnerabilities in cloud can prove to be far more devastating than the traditional Web applications. Co-location of multiple users, their data, and

other resources makes it much greater issue. The top ten risks in the web applications have been identified as : Injection (SQL, OS, and LDAP) , Broken Authentication and Session Management, Cross-Site Scripting (XSS) , Insecure Direct Object References , Security Misconfiguration , Sensitive Data Exposure , Missing Function Level Access Control, Cross-Site Request Forgery (CSRF) ,Using Known Vulnerable Components And Invalidated Redirects and Forwards The development, management, and use of Web applications must consider the above risks to protect the web applications and users resources. The user and the services in the cloud are linked by the APIs. The security of APIs highly control the security and availability of the cloud services. The secure APIs ensure the protected and non-malicious use of the cloud services. An API can be thought of a user guide that describes the details about the CSPs cloud architecture and features. The users build or extend the services using the APIs. The CSPs usually publish their APIs to promote the features of their cloud. On other hand, the publishing of APIs helps the users to know the details about the components and functions of the cloud. also, the cloud architecture to some extent is exposed to the attackers. Therefore, insecure APIs can be troublesome for both the cloud and the users. The vulnerabilities of APIs include weak credentials, insufficient authorization and input-data validation. Moreover, the frequent updates of APIs may introduce security holes in the applications [54].

3.5.2.4 Identity Management and Access Control

In a cloud environment, the confidentiality and integrity of data and services is also linked with the identity management and access control. It is exceptionally important to keep track of the user's identity and controlling unauthorized access to the information. The issue of identity management and access control become more complex in cloud environment due to the fact that the owner and resources are in different administrative domains, also organization's authentication and authorization may not be exported to the cloud in the existing form. Moreover, unlike the traditional IT setup, the cloud may deal with users of different organization with different authentication and authorization frameworks, at the same time and with the same physical resources. The use of separate authentication and authorization systems for internal organization and cloud may give rise to complex situations over time. The cloud services are flexible, the IP addresses are frequently

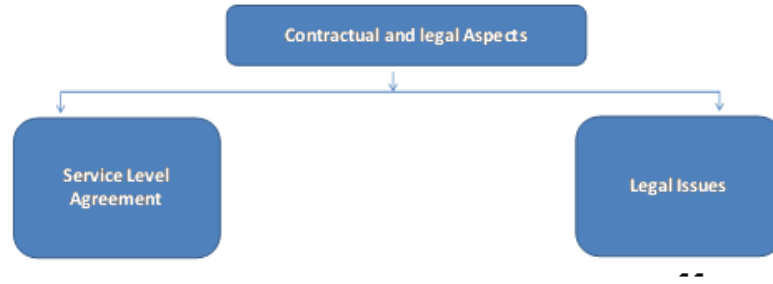


Figure 3.11: Contractual and Legal Aspect [57]

reassigned, the services are started or re-started over shorter period of time, pay-as-you-use feature allows the users to join and leave cloud frequently. For All these characteristics, the conventional identity management and access control systems are not enough for the cloud environment. A cloud needs a dynamic, more accurate , and strict access control mechanisms to control unauthorized operations within the cloud . Moreover, there is need of some control of organizations over identity management system to quickly update the access control policies in case of newly joining and leaving employees . There are many issues that can arise in cloud due to weak identity management and access control, for example, denial of service by account lock-out, weak credential reset mechanisms, insufficient authorization checks, cross domain authentication, insufficient logging and monitoring possibilities, weakness of eXtensible Access Control Markupup Language (XACML) messages, and XML wrapping attacks [56].

3.5.3 Challenges at contractual and legal levels

Adopting the cloud computing, results in moving the organizations data and applications to the administrative control of CSP. This brings many issues to the front for instance, performance assurance, regulatory laws compliance, geographic jurisdictions, monitoring of contract enforcement, etc. The afore-said problems are related to the service level agreement (SLA), legalities, and physical locations of the data [57].

3.5.3.1 Service Level Agreements

The SLA is a document that specifies the terms and conditions between the user and CSP. The SLA also indicates: minimum performance level that CSP

has to provide, counteractive actions and consequences in case of breach of the agreement between user and CSP. The users must be very clear about security requirements for their assets and all the requirement should be thoroughly agreed upon in the SLA. In case of ambiguities, it is harder to claim. For example, if a CSP sub-contracts any service to a third party then in case of a problem it becomes hard to claim at CSP. Accountability of a sub-contractor is often inadequate. Likewise, monitoring of contract enforcement becomes an issue because the users cannot totally rely on statistics provided by the CSP. In such a case of conflict between the CSP and user statistics, evaluation of statistics and determination of responsibility also becomes an issue [57].

3.5.3.2 Legal Issues

legal issues pertaining to the cloud computing also arise due to presence of CSP resources in geographically different and sometimes conflicting legal jurisdictions. If the data of the user is migrated to a location having different laws, it becomes difficult for the user to configure the security policies to comply with the new legal jurisdictions. Sometime, the data may be present in more than one location having different laws about digital security. Moreover, in case of a dispute the issue of jurisdiction arises as to which laws would be applicable. The E-discovery poses another security issue. The E-discovery refers to an issue that arises when the hardware of the CSP gets seized for investigations related to particular customer according to the laws of geographic location. Such a case, results in risk of privacy breach of other users [57].

3.6 Security Solutions

for communication issues To secure the communication and network, the CSA guidelines recommend the use of a combination of virtual LANs, IDS, IPS, and firewalls to protect the data in transit. The guidelines also focus on leakage of customers data due to a virtual network and the use of same underlying infrastructure. The CSA recommends the use of aforementioned tools with strict access management policies. Use of virtual devices and conventional physical devices with close-fitting assimilation with the hypervisor is endorsed by the CSA to ensure visibility and monitoring of traffic over the virtual network. Advanced cloud protection system (ACPS) is proposed in that aim at providing greater security to the cloud resources. The ACPS pro-

vides various security services to the CSP resources including network against attacks on user and CSP data. The cross tenant attacks are also neutralized by constant monitoring of the VMs running at host platform. Additionally, the ACPS also provides audit ability for the actions of VMs. The ACPS is divided into multiple modules located at the host platform. The interceptor module is responsible for detecting any suspicious activities at the host. The detected suspicious activities are recorded by the warning recorder module and are stored in the warning pool. The assessment of recorded activities is performed by the evaluator. An increase in rate of warning generations is treated as a security threat that activates the actuator module for reaction according to the security policies. The ACPS computes the checksums for critical infrastructure including the network at the setup time. The state of the infrastructure is asynchronously determined by re-computing checksum for the scrutinized objects. In case of anomalies the warnings are sent to the evaluator. The periodic checksum verification also keeps the cloud entry points under constant monitoring. To prevent the attacks on network infrastructure, the ACPS utilizes the method presented in where network probing is detected by using IP tables and warnings are recorded in the warning pool. In addition to securing network and other critical infrastructure, the ACPS provides security against malicious VMs and data attacks. One of the important features of the ACPS is that it remains transparent to the VMs and remains undetectable. The interceptor module does not block any system call to prevent itself being detected. However, if the attack activity is confirmed then the action is taken. Allowing the initial system call to be executed neutralizes the timing attacks for detection of any monitoring system [58]. The ACPS prototype was implemented on Eucalyptus and OpenECP that are open source cloud systems.

A security tool for the cloud computing, called CyberGuarder proposed in provides virtual network security through the deployment of virtual network devices. Moreover, virtual network isolation is introduced by utilizing layer-two tunnel Virtual Private Network (VPN) between virtual bridges.

The data is transmitted between VMs in peer-to-peer (P2P) manner without transiting through the central server. However, the metadata is stored on the central node for optimized traffic between the VMs. The software ports are designed to monitor the network traffic. Conventional network security systems like Intrusion Detection System (IDS) are adaptively deployed

into the virtual network for security of applications running on the virtual network. Additionally, the CyberGuarder also provide VM security through the integrity verification of applications and by monitoring of system calls invoked by the applications.

The experimental results showed a 10% overhead in performance due to Cyberguarder and 5% increase in the energy consumption. Wu et al. proposed a virtual network model that safeguards the virtual networks against sniffing and spoofing attacks. The Xen hypervisor is used to demonstrate the proposed model. [58]

The proposed model utilizes both the bridge and route modes of Xen hypervisor for virtual network configuration. In bridge mode the Xen attaches the VM directly to the virtual Ethernet bridge. The bridge in turn connects to the physical network. The route mode creates a P2P link between the VM and the domain (the VM management domain). The proposed model is divided into three layers, namely: routing, firewall, and shared network layer. The routing layer establishes a dedicated logical channel between virtual and physical network. Each channel is assigned a unique logical ID that is used to monitor the source of packets originating from the shared network. The firewall layer is responsible for protecting against the spoofing attacks from the shared network. This layer guarantees that any virtual interface connected to a shared virtual network does not communicate with any other virtual shared network. The monitoring is performed based on the logical IDs assigned by the routing layer. Secondly, firewall layer does not allow the packets to update the routing table. All such packets are discarded. The shared network layer prohibits the communication between VMs belonging to different virtual network channels. He et al. presented a cloud network security solution in by implementing a novel tree-rule firewall. The authors demonstrated that the conventionally used listed-rule firewalls are prone to security issues of shadowed rule, swapping positions, and redundant rules. Moreover, the listed-rule firewalls decrease performance due to sequential rule searching and arrangement of bigger rules after the smaller rules. To remove the aforementioned problems, there are many proposed tree-rule firewall that arranges rules in the form of a tree instead of list [58].

the packet header at the root nodes of the tree indicate to next level of tree. The next level will check for the next attribute and the process continues till the firewall reaches the specified security policy for the given at-

tributes. ,for example the source IP can be at root with the destination IP at leaf nodes. Authors in presented a technique named DCPortalsNg for isolation of virtual networks for various VMs. The presented technique follows Software-Defined Network (SDN) methodology for isolating virtual network. The DCPortalsNg interacts with the open stack through a neutron plugin and obtains all of the required virtual network information. The DCPortal-sNg then builds its own data of mapping networks to tenant and tenants to network. Subsequently, a unique identifier is assigned to each of the VMs. For network isolation, the concept of packet rewriting is used that opens the original packet and extracts source and destination addresses from the packet. The packets destined for the same network are further processed while other are discarded. In case of a valid transmission, the Open Flow message is sent to the appropriate virtual switch to rewrite the packet with destination/-source IP addresses replaced with identifiers. Moreover, the MAC addresses are replaced by the MAC addresses of the physical host. This avoids the cross tenant attack on the virtual network. The traffic is controlled by MAC addresses only in the presented technique. The presented technique also prevents the cross VM denial of service (DoS) attack.

Xing et al. proposed a system called SnortFlow for intrusion prevention within cloud environment. The SnortFlow utilizes the features of Snort and OpenFlow systems. The prototype of SnortFlow is built and tested over Xen-based cloud. The suspicious traffic is collected by the component called snortFlow demon. The alert is pushed into alert interpreter that analyzes the generated alert and invokes the rules generator. The rules generator develops the rules for the suspect traffic and forwards them to the openflow device. The openflow device reconfigures the network according to the developed rules. The evaluation of SnortFlow exhibited good performance in terms of traffic analysis and prevention against intrusion [58].

3.7 Computing in Health Care

Computer technologies utilization in hospital has become important to support an electronic health record (EHR). For doctors, nurses and other health-care team members, to provide quick access to important data about the patients.

Using of computing Systems in Health Care has many benefits such as,

Development of health Care Quality because the Automated hospitals lead to more accurate results in treatment and improve quality of care because all works flow in systematic way, the automated hospitals also support not only the daily implementation of an HIS but also includes ADT, Order Entry/Charge Capture, Pharmacy, Radiology, Nursing documentation and ICU Monitoring. Another benefit of this systems is reducing of costs, for example if a doctor requests a tests, the computer will automatically display the result and save information without need to any paper the thing which reduces the costs [58].

By using computers in healthcare systems, the criteria of unified medical references can take place in hospitals and offices throughout the world. By this specific system, healthcare services, hospital cost and the efficiency of treatment can all be evaluated on the same basis. computer also allows patients to understand the reality of their health. Radiographs, x-rays, and several other test results could help patient to know their own issues that related to their health. These systems create more advanced way of register, analyzing and understanding the patient's situation, Without need to advanced technologies. we can say that The availability of the Internet has brought significant changes to health services. With Internet access and using of wireless technologies, the services became easier , the patient can reserve a hospital and looking for his profile in the hospital portal using the internet. In addition to this patients will be more pro-active toward their lifestyle choices by tracking their daily activities with specific application to improve healthy decisions, computers also help patients navigate their lives in a beneficial manner.

The healthcare industry has been improving widely and quickly. Today new technologies, tools and equipment have been discovered to collect information about patients as much as possible, with “big data”.

Gathering information in healthcare can also support efficient communication between doctors and patients, and increases the overall quality of patient care In order to comprehend the important role of healthcare data collection, we need to have a closer look at problems that patients are facing, like wrong Diagnosis. At the same time, we should evaluate data collection tools and methods [58].

3.7.1 Healthcare Data Standards

In the situation of health care, the expression data standards mean main information component substantial for information flow like method, protocols, terminologies, and specifications for the collection, exchange, storage, and retrieval of information associated with health care applications, including medical records, medications, radiological images and payment. In the issue of health care many terms may be arise for instance the term Healthcare data management, it is the procedure of storing, protecting, and analyzing data coming from different sources. Managing the resources of available healthcare data allows health systems to create holistic views of patients, personalize treatments, improve communication, and enhance health outcomes. Healthcare Data Management has many benefits such as Initiate 360-degree vision of patients and deploy personalized interactions by integrating patient data from all available resources, Modulate patient connection with predictive design and analysis based on healthcare data, Improve people health outcomes through the follow up and prognosis. and Realize physician decisions and link them to the ministry of health [59].

Organizations can manage their healthcare data by using technology like: Electronic health records (EHR) which allow doctors to register and save patient data electronically, simplify the medical recording process for authorized users. With this tool, healthcare organizations are able to merge, centralize, and securely access patient medical data, the second technology that manages data is Healthcare Customer relationship management system (HCRM) which has the capability to integrate, analyze, and report data from different sources to one data centre. With CRM technology in healthcare organizations can create a 360-degree view of patients that includes not only the patient lifecycle, but also includes patient profiles, priority, and attitude. By using several data management software, including EHRs and HCRM, health systems can create general view of patients on a single console, other way that manage data is Revenue cycle management (RCM), it is a financial method, using medical billing software that healthcare facilities use to track patient care steps from registration and appointment scheduling to the final payment of a bill.

Healthcare Data Management can face many chalinges like: The amount of healthcare data can be very large and overwhelming, so we must Plan

for how to manage all this data which is a daunting task, other challenge is that Administrators and doctors need to be assiduous about collecting patient information also Making data management as a priority requires involvement from all members of healthcare industry, which can present a challenge [59].

3.7.2 Health Analytics Role in Predictive Modeling

By using health analytic system doctors can make predictions about which groups of patients are the most likely candidates for certain diseases, It also can predict how to behave with patients based on stored data and initiate predictive document based on analytical data that saved in healthcare records.

we find that using technology is easy and help reach to successful healthcare data management, for example Healthcares CRM which can gather information, save them , estimate and generate reports of patient data, this work relieves the effort of managing it manually. Additionally the accessible data that existed on specific portal makes the matter easier for patients to interact with healthcare organizations [59].

Sometimes the patient needs to be seen by another doctor for more accurate diagnosis, to do this, the patient needs a clinician's report.

There are two types of medical reports, the first one is Electronic Medical Record (EMR): which refers to everything about one patient printed in a paper, such as medical history, diagnoses, drugs, last visit date. Although EMRs is good, it is limited because the patient's medical record released for only one organization. The second one is Electronic Health Records (EHR) which is more than just a record of data collected from one visit, it includes detailed information about patient history [59].

EHRs is prepared to gather patient data from all providers who concerned with the patient's care. EHR data can be initiated, controlled, and reviewed by authorized person and staff from over more than one health care organization.

EHRs also makes the patient's health record more accessible to other health care organization, specialists even if they are across states.

The Differences between EMR and HER is that (EMRs) is a soft copy of the paper table in the clinician's office, An it consists of the medical status and treatment history of the patients in one visit, The data in EMRs doesn't go easily out of the organization because the patient's record must be printed out and sent by mail to the specialists wherever they are so In that regard, EMRs

is not better than a paper record, but EMR allows clinicians to Follow up data over time, Easily distinguish which patients are due to have preventive test or checkups, Check how their patients are doing on particular parameters—such as blood pressure or vaccinations, observe and improve overall quality of health care.

On other hand, Electronic health records (EHR) concentrates on the overall health data of the patient that gathered from many hospitals and consist of a clear view on a patient's status. it is prepared to share information with other specialists in other hospitals so it includes information from all the clinicians involved in the patient's situation from different locations [54].

HER has many benefits like: it Gives The information that collected by the doctors who follow the patient and delivers them to the emergency section, so that the procedures can be set appropriately, even if the patient was unconscious, Another benefit is that the patient can log in to his own record in the portal and see the lab results over the last year which can help him to improve health medications and keep up with the lifestyle, also The lab results of the time being are updated to inform the specialist about the status of the patient without doing duplicate tests. Additionally The clinician's report from the patient's hospital helps knowing the doctor instructions and follow-up visits and guides the patient to go from any one care center to another one more comfortably [59].

Chapter Four

Proposed SaaS Implementation

4.1 Proposed SaaS Architecture

Cloud Provider introduce virtual Infrastructure such as Storage, CPU and RAM to the customer to install the applications and using it remotely, in Africa city cloud the virtual server with Linux operating system . Cloud provider also introduce security protection to given virtual servers such as firewall , IDS and IPS. the Customer can access it using IP address and work in it using private username and password. SaaS customer login to the virtual server using special program and work with server using Linux command. The client access the SaaS application using identified URL that known to every one .

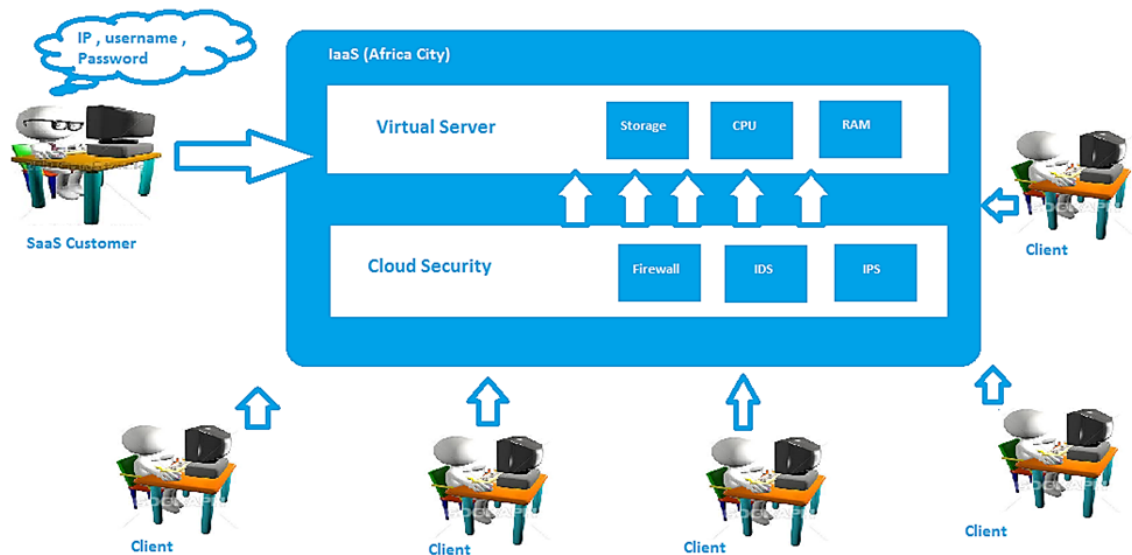


Figure 4.1: Proposed SaaS Architecture

4.2 Proposed Security Mechanism

Cloud provider introduces security mechanism to protect cloud customer against common threats shown in Figure 4.2:

1. Advance perimeter firewall to Check file packet integrity.
2. IDS with event logging Log any malicious activity.
3. Internal Firewall for each application and database To prevent internal attack.
4. Data reset encryption To save and secure data from unauthorized access.

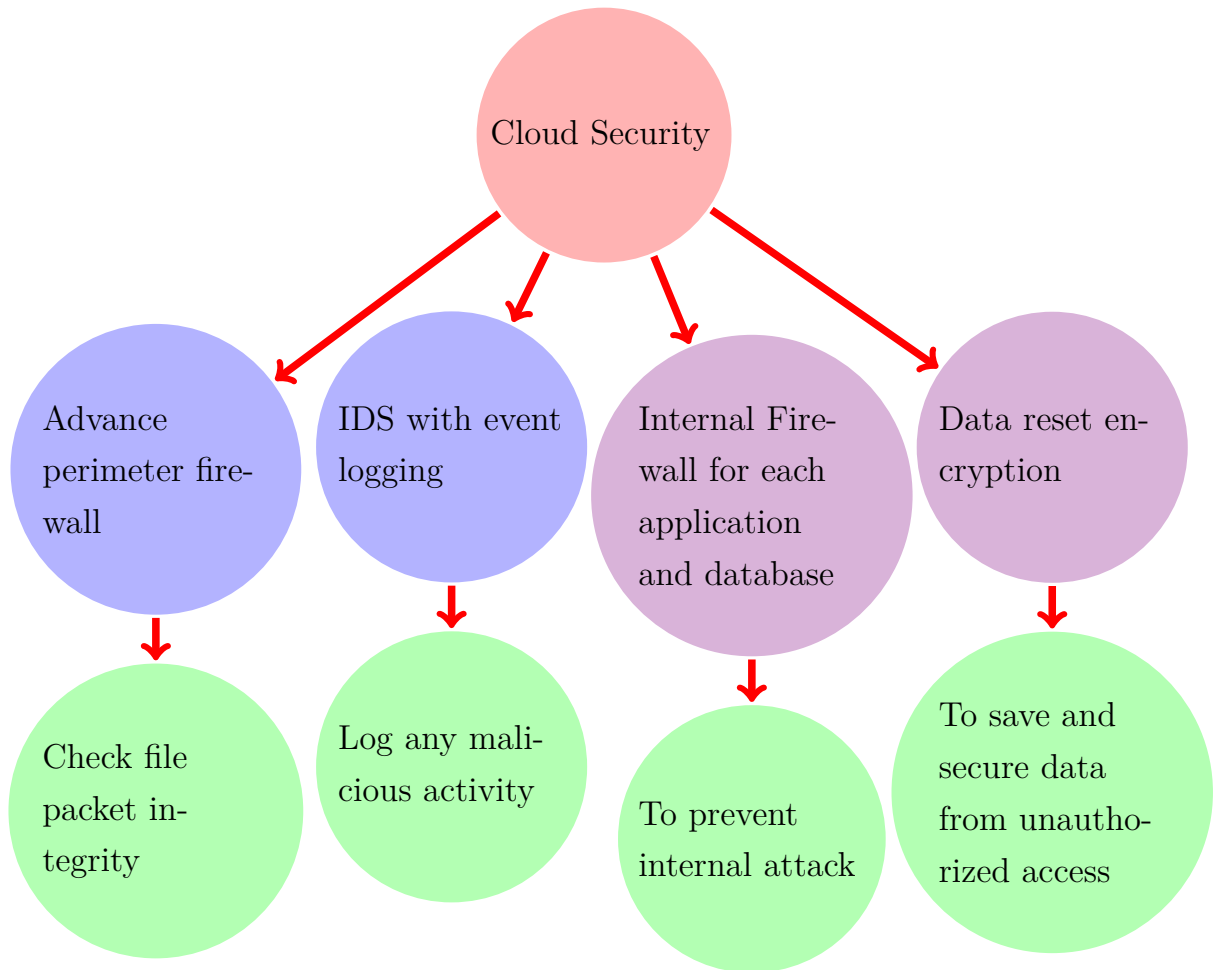


Figure 4.2: Security Provided by Cloud

4.3 Proposed Webfront Workflow

```
1  Begin
2      Patient register from home page;
3      Receptionist enter patient to the doctor;
4      Doctor do
```



```
5      {
6          view patient pass history;
7          Add new risk factor;
8          Add new symptoms;
9          If test required:
10             Add test;
11         View result;
12     }
13     Add new diagnosis;
14     Add new drugs;
15     Delete patient from list;
16 End
```

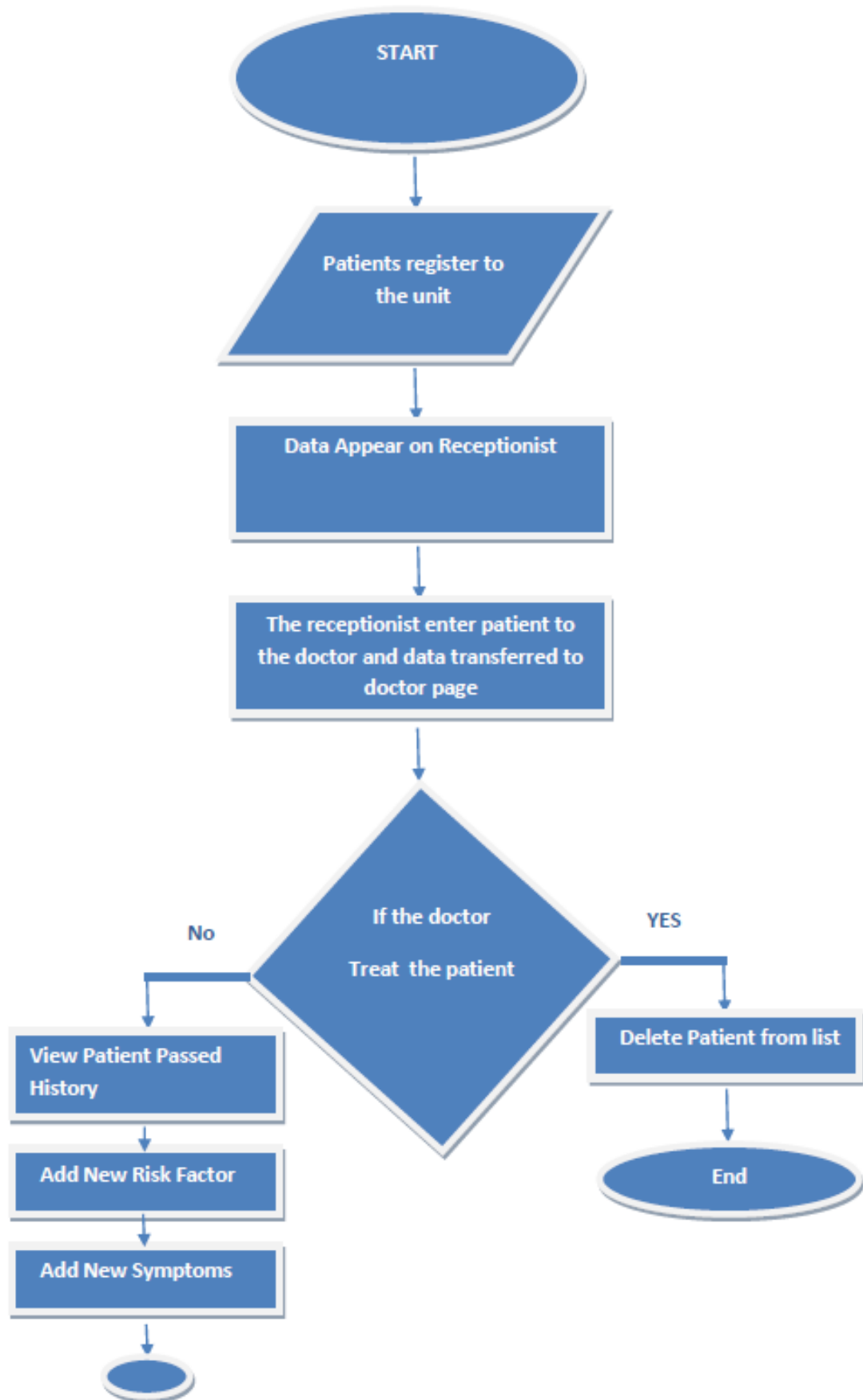


Figure 4.3: Webfront Workflow (Part a)

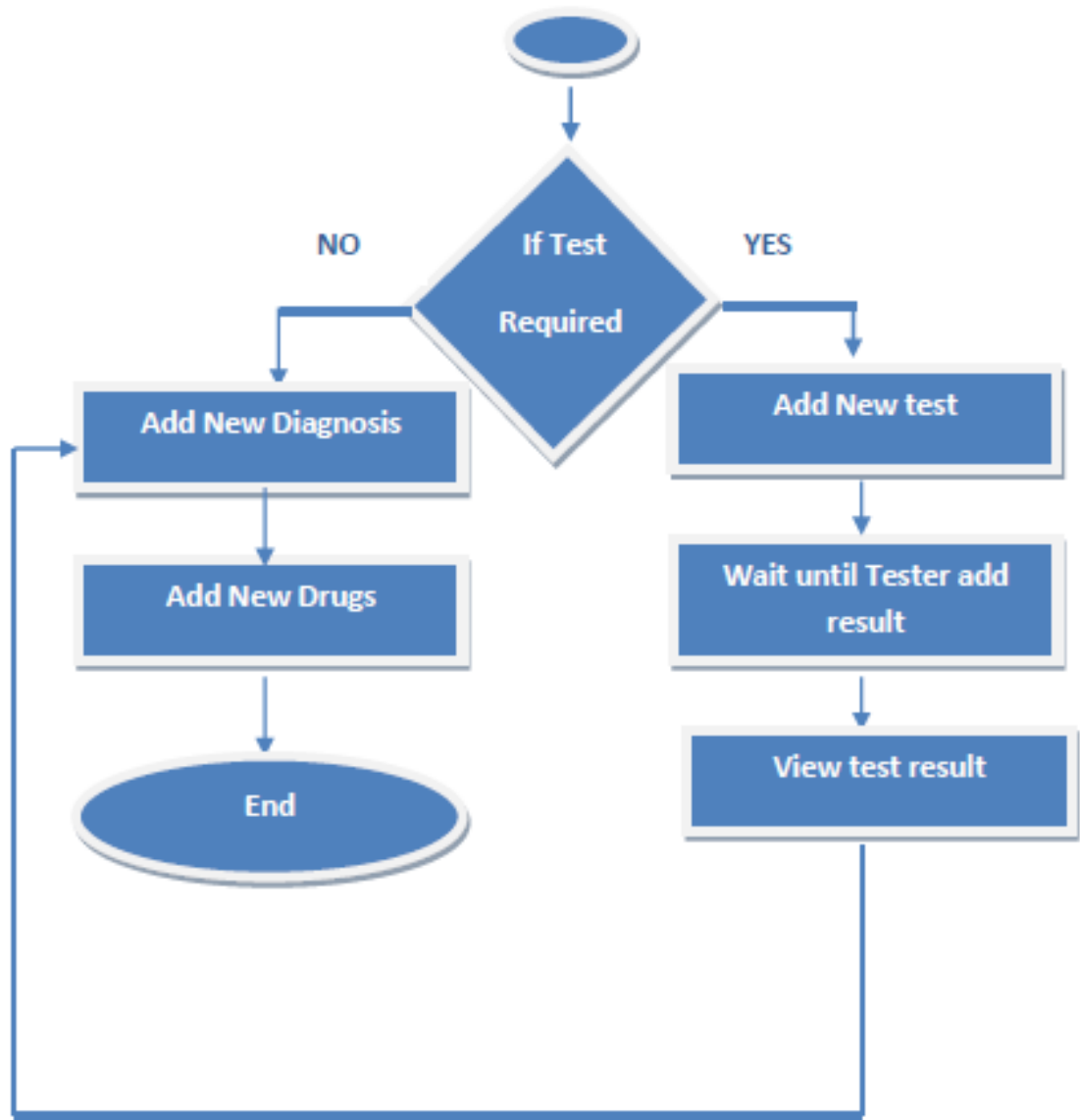


Figure 4.4: Webfront Workflow (Part b)

4.4 DataBase Process Flow

```

1 Begin
2   Entered data inserted in patient table;
3   If receptionist enter patient to doctor:
4   {
5     Data deleted from patient table;
6     Data inserted in doctor table;
7   }
8   If doctor treat patient:

```

```
9      {
10          Data deleted from doctor table;
11          Data inserted in pinfo table;
12      }
13      Else
14      {
15          Insert risk factor in risktrac table;
16          Insert symptoms in symtrac table;
17          Insert test in testtrac table;
18          Insert test result in testresulttrac table;
19          Insert diagnosis in diagtrac table;
20          Insert drug in drugtrac table;
21      }
22      End
```

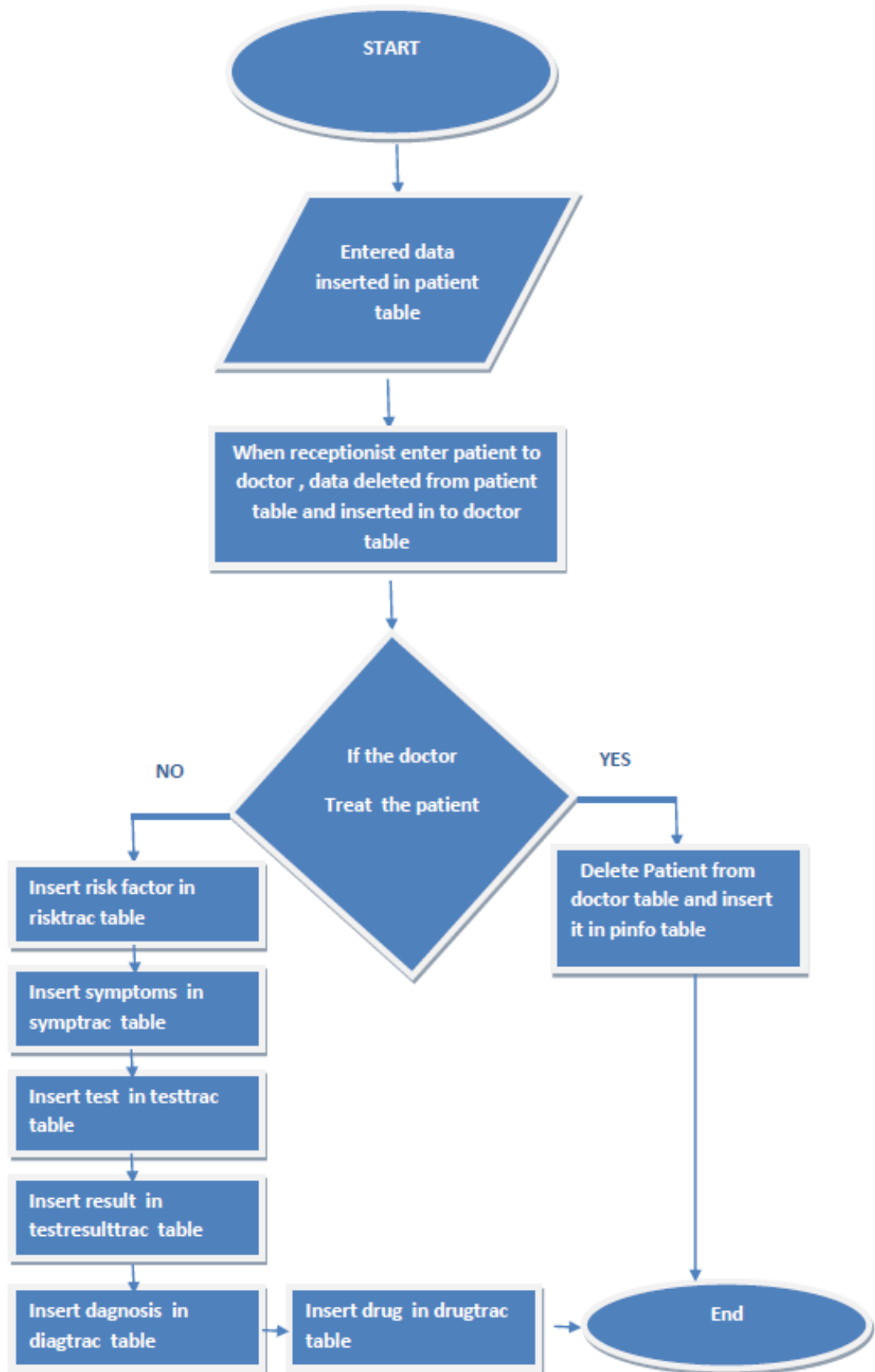


Figure 4.5: Data Base Flow Chart

Chapter Five

Cloud Model Implementation and Web Front Design

5.1 Implementation of Cloud Hosting

To explain the choice of hosting method, let us consider the following concepts. There are two types of Traditional hosting, dedicated hosting and shared hosting. The former, a customer rent a full resources from service provider for one or more servers, The client has special bandwidth, CPU, RAM, and drive space, the client also has full control over the servers resources.in the latter, the client rents only space (storage) on one server, and that server's resources are shared by a number of other websites and the hosting provider is responsible for control it. The drawbacks of shared hosting, is that the using single server decreased the performance and If the server itself has technical problems, everyone hosted on that server will be affected. Shared hosting is a good solution If you expect the flow of traffic But if the traffic increases rapidly you may face problems in the amount of storage you currently have.

In this research the system that implemented to ministry of health is hosted on Africa city of technology cloud as software as a service. The virtual server with Ubuntu 14.04 LTS operating system, to configure it we use the settings shown in figure 5.1. The login page is shown in Figure 5.2. After login system information appeared as shown in the code snippet of Listings 5.1.1.

Listing 5.1.1: System Information After Logging

```
1 Server operating system:  Ubuntu 14.04.1 LTS (GNU/Linux ...  
   3.13.0-32-generic x86-64)  
2 System information as of Wed Oct  3 00:47:43 EAT 2018  
3 Processes:  153  
4 Usage of /: 2.3\% of 55.00GB  
5 IP address for eth0: 197.251.5.238
```

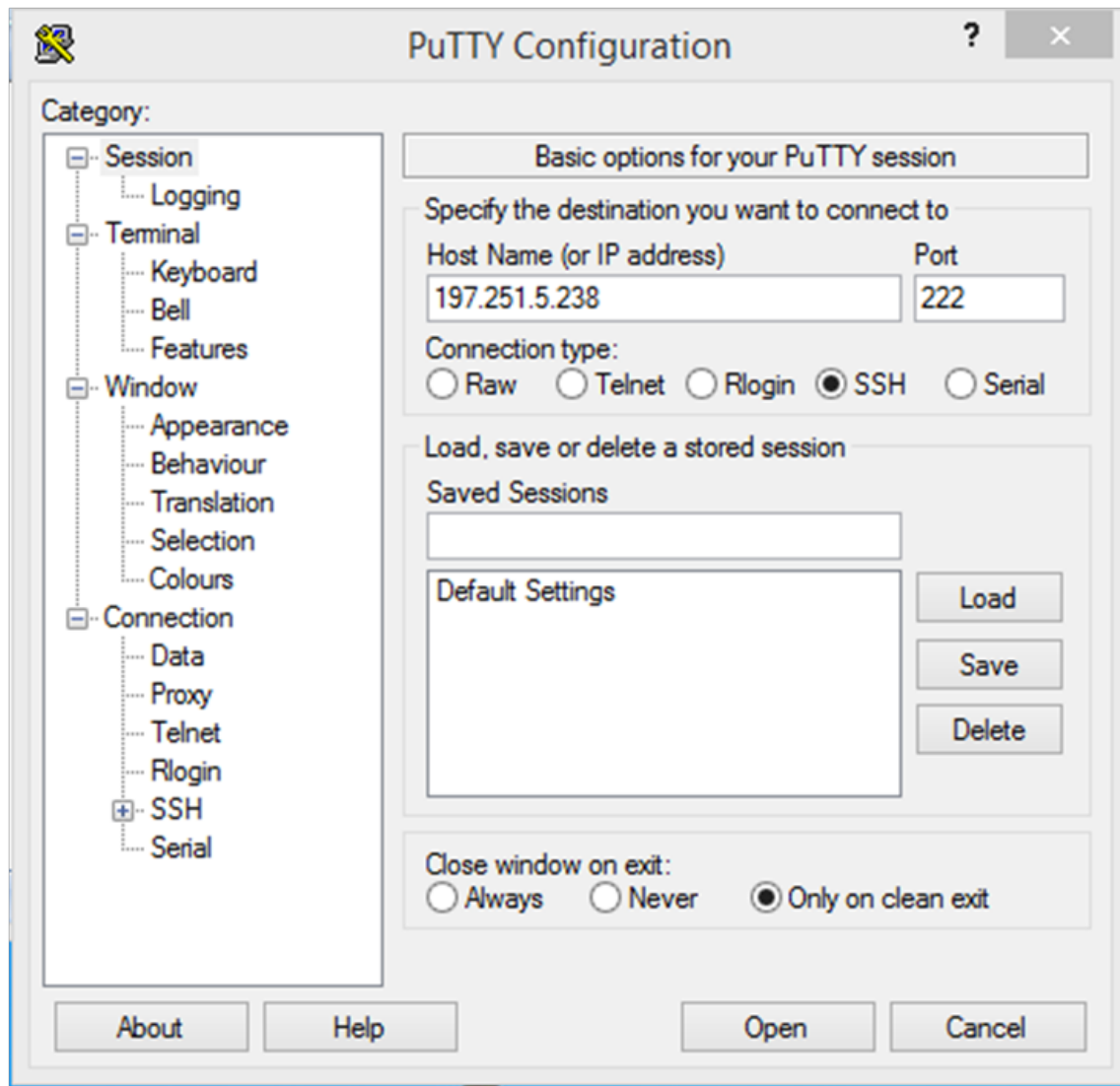


Figure 5.1: Putty Page

After this step we can access the server using user name and password

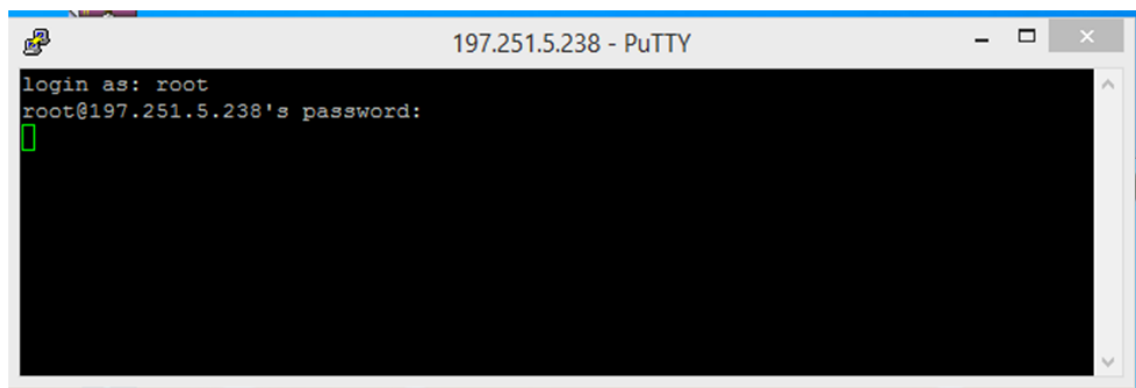


Figure 5.2: Login page



A terminal window titled 'ubuntu@ubuntu: ~' with standard window controls. The terminal output shows a login sequence for user 'ubuntu' at IP '197.251.5.238', followed by system information including date, time, system load, memory usage, and network details. The prompt 'ubuntu@ubuntu:~\$' is visible at the bottom.

```
login as: ubuntu
ubuntu@197.251.5.238's password:
Welcome to Ubuntu 14.04.1 LTS (GNU/Linux 3.13.0-32-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

System information as of Tue Oct  2 19:28:18 EAT 2018

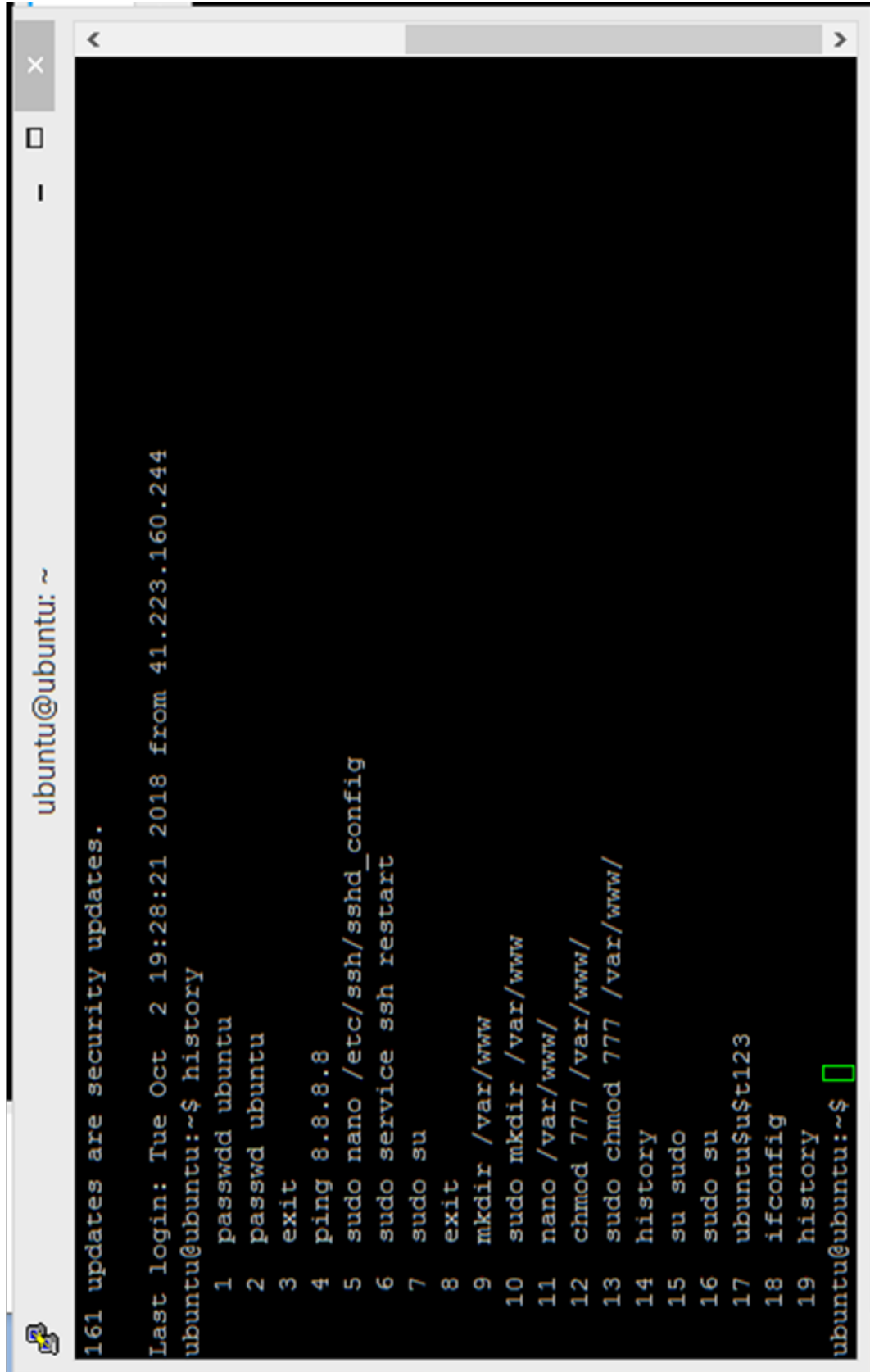
System load:  0.0           Processes:      153
Usage of /:   2.3% of 55.00GB Users logged in:   0
Memory usage: 3%           IP address for eth0: 197.251.5.238
Swap usage:  0%

Graph this data and manage this system at:
https://landscape.canonical.com/

225 packages can be updated.
161 updates are security updates.

Last login: Tue Oct  2 19:28:21 2018 from 41.223.160.244
ubuntu@ubuntu:~$
```

Figure 5.3: Server Information

A terminal window titled 'ubuntu@ubuntu: ~' with standard window controls. The terminal output shows a list of 19 commands from the history, numbered 1 to 19. The commands include system updates, login information, password setting, ping, nano editor usage, service restart, directory creation, file modification, and the 'history' command itself. The prompt 'ubuntu@ubuntu:~\$' is visible at the bottom.

```
161 updates are security updates.  
Last login: Tue Oct 2 19:28:21 2018 from 41.223.160.244  
ubuntu@ubuntu:~$ history  
1  passwd ubuntu  
2  passwd ubuntu  
3  exit  
4  ping 8.8.8.8  
5  sudo nano /etc/ssh/sshd_config  
6  sudo service ssh restart  
7  sudo su  
8  exit  
9  mkdir /var/www  
10 sudo mkdir /var/www  
11 nano /var/www/  
12 chmod 777 /var/www/  
13 sudo chmod 777 /var/www/  
14 history  
15 su sudo  
16 sudo su  
17 ubuntu$ut123  
18 ifconfig  
19 history  
ubuntu@ubuntu:~$
```

Figure 5.4: History Commands (Showing previous commands that executed before by using history command)

First, we need to install Apache, php and mySQL in order to work through these steps to install these programs on the server through "apt-get". To get update we must login with "sudo" to get administrator access, then use the command "sudo apt-get update". This is illustrated in figure 5.5.

```

ubuntu@ubuntu: ~
Memory usage: 3%      IP address for eth0: 197.251.5.238
Swap usage:  0%

Graph this data and manage this system at:
https://landscape.canonical.com/

225 packages can be updated.
161 updates are security updates.

New release '16.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Wed Oct  3 01:21:42 2018 from 154.103.153.232
ubuntu@ubuntu:~$ sudo apt-get update
[sudo] password for ubuntu:
Get:1 http://security.ubuntu.com trusty-security InRelease [65.9 kB]
Get:2 http://security.ubuntu.com trusty-security/main Sources [162 kB]
Get:3 http://security.ubuntu.com trusty-security/restricted Sources [4,931 B]
Get:4 http://security.ubuntu.com trusty-security/universe Sources [83.8 kB]
Get:5 http://security.ubuntu.com trusty-security/multiverse Sources [3,261 B]
Get:6 http://security.ubuntu.com trusty-security/main amd64 Packages [771 kB]
Get:7 http://security.ubuntu.com trusty-security/restricted amd64 Packages [14.2 kB]
Get:8 http://security.ubuntu.com trusty-security/universe amd64 Packages [261 kB]

```

Figure 5.5: Get Update

5.1.1 Adding PHP7 Functionality

To Install PHP7, first, install the "python-software-properties" package on the system which provides "add-apt-repository" command then use the following set of commands to add PPA for PHP7 in your Ubuntu system and install it. The steps are summarized in Listing 5.1.2.

Listing 5.1.2: Command Sequence for adding PPA and PHP7

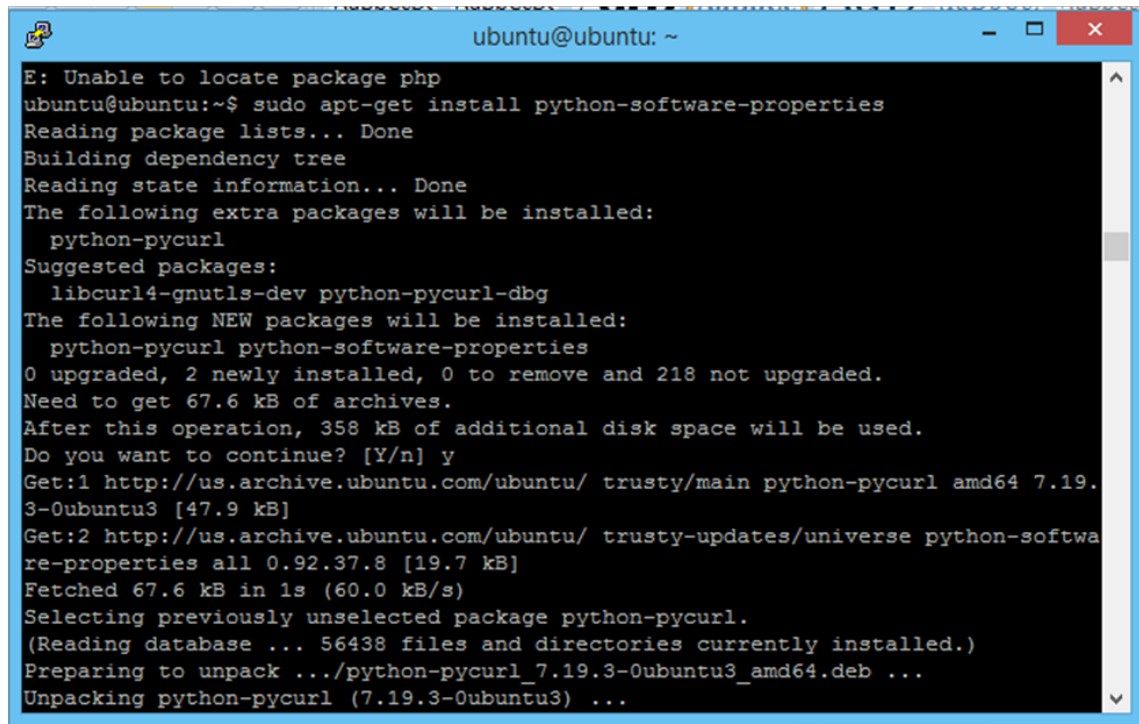
```

1 sudo apt-get install python-software-properties
2 sudo add-apt-repository ppa:ondrej/php
3 sudo apt-get update
4 sudo apt-get install -y php7.0

```

The outcomes after execution are shown in Figure 5.6, which shows how Python was added, the Figure 5.7 shows the outcomes for executing the com-

mands to add PPA and PHP7.

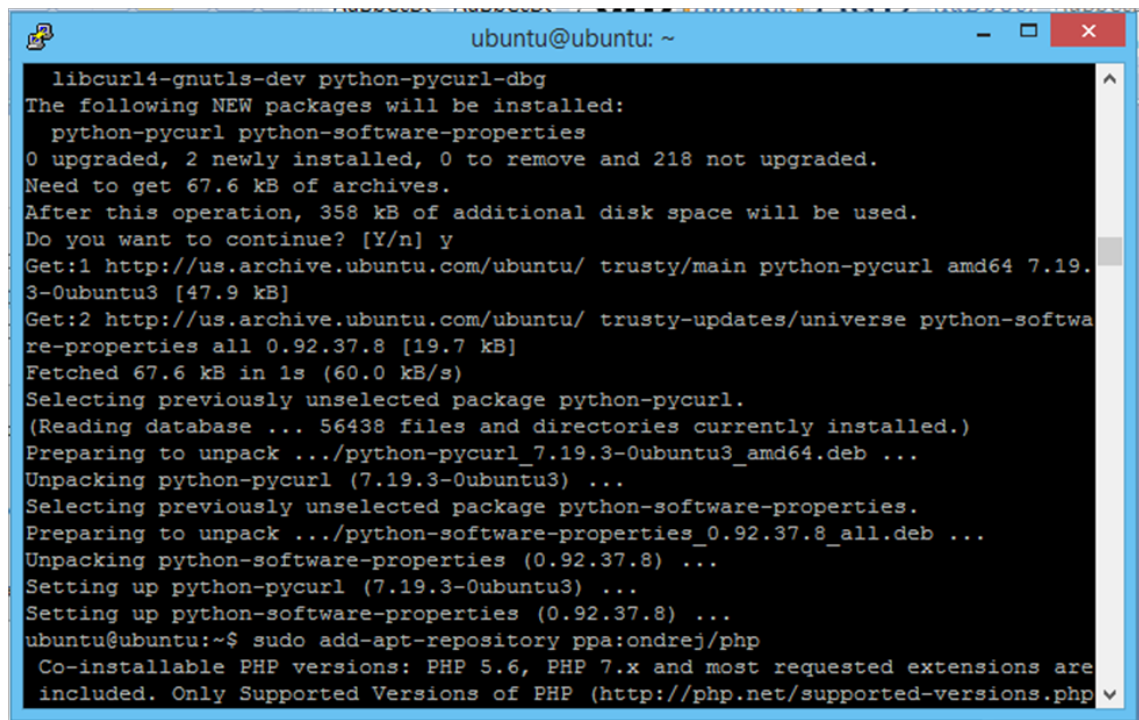


```

ubuntu@ubuntu: ~
E: Unable to locate package php
ubuntu@ubuntu:~$ sudo apt-get install python-software-properties
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  python-pycurl
Suggested packages:
  libcurl4-gnutls-dev python-pycurl-dbg
The following NEW packages will be installed:
  python-pycurl python-software-properties
0 upgraded, 2 newly installed, 0 to remove and 218 not upgraded.
Need to get 67.6 kB of archives.
After this operation, 358 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu/ trusty/main python-pycurl amd64 7.19.3-0ubuntu3 [47.9 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu/ trusty-updates/universe python-software-properties all 0.92.37.8 [19.7 kB]
Fetched 67.6 kB in 1s (60.0 kB/s)
Selecting previously unselected package python-pycurl.
(Reading database ... 56438 files and directories currently installed.)
Preparing to unpack .../python-pycurl_7.19.3-0ubuntu3_amd64.deb ...
Unpacking python-pycurl (7.19.3-0ubuntu3) ...

```

Figure 5.6: Python Installation

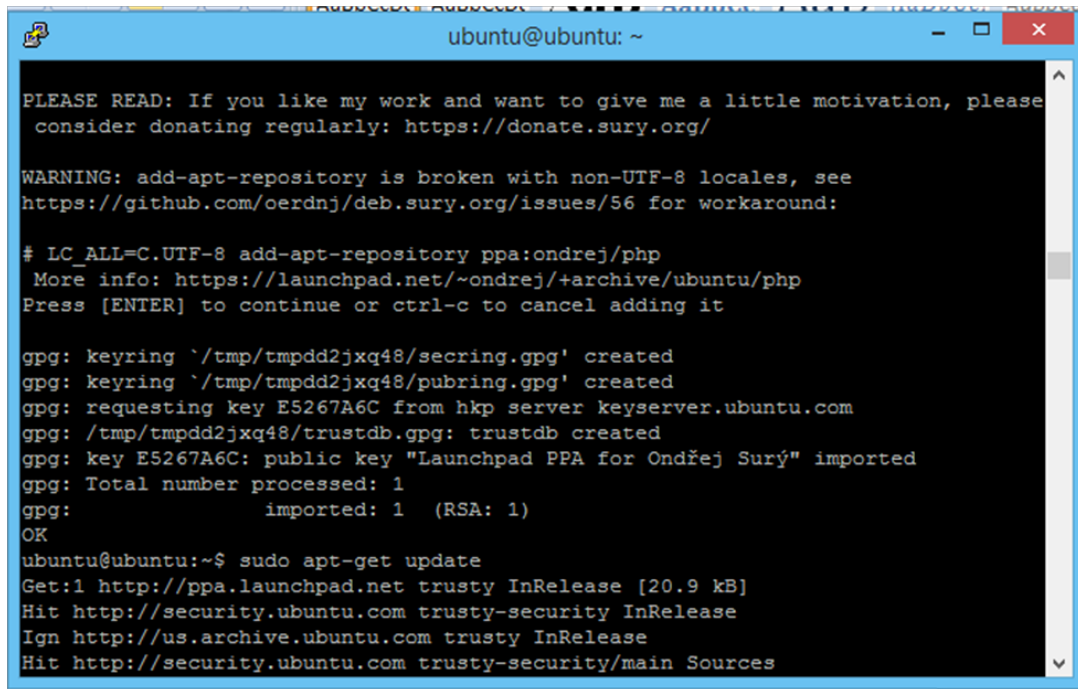


```

libcurl4-gnutls-dev python-pycurl-dbg
The following NEW packages will be installed:
  python-pycurl python-software-properties
0 upgraded, 2 newly installed, 0 to remove and 218 not upgraded.
Need to get 67.6 kB of archives.
After this operation, 358 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu/ trusty/main python-pycurl amd64 7.19.3-0ubuntu3 [47.9 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu/ trusty-updates/universe python-software-properties all 0.92.37.8 [19.7 kB]
Fetched 67.6 kB in 1s (60.0 kB/s)
Selecting previously unselected package python-pycurl.
(Reading database ... 56438 files and directories currently installed.)
Preparing to unpack .../python-pycurl_7.19.3-0ubuntu3_amd64.deb ...
Unpacking python-pycurl (7.19.3-0ubuntu3) ...
Selecting previously unselected package python-software-properties.
Preparing to unpack .../python-software-properties_0.92.37.8_all.deb ...
Unpacking python-software-properties (0.92.37.8) ...
Setting up python-pycurl (7.19.3-0ubuntu3) ...
Setting up python-software-properties (0.92.37.8) ...
ubuntu@ubuntu:~$ sudo add-apt-repository ppa:ondrej/php
Co-installable PHP versions: PHP 5.6, PHP 7.x and most requested extensions are included. Only Supported Versions of PHP (http://php.net/supported-versions.php)

```

Figure 5.7: Adding Repository "ppa:ondrej/php"



```

ubuntu@ubuntu: ~
PLEASE READ: If you like my work and want to give me a little motivation, please
consider donating regularly: https://donate.sury.org/

WARNING: add-apt-repository is broken with non-UTF-8 locales, see
https://github.com/oerdnj/deb.sury.org/issues/56 for workaround:

# LC_ALL=C.UTF-8 add-apt-repository ppa:ondrej/php
More info: https://launchpad.net/~ondrej/+archive/ubuntu/php
Press [ENTER] to continue or ctrl-c to cancel adding it

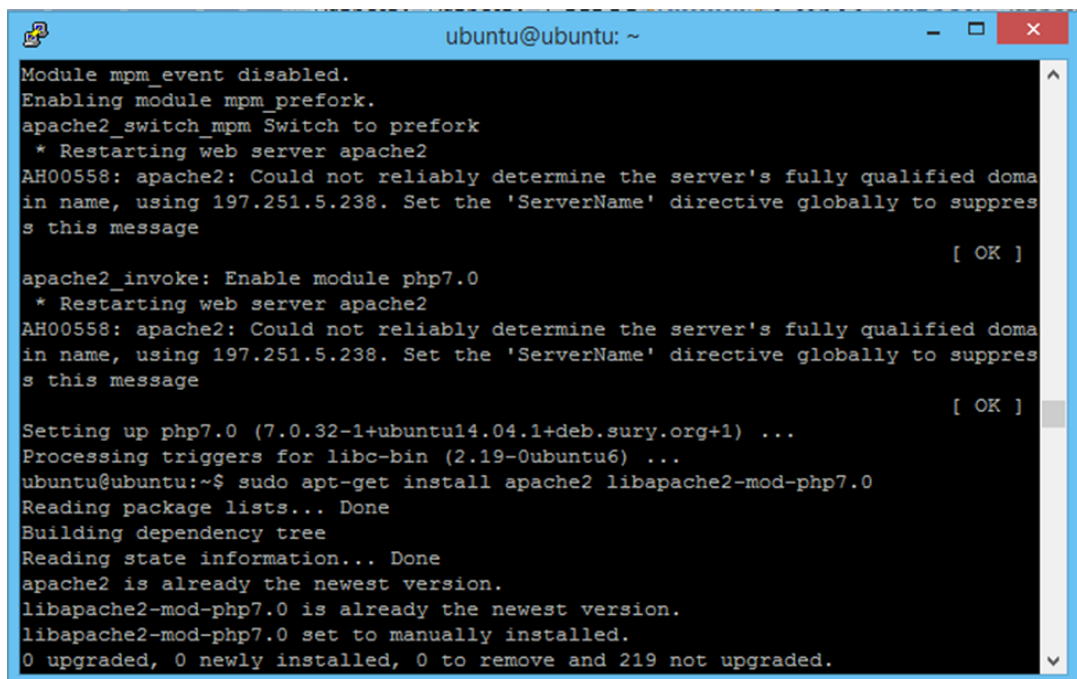
gpg: keyring `/tmp/tmpdd2jxq48/secring.gpg' created
gpg: keyring `/tmp/tmpdd2jxq48/pubring.gpg' created
gpg: requesting key E5267A6C from hkp server keyserver.ubuntu.com
gpg: /tmp/tmpdd2jxq48/trustdb.gpg: trustdb created
gpg: key E5267A6C: public key "Launchpad PPA for Ondřej Surý" imported
gpg: Total number processed: 1
gpg:             imported: 1 (RSA: 1)
OK
ubuntu@ubuntu:~$ sudo apt-get update
Get:1 http://ppa.launchpad.net trusty InRelease [20.9 kB]
Hit http://security.ubuntu.com trusty-security InRelease
Ign http://us.archive.ubuntu.com trusty InRelease
Hit http://security.ubuntu.com trusty-security/main Sources

```

Figure 5.8: Get Update

5.1.2 Adding Apache 2.4 Server Functionality

After successful installation, let's begin installing Apache 2.4. Use the following set of commands to install Apache2 on Ubuntu system available in default apt repositories. `sudo apt-get install apache2 libapache2-mod-php7.0`



```

ubuntu@ubuntu: ~
Module mpm_event disabled.
Enabling module mpm_prefork.
apache2_switch_mpm Switch to prefork
* Restarting web server apache2
AH00558: apache2: Could not reliably determine the server's fully qualified domain
name, using 197.251.5.238. Set the 'ServerName' directive globally to suppress
this message

[ OK ]

apache2_invoke: Enable module php7.0
* Restarting web server apache2
AH00558: apache2: Could not reliably determine the server's fully qualified domain
name, using 197.251.5.238. Set the 'ServerName' directive globally to suppress
this message

[ OK ]

Setting up php7.0 (7.0.32-1+ubuntu14.04.1+deb.sury.org+1) ...
Processing triggers for libc-bin (2.19-0ubuntu6) ...
ubuntu@ubuntu:~$ sudo apt-get install apache2 libapache2-mod-php7.0
Reading package lists... Done
Building dependency tree
Reading state information... Done
apache2 is already the newest version.
libapache2-mod-php7.0 is already the newest version.
libapache2-mod-php7.0 set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 219 not upgraded.

```

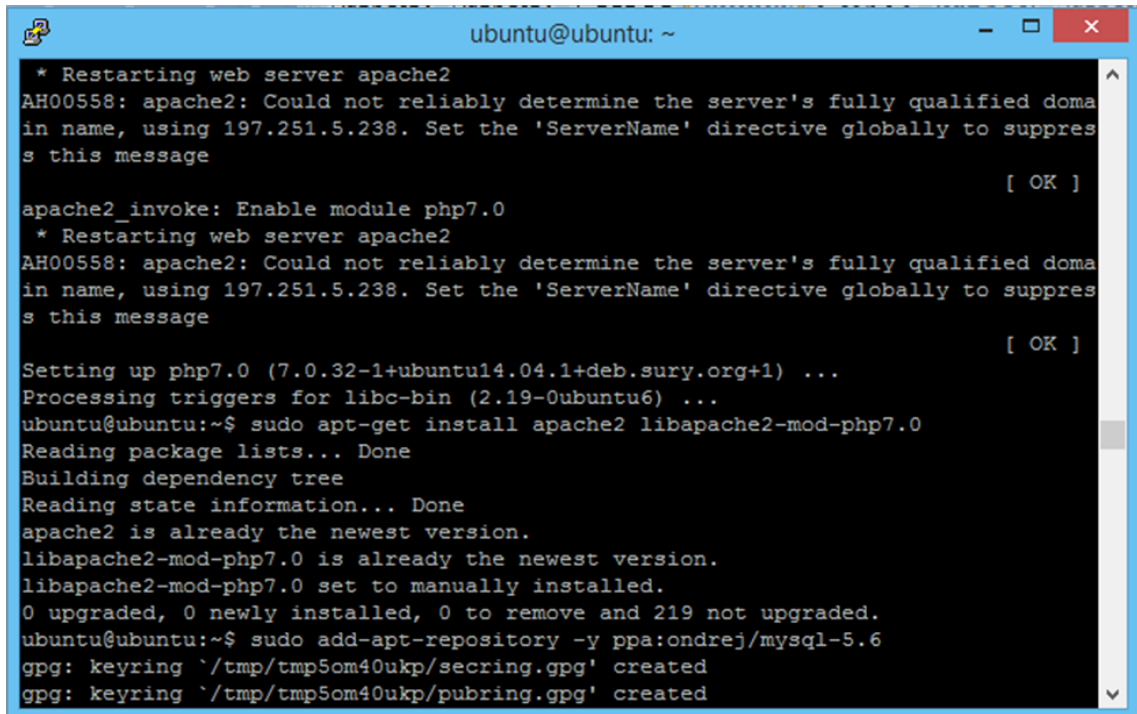
Figure 5.9: Installing Apache 2.4

5.1.3 Adding MySQL 5.6 Functionality

We Use the following commands (summarized in Listing 5.1.3) to install or upgrade MySQL 5.6 on Ubuntu systems. At the last update of MySQL, 5.6.27 is latest available MySQL version series of MySQL 5.6.X.

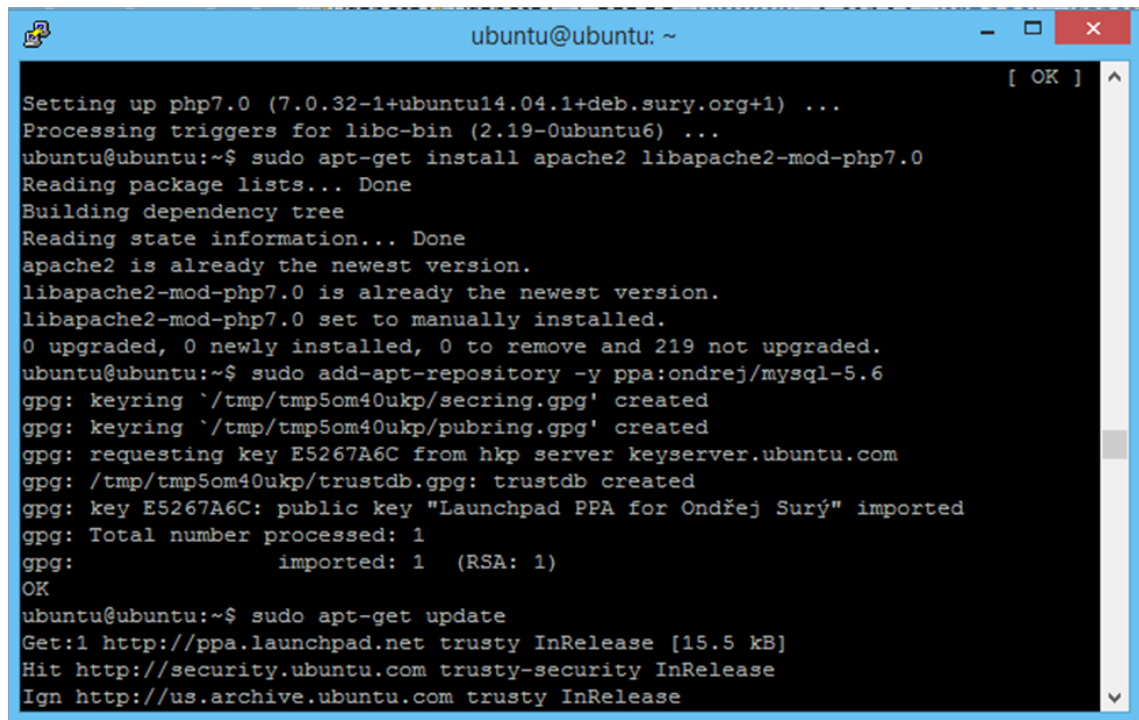
Listing 5.1.3: Command Sequence for adding MySQL 5.6

```
1 sudo add-apt-repository -y ppa:ondrej/mysql-5.6
2 sudo apt-get update
3 sudo apt-get install mysql-server-5.6
```



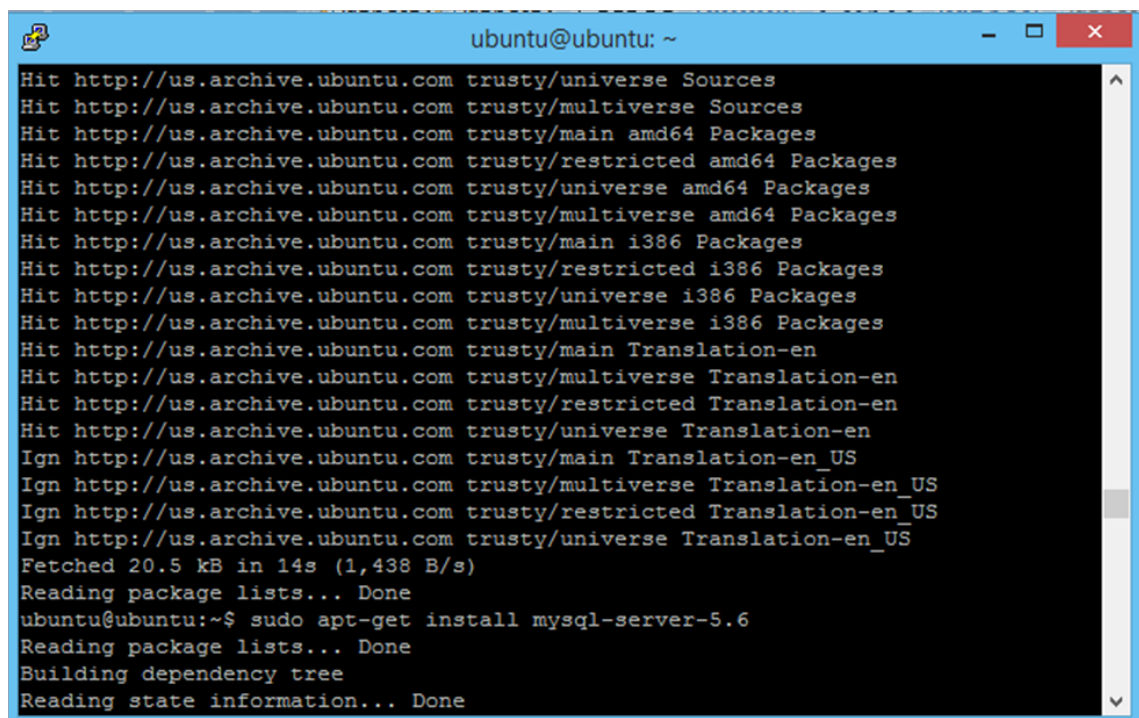
```
ubuntu@ubuntu: ~
* Restarting web server apache2
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 197.251.5.238. Set the 'ServerName' directive globally to suppress this message
[ OK ]
apache2_invoke: Enable module php7.0
* Restarting web server apache2
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 197.251.5.238. Set the 'ServerName' directive globally to suppress this message
[ OK ]
Setting up php7.0 (7.0.32-1ubuntu14.04.1+deb.sury.org+1) ...
Processing triggers for libc-bin (2.19-0ubuntu6) ...
ubuntu@ubuntu:~$ sudo apt-get install apache2 libapache2-mod-php7.0
Reading package lists... Done
Building dependency tree
Reading state information... Done
apache2 is already the newest version.
libapache2-mod-php7.0 is already the newest version.
libapache2-mod-php7.0 set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 219 not upgraded.
ubuntu@ubuntu:~$ sudo add-apt-repository -y ppa:ondrej/mysql-5.6
gpg: keyring `/tmp/tmp5om40ukp/secring.gpg' created
gpg: keyring `/tmp/tmp5om40ukp/pubring.gpg' created
```

Figure 5.10: Executing Command: add-apt-repository-y ppa



```
ubuntu@ubuntu: ~  
Setting up php7.0 (7.0.32-1+ubuntu14.04.1+deb.sury.org+1) ...  
Processing triggers for libc-bin (2.19-0ubuntu6) ...  
ubuntu@ubuntu:~$ sudo apt-get install apache2 libapache2-mod-php7.0  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
apache2 is already the newest version.  
libapache2-mod-php7.0 is already the newest version.  
libapache2-mod-php7.0 set to manually installed.  
0 upgraded, 0 newly installed, 0 to remove and 219 not upgraded.  
ubuntu@ubuntu:~$ sudo add-apt-repository -y ppa:ondrej/mysql-5.6  
gpg: keyring `/tmp/tmp5om40ukp/secring.gpg' created  
gpg: keyring `/tmp/tmp5om40ukp/pubring.gpg' created  
gpg: requesting key E5267A6C from hkp server keyserver.ubuntu.com  
gpg: /tmp/tmp5om40ukp/trustdb.gpg: trustdb created  
gpg: key E5267A6C: public key "Launchpad PPA for Ondřej Surý" imported  
gpg: Total number processed: 1  
gpg: imported: 1 (RSA: 1)  
OK  
ubuntu@ubuntu:~$ sudo apt-get update  
Get:1 http://ppa.launchpad.net trusty InRelease [15.5 kB]  
Hit http://security.ubuntu.com trusty-security InRelease  
Ign http://us.archive.ubuntu.com trusty InRelease
```

Figure 5.11: Executing Command: apt-get update



```
ubuntu@ubuntu: ~  
Hit http://us.archive.ubuntu.com trusty/universe Sources  
Hit http://us.archive.ubuntu.com trusty/multiverse Sources  
Hit http://us.archive.ubuntu.com trusty/main amd64 Packages  
Hit http://us.archive.ubuntu.com trusty/restricted amd64 Packages  
Hit http://us.archive.ubuntu.com trusty/universe amd64 Packages  
Hit http://us.archive.ubuntu.com trusty/multiverse amd64 Packages  
Hit http://us.archive.ubuntu.com trusty/main i386 Packages  
Hit http://us.archive.ubuntu.com trusty/restricted i386 Packages  
Hit http://us.archive.ubuntu.com trusty/universe i386 Packages  
Hit http://us.archive.ubuntu.com trusty/multiverse i386 Packages  
Hit http://us.archive.ubuntu.com trusty/main Translation-en  
Hit http://us.archive.ubuntu.com trusty/multiverse Translation-en  
Hit http://us.archive.ubuntu.com trusty/restricted Translation-en  
Hit http://us.archive.ubuntu.com trusty/universe Translation-en  
Ign http://us.archive.ubuntu.com trusty/main Translation-en_US  
Ign http://us.archive.ubuntu.com trusty/multiverse Translation-en_US  
Ign http://us.archive.ubuntu.com trusty/restricted Translation-en_US  
Ign http://us.archive.ubuntu.com trusty/universe Translation-en_US  
Fetched 20.5 kB in 14s (1,438 B/s)  
Reading package lists... Done  
ubuntu@ubuntu:~$ sudo apt-get install mysql-server-5.6  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done
```

Figure 5.12: Executing Command: install mysql-server-5.6

5.1.4 Adding phpMyAdmin Functionality

The use of phpMyAdmin software functionalities is required to handle the administration of MySQL over the Web. First, run updates through using the command

```
sudo apt-get update
```

Second, run the command

```
sudo apt-get install phpMyAdmin
```

Next, you will be asked a few questions in order to configure the installation correctly. Here is a summary for the setting used in this thesis.

- For the server selection, choose `apache2`.
- Select yes when asked whether to use `"dbconfig-common"` to set up the database
- You will be prompted for your database administrator's password
- You will then be asked to choose and confirm a password for the php-MyAdmin application itself.

The installation process actually adds the phpMyAdmin Apache configuration file into the `"/etc/apache2/conf-enabled/"` directory, where it is automatically read. The only thing we need to do is explicitly enable the `"php7-mcrypt"` extension, which we can do by typing the command

```
sudo php7enmod mcrypt
```

Afterwards, you'll need to restart Apache for your changes to be recognized:

```
sudo service apache2 restart
```

5.2 Cloud Web Interface Design and Access

You can now access the web interface by visiting your server's domain name or public IP address followed by `/phpmyadmin`:

```
http://197.251.5.238/phpmyadmin
```

The PHP myAdmin page is shown in Figure 5.13. When you log in, you'll see the user interface, which will look as shown in Figure 5.14. To Upload all files to virtual server in cloud FileZilla software is used as shown in Figure 5.15

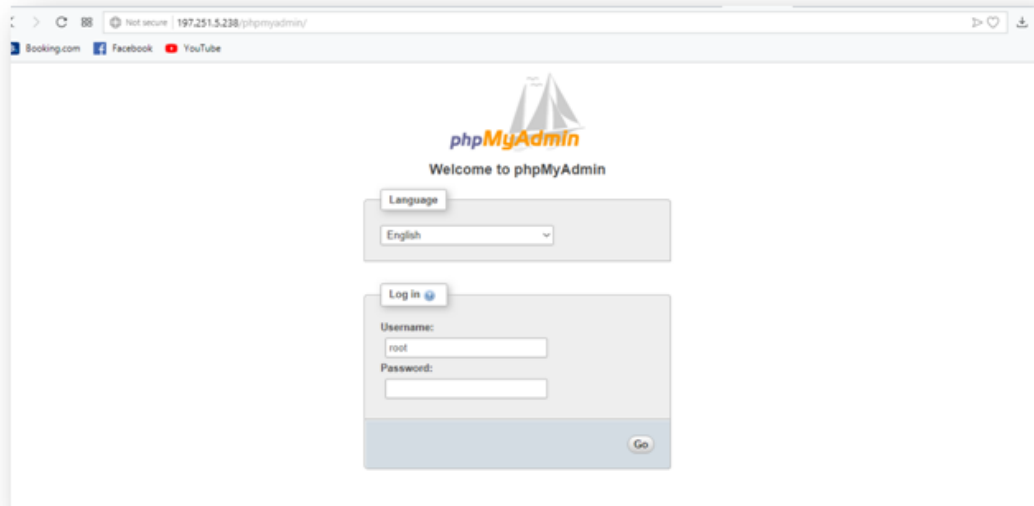


Figure 5.13: PHP Myadmin home page from browser

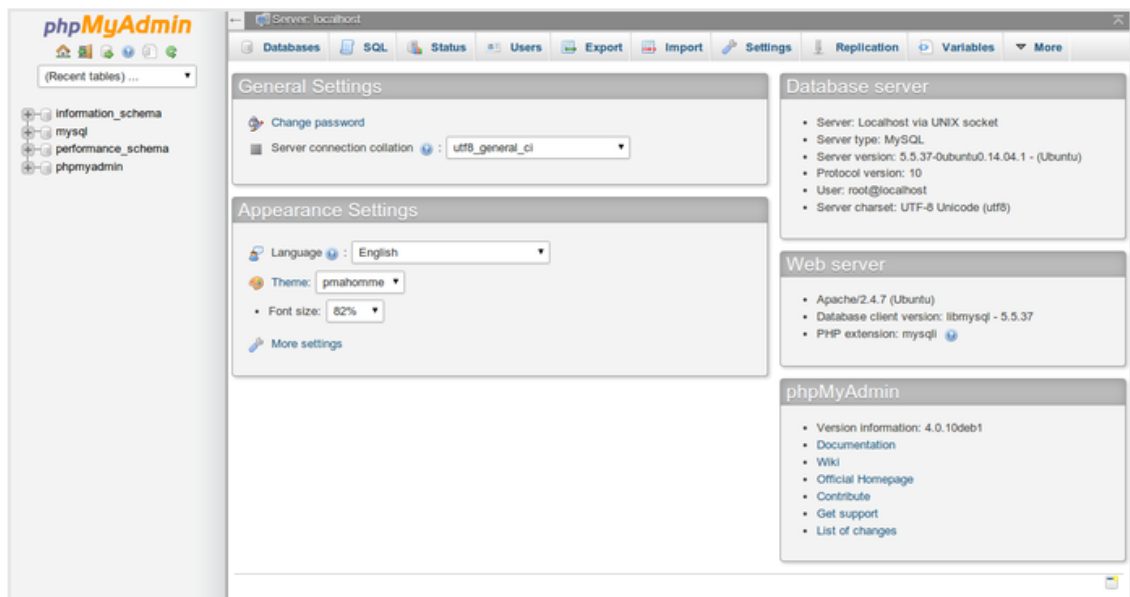


Figure 5.14: Interface (After Logging)

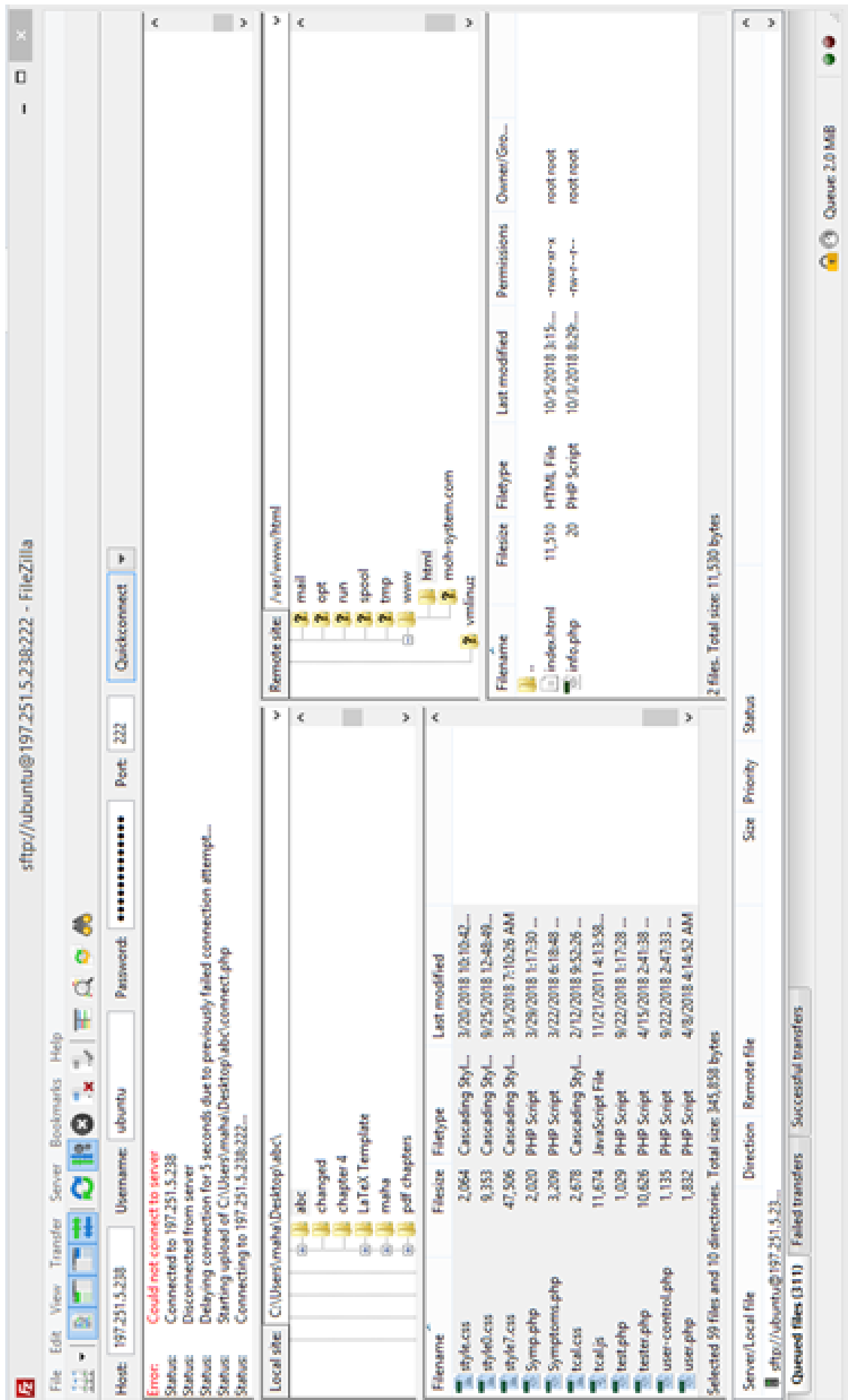


Figure 5.15: Utilizing FileZilla to upload files to virtual server

5.3 Web Interface Home Page

5.3.1 Creating Patient File

The home page is shown in Figure 5.16. To create a patient's file, the required information is:

- Full patient name
- Address
- Age
- Phone number
- Sex

The web-front user should have general information about hospitals duty and contact information to each one. Also, the patient can register from homepage before you come to hospital and reserve your position in doctor list. The web front also contains login button for worker in hospital field (Receptionist , Doctor, Tester).

The screenshot shows a web browser window displaying the 'Ministry of Health' homepage. The browser's address bar shows 'localhost/abc/index.php'. The page has a blue header with the 'Ministry of Health' logo and navigation links: 'Home', 'About Us', '(+249) 912345678', 'Email Us', and 'Login'. Below the header is a registration form with fields for 'Name', 'Address', 'Phone', 'National-number', and 'Birth date', along with a 'choose unit' dropdown menu and a 'Register' button. To the right of the form, contact information is displayed: 'Mon - Sat 08:00 - 21:00 Sunday CLOSED', '0080 673 729 766 contact@business.com', and 'Lamas Str, no 14-18 41770 Miami'. At the bottom, there are three promotional boxes: 'Emergency Room' with a 'Cardiology' logo, 'The Best Doctors' with placeholder text, and 'Online results' with placeholder text.

Figure 5.16: Home Page

5.3.2 Login Page

From this page (see figure 5.17) you can insert your user name and password and do your works depend on your role.

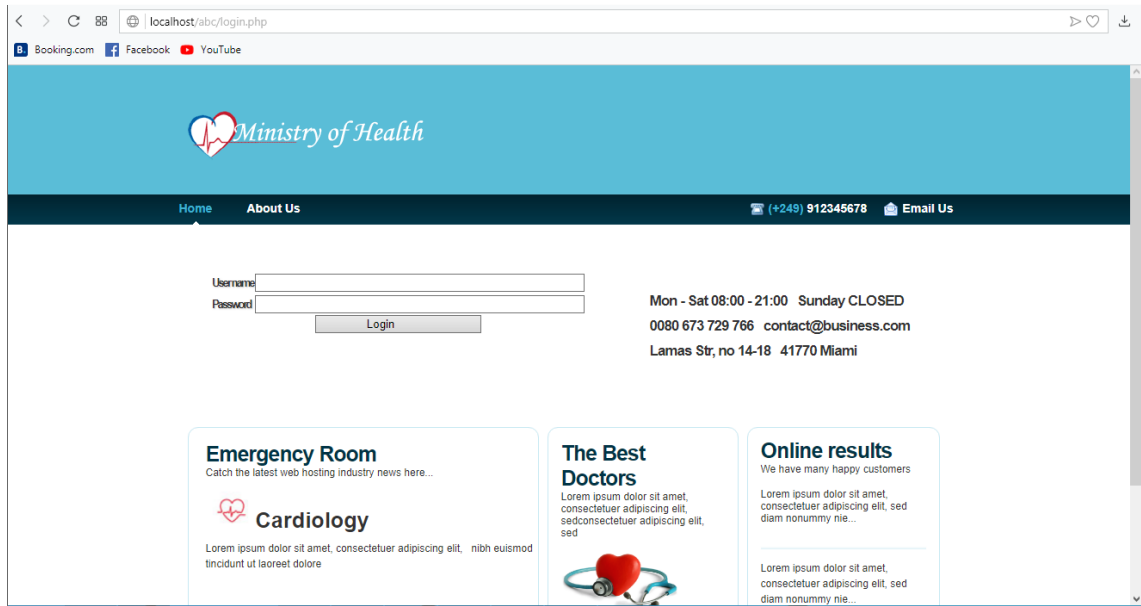


Figure 5.17: Login Page

5.3.3 Reception Page

From this page (see figure 5.18) the receptionist control the process of patients access to the doctor (see Figure 5.18 and Figure 5.19).

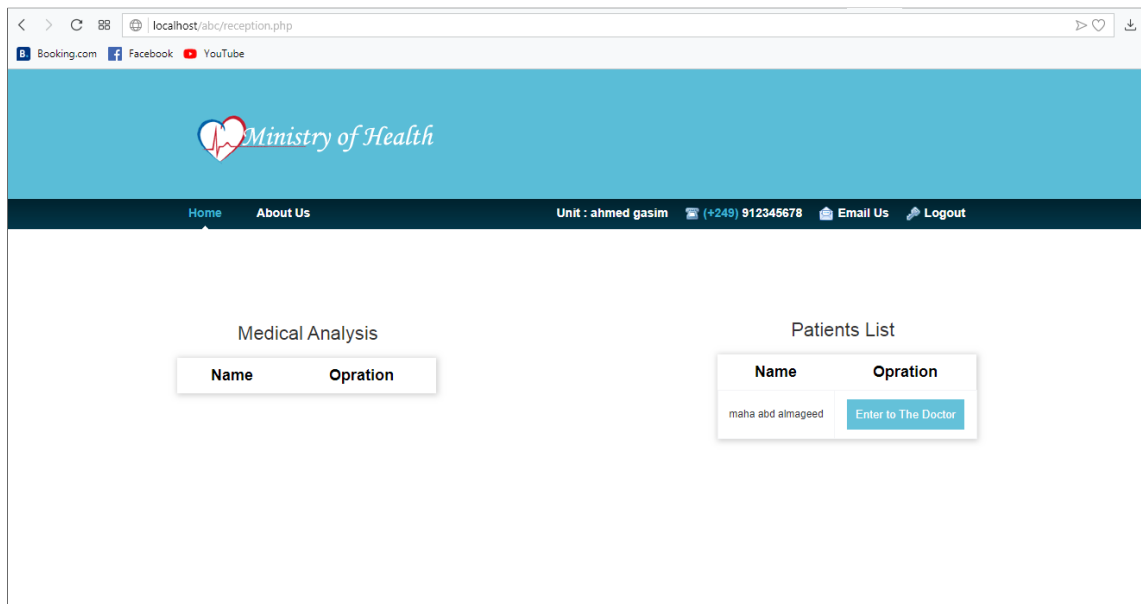


Figure 5.18: Reception Page

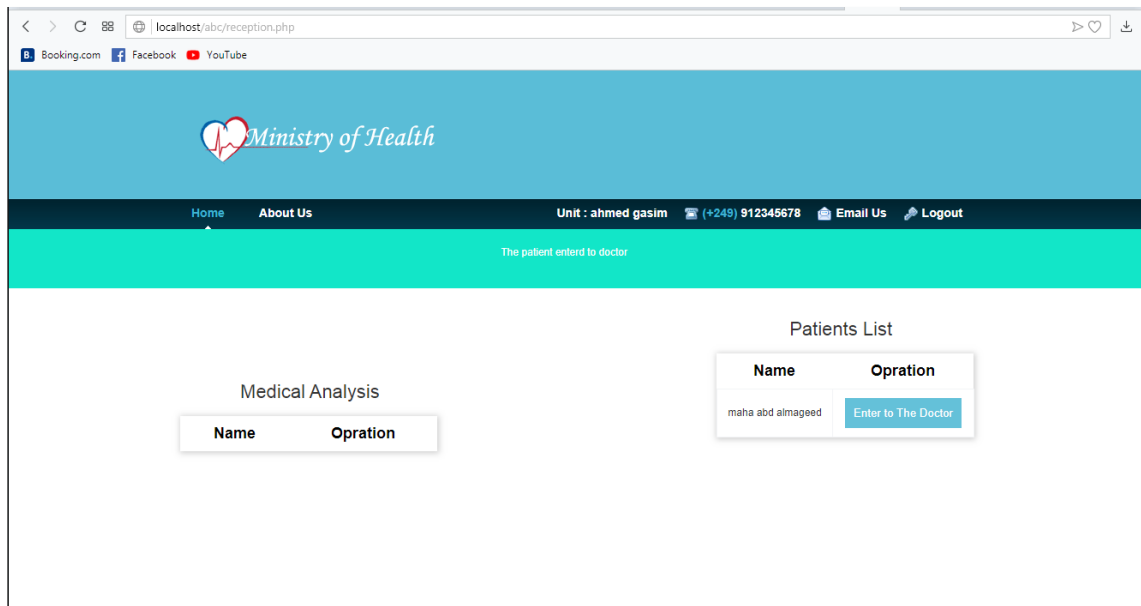


Figure 5.19: Reception Page: Control of Patients Access to Doctors

5.3.4 Doctor Page

This page (see Figure 5.20) allows the doctor to view patient details or delete the patient from list after the appointment. First, the patient personal information appear, and the doctor can view the past history data (see Figure 5.21). The doctor can add extra information such as a new risk factor, additional symptoms, test, diagnosis and prescribed drugs. This is illustrated in Figure 5.22.

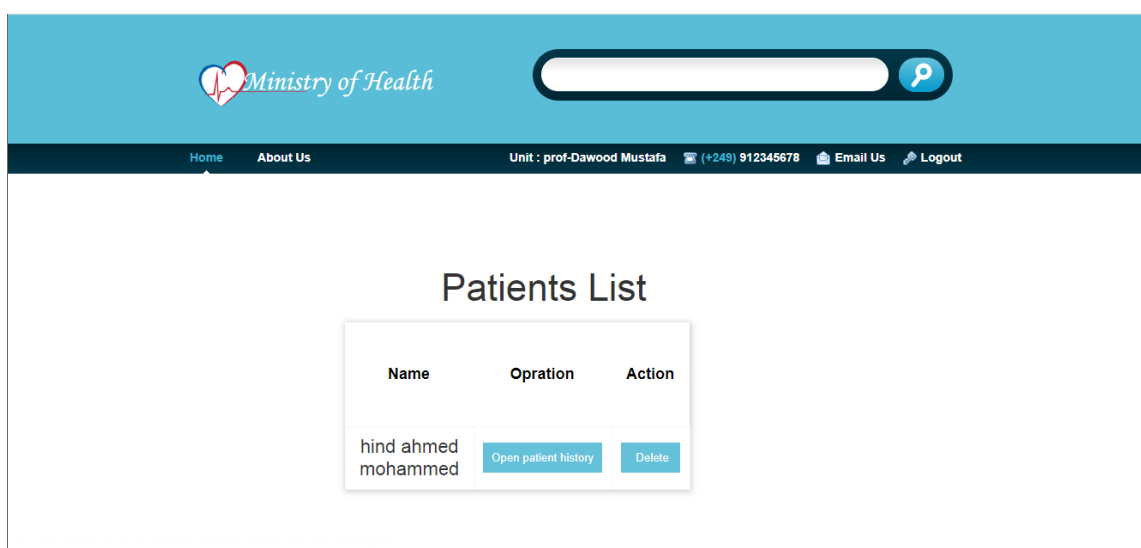


Figure 5.20: Doctor Page: Viewing the Patients List

The screenshot shows a web application for the Ministry of Health. The header is blue with the Ministry of Health logo and name. Below the header is a dark blue navigation bar with links: Home, About Us, Unit : prof-Dawood Mustafa, (+249) 912345678, Email Us, and Logout. The main content area is white. On the right, there is a 'Patient info' section with a green header and a table of patient details. On the left, there is a 'Patient History' section with a 'Risk Factor' dropdown and an 'insert' button.

Patient info	
Name	maha abd almageed
National Number	1111111
Address	khartoum
Birth date	1980-10-29
phone number	9111111111

Patient History

Risk Factor

choose risk Factor

Figure 5.21: Doctor Page: Viewing the Patients Past History

The screenshot shows the 'Patient History' section of the web application. It contains several input fields and buttons for adding extra patient information. The fields are: Risk Factor (dropdown), Symptoms (dropdown), Test For (dropdown), diagnosis (dropdown), and Drugs (dropdown). Each field has an 'insert' button next to it. There is also a 'show result' button and a 'transfer to test' button.

Patient History

Risk Factor

choose risk Factor

Symptoms

choose symptoms

Test For

choose test

show result

diagnosis

choose diagnosis

Drugs

choose drug

Figure 5.22: Doctor Page: Adding Extra Patients Information

The screenshot shows a web browser window with the address bar displaying 'localhost/abc/history1.php'. The website has a blue header with the 'Ministry of Health' logo and a dark blue navigation bar with links for 'Home', 'About Us', 'Unit : (+249) 912345678', and 'Email Us'. The main content area displays three tables: 'Risk Factor', 'Symptoms', and 'Diagnosis', each with patient history data.

ID	Riskname	Doctor Name	Unit Name	Date
63	High blood pressure	maha abdelmjeed	prof-Dawood Mustafa	2018-10-25 03:16:04

ID	Symptom name	Doctor Name	Unit Name	Date
106	Chest pain	maha abdelmjeed2	ahmed gasim	2018-10-24 03:19:47

ID	Diagnosis name	Doctor Name	Unit Name	Date
28	stable	maha abdelmjeed2	ahmed gasim	2018-10-24 03:19:55

ID	Drug name	Doctor Name	Unit Name	Date
38	drug1	maha abdelmjeed2	ahmed gasim	2018-10-24 03:20:01

Figure 5.23: Doctor Page: Patient Past History Data

5.3.5 Receptionist Page

The receptionist is also responsible for entering patients to medical labs. The receptionist can use the patients list through the web page shown in Figure 5.24. The enter-to-Lab status can be managed through the web page shown in Figure 5.25.

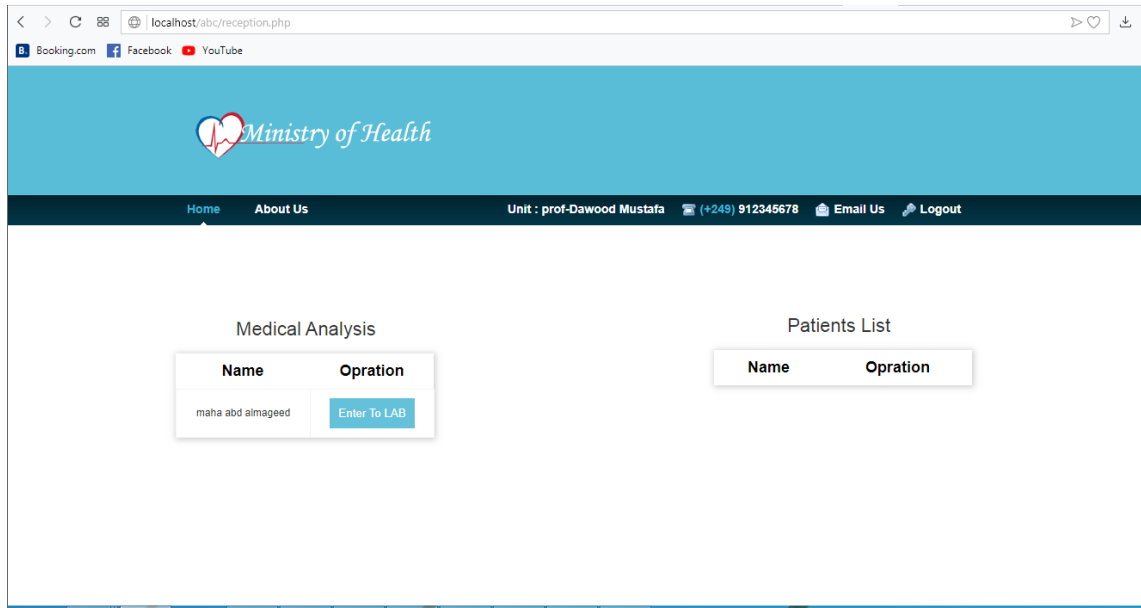


Figure 5.24: Reception Page: Patients list

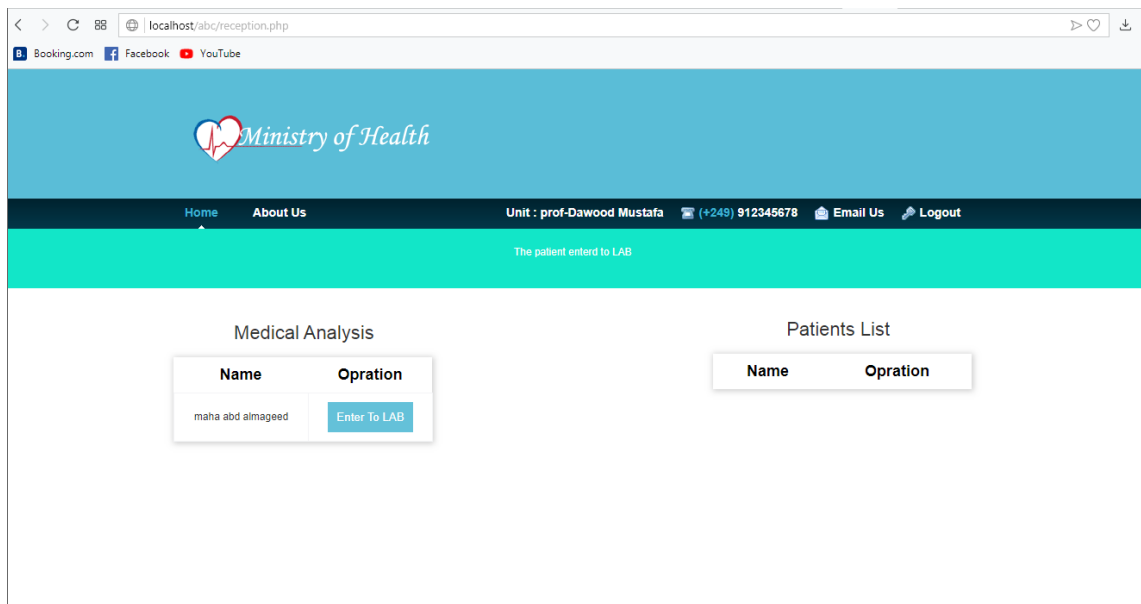


Figure 5.25: Reception Page: Enter-to-Lab Status

5.3.6 Medical Lab Assistant Page

The medical lab assistant can view requested test or delete a specific patient from list after finishing through the web page shown in Figure 5.26. The medical lab assistant can view patient personal information and required tests through the web page shown in Figure 5.27. Furthermore, the doctor can view the lab results through the web page shown in Figure 5.28. In general

- When medical lab assistant login, the patient appear and tester can view test required and add the result from drop down list.
- After the medical lab assistant submits the result, the doctor can see this information in test result in patient file.

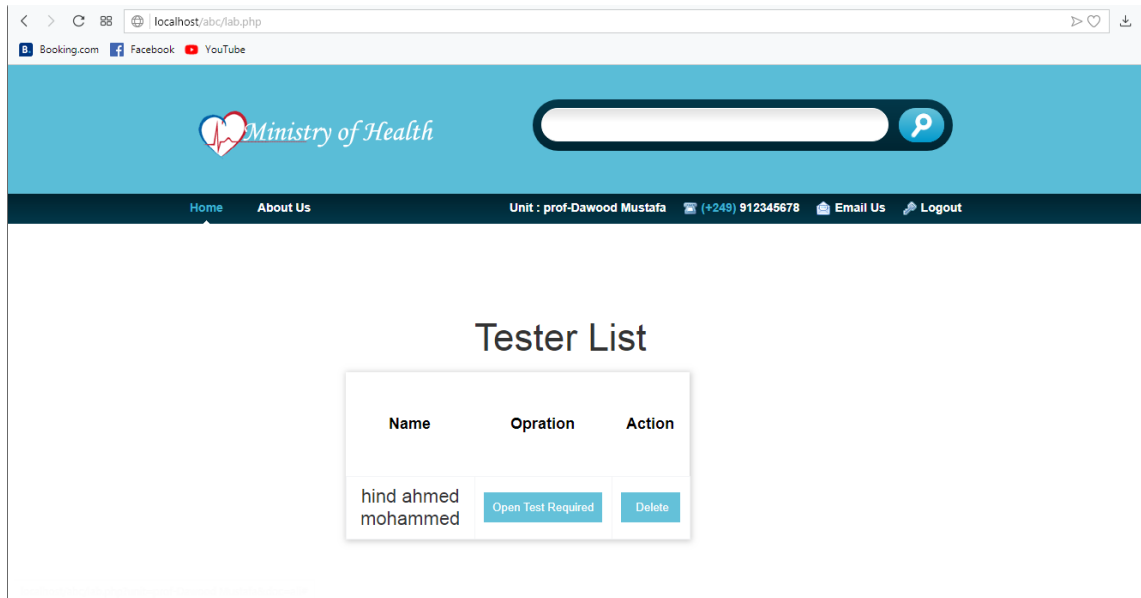


Figure 5.26: Medical Lab Assistant Page

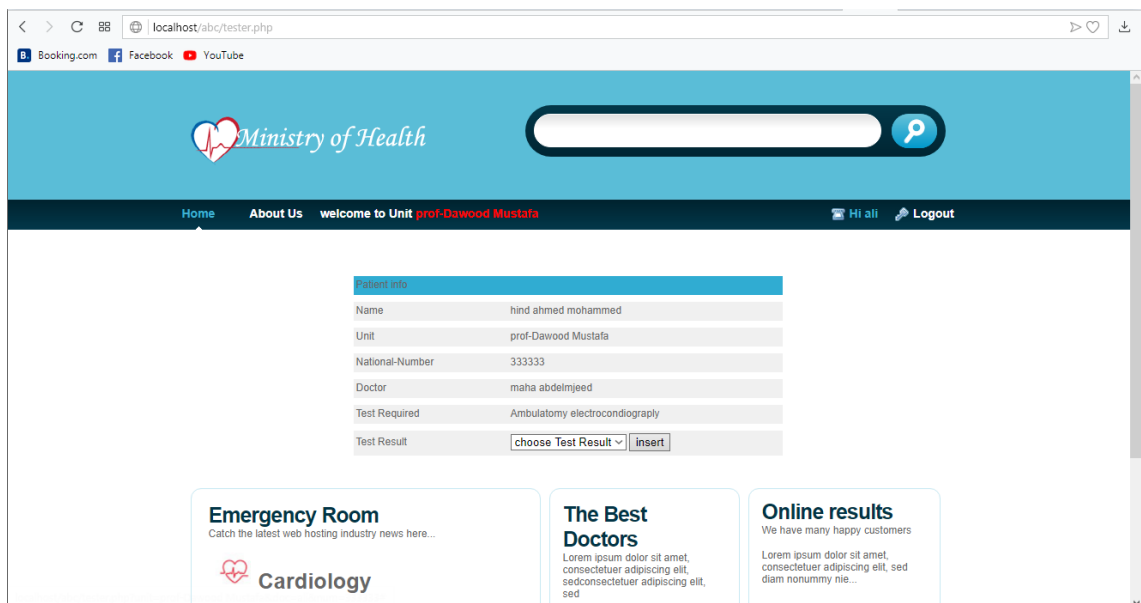


Figure 5.27: Medical Lab Assistant Page: Patient's Personal Information

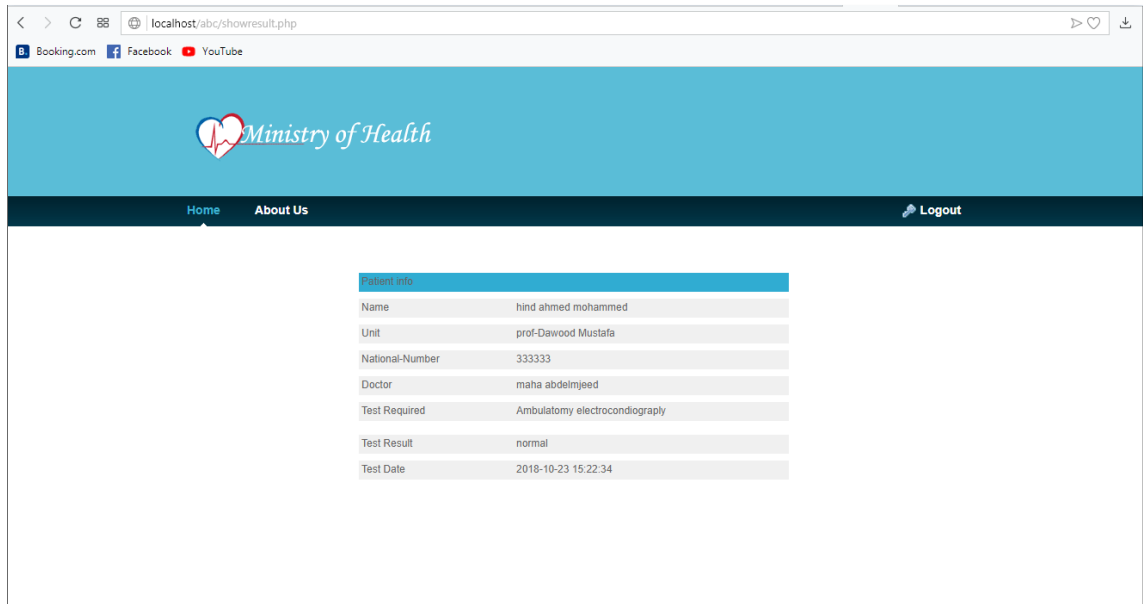


Figure 5.28: Doctor Page For Viewing Lab Results

5.3.7 Patients Database

The patient database can be viewed for a specific patient. For example see Figure 5.29. However from, a designer/administrator point of view, the patient's database looks as shown in Figure 5.30.

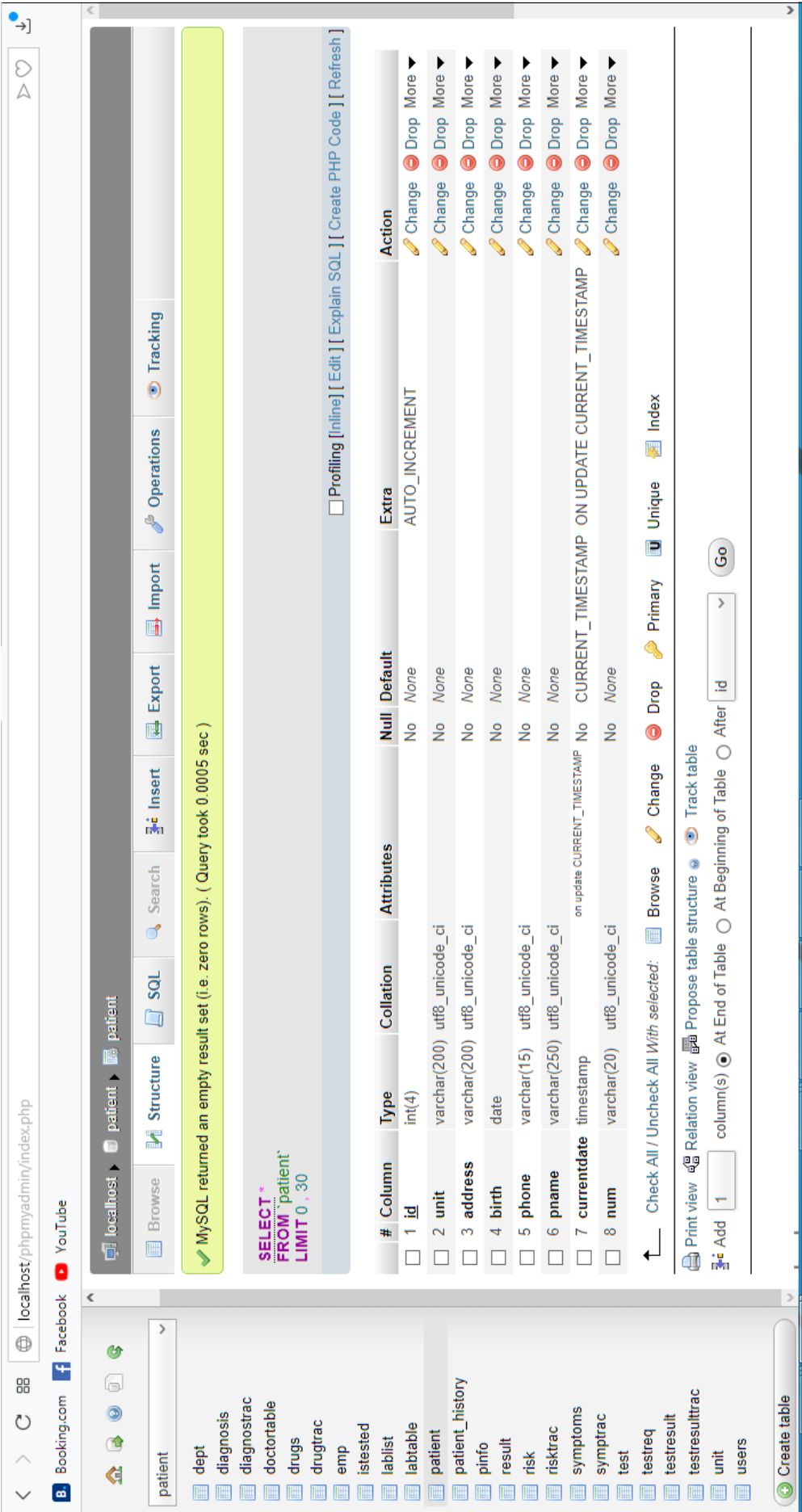


Figure 5.29: Patient Database

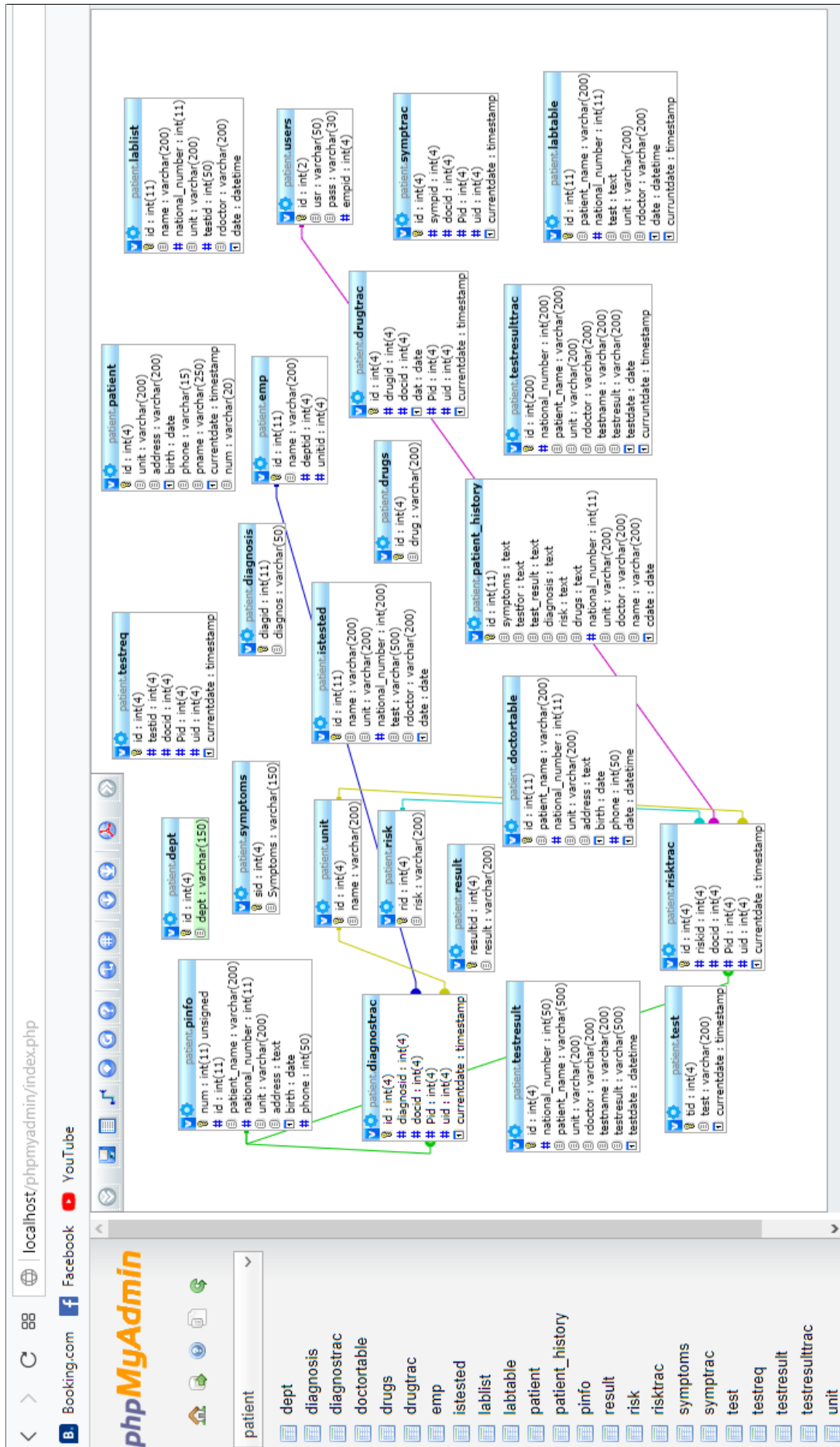


Figure 5.30: Designer View of Patient Database

Chapter Six

Conclusions and Recommendations

6.1 Conclusion

Ultimately The enterprise software is not a sufficient idea to follow up patients diagnosis and introduce health services to cover the whole country, For the reasons mentioned in the research, but the SaaS cloud computing is achieve the requirements with high efficiency , for example by implementing SaaS in ministry of health we can request a report of every patient even from the past time and know who is the doctor that follows the patient in specific period of time and witch risk factors threaten his live and which drug can treat the specific problem and the doctor can send medical report to another doctor outside the Sudan using specific email indicates that the doctor follow to ministry of health in Sudan.

6.2 Recommendations

This research recommends further works to: Activation of the medical number in Sudan and linking it to the national number and insurance card; Consulting the professional in every section of the medical field to provide reliable medical data to the system, review it and test the system before applying it officially in Sudan; Add role to pharmacist in the system to be able to determine the drug; Provide a feature in the system indicating that the reservation is over for this unit today and can be available for booking tomorrow; Linking the system to civil registry system so that the system can bring the basic data of the patient through entering the medical number; Create E-mail to each doctors at the Ministry of Health domain, so that the doctor can send a report about the patient to another doctor outside the country if required; Add the possibility of ordering the ambulance through the system and identify the location using GPS technique; Link the system with the EBS Portal so that the patient can pay the visitta electronically by using the barcode scanners;

Create a system to the Ministry of Labor and administrative reform linking all governmental institutions ; Create a system to the Ministry of Education to link all schools with the Ministry.

Bibliography

- [1] Z. K. Rawezh, T. Yahiya, and N. B. Mustafa, “An implementation of software routing for building a private cloud,” *International Journal of Computer Network and Information Security*, vol. 10, no. 3, p. 1, 2018.
- [2] M. Yousif, “Introducing ieee cloud computing: a very timely magazine,” *IEEE Cloud Computing*, vol. 1, no. 1, pp. 4–7, 2014.
- [3] G. Conway, “Introduction to cloud computing,” 2011.
- [4] K. So, “Cloud computing security issues and challenges,” *International Journal of Computer Networks*, vol. 3, no. 5, pp. 247–55, 2011.
- [5] A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, and I. Stoica, “Above the clouds: A berkeley view of cloud computing,” *Dept. Electrical Eng. and Comput. Sciences, University of California, Berkeley, Rep. UCB/EECS*, vol. 28, no. 13, p. 2009, 2009.
- [6] Y. Liu and H. Song, “Levering mobile cloud computing for mobile big data analytics,” in *Mobile Big Data*. Springer, 2018, pp. 21–39.
- [7] H. Katzan, “On an ontological view of cloud computing,” *Journal of Service Science*, vol. 3, no. 1, pp. 1–6, 2010.
- [8] L. Wang, J. Tao, M. Kunze, A. C. Castellanos, D. Kramer, and W. Karl, “Scientific cloud computing: Early definition and experience,” in *High Performance Computing and Communications, 2008. HPCC’08. 10th IEEE International Conference on*. Ieee, 2008, pp. 825–830.
- [9] P. K. Chouhan, F. Yao, S. Y. Yerima, and S. Sezer, “Software as a service: Analyzing security issues,” *arXiv preprint arXiv:1505.01711*, 2015.
- [10] S. Pearson, “Taking account of privacy when designing cloud computing services,” in *Software Engineering Challenges of Cloud Computing, 2009. CLOUD’09. ICSE Workshop on*. IEEE, 2009, pp. 44–52.

- [11] C. Tan, K. Liu, and L. Sun, “A design of evaluation method for saas in cloud computing,” *Journal of Industrial Engineering and Management*, vol. 6, no. 1, pp. 50–72, 2013.
- [12] K. K. M. Kumar, “Software as a service for efficient cloud computing,” *environment*, vol. 7, p. 10, 2014.
- [13] W.-T. Tsai, X. Sun, and J. Balasooriya, “Service-oriented cloud computing architecture,” in *Information Technology: New Generations (ITNG), 2010 Seventh International Conference on.* IEEE, 2010, pp. 684–689.
- [14] M. Ali, S. U. Khan, and A. V. Vasilakos, “Security in cloud computing: Opportunities and challenges,” *Information sciences*, vol. 305, pp. 357–383, 2015.
- [15] A. Behl and K. Behl, “An analysis of cloud computing security issues,” in *Information and Communication Technologies (WICT), 2012 World Congress on.* IEEE, 2012, pp. 109–114.
- [16] K. Zunnurhain and S. V. Vrbsky, “Security in cloud computing,” in *Proceedings of the International Conference on Security and Management (SAM).* The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), 2011, p. 1.
- [17] R. R. Chowdhury, “Security in cloud computing,” *International Journal of Computer Applications*, vol. 96, no. 15, 2014.
- [18] B. Grobauer, T. Walloschek, and E. Stocker, “Understanding cloud computing vulnerabilities,” *IEEE Security & Privacy*, vol. 9, no. 2, pp. 50–57, 2011.
- [19] V. D. Sharma, S. Agarwai, S. S. Moin, and M. A. Qadeer, “Security in cloud computing,” in *2017 7th International Conference on Communication Systems and Network Technologies (CSNT).* IEEE, 2017, pp. 234–239.
- [20] Q. Jiang, J. Ma, and F. Wei, “On the security of a privacy-aware authentication scheme for distributed mobile cloud computing services,” *IEEE Systems Journal*, vol. 12, no. 2, pp. 2039–2042, 2018.

- [21] E. Gorelik, “Cloud computing models,” Ph.D. dissertation, Massachusetts Institute of Technology, 2013.
- [22] C. Rose, “A break in the clouds: Towards a cloud definition,” 2011.
- [23] A. Sharma and U. Singh, “Study on load balancing techniques in ant colony optimization for cloud computing,” *International Journal of Computer Applications*, pp. 5–10, 2016.
- [24] S. Zhang, S. Zhang, X. Chen, and X. Huo, “Cloud computing research and development trend,” in *2010 Second international conference on future networks*. Ieee, 2010, pp. 93–97.
- [25] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica *et al.*, “A view of cloud computing,” *Communications of the ACM*, vol. 53, no. 4, pp. 50–58, 2010.
- [26] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, “Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility,” *Future Generation computer systems*, vol. 25, no. 6, pp. 599–616, 2009.
- [27] L. Wang, G. Von Laszewski, A. Younge, X. He, M. Kunze, J. Tao, and C. Fu, “Cloud computing: a perspective study,” *New Generation Computing*, vol. 28, no. 2, pp. 137–146, 2010.
- [28] S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, and A. Ghalsasi, “Cloud computing—the business perspective,” *Decision support systems*, vol. 51, no. 1, pp. 176–189, 2011.
- [29] C. Gong, J. Liu, Q. Zhang, H. Chen, and Z. Gong, “The characteristics of cloud computing,” in *Parallel Processing Workshops (ICPPW), 2010 39th International Conference on*. IEEE, 2010, pp. 275–279.
- [30] N. K. Salih and T. Zang, “Survey and comparison for open and closed sources in cloud computing,” *arXiv preprint arXiv:1207.5480*, 2012.
- [31] Z. Yang, M. Hoseinzadeh, P. Wong, J. Artoux, C. Mayers, D. T. Evans, R. T. Bolt, J. Bhimani, N. Mi, and S. Swanson, “H-nvme: a hybrid framework of nvme-based storage system in cloud computing environment,” in *Performance Computing and Communications Conference (IPCCC), 2017 IEEE 36th International*. IEEE, 2017, pp. 1–8.

- [32] D. Chen and H. Zhao, “Data security and privacy protection issues in cloud computing,” in *Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on*, vol. 1. IEEE, 2012, pp. 647–651.
- [33] M. Janssen and A. Joha, “Challenges for adopting cloud-based software as a service (saas) in the public sector.” in *ECIS*, 2011, p. 80.
- [34] S. Chhabra and V. S. Dixit, “Cloud computing: State of the art and security issues,” *ACM SIGSOFT Software Engineering Notes*, vol. 40, no. 2, pp. 1–11, 2015.
- [35] P. Buxmann, T. Hess, and S. Lehmann, “Software as a service,” *Wirtschaftsinformatik*, vol. 50, no. 6, pp. 500–503, 2008.
- [36] S. Satyanarayana, “Cloud computing: Saas,” *Computer Sciences and Telecommunications*, no. 4, pp. 76–79, 2012.
- [37] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina, “Controlling data in the cloud: outsourcing computation without outsourcing control,” in *Proceedings of the 2009 ACM workshop on Cloud computing security*. ACM, 2009, pp. 85–90.
- [38] S. Rehman and R. Gautam, “Research on access control techniques in saas of cloud computing,” in *International Symposium on Security in Computing and Communication*. Springer, 2014, pp. 92–100.
- [39] V. V. H. Pham, X. Liu, X. Zheng, M. Fu, S. V. Deshpande, W. Xia, R. Zhou, and M. Abdelrazek, “Paas-black or white: an investigation into software development model for building retail industry saas,” in *Software Engineering Companion (ICSE-C), 2017 IEEE/ACM 39th International Conference on*. IEEE, 2017, pp. 285–287.
- [40] G. A.-M. Taufiq-Hail, H. Ibrahim, and S. A. M. Yusof, “Saas cloud computing as a means of green it acceptance model: A theory of planned behavior model at malaysian public universities’ context,” *Journal of Information*, vol. 2, no. 4, pp. 01–17, 2017.
- [41] C. P. Wale, “Cloudy with a chance of open source: open source integrated library systems and cloud computing in academic law libraries,” *Legal Reference Services Quarterly*, vol. 30, no. 4, pp. 310–331, 2011.

- [42] M. Decat, B. Lagaisse, D. Van Landuyt, B. Crispo, and W. Joosen, “Federated authorization for software-as-a-service applications,” in *OTM Confederated International Conferences” On the Move to Meaningful Internet Systems*. Springer, 2013, pp. 342–359.
- [43] F. R. Martinez and E. Pulier, “System and method for a cloud computing abstraction layer with security zone facilities,” Jun. 30 2015, uS Patent 9,069,599.
- [44] D. Li, C. Liu, and B. Liu, “H-rbac: a hierarchical access control model for saas systems,” *International Journal of Modern Education and Computer Science*, vol. 3, no. 5, p. 47, 2011.
- [45] X. Jin, *Attribute-based access control models and implementation in cloud infrastructure as a service*. The University of Texas at San Antonio, 2014.
- [46] V. C. Hu, D. Ferraiolo, R. Kuhn, A. R. Friedman, A. J. Lang, M. M. Cogdell, A. Schnitzer, K. Sandlin, R. Miller, K. Scarfone *et al.*, “Guide to attribute based access control (abac) definition and considerations (draft),” *NIST special publication*, vol. 800, no. 162, 2013.
- [47] H. Katzan Jr, “Introduction to attribute based access control.”
- [48] B. Balamurugan and P. V. Krishna, “Extensive survey on usage of attribute based encryption in cloud,” *journal of emerging technologies in web intelligence*, vol. 6, no. 3, pp. 263–272, 2014.
- [49] A. Cavoukian, M. Chibba, G. Williamson, and A. Ferguson, “The importance of abac: Attribute-based access control to big data: Privacy and context,” *Privacy and Big Data Institute, Ryerson University, Toronto, Canada*, 2015.
- [50] K. A. Shakil and M. Alam, “Cloud computing in bioinformatics and big data analytics: Current status and future research,” in *Big Data Analytics*. Springer, 2018, pp. 629–640.
- [51] I. Foster, Y. Zhao, I. Raicu, and S. Lu, “Cloud computing and grid computing 360-degree compared,” in *Grid Computing Environments Workshop, 2008. GCE’08*. Ieee, 2008, pp. 1–10.

- [52] T. Dillon, C. Wu, and E. Chang, “Cloud computing: issues and challenges,” in *Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on*. Ieee, 2010, pp. 27–33.
- [53] T. Baker, E. Ugljanin, N. Faci, M. Sellami, Z. Maamar, and E. Kajan, “Everything as a resource: Foundations and illustration through internet-of-things,” *Computers in Industry*, vol. 94, pp. 62–74, 2018.
- [54] C. Stergiou, K. E. Psannis, B.-G. Kim, and B. Gupta, “Secure integration of iot and cloud computing,” *Future Generation Computer Systems*, vol. 78, pp. 964–975, 2018.
- [55] O. Shimrat, “Cloud computing and healthcare,” *San Diego Physician.org*, pp. 26–29, 2009.
- [56] C. G. Kochan, D. R. Nowicki, B. Sauser, and W. S. Randall, “Impact of cloud-based information sharing on hospital supply chain performance: A system dynamics framework,” *International Journal of Production Economics*, vol. 195, pp. 168–185, 2018.
- [57] R. Mahmud, F. L. Koch, and R. Buyya, “Cloud-fog interoperability in iot-enabled healthcare solutions,” in *Proceedings of the 19th International Conference on Distributed Computing and Networking*. ACM, 2018, p. 32.
- [58] C. O. Rolim, F. L. Koch, C. B. Westphall, J. Werner, A. Fracalossi, and G. S. Salvador, “A cloud computing solution for patient’s data collection in health care institutions,” in *eHealth, Telemedicine, and Social Medicine, 2010. ETELEMED’10. Second International Conference on*. IEEE, 2010, pp. 95–99.
- [59] C. Vecchiola, S. Pandey, and R. Buyya, “High-performance cloud computing: A view of scientific applications,” in *Pervasive Systems, Algorithms, and Networks (ISPAN), 2009 10th International Symposium on*. IEEE, 2009, pp. 4–16.
- [60] P. Pocatilu, “Cloud computing benefits for e-learning solutions,” *Economics of Knowledge*, vol. 2, no. 1, p. 9, 2010.
- [61] “Saas cloud.” [Online]. Available: <https://www.infinitesource.com/blog/topic/construction-industry/page>

- [62] “Mongodb - sharding - tutorialspoint.” [Online]. Available: https://www.tutorialspoint.com/mongodb/mongodb_sharding.htm
- [63] “ququing system.” [Online]. Available: <https://www.paxata.com/intelligent-automation>