

1. INTRODUCTION

1.1 What is cloud computing?

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers.

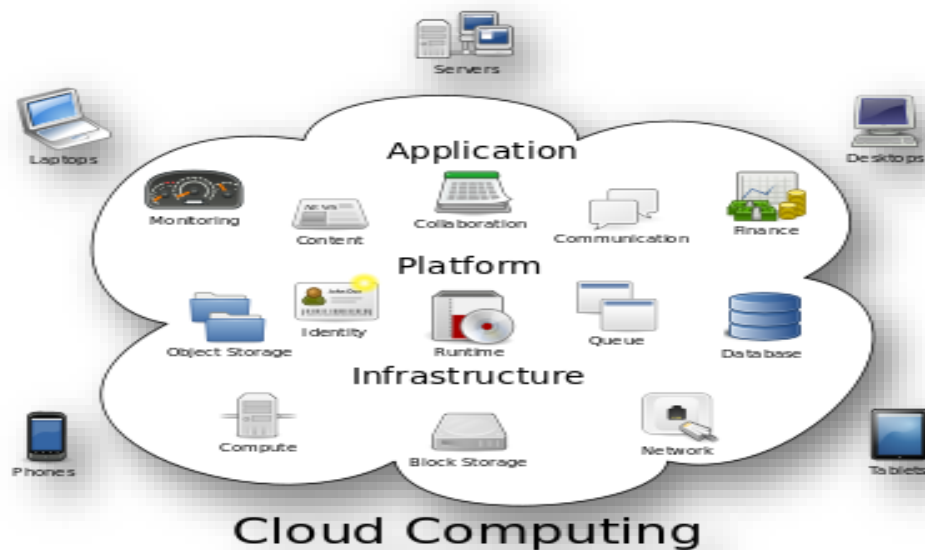


Fig 1.1: Structure of cloud computing

1.2 How Cloud Computing Works?

The goal of cloud computing is to apply traditional supercomputing, or high-performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive computer games.

The cloud computing uses networks of large groups of servers typically running low-cost consumer PC technology with specialized connections to spread data-processing chores across them. This shared IT infrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing.

1.3 Characteristics and Services Models:

The salient characteristics of cloud computing based on the definitions provided by the National Institute of Standards and Terminology (NIST) are outlined below:

- **On-demand self-service:** A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.
- **Broad network access:** Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).
- **Resource pooling:** The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location-independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data

center). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

- **Rapid elasticity:** Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
- **Measured service:** Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be managed, controlled, and reported providing transparency for both the provider and consumer of the utilized service.



Fig 1.2: Characteristics of cloud computing

Services Models:

Cloud Computing comprises three different service models, namely Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). The three service models or layer are completed by an end user layer that encapsulates the end user perspective on cloud services. The model is shown in figure below. If a cloud user accesses services on the infrastructure layer, for instance, she can run her own applications on the resources of a cloud infrastructure and remain responsible for the support, maintenance, and security of these applications herself. If she accesses a service on the application layer, these tasks are normally taken care of by the cloud service provider.

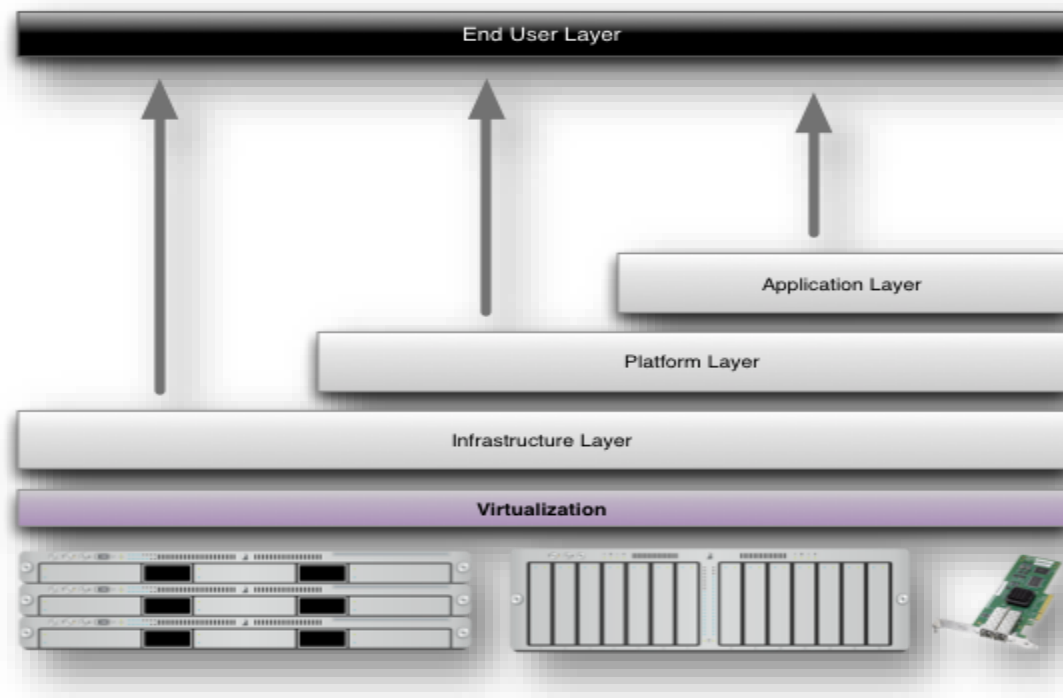


Fig 1.3: Structure of service models

1.4 Benefits of cloud computing:

1. **Achieve economies of scale** – increase volume output or productivity with fewer people. Your cost per unit, project or product plummets.
2. **Reduce spending on technology infrastructure.** Maintain easy access to your information with minimal upfront spending. Pay as you go (weekly, quarterly or yearly), based on demand.
3. **Globalize your workforce on the cheap.** People worldwide can access the cloud, provided they have an Internet connection.
4. **Streamline processes.** Get more work done in less time with less people.
5. **Reduce capital costs.** There's no need to spend big money on hardware, software or licensing fees.
6. **Improve accessibility.** You have access anytime, anywhere, making your life so much easier!
7. **Monitor projects more effectively.** Stay within budget and ahead of completion cycle times.
8. **Less personnel training is needed.** It takes fewer people to do more work on a cloud, with a minimal learning curve on hardware and software issues.
9. **Minimize licensing new software.** Stretch and grow without the need to buy expensive software licenses or programs.
10. **Improve flexibility.** You can change direction without serious “people” or “financial” issues at stake.

1.5 Advantages:

1. **Price:** Pay for only the resources used.
2. **Security:** Cloud instances are isolated in the network from other instances for improved security.
3. **Performance:** Instances can be added instantly for improved performance. Clients have access to the total resources of the Cloud's core hardware.
4. **Scalability:** Auto-deploy cloud instances when needed.
5. **Uptime:** Uses multiple servers for maximum redundancies. In case of server failure, instances can be automatically created on another server.
6. **Control:** Able to login from any location. Server snapshot and a software library lets you deploy custom instances.
7. **Traffic:** Deals with spike in traffic with quick deployment of additional instances to handle the load.

2. LITERATURE SURVEY

2.1. Guidelines on Security and Privacy in Public Cloud Computing

AUTHORS: W. Jansen and T. Grance

Cloud computing can and does mean different things to different people. The common characteristics most interpretations share are on-demand scalability of highly available and reliable pooled computing resources, secure access to metered services from nearly anywhere, and displacement of data and services from inside to outside the organization. While aspects of these characteristics have been realized to a certain extent, cloud computing remains a work in progress. This publication provides an overview of the security and privacy challenges pertinent to public cloud computing and points out considerations organizations should take when outsourcing data, applications, and infrastructure to a public cloud environment.

2.2. Depot: Cloud Storage with Minimal Trust

AUTHORS P. Mahajan, S. Setty, S. Lee, A. Clement, L. Alvisi, M. Dahlin, and M. Walfish,

This article describes the design, implementation, and evaluation of Depot, a cloud storage system that minimizes trust assumptions. Depot tolerates buggy or malicious behavior by any number of clients or servers, yet it provides safety and liveness guarantees to correct clients. Depot provides these guarantees using a two-layer architecture. First, Depot ensures that the updates observed by correct nodes are consistently ordered under Fork-Join-Causal consistency (FJC). FJC is a slight weakening of causal consistency that can be both safe and live despite faulty nodes. Second, Depot implements protocols that use this consistent ordering of updates to provide other desirable consistency, staleness, durability, and recovery properties. Our evaluation suggests that the costs of these guarantees are

modest and that Depot can tolerate faults and maintain good availability, latency, overhead, and staleness even when significant faults occur.

2.3. Providing Database as a Service

AUTHORS H. Hacigüms, B. Iyer, and S. Mehrotra

We explore a novel paradigm for data management in which a third party service provider hosts "database as a service", providing its customers with seamless mechanisms to create, store, and access their databases at the host site. Such a model alleviates the need for organizations to purchase expensive hardware and software, deal with software upgrades, and hire professionals for administrative and maintenance tasks which are taken over by the service provider. We have developed and deployed a database service on the Internet, called NetDB2, which is in constant use. In a sense, a data management model supported by NetDB2 provides an effective mechanism for organizations to purchase data management as a service, thereby freeing them to concentrate on their core businesses. Among the primary challenges introduced by "database as a service" are the additional overhead of remote access to data, an infrastructure to guarantee data privacy, and user interface design for such a service. These issues are investigated. We identify data privacy as a particularly vital problem and propose alternative solutions based on data encryption. The paper is meant as a challenge for the database community to explore a rich set of research issues that arise in developing such a service.

2.4. Fully Homomorphic Encryption Using Ideal Lattices

AUTHORS C. Gentry

We propose a fully homomorphic encryption scheme -- i.e., a scheme that allows one to evaluate circuits over encrypted data without being able to decrypt. Our solution comes in three steps. First, we provide a general result -- that, to construct an encryption scheme that permits evaluation of arbitrary circuits, it suffices to construct an encryption scheme that can evaluate (slightly augmented versions of) its own decryption circuit; we call a scheme that can evaluate its (augmented) decryption circuit bootstrappable.

Next, we describe a public key encryption scheme using ideal lattices that is almost bootstrappable.

Lattice-based cryptosystems typically have decryption algorithms with low circuit complexity, often dominated by an inner product computation that is in NC1. Also, ideal lattices provide both additive and multiplicative homomorphisms (modulo a public-key ideal in a polynomial ring that is represented as a lattice), as needed to evaluate general circuits.

Unfortunately, our initial scheme is not quite bootstrappable -- i.e., the depth that the scheme can correctly evaluate can be logarithmic in the lattice dimension, just like the depth of the decryption circuit, but the latter is greater than the former. In the final step, we show how to modify the scheme to reduce the depth of the decryption circuit, and thereby obtain a bootstrappable encryption scheme, without reducing the depth that the scheme can evaluate. Abstractly, we accomplish this by enabling the encrypter to start the decryption process, leaving less work for the decrypter, much like the server leaves less work for the decrypter in a server-aided cryptosystem.

2.5. Executing SQL over Encrypted Data in the Database-Service-Provider Model

AUTHORS H. Hacigu mu s, B. Iyer, C. Li, and S. Mehrotra

Rapid advances in networking and Internet technologies have fueled the emergence of the "software as a service" model for enterprise computing. Successful examples of commercially viable software services include rent-a-spreadsheet, electronic mail services, general storage services, disaster protection services. "Database as a Service" model provides users power to create, store, modify, and retrieve data from anywhere in the world, as long as they have access to the Internet. It introduces several challenges, an important issue being data privacy. It is in this context that we specifically address the issue of data privacy.

3. SYSTEM ANALYSIS

3.1 EXISTING SYSTEM:

- ❖ Original plain data must be accessible only by trusted parties that do not include cloud providers, intermediaries, and Internet; in any untrusted context, data must be encrypted. Satisfying these goals has different levels of complexity depending on the type of cloud service. There are several solutions ensuring confidentiality for the storage as a service paradigm, while guaranteeing confidentiality in the database as a service (DBaaS) paradigm is still an open research area.

3.2 DISADVANTAGES OF EXISTING SYSTEM:

- ❖ Cannot apply fully homomorphic encryption schemes because of their excessive computational complexity.

3.3 PROPOSED SYSTEM:

- ❖ We propose a novel architecture that integrates cloud database services with data confidentiality and the possibility of executing concurrent operations on encrypted data.
- ❖ This is the first solution supporting geographically distributed clients to connect directly to an encrypted cloud database, and to execute concurrent and independent operations including those modifying the database structure.
- ❖ The proposed architecture has the further advantage of eliminating intermediate proxies that limit the elasticity, availability, and scalability properties that are intrinsic in cloud-based solutions.
- ❖ Secure DBaaS provides several original features that differentiate it from previous work in the field of security for remote database services.

3.4 ADVANTAGES OF PROPOSED SYSTEM:

- ❖ The proposed architecture does not require modifications to the cloud database, and it is immediately applicable to existing cloud DBaaS, such as the experimented PostgreSQL plus Cloud Database, Windows Azure and Xeround.
- ❖ There are no theoretical and practical limits to extend our solution to other platforms and to include new encryption algorithm.
- ❖ It guarantees data confidentiality by allowing a cloud database server to execute concurrent SQL operations (not only read/write, but also modifications to the database structure) over encrypted data.
- ❖ It provides the same availability, elasticity, and scalability of the original cloud DBaaS because it does not require any intermediate server.

3.5 SYSTEM ARCHITECTURE:

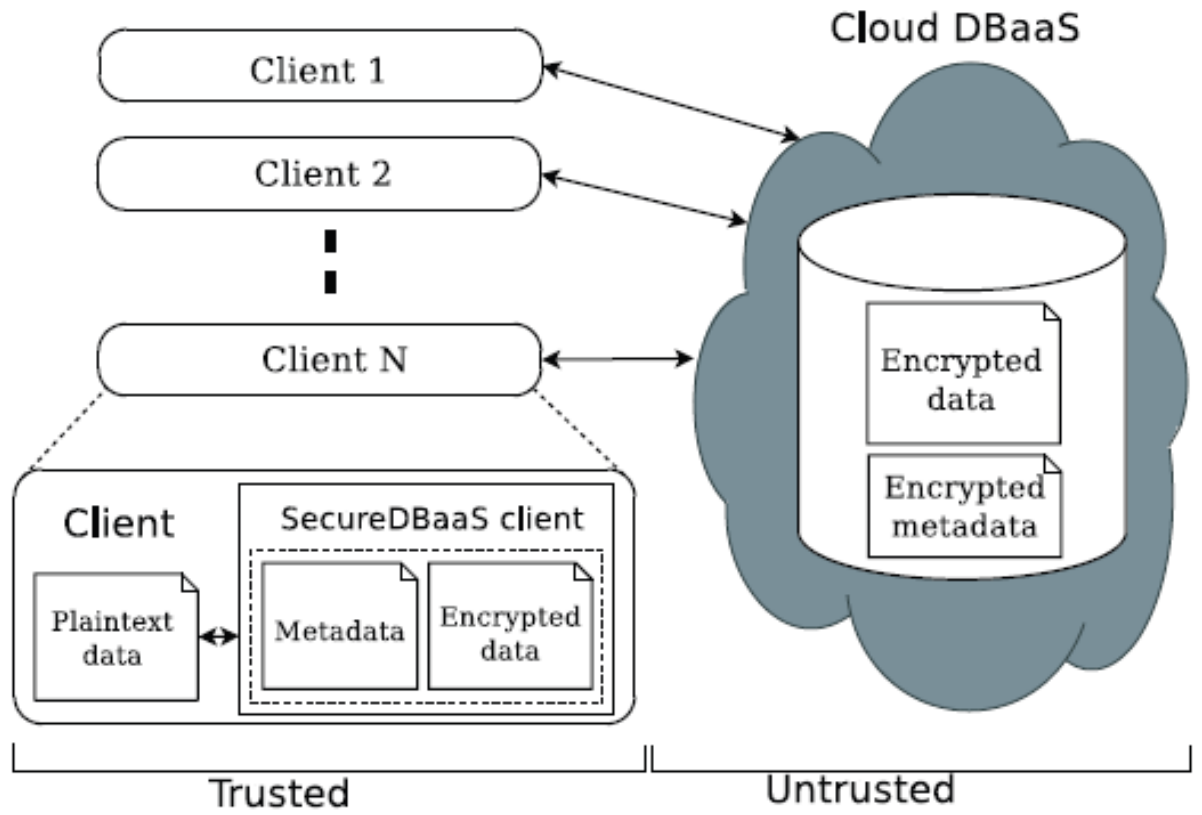


Fig 3.1: System Architecture

3.6 MODULES:

1. Setup Phase
2. Meta Data Module
3. Sequential SQL Operations
4. Concurrent SQL Operations

3.7 MODULES DESCRIPTION:

3.7.1 Setup Phase:

- * We describe how to initialize a Secure DBaaS architecture from a cloud database service acquired by a tenant from a cloud provider.
- * We assume that the DBA creates the metadata storage table that at the beginning contains just the database metadata, and not the table metadata.
- * The DBA populates the database metadata through the Secure DBaaS client by using randomly generated encryption keys for any combinations of data types and encryption types, and stores them in the metadata storage table after encryption through the master key.
- * Then, the DBA distributes the master key to the legitimate users. User access control policies are administrated by the DBA through some standard data control language as in any unencrypted database. In the following steps, the DBA creates the tables of the encrypted database.

3.7.2 Meta Data Module:

- * In this module, we develop Meta data. So our system does not require a trusted broker or a trusted proxy because tenant data and metadata stored by the cloud database are always encrypted.
- * In this module, we design such as Tenant data, data structures, and metadata must be encrypted before exiting from the client.
- * The information managed by SecureDBaaS includes plaintext data, encrypted data, metadata, and encrypted metadata. Plaintext data consist of information that a tenant wants to store and process remotely in the cloud DBaaS.

- * SecureDBaaS clients produce also a set of metadata consisting of information required to encrypt and decrypt data as well as other administration information. Even metadata are encrypted and stored in the cloud DBaaS.

3.7.3 Sequential SQL Operations:

- * The first connection of the client with the cloud DBaaS is for authentication purposes. Secure DBaaS relies on standard authentication and authorization mechanisms provided by the original DBMS server. After the authentication, a user interacts with the cloud database through the Secure DBaaS client.
- * Secure DBaaS analyzes the original operation to identify which tables are involved and to retrieve their metadata from the cloud database. The metadata are decrypted through the master key and their information is used to translate the original plain SQL into a query that operates on the encrypted database.
- * Translated operations contain neither plaintext database (table and column names) nor plaintext tenant data. Nevertheless, they are valid SQL operations that the Secure DBaaS client can issue to the cloud database. Translated operations are then executed by the cloud database over the encrypted tenant data. As there is a one-to-one correspondence between plaintext tables and encrypted tables, it is possible to prevent a trusted database user from accessing or modifying some tenant data by granting limited privileges on some tables.
- * User privileges can be managed directly by the untrusted and encrypted cloud database. The results of the translated query that includes encrypted tenant data and metadata are received by the Secure DBaaS client, decrypted, and delivered to the user. The complexity of the translation process depends on the type of SQL statement.

3.7.4 Concurrent SQL Operations:

- * The support to concurrent execution of SQL statements issued by multiple independent (and possibly geographically distributed) clients is one of the most important benefits of Secure DBaaS with respect to state-of-the-art solutions.
- * Our architecture must guarantee consistency among encrypted tenant data and encrypted metadata because corrupted or out-of-date metadata would prevent clients from decoding encrypted tenant data resulting in permanent data losses.
- * A thorough analysis of the possible issues and solutions related to concurrent SQL operations on encrypted tenant data. Here, we remark the importance of distinguishing two classes of statements that are supported by Secure DBaaS: SQL operations not causing modifications to the database structure, such as read, write, and update; operations involving alterations of the database structure through creation, removal, and modification of database tables (data definition layer operators).

3.8 FEASIBILITY STUDY:

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.

Three key considerations involved in the feasibility analysis are

- ❖ ECONOMICAL FEASIBILITY
- ❖ TECHNICAL FEASIBILITY
- ❖ SOCIAL FEASIBILITY

3.8.1 ECONOMICAL FEASIBILITY:

This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

3.8.2 TECHNICAL FEASIBILITY:

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

3.8.3 SOCIAL FEASIBILITY:

The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he is the final user of the system.

3.9 SOFTWARE REQUIREMENT SPECIFICATION:

Software Requirements Specification plays an important role in creating quality software solutions. Specification is basically a representation process. Requirements are represented in a manner that ultimately leads to successful software implementation.

Requirements may be specified in a variety of ways. However there are some guidelines worth following: -

- ❖ Representation format and content should be relevant to the problem
- ❖ Information contained within the specification should be nested
- ❖ Diagrams and other notational forms should be restricted in number and consistent in use.
- ❖ Representations should be revisable.

Non-Functional Requirements

Non-functional requirements describe user-visible aspects of the system that are not directly related to functionality of the system.

User Interface

A menu interface has been provided to the client to be user friendly.

Documentation

The client is provided with an introductory help about the client interface and the user documentation has been developed through help hyperlink.

Performance Constraints

- ❖ Requests should be processed within no time.
- ❖ Users should be authenticated for accessing the requested data.

Error Handling and Extreme Conditions

In case of User Error, the System should display a meaningful error message to the user, such that the user can correct his Error.

The high level components in proposed system should handle exceptions that occur while connecting to database server, IOExceptions etc.

Quality Issues

Quality issues refer to how reliable, available and robust should the system be? While developing the proposed system the developer must be able to guarantee the reliability transactions so that they will be processed completely and accurately.

3.9.1 SYSTEM REQUIREMENTS:

HARDWARE REQUIREMENTS:

- System : Pentium IV 2.4 GHz.
- Hard Disk : 40 GB.
- Monitor : 15 VGA Colour.
- Ram : 512 Mb.

SOFTWARE REQUIREMENTS:

- Operating system : - Windows XP.
- Coding Language : C#.NET
- Data Base : MS SQL SERVER 2005

4. SYSTEM DESIGN

4. 1 INTRODUCTION:

Design is concerned with identifying software components specifying relationships among components. Specifying software structure and providing blue print for the document phase. Design will explain software components in detail. This will help the implementation of the system. Moreover, this will guide the further changes in the system to satisfy the future requirements. Modularity is one of the desirable properties of large systems. It implies that the system is divided into several parts. In such a manner, the interaction between parts is minimal clearly specified.

4.1.1 UNIFIED MODELING LANGUAGE:

Grady Booch, James Rumbaugh and Ivar Jacobson have collaborated to combine the best features of their individual object oriented analysis and design methods into a unified method the unified modeling language, the version 1.0 for the Unified Modeling was released in January 1997 the main parts of UML are based on the Booch, OMT and OOSE methods.

The goals of UML are

- ❖ To model systems using object-oriented concepts.
- ❖ To establish an explicit coupling between conceptual as well as executable.
- ❖ To address the issues of scale inherent in complex, mission critical system.
- ❖ To create a modeling language usable by both humans and machines.

4.1.2 BASIC BUILDING BLOCKS OF UML:

The basic building blocks in UML are things and relationships; these are combined in different ways following different rules to create different types of diagrams. In UML there are nine types of diagrams, below is a list and brief description of them. The more in depth descriptions in the document, will focus on the first five diagrams in the list, which can be seen as the most general, sometimes also referred to as the UML core diagrams.

- ❖ **Use Case Diagrams:** Shows a set of use cases, and how actors can use them.
- ❖ **Class Diagrams:** Describes the structure of the system, divided in classes with different connections and relationships.
- ❖ **Sequence Diagrams:** Shows the interaction between a set of objects, through the messages that may be dispatched between them.
- ❖ **State Chart Diagrams:** State machines, consisting of states, transitions, events and activities.
- ❖ **Activity Diagrams:** Shows the flow through a program from a defined start point to an end point.
- ❖ **Object Diagrams:** A set of objects and their relationships, this is a snapshot of instances of the things found in the class objects.
- ❖ **Collaboration Diagrams:** Collaboration diagram emphasize structural ordering of objects that send and receive messages.
- ❖ **Component Diagrams:** Shows organizations and dependencies among a set of components. These diagrams address static implementation view of the system.
- ❖ **Deployment Diagrams:** Show the configuration of run-time processing nodes and components that live on them.

4.2 UML DIAGRAMS:

UML stands for Unified Modeling Language. UML is a standardized general-purpose modeling language in the field of object-oriented software engineering. The standard is managed, and was created by, the Object Management Group.

The goal is for UML to become a common language for creating models of object oriented computer software. In its current form UML is comprised of two major components: a Meta-model and a notation. In the future, some form of method or process may also be added to; or associated with, UML.

The Unified Modeling Language is a standard language for specifying, Visualization, Constructing and documenting the artifacts of software system, as well as for business modeling and other non-software systems.

The UML represents a collection of best engineering practices that have proven successful in the modeling of large and complex systems.

The UML is a very important part of developing objects oriented software and the software development process. The UML uses mostly graphical notations to express the design of software projects.

GOALS:

The Primary goals in the design of the UML are as follows:

1. Provide users a ready-to-use, expressive visual modeling Language so that they can develop and exchange meaningful models.
2. Provide extendibility and specialization mechanisms to extend the core concepts.
3. Be independent of particular programming languages and development process.
4. Provide a formal basis for understanding the modeling language.
5. Encourage the growth of OO tools market.
6. Support higher level development concepts such as collaborations, frameworks, patterns and components.
7. Integrate best practices.

4.2.1 USE CASE DIAGRAM:

A use case diagram in the Unified Modeling Language (UML) is a type of behavioral diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted.

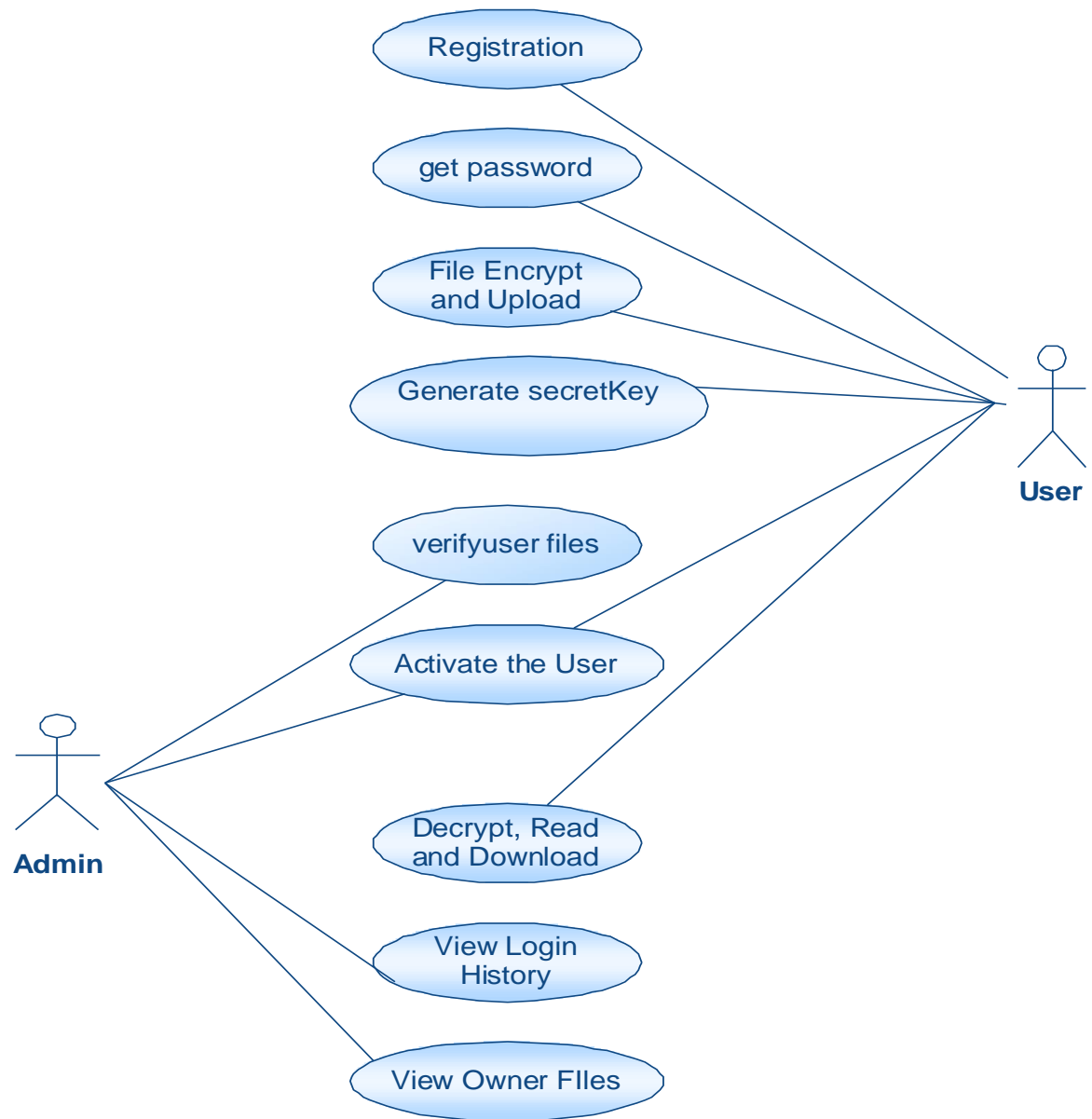


Fig 4.1: Use Case Diagram

4.2.2 CLASS DIAGRAM:

In software engineering, a class diagram in the Unified Modeling Language (UML) is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, operations (or methods), and the relationships among the classes. It explains which class contains information.

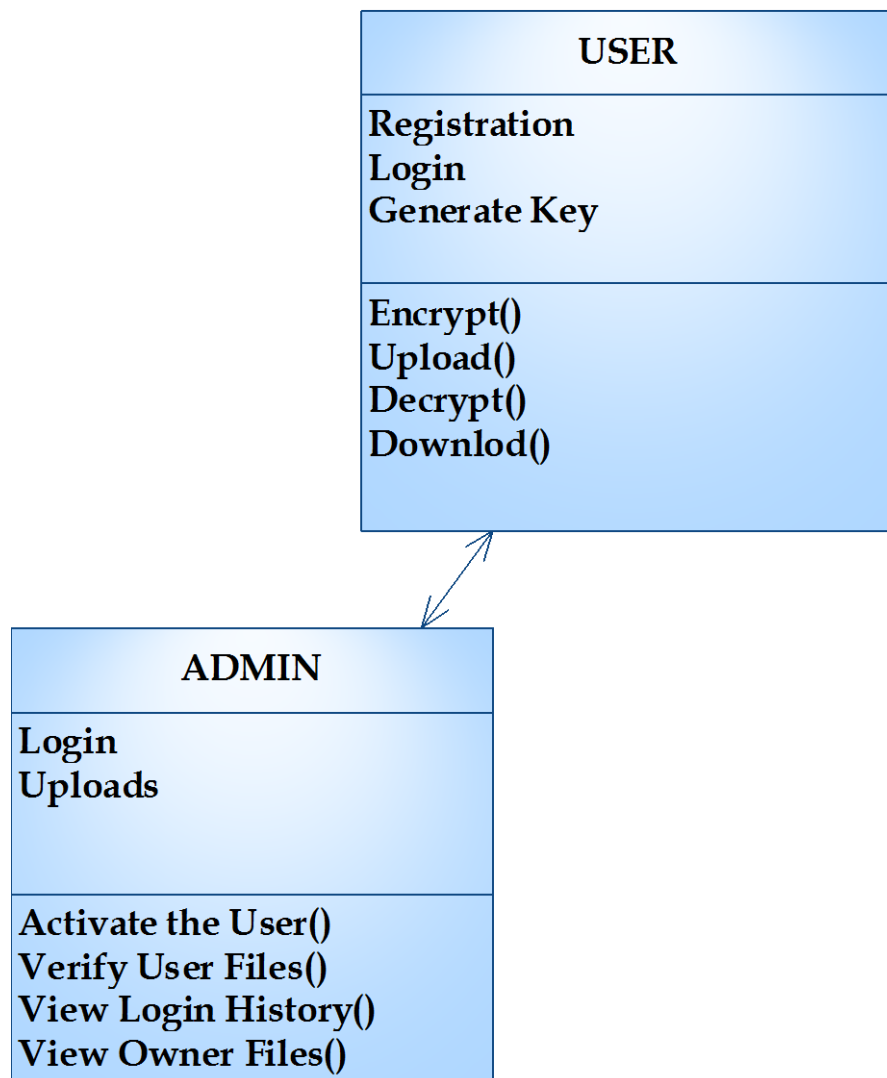


Fig 4.2: Class Diagram

4.2.3 SEQUENCE DIAGRAM:

A sequence diagram in Unified Modeling Language (UML) is a kind of interaction diagram that shows how processes operate with one another and in what order. It is a construct of a Message Sequence Chart. Sequence diagrams are sometimes called event diagrams, event scenarios, and timing diagrams.

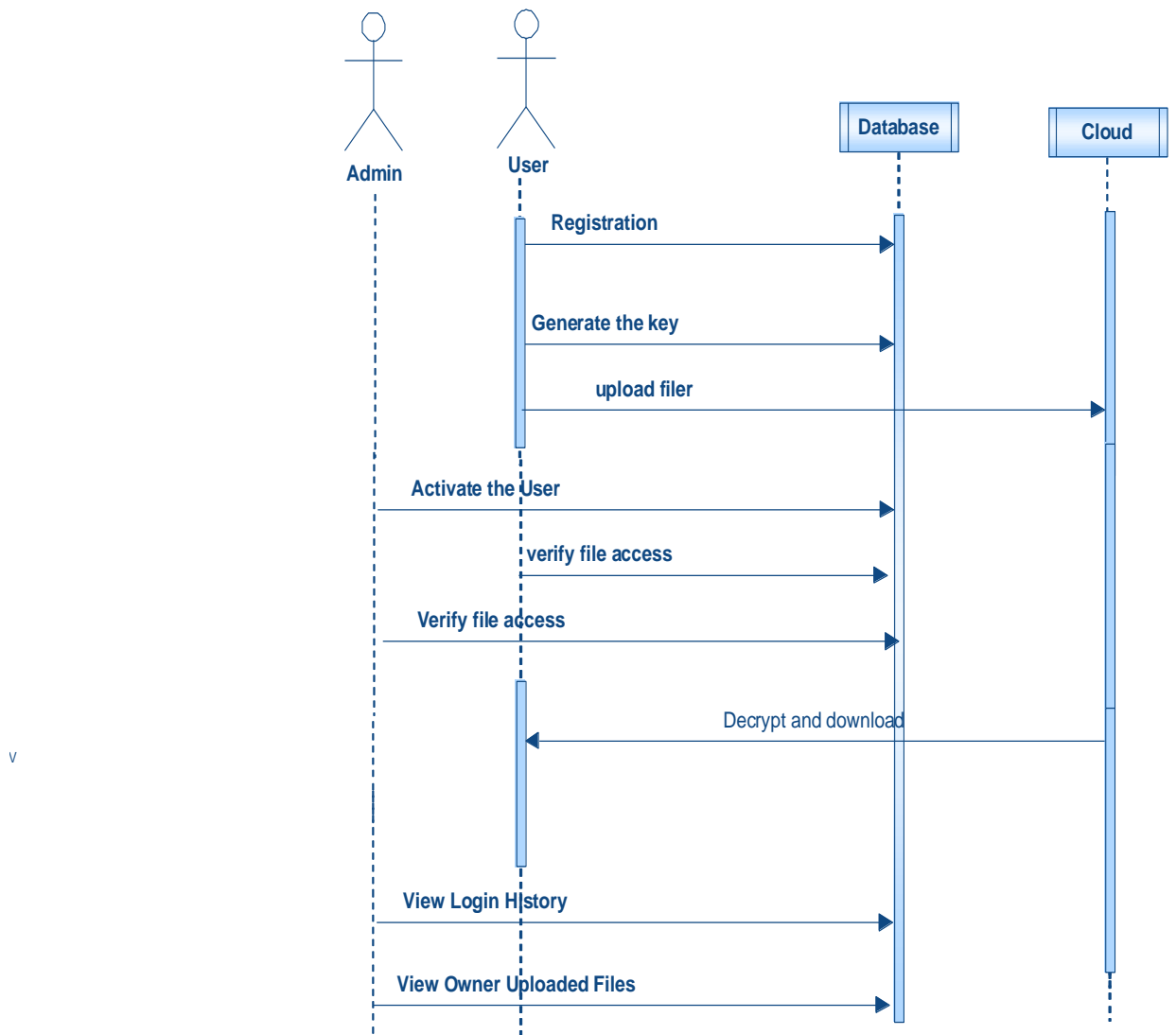


Fig 4.3: Sequence Diagram

4.2.4 ACTIVITY DIAGRAM:

Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. In the Unified Modeling Language, activity diagrams can be used to describe the business and operational step-by-step workflows of components in a system. An activity diagram shows the overall flow of control.

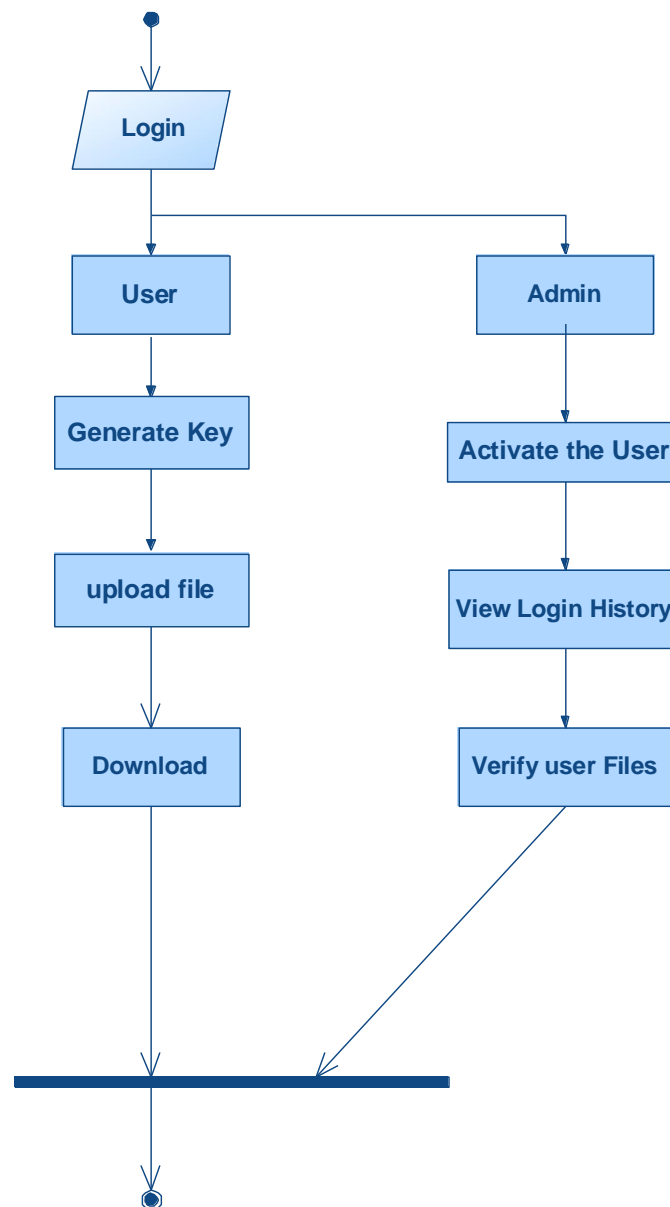


Fig 4.4: Activity Diagram

4.3 DATA FLOW DIAGRAM:

1. The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system.
2. The data flow diagram (DFD) is one of the most important modeling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system.
3. DFD shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations that are applied as data moves from input to output.
4. DFD is also known as bubble chart. A DFD may be used to represent a system at any level of abstraction. DFD may be partitioned into levels that represent increasing information flow and functional detail.

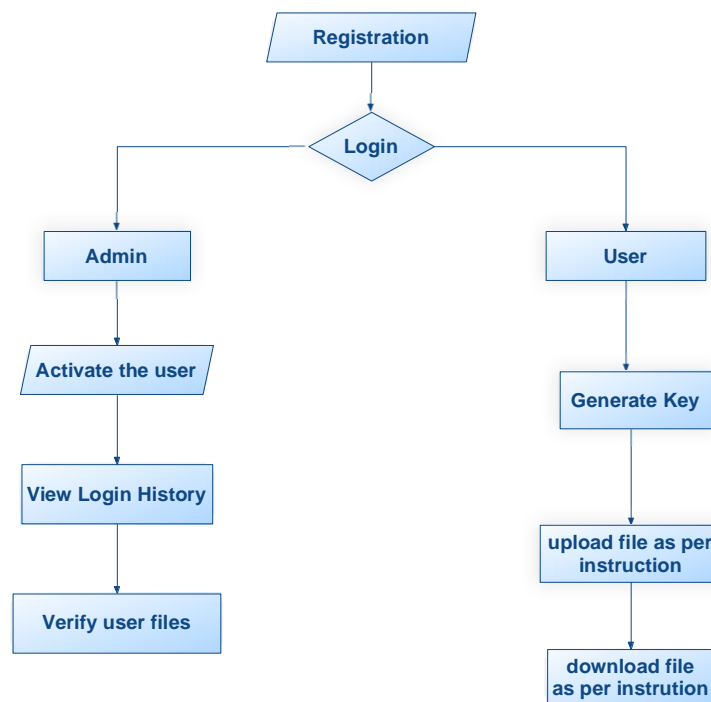


Fig 4.5: Data Flow Diagram

5. IMPLEMENTATION

5.1 Features OF. Net

Microsoft .NET is a set of Microsoft software technologies for rapidly building and integrating XML Web services, Microsoft Windows-based applications, and Web solutions. The .NET Framework is a language-neutral platform for writing programs that can easily and securely interoperate. There's no language barrier with .NET: there are numerous languages available to the developer including Managed C++, C#, Visual Basic and Java Script. The .NET framework provides the foundation for components to interact seamlessly, whether locally or remotely on different platforms. It standardizes common data types and communications protocols so that components created in different languages can easily interoperate.

“.NET” is also the collective name given to various software components built upon the .NET platform. These will be both products (Visual Studio.NET and Windows.NET Server, for instance) and services (like Passport, .NET My Services, and so on).

5.2 THE .NET FRAMEWORK

The .NET Framework has two main parts:

1. The Common Language Runtime (CLR).
2. A hierarchical set of class libraries.

The CLR is described as the “execution engine” of .NET. It provides the environment within which programs run. The most important features are

- ❖ Conversion from a low-level assembler-style language, called Intermediate Language (IL), into code native to the platform being executed on.
- ❖ Memory management, notably including garbage collection.
- ❖ Checking and enforcing security restrictions on the running code.
- ❖ Loading and executing programs, with version control and other such features.

The following features of the .NET framework are also worth description:

Managed Code:

The code that targets .NET, and which contains certain extra Information - “metadata” - to describe itself. Whilst both managed and unmanaged code can run in the runtime, only managed code contains the information that allows the CLR to guarantee, for instance, safe execution and interoperability.

Managed Data:

With Managed Code comes Managed Data. CLR provides memory allocation and Deallocation facilities, and garbage collection. Some .NET languages use Managed Data by default, such as C#, Visual Basic.NET and JScript.NET, whereas others, namely C++, do not. Targeting CLR can, depending on the language you’re using, impose certain constraints on the features available. As with managed and unmanaged code, one can have both managed and unmanaged data in .NET applications - data that doesn’t get garbage collected but instead is looked after by unmanaged code.

Common Type System:

The CLR uses something called the Common Type System (CTS) to strictly enforce type-safety. This ensures that all classes are compatible with each other, by describing types in a common way. CTS define how types work within the runtime, which enables types in one language to interoperate with types in another language, including cross-language exception handling. As well as ensuring that types are only used in appropriate ways, the runtime also ensures that code doesn’t attempt to access memory that hasn’t been allocated to it.

Common Language Specification:

The CLR provides built-in support for language interoperability. To ensure that you can develop managed code that can be fully used by developers using any programming language, a set of language features and rules for using them called the Common Language Specification (CLS) has been defined. Components that follow these rules and expose only CLS features are considered CLS-compliant.

5.3 THE CLASS LIBRARY

.NET provides a single-rooted hierarchy of classes, containing over 7000 types. The root of the namespace is called System; this contains basic types like Byte, Double, Boolean, and String, as well as Object. All objects derive from System. Object. As well as objects, there are value types. Value types can be allocated on the stack, which can provide useful flexibility. There are also efficient means of converting value types to object types if and when necessary.

The set of classes is pretty comprehensive, providing collections, file, screen, and network I/O, threading, and so on, as well as XML and database connectivity.

The class library is subdivided into a number of sets (or namespaces), each providing distinct areas of functionality, with dependencies between the namespaces kept to a minimum.

5.4 LANGUAGES SUPPORTED BY .NET

The multi-language capability of the .NET Framework and Visual Studio .NET enables developers to use their existing programming skills to build all types of applications and XML Web services. The .NET framework supports new versions of Microsoft's old favorites Visual Basic and C++ (as VB.NET and Managed C++), but there are also a number of new additions to the family.

Visual Basic .NET has been updated to include many new and improved language features that make it a powerful object-oriented programming language. These features include inheritance, interfaces, and overloading, among others. Visual Basic also now supports structured exception handling, custom attributes and also supports multi-threading.

Visual Basic .NET is also CLS compliant, which means that any CLS-compliant language can use the classes, objects, and components you create in Visual Basic .NET.

Managed Extensions for C++ and attributed programming are just some of the enhancements made to the C++ language. Managed Extensions simplify the task of migrating existing C++ applications to the new .NET Framework.

C# is Microsoft's new language. It's a C-style language that is essentially "C++ for Rapid Application Development".

Unlike other languages, its specification is just the grammar of the language. It has no standard library of its own, and instead has been designed with the intention of using the .NET libraries as its own.

Microsoft Visual J# .NET provides the easiest transition for Java-language developers into the world of XML Web Services and dramatically improves the interoperability of Java-language programs with existing software written in a variety of other programming languages.

Active State has created Visual Perl and Visual Python, which enable .NET-aware applications to be built in either Perl or Python. Both products can be integrated into the Visual Studio .NET environment. Visual Perl includes support for Active State's Perl Dev Kit.

Other languages for which .NET compilers are available include

- FORTRAN
- COBOL
- Eiffel

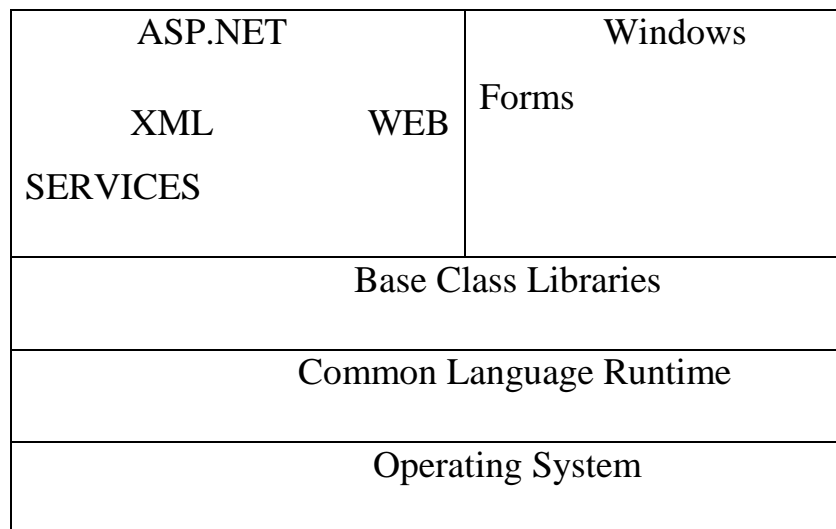


Fig 5.1: .Net Framework

C#.NET is also compliant with CLS (Common Language Specification) and supports structured exception handling. CLS is set of rules and constructs that are supported by the CLR (Common Language Runtime). CLR is the runtime environment provided by the .NET Framework; it manages the execution of the code and also makes the development process easier by providing services.

C#.NET is a CLS-compliant language. Any objects, classes, or components that created in C#.NET can be used in any other CLS-compliant language. In addition, we can use objects, classes, and components created in other CLS-compliant languages in C#.NET. The use of CLS ensures complete interoperability among applications, regardless of the languages used to create the application.

CONSTRUCTORS AND DESTRUCTORS:

Constructors are used to initialize objects, whereas destructors are used to destroy them. In other words, destructors are used to release the resources allocated to the object. In C#.NET the sub finalize procedure is available. The sub finalize procedure is used to complete the tasks that must be performed when an object is destroyed. The sub finalize procedure is called automatically when an object is destroyed. In addition, the sub finalize procedure can be called only from the class it belongs to or from derived classes.

GARBAGE COLLECTION:

Garbage Collection is another new feature in C#.NET. The .NET Framework monitors allocated resources, such as objects and variables. In addition, the .NET Framework automatically releases memory for reuse by destroying objects that are no longer in use.

In C#.NET, the garbage collector checks for the objects that are not currently in use by applications. When the garbage collector comes across an object that is marked for garbage collection, it releases the memory occupied by the object.

OVERLOADING:

Overloading is another feature in C#. Overloading enables us to define multiple procedures with the same name, where each procedure has a different set of arguments. Besides using overloading for procedures, we can use it for constructors and properties in a class.

MULTITHREADING:

C#.NET also supports multithreading. An application that supports multithreading can handle multiple tasks simultaneously, we can use multithreading to decrease the time taken by an application to respond to user interaction.

STRUCTURED EXCEPTION HANDLING:

C#.NET supports structured handling, which enables us to detect and remove errors at runtime. In C#.NET, we need to use Try...Catch...Finally statements to create exception handlers. Using Try...Catch...Finally statements, we can create robust and effective exception handlers to improve the performance of our application.

THE .NET FRAMEWORK:

The .NET Framework is a new computing platform that simplifies application development in the highly distributed environment of the Internet.

OBJECTIVES OF .NET FRAMEWORK:

1. To provide a consistent object-oriented programming environment whether object codes is stored and executed locally on Internet-distributed, or executed remotely.
2. To provide a code-execution environment to minimizes software deployment and guarantees safe execution of code.
3. Eliminates the performance problems.

There are different types of application, such as Windows-based applications and Web-based applications.

5.5 Features of SQL-SERVER

The OLAP Services feature available in SQL Server version 7.0 is now called SQL Server 2000 Analysis Services. The term OLAP Services has been replaced with the term Analysis Services. Analysis Services also includes a new data mining component. The Repository component available in SQL Server version 7.0 is now called Microsoft SQL Server 2000 Meta Data Services. References to the component now use the term Meta Data Services. The term repository is used only in reference to the repository engine within Meta Data Services

SQL-SERVER database consist of six type of objects,

They are,

1. TABLE
2. QUERY
3. FORM
4. REPORT
5. MACRO

TABLE:

A database is a collection of data about a specific topic.

VIEWS OF TABLE:

We can work with a table in two types,

1. Design View
2. Datasheet View

Design View:

To build or modify the structure of a table we work in the table design view. We can specify what kind of data will be hold.

Datasheet View:

To add, edit or analyses the data itself we work in tables datasheet view mode.

QUERY:

A query is a question that has to be asked the data. Access gathers data that answers the question from one or more table. The data that make up the answer is either dynaset (if you edit it) or a snapshot (it cannot be edited). Each time we run query, we get latest information in the dynaset. Access either displays the dynaset or snapshot for us to view or perform an action on it, such as deleting or updating.

5.6 INPUT DESIGN

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things:

- ❖ What data should be given as input?
- ❖ How the data should be arranged or coded?
- ❖ The dialog to guide the operating personnel in providing input.
- ❖ Methods for preparing input validations and steps to follow when error occur.

OBJECTIVES:

1. Input Design is the process of converting a user-oriented description of the input into a computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system.
2. It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities.
3. When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so that the user will not be in maize of instant. Thus the objective of input design is to create an input layout that is easy to follow.

5.7 OUTPUT DESIGN

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

1. Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.

2. Select methods for presenting information.
3. Create document, report, or other formats that contain information produced by the system.

The output form of an information system should accomplish one or more of the following objectives.

- ❖ Convey information about past activities, current status or projections of the
- ❖ Future.
- ❖ Signal important events, opportunities, problems, or warnings.
- ❖ Trigger an action.
- ❖ Confirm an action.

5.8 SAMPLE CODE:

Main page.master

```
<% @ Master Language="C#" AutoEventWireup="true" CodeFile="Mainpage.master.cs"
Inherits="Mainpage" %>
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
```

```
<html xmlns="http://www.w3.org/1999/xhtml">
<head runat="server">
  <title>Main Page</title>
  <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
  <script src="App/js/arial.js" type="text/javascript"></script>
  <link href="App/style.css" rel="stylesheet" type="text/css" />
  <script src="App/js/cufon-yui.js" type="text/javascript"></script>
  <script src="App/js/cuf_run.js" type="text/javascript"></script>
</head>
<body>
  <div class="main">

    <div class="header">
      <div class="header_resize">
        <div class="menu_nav">
          <ul>
```

```

        <li class="active"><a href="Home.aspx">HOME</a></li>
        <li><a href="clientlogin.aspx">CLIENT</a></li>
        <li><a href="cloud.aspx">CLOUD DBaaS</a></li>
    </ul>
    <div class="clr"></div>
</div>
<div class="clr"></div>
<div class="logo"><h1>Distributed, Concurrent, and Independent Access to
Encrypted Cloud Databases</h1></div>
</div>
</div>

<div class="content">
    <div class="content_resize">
        <div class="mainbar">
            <form id="form1" runat="server">
                <div>
                    <asp:ContentPlaceHolder id="ContentPlaceHolder1" runat="server">

                        </asp:ContentPlaceHolder>
                    </div>
                </form>
            </div>
            <div class="sidebar">
                <div class="gadget">
                    <h2 class="star">Menu</h2>
                    <ul class="sb_menu">
                        <li><a href="Home.aspx">Home</a></li>
                        <li><a href="clientlogin.aspx">Client</a></li>
                        <li><a href="cloud.aspx">cloud DBaaS</a></li>
                    </ul>
                </div>
                <div class="gadget">
                    </div>
            </div>
            <div class="clr"></div>
        </div>
    </div>

<div class="footer">
</div>
</div>
</body>
</html>

```

Client_login.aspx

```
<% @ Page Language="C#" AutoEventWireup="true" CodeFile="clientlogin.aspx.cs"
Inherits="clientlogin" %>
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
```

```
<html xmlns="http://www.w3.org/1999/xhtml">
<head runat="server">
  <title>Client Login</title>
  <link href="App/style.css" rel="stylesheet" type="text/css" />
  <script src="App/js/cufon-yui.js" type="text/javascript"></script>
  <script src="App/js/cuf_run.js" type="text/javascript"></script>
  <script src="App/js/arial.js" type="text/javascript"></script>
  <style type="text/css">
    .style1
    {
      height: 32px;
    }
  </style>
</head>
<body>
  <div class="main">

    <div class="header">
      <div class="header_resize">
        <div class="menu_nav">
          <ul>
            <li><a href="Home.aspx">HOME</a></li>
            <li class="active"><a href="clientlogin.aspx">Login</a></li>
          </ul>
          <div class="clr"></div>
        </div>
        <div class="clr"></div>
        <div class="logo"><h1>Distributed, Concurrent, and Independent Access to
Encrypted Cloud Databases</h1></div>
      </div>
    </div>

    <div class="content">
      <br />
      <br />
      <br />
      <div class="content_resize">
        <div class="mainbar">
          <form id="form1" runat="server">
```

```
</div>
<center>

    <asp:Label ID="Label3" runat="server" Text="Client Login" Font-Bold="True"
        Font-Names="Californian FB" Font-Size="XX-Large"
ForeColor="#0099CC"></asp:Label>
    <br />
    <br />
    <table><tr><td><table align="center">
<tr><td class="style1"></td><td class="style1">
    <asp:Label ID="Label1" runat="server" Text="User Name :" Font-Bold="True"
        Font-Size="Large" Font-Names="Californian FB"></asp:Label></td>
    <td class="style1">
        <asp:TextBox ID="TextBox1" runat="server" Height="28px"
            Width="196px"></asp:TextBox></td></tr>
    <tr><td></td><td></td><td></td></tr>
<tr><td></td><td>
    <asp:Label ID="Label2" runat="server" Text="Password :" Font-Bold="True"
        Font-Size="Large" Font-Names="Californian FB"></asp:Label></td><td>
    <asp:TextBox ID="TextBox2" runat="server" Height="29px"
        Width="195px" TextMode="Password"></asp:TextBox></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td>&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&~
&nbsp;&nbsp;&nbsp;&nbsp;&~
    <asp:Button ID="Button1" runat="server" Text="Login" Font-Bold="False" Font-
Size="Medium" Height="35px"
        Width="75px" Font-Names="Californian FB" onclick="Button1_Click" />
        </td><td>

&nbsp;&nbsp;&nbsp;&nbsp;&~
&nbsp;&nbsp;&~
    <asp:Button ID="Button2" runat="server" Text="Clear" Font-Bold="False"
        Font-Size="Medium" Height="35px"
        Width="75px" Font-Names="Californian FB" onclick="Button2_Click" />
    </td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
    <tr><td></td><td>
        <asp:LinkButton ID="LinkButton1" runat="server"
onclick="LinkButton1_Click"
            Font-Names="Arial Narrow" Font-Size="Medium">Click Here to
Register</asp:LinkButton>
        </td><td>
&nbsp;&nbsp;&~</td></tr></table></td></tr></table>
```



```

        <br />
        <br />
        <br />
        <br />
        <br />
    </center>
</div>
</form>
</div>
<div class="sidebar">
    <div class="gadget">
        <h2 class="star">Menu</h2>
        <ul class="sb_menu">
            <li><a href="Home.aspx">Home</a></li>
            <li><a href="#">Client</a></li>
            <li><a href="#">Cloud Database</a></li>
        </ul>
    </div>
    <div class="gadget">
    </div>
    <div class="clr"></div>
</div>

<div class="footer">
</div>
</div>
</body>
</html>

```

Client_login.aspx.cs

```

using System;
using System.Collections;
using System.Configuration;
using System.Data;
using System.Linq;
using System.Web;
using System.Web.Security;
using System.Web.UI;
using System.Web.UI.HtmlControls;
using System.Web.UI.WebControls;
using System.Web.UI.WebControls.WebParts;
using System.Xml.Linq;

```

```
using System.Data.SqlClient;
```

```
public partial class clientlogin : System.Web.UI.Page
{
    SqlConnection con = new
    SqlConnection(System.Configuration.ConfigurationManager.ConnectionStrings["con"].
    ConnectionString);
    protected void Page_Load(object sender, EventArgs e)
    {

    }
    protected void Button1_Click(object sender, EventArgs e)
    {
        if (TextBox1.Text != "" && TextBox2.Text != "")
        {
            string uname = TextBox1.Text;
            string pwd = TextBox2.Text;
            con.Open();
            string str1 = "SELECT username,password FROM register WHERE username="
+ TextBox1.Text + """;

            SqlDataAdapter objadapter = new SqlDataAdapter(str1, con);
            DataSet dataset = new DataSet();
            objadapter.Fill(dataset, "register");
            DataTable datatable = dataset.Tables[0];
            for (int i = 0; i < datatable.Rows.Count; i++)
            {
                string unam1 = datatable.Rows[i]["username"].ToString();
                string upwd1 = datatable.Rows[i]["password"].ToString();

                if (((unam1.Trim() == uname) && (upwd1.Trim() == pwd)))
                {
                    Page.ClientScript.RegisterStartupScript(this.GetType(), "Message",
                    "alert('Login Successfull...');window.location="" + "client" + ".aspx";", true);
                }
                else
                {
                    Response.Write("<script>alert('Check Your Name and
                    Password...')</script>");
                }
                Session["name"] = TextBox1.Text;
            }
        }
        else
        {
```

```

        Response.Write("<script>alert('Please Enter Your username and
Password...')</script>");
    }
}
protected void LinkButton1_Click(object sender, EventArgs e)
{
    Response.Redirect("register.aspx");
}
protected void Button2_Click(object sender, EventArgs e)
{
    TextBox1.Text = "";
    TextBox2.Text = "";
}
}

```

Cloud.aspx

```

<% @ Page Language="C#" AutoEventWireup="true" CodeFile="cloud.aspx.cs"
Inherits="cloud" %>

```

```

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

```

```

<html xmlns="http://www.w3.org/1999/xhtml">
<head runat="server">
    <title>Cloud Service</title>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <script src="App/js/arial.js" type="text/javascript"></script>
    <link href="App/style.css" rel="stylesheet" type="text/css" />
    <script src="App/js/cufon-yui.js" type="text/javascript"></script>
    <script src="App/js/cuf_run.js" type="text/javascript"></script>
</head>
<body>
<div class="main">

    <div class="header">
        <div class="header_resize">
            <div class="menu_nav">
                <ul>
                    <li class="active"><a href="Home.aspx">HOME</a></li>
                    <li><a href="cloud.aspx">LOGIN</a></li>
                </ul>
                <div class="clr"></div>
            </div>
            <div class="clr"></div>

```

```

    <div class="logo"><h1>Distributed, Concurrent, and Independent Access to
    Encrypted Cloud Databases</h1></div>
  </div>
</div>

<div class="content">
  <div class="content_resize">
    <div class="mainbar">
      <form id="form1" runat="server">
        <div>
          <center> <table><tr><td><table align="center" cellpadding="10"
          bgcolor="#CCCCCC">
            <tr><td></td></tr>
            <asp:Label ID="Label3" runat="server" Text="Cloud Login" Font-Bold="True"
            Font-Names="Californian FB" Font-Size="XX-Large"
            ForeColor="#0099CC"></asp:Label></td></tr>
            <tr><td></td><td></td><td></td><td></td></tr>
            <tr><td></td><td></td>
            <asp:Label ID="Label1" runat="server" Text="Cloud Name : " Font-Bold="True"
            Font-Size="Large" Font-Names="Californian FB"></asp:Label></td><td>
            <asp:TextBox ID="TextBox1" runat="server" Height="28px"
            Width="134px"></asp:TextBox></td><td> <asp:RequiredFieldValidator
            ID="RV1" runat="server" ControlToValidate="TextBox1"
            SetFocusOnError="True" ErrorMessage="*" Font-Size="X-
            Large"></asp:RequiredFieldValidator></td></tr>
            <tr><td></td><td></td><td></td><td></td></tr>
            <tr><td></td><td></td>
            <asp:Label ID="Label2" runat="server" Text="Password : " Font-Bold="True"
            Font-Size="Large" Font-Names="Californian FB"></asp:Label></td><td>
            <asp:TextBox ID="TextBox2" runat="server" Height="29px"
            Width="136px" TextMode="Password"></asp:TextBox></td><td>
            <asp:RequiredFieldValidator ID="RequiredFieldValidator1" runat="server"
            ControlToValidate="TextBox2"
            SetFocusOnError="True" ErrorMessage="*" Font-Size="X-
            Large"></asp:RequiredFieldValidator></td></tr>
            <tr><td></td><td></td><td></td><td></td></tr>
            <tr><td></td><td></td><td></td>
            <asp:Button ID="Button1" runat="server"
            Text="Login" Font-Bold="False" Font-Size="Medium" Height="35px"
            Width="75px" Font-Names="Californian FB" onclick="Button1_Click" />
            </td><td></td></tr></table></td><td>
            <asp:Image ID="Image1" runat="server"
            ImageUrl="~/App/images/cloudrarch.png"
            Height="305px" /></td></tr></table>
          </center>
        </div>
      </form>
    </div>
  </div>
</div>

```

```

</form>
</div>
<div class="sidebar">
  <div class="gadget">
    <h2 class="star">Menu</h2>
    <ul class="sb_menu">
      <li><a href="Home.aspx">Home</a></li>
      <li><a href="clientlogin.aspx">Client</a></li>
      <li><a href="cloud.aspx">cloud DBaaS</a></li>
    </ul>
  </div>
  <div class="gadget">
  </div>
</div>
<div class="clr"></div>
</div>
</div>

<div class="footer">
</div>
</div>
</body>
</html>

```

Cloud.aspx

```

<% @ Page Language="C#" AutoEventWireup="true" CodeFile="cloud.aspx.cs"
Inherits="cloud" %>

```

```

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

```

```

<html xmlns="http://www.w3.org/1999/xhtml">
<head runat="server">
  <title>Cloud Service</title>
  <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
  <script src="App/js/arial.js" type="text/javascript"></script>
  <link href="App/style.css" rel="stylesheet" type="text/css" />
  <script src="App/js/cufon-yui.js" type="text/javascript"></script>
  <script src="App/js/cuf_run.js" type="text/javascript"></script>
</head>
<body>
<div class="main">

  <div class="header">
    <div class="header_resize">

```

```

<div class="menu_nav">
  <ul>
    <li class="active"><a href="Home.aspx">HOME</a></li>
    <li><a href="cloud.aspx">LOGIN</a></li>
  </ul>
  <div class="clr"></div>
</div>
<div class="clr"></div>
<div class="logo"><h1>Distributed, Concurrent, and Independent Access to
Encrypted Cloud Databases</h1></div>
</div>
</div>

<div class="content">
  <div class="content_resize">
    <div class="mainbar">
      <form id="form1" runat="server">
        <div>
          <center> <table><tr><td><table align="center" cellpadding="10"
bgcolor="#CCCCCC">
          <tr><td></td><td>
            <asp:Label ID="Label3" runat="server" Text="Cloud Login" Font-Bold="True"
              Font-Names="Calibri" Font-Size="XX-Large"
              ForeColor="#0099CC"></asp:Label></td></tr>
            <tr><td></td><td></td><td></td><td></td><td></td></tr>
            <tr><td></td><td>
              <asp:Label ID="Label1" runat="server" Text="Cloud Name : " Font-Bold="True"
                Font-Size="Large" Font-Names="Calibri"></asp:Label></td><td>
                <asp:TextBox ID="TextBox1" runat="server" Height="28px"
                  Width="134px"></asp:TextBox></td><td> <asp:RequiredFieldValidator
                  ID="RV1" runat="server" ControlToValidate="TextBox1"
                    SetFocusOnError="True" ErrorMessage="*" Font-Size="X-
                    Large"></asp:RequiredFieldValidator></td></tr>
            <tr><td></td><td></td><td></td><td></td><td></td></tr>
            <tr><td></td><td>
              <asp:Label ID="Label2" runat="server" Text="Password : " Font-Bold="True"
                Font-Size="Large" Font-Names="Calibri"></asp:Label></td><td>
                <asp:TextBox ID="TextBox2" runat="server" Height="29px"
                  Width="136px" TextMode="Password"></asp:TextBox></td><td>
                <asp:RequiredFieldValidator ID="RequiredFieldValidator1" runat="server"
                  ControlToValidate="TextBox2"
                    SetFocusOnError="True" ErrorMessage="*" Font-Size="X-
                    Large"></asp:RequiredFieldValidator></td></tr>
            <tr><td></td><td></td><td></td><td></td><td></td></tr>
            <tr><td></td><td></td><td></td><td>
              <asp:Button ID="Button1" runat="server"

```

```

        Text="Login" Font-Bold="False" Font-Size="Medium" Height="35px"
        Width="75px" Font-Names="Californian FB" onclick="Button1_Click" />
    </td><td></td></tr></table></td><td>
        <asp:Image ID="Image1" runat="server"
ImageUrl="~/App/images/cloudrarch.png"
        Height="305px" /></td></tr></table>
    </center>
</div>
</form>
</div>
<div class="sidebar">
    <div class="gadget">
        <h2 class="star">Menu</h2>
        <ul class="sb_menu">
            <li><a href="Home.aspx">Home</a></li>
            <li><a href="clientlogin.aspx">Client</a></li>
            <li><a href="cloud.aspx">cloud DBaaS</a></li>
        </ul>
    </div>
    <div class="gadget">
    </div>
</div>
<div class="clr"></div>
</div>

<div class="footer">
</div>
</div>
</body>
</html>

```

CloudDBaaS.aspx

```

<% @ Page Language="C#" AutoEventWireup="true" CodeFile="cloudDBaaS.aspx.cs"
Inherits="cloudDBaaS" %>

```

```

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

```

```

<html xmlns="http://www.w3.org/1999/xhtml">
<head runat="server">
    <title>cloud DBaaS</title>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <script src="App/js/arial.js" type="text/javascript"></script>
    <link href="App/style.css" rel="stylesheet" type="text/css" />

```

```

    <script src="App/js/cufon-yui.js" type="text/javascript"></script>
    <script src="App/js/cuf_run.js" type="text/javascript"></script>
</head>
<body>
    <div class="main">

<div class="header">
    <div class="header_resize">
        <div class="menu_nav">
            <ul>
                <li><a href="Home.aspx">HOME</a></li>
                <li><a href="clientlogin.aspx">CLIENT</a></li>
                <li class="active"><a href="cloudDBaaS.aspx">cloud DBaaS</a></li>
            </ul>
            <div class="clr"></div>
        </div>
        <div class="clr"></div>
        <div class="logo"><h1>Distributed, Concurrent, and Independent Access to
Encrypted Cloud Databases</h1></div>
    </div>
</div>

<div class="content">
    <div class="content_resize">
        <div class="mainbar">
            <form id="form1" runat="server">
                <div>
                    <center>
                        <h2>View Cloud DBaaS</h2>
                        <asp:GridView ID="GridView1" runat="server" AutoGenerateColumns="False"
Font-Names="Calisto MT" Font-Size="Medium"
                        HorizontalAlign="Center" Width="656px" Height="151px"
DataSourceID="SqlDataSource1">
                            <Columns>
                                <asp:BoundField DataField="ID" HeaderText="ID" SortExpression="ID"
                                    ItemStyle-Width="50px" ItemStyle-VerticalAlign="Top" >
<ItemStyle VerticalAlign="Top" Width="50px"></ItemStyle>
                                </asp:BoundField>

                                <asp:BoundField DataField="enyfile" HeaderText="File Name"
                                    SortExpression="enyfile" ItemStyle-Width="50px"
                                    ItemStyle-VerticalAlign="Top" >
<ItemStyle VerticalAlign="Top" Width="50px"></ItemStyle>
                                </asp:BoundField>
                                <asp:BoundField DataField="enfname" HeaderText="File"
                                    SortExpression="enfname" ItemStyle-Width="50px"

```



```

        ItemStyle-VerticalAlign="Top" >
<ItemStyle VerticalAlign="Top" Width="50px"></ItemStyle>
        </asp:BoundField>

        <asp:TemplateField HeaderText="Meta Data">
            <ItemTemplate>
                <asp:TextBox ID="TextBox1" runat="server" Text='<%#
Eval("metadata") %>' ReadOnly="true"></asp:TextBox>
            </ItemTemplate>
        </asp:TemplateField>
    </Columns>
    <PagerStyle Font-Names="Calisto MT" Font-Size="Small"
HorizontalAlign="Center"
        VerticalAlign="Top" />
    <HeaderStyle BackColor="#00BBEA" Font-Names="Calisto MT" Font-
Size="Medium" />
    <EditRowStyle Font-Bold="True" Font-Size="Medium" />
    <AlternatingRowStyle BackColor="#D7F7FF" />
</asp:GridView>
        <asp:SqlDataSource ID="SqlDataSource1" runat="server"
            ConnectionString="<%=
ConnectionStrings:DistributedConnectionString3 %>"
            SelectCommand="SELECT [ID], [enfile], [metadata], [enfname]
FROM [upload]">
        </asp:SqlDataSource>
        <br />
    </center>

</div>
</form>
</div>
<div class="sidebar">
    <div class="gadget">
        <h2 class="star">Menu</h2>
        <ul class="sb_menu">
            <li><a href="Home.aspx">Home</a></li>
            <li><a href="clientlogin.aspx">Client</a></li>
            <li><a href="cloud.aspx">cloud DBaaS</a></li>
        </ul>
    </div>
    <div class="gadget">
    </div>
</div>
<div class="clr"></div>
</div>
</div>

```

```
<div class="footer">  
</div>  
</div>  
</body>  
</html>
```

6. SYSTEM TESTING

6.1 Introduction

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub assemblies, assemblies and/or a finished product it is the process of exercising software with the intent of ensuring that the Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

6.1.1 Testing Strategies

A strategy for software testing may also be viewed in the context of the spiral. Unit testing begins at the vertex of the spiral and concentrates on each unit of the software as implemented in source code. Testing progress by moving outward along the spiral to integration testing,

Here focus is on the design and construction of software architecture. Talking another turn on outward on the spiral we encounter validation testing where requirements established as part of software requirements analysis are validated against the software that has been constructed. Finally we arrive at system testing, where the software and other system elements are tested as a whole.

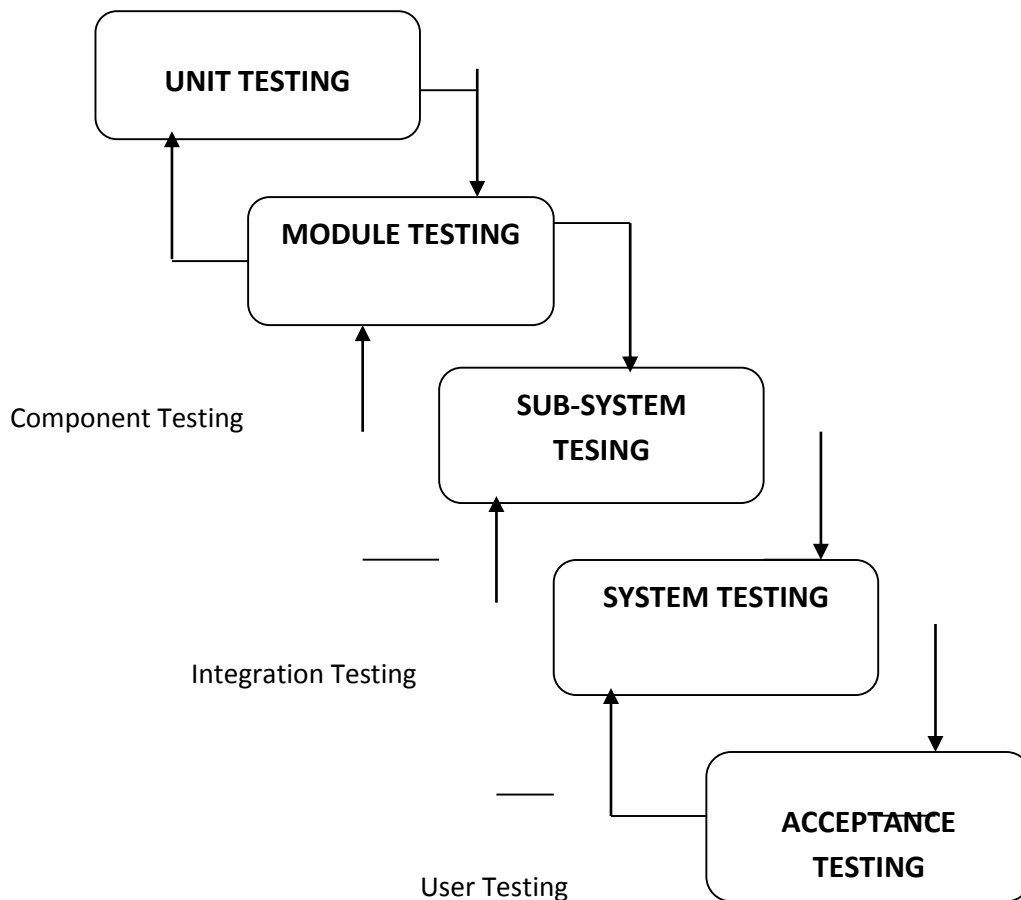


Fig 6.1: Testing Strategies

❖ Unit testing:

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program inputs produce valid outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application. It is done after the completion of an individual unit before integration. This is a structural testing, that relies on knowledge of its construction and is invasive. Unit tests perform basic tests at component level and test a specific business process, application, and/or system configuration. Unit tests ensure that each unique path of a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.

Unit testing is usually conducted as part of a combined code and unit test phase of the software lifecycle, although it is not uncommon for coding and unit testing to be conducted as two distinct phases.

Test strategy and approach

Field testing will be performed manually and functional tests will be written in detail.

Test objectives

- All field entries must work properly.
- Pages must be activated from the identified link.
- The entry screen, messages and responses must not be delayed.

Features to be tested

- Verify that the entries are of the correct format
- No duplicate entries should be allowed
- All links should take the user to the correct page.

❖ Integration testing:

Integration tests are designed to test integrated software components to determine if they actually run as one program. Testing is event driven and is more concerned with the basic outcome of screens or fields. Integration tests demonstrate that although the components were individually satisfaction, as shown by successfully unit testing, the combination of components is correct and consistent. Integration testing is specifically aimed at exposing the problems that arise from the combination of components.

Software integration testing is the incremental integration testing of two or more integrated software components on a single platform to produce failures caused by interface defects.

The task of the integration test is to check that components or software applications, e.g. components in a software system or – one step up – software applications at the company level – interact without error.

Test Results: All the test cases mentioned above passed successfully. No defects encountered.

❖ **Functional test:**

Functional tests provide systematic demonstrations that functions tested are available as specified by the business and technical requirements, system documentation, and user manuals.

Functional testing is centered on the following items:

Valid Input : identified classes of valid input must be accepted.

Invalid Input : identified classes of invalid input must be rejected.

Functions : identified functions must be exercised.

Output : identified classes of application outputs must be exercised.

Systems/Procedures: interfacing systems or procedures must be invoked.

Organization and preparation of functional tests is focused on requirements, key functions, or special test cases. In addition, systematic coverage pertaining to identify Business process flows; data fields, predefined processes, and successive processes must be considered for testing. Before functional testing is complete, additional tests are identified and the effective value of current tests is determined.

❖ **System Test:**

System testing ensures that the entire integrated software system meets requirements. It tests a configuration to ensure known and predictable results. An example of system testing is the configuration oriented system integration test. System testing is based on process descriptions and flows, emphasizing pre-driven process links and integration points.

❖ White Box Testing:

White Box Testing is a testing in which the software tester has knowledge of the inner workings, structure and language of the software, or at least its purpose. It is used to test areas that cannot be reached from a black box level.

❖ Black Box Testing:

Black Box Testing is testing the software without any knowledge of the inner workings, structure or language of the module being tested. Black box tests, as most other kinds of tests, must be written from a definitive source document, such as specification or requirements document. It is a testing in which the software under test is treated, as a black box .you cannot “see” into it. The test provides inputs and responds to outputs without considering how the software works.

❖ Acceptance Testing:

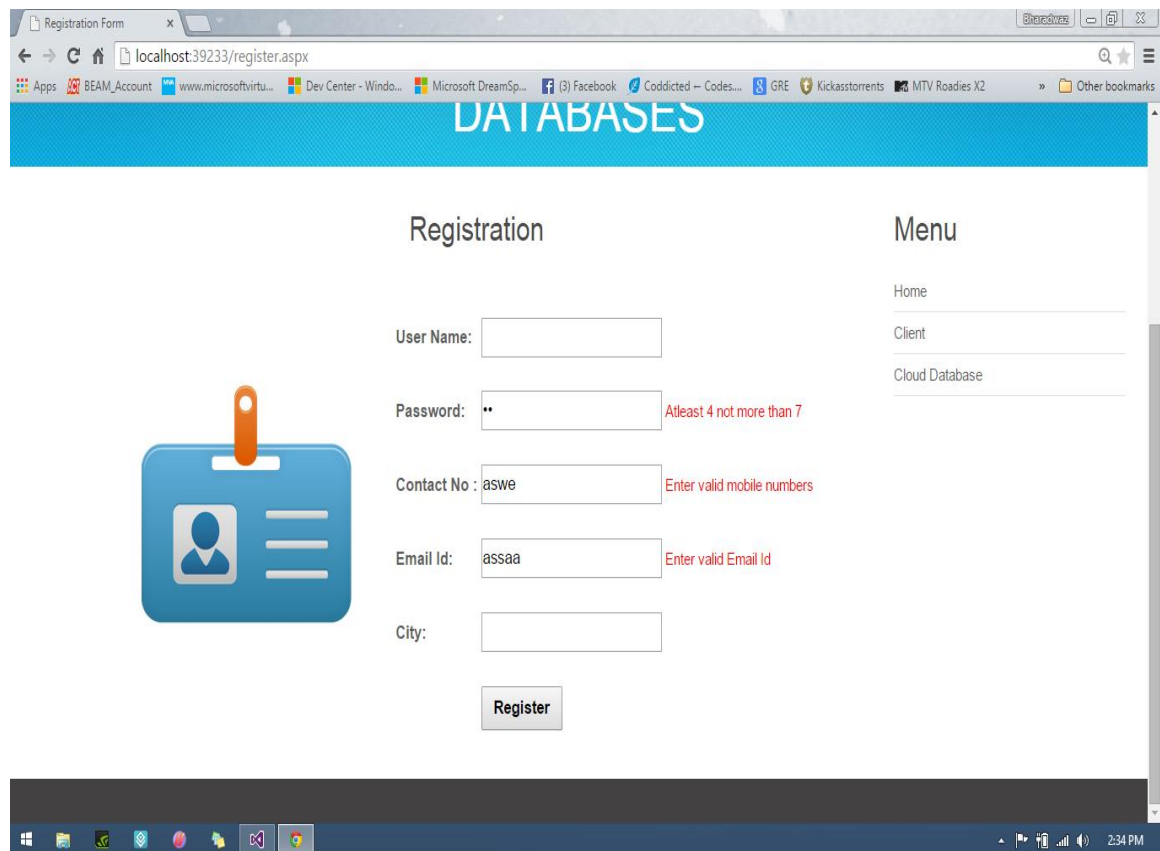
User Acceptance Testing is a critical phase of any project and requires significant participation by the end user. It also ensures that the system meets the functional requirements.

Test Results: All the test cases mentioned above passed successfully. No defects encountered.

6.2 Test Cases

❖ Negative Test Case:

In this negative test case let us consider the scenario of a false registration or a blank attempt to register a user. This case is overcome by the attempt to validate the respective fields.



The screenshot shows a web browser window with the address bar displaying 'localhost:39233/register.aspx'. The page has a blue header with the word 'DATABASES' in white. Below the header, there is a 'Registration' section on the left and a 'Menu' section on the right. The 'Registration' section contains a blue icon of a person with a checkmark, followed by input fields for 'User Name:', 'Password:', 'Contact No:', 'Email Id:', and 'City:'. The 'Password:' field has a red error message 'Atleast 4 not more than 7'. The 'Contact No:' field has a red error message 'Enter valid mobile numbers'. The 'Email Id:' field has a red error message 'Enter valid Email Id'. A 'Register' button is located below the 'City:' field. The 'Menu' section contains links for 'Home', 'Client', and 'Cloud Database'. The browser's taskbar at the bottom shows various application icons and the system clock indicating 2:34 PM.

Fig 6.2.1: Register Form validation

Let us consider another scenario of a false login or a blank attempt to login a user. This case is overcome by the attempt to validate the respective fields.

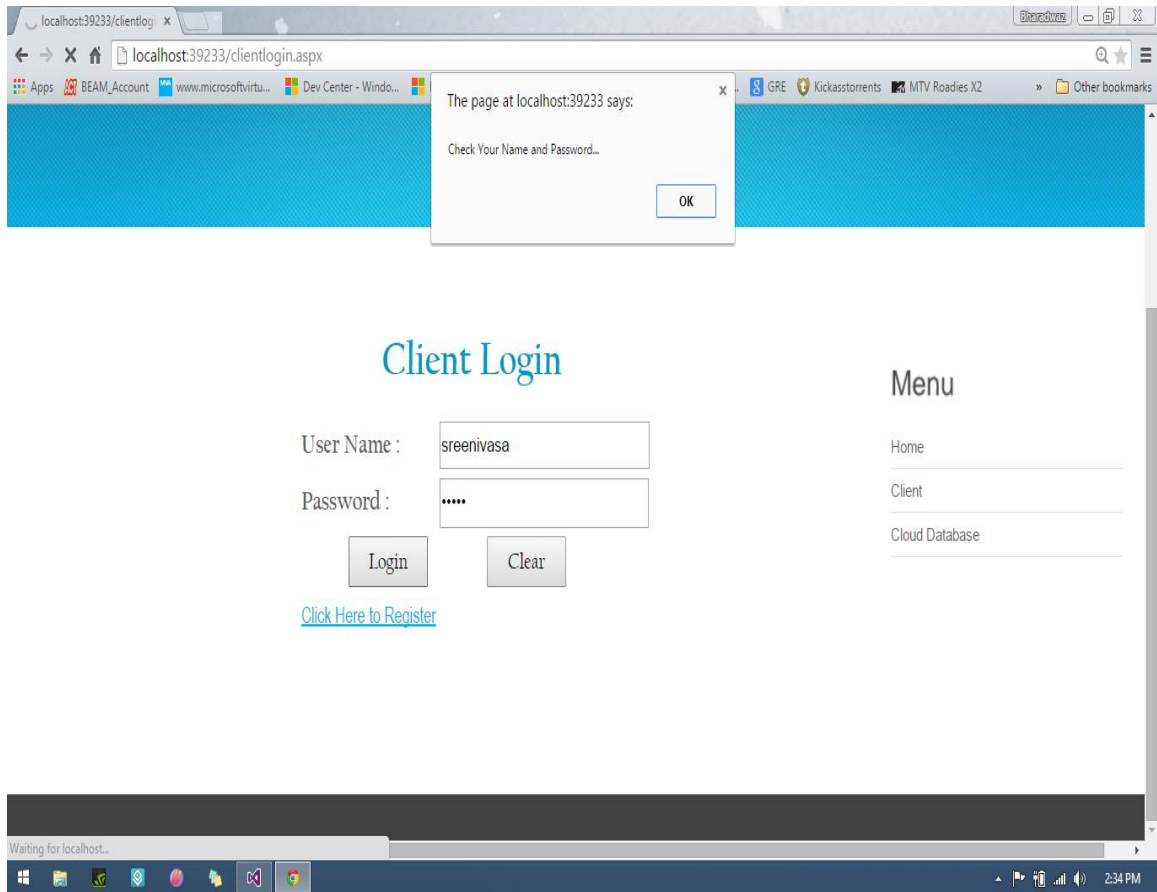


Fig 6.2.2: Login Form validation

❖ Positive Test Case:

Let us consider a case in the successful login of an user to show the positive test case of our program.

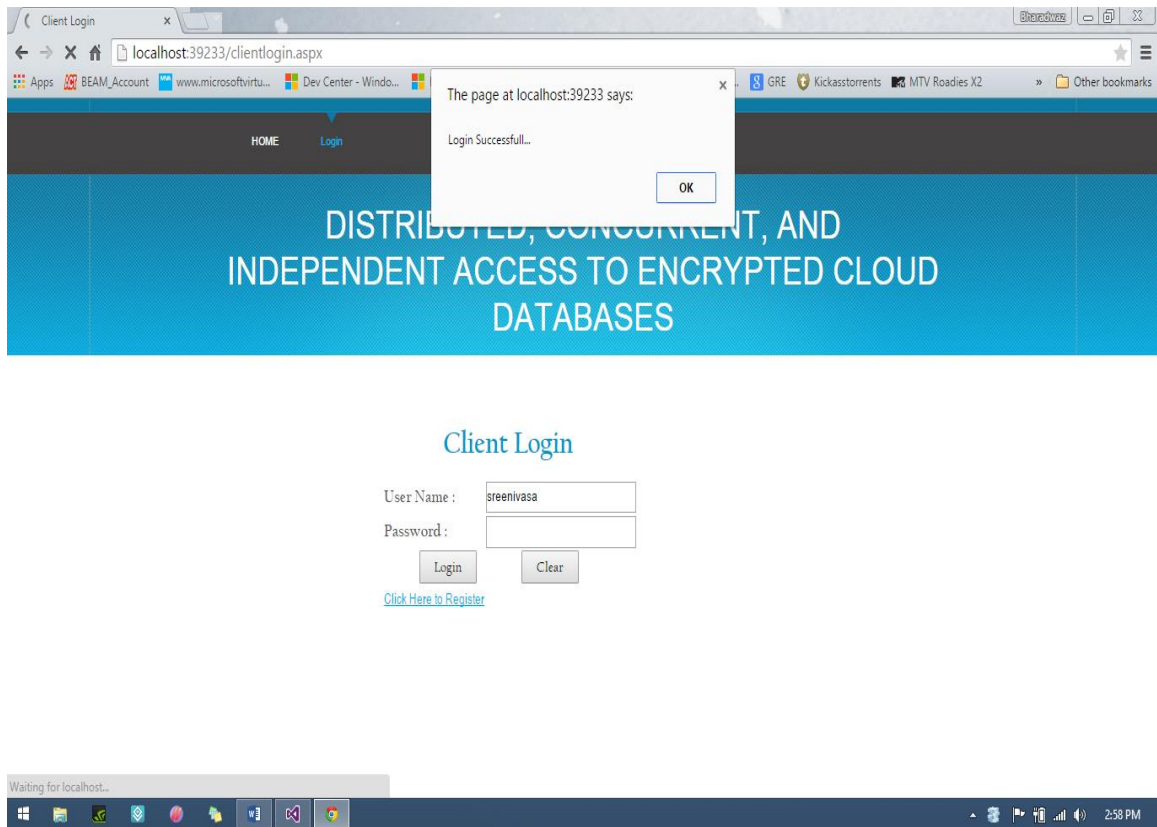


Fig 6.2.3: Login Successful

7. RESULTS

7.1 SCREEN SHOTS:

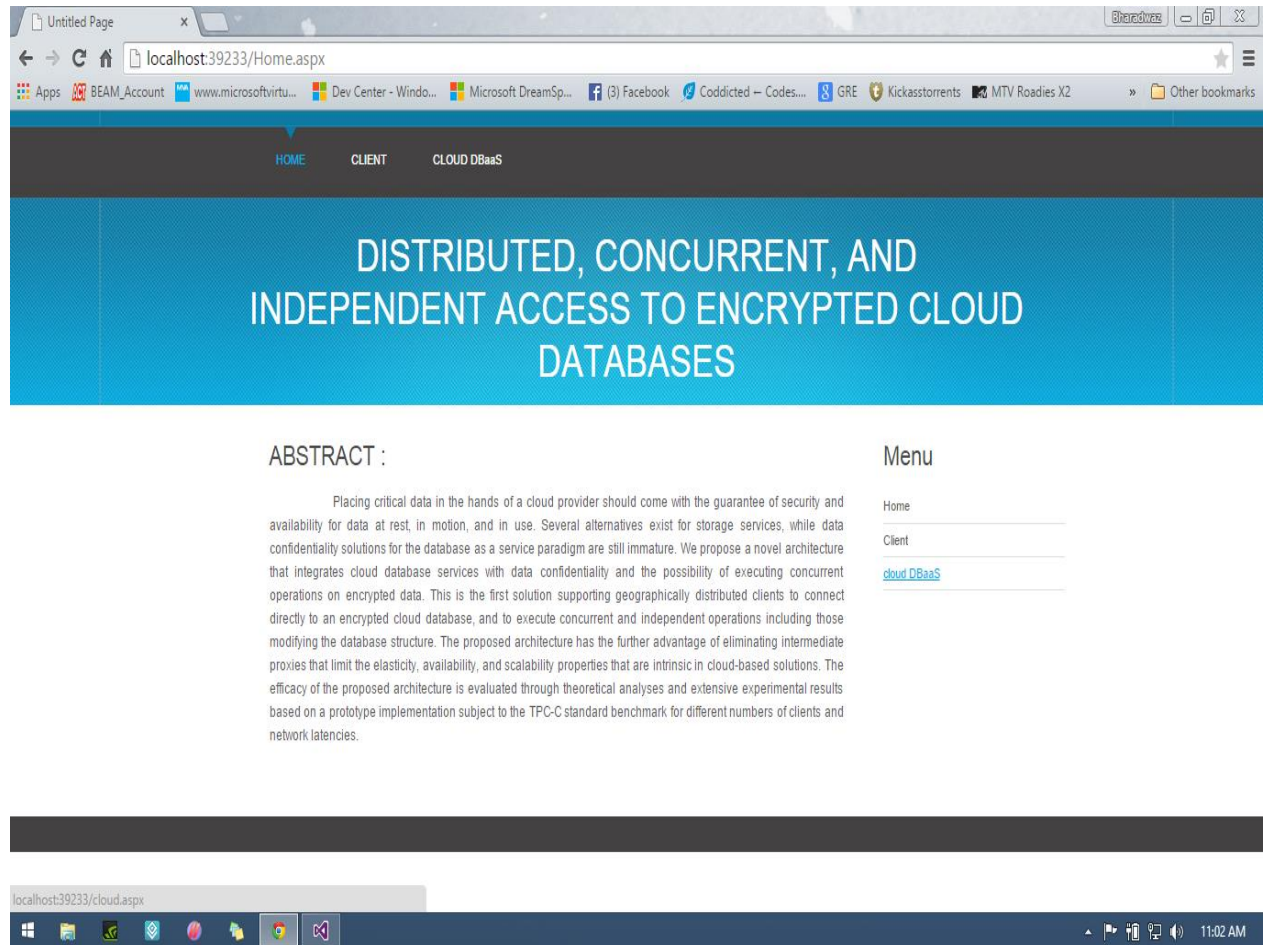


Fig 7.1: Home Page

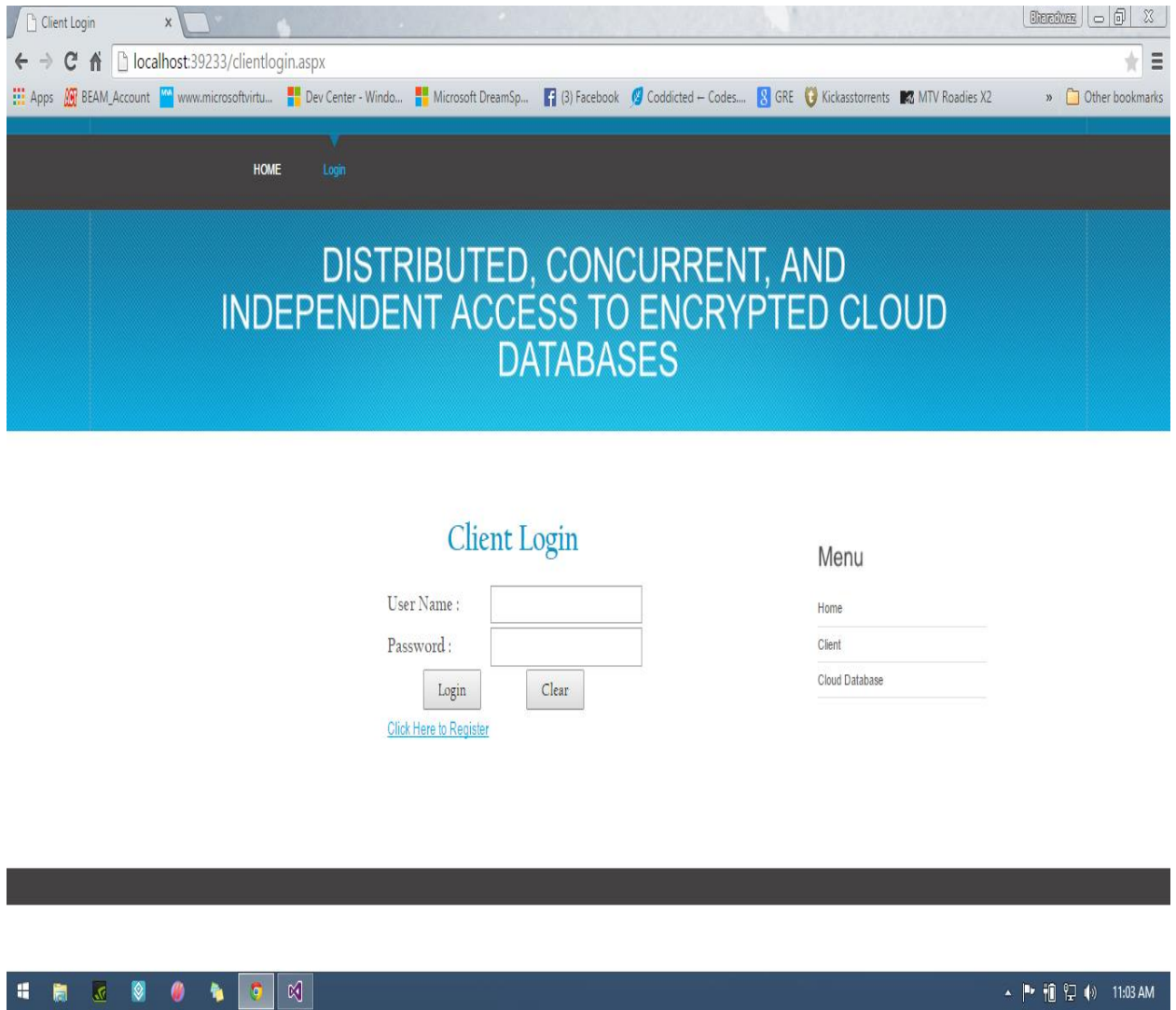


Fig 7.2: Client Login

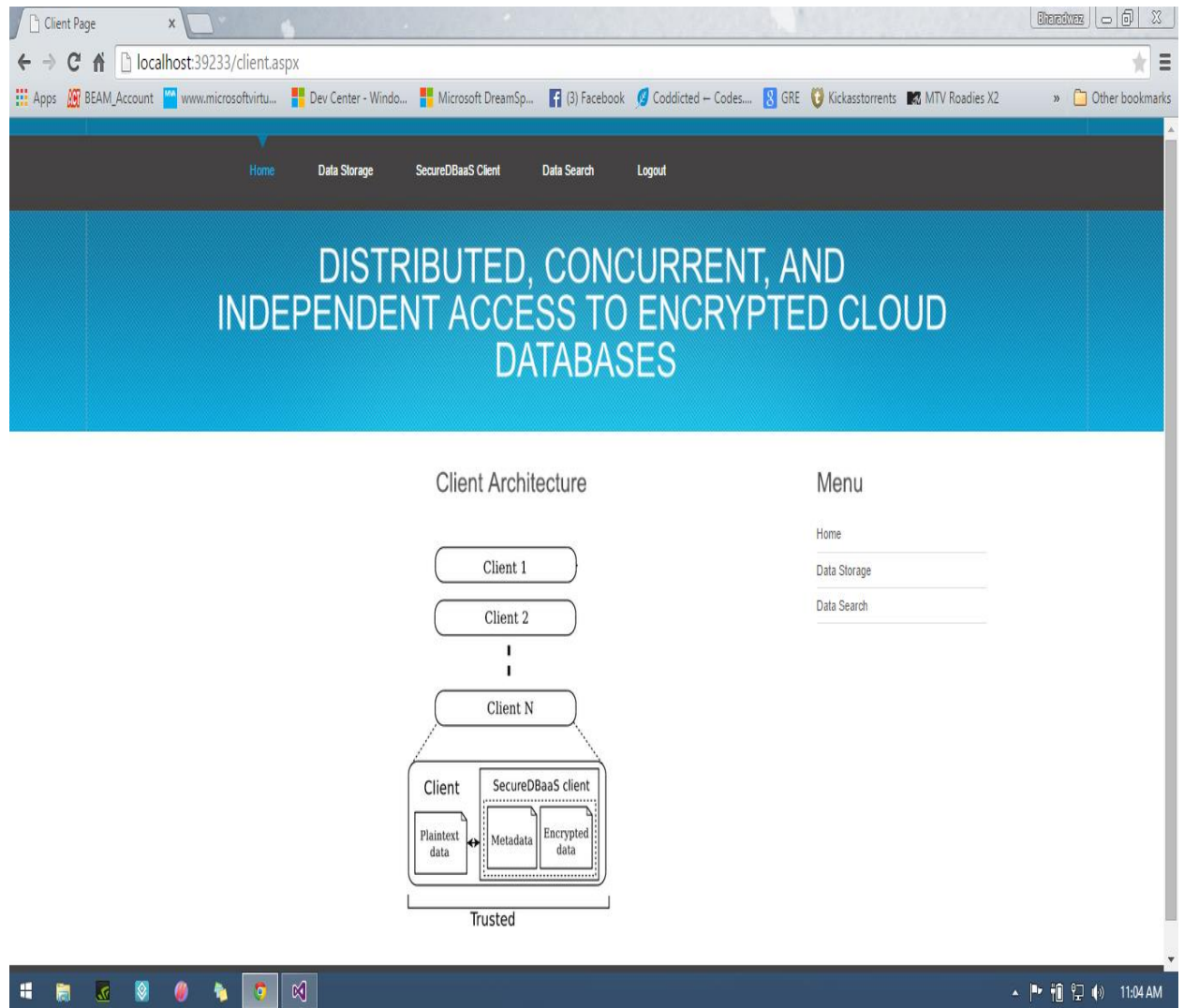


Fig 7.3: Client Home Page

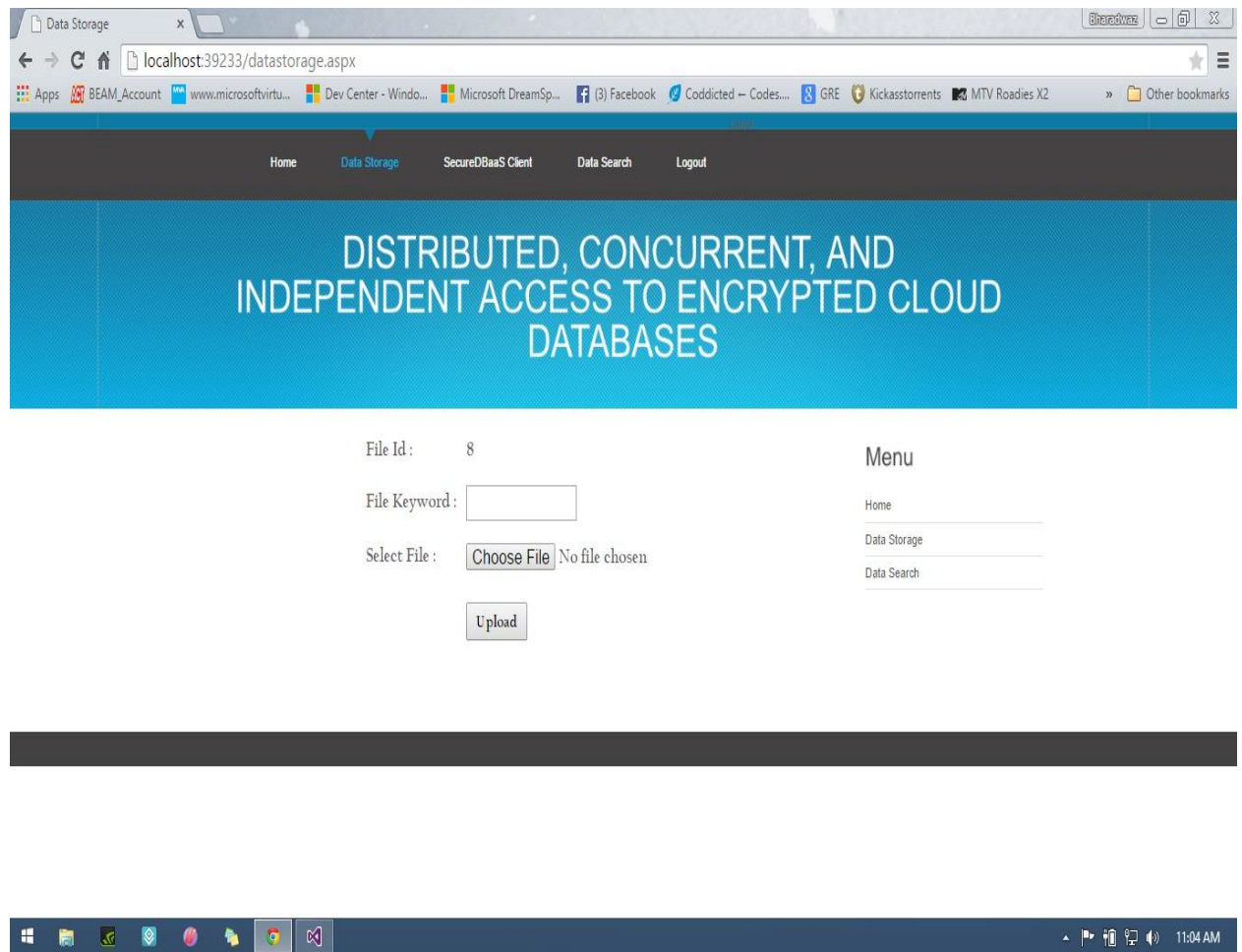


Fig 7.4: Client Upload (Empty)

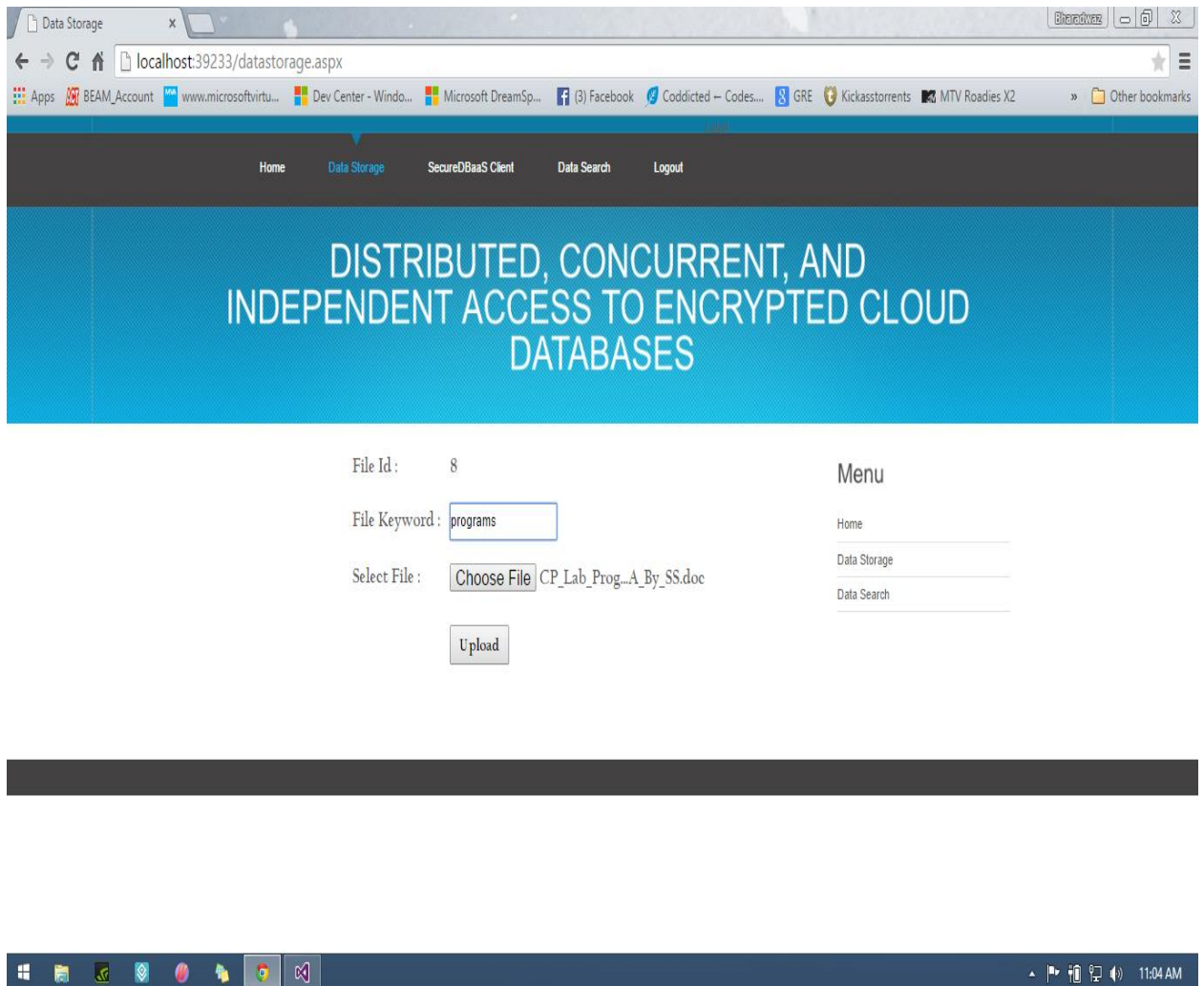
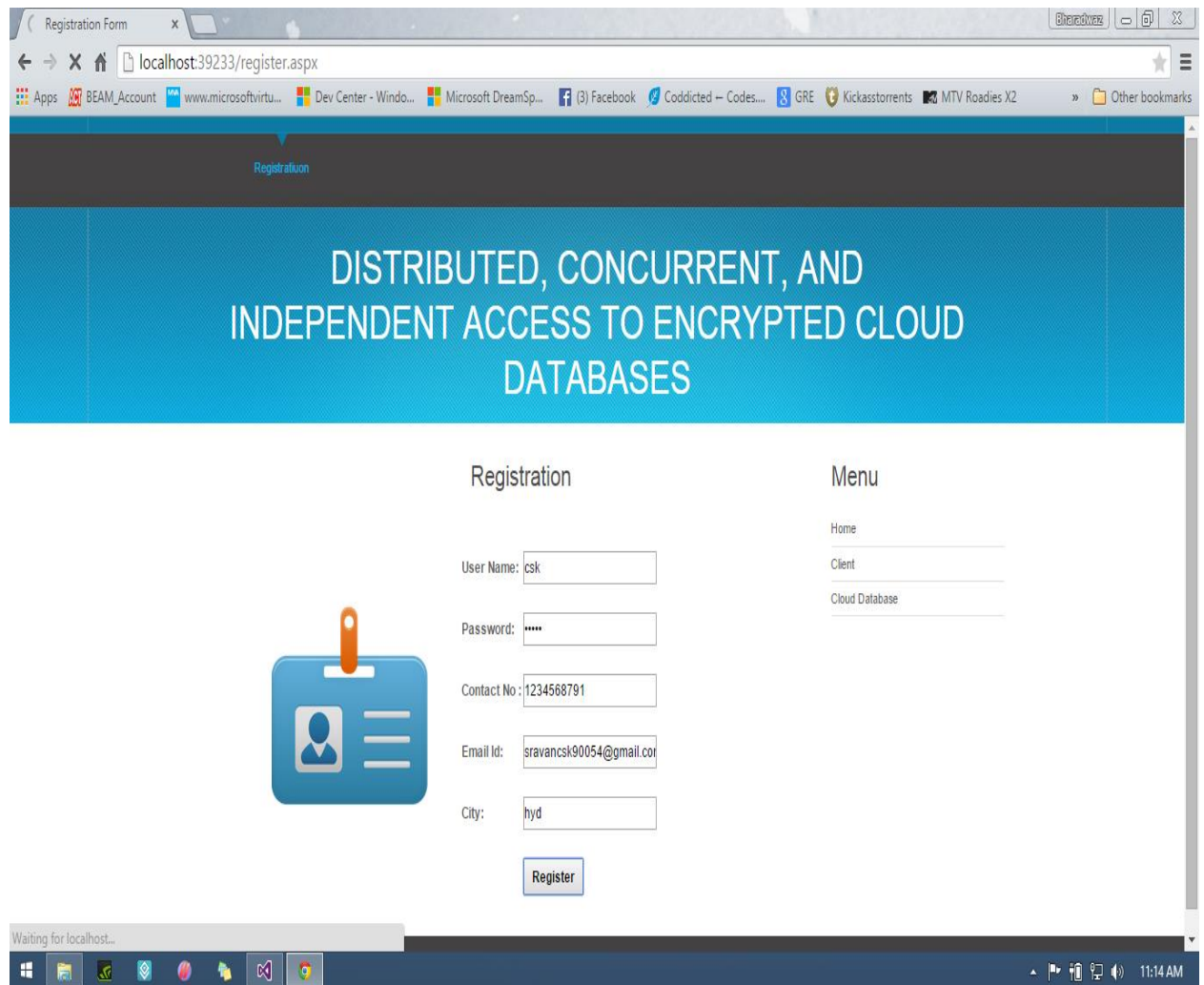


Fig 7.5: Client Upload (Full)

The screenshot displays a web browser window with the address bar showing 'localhost:39233/register.aspx'. The page has a dark blue header with the word 'Registration' in white. Below the header, a large blue banner contains the text 'DISTRIBUTED, CONCURRENT, AND INDEPENDENT ACCESS TO ENCRYPTED CLOUD DATABASES' in white. The main content area is white and features a registration form. To the left of the form is a blue icon of a person with a white outline. The form has five input fields: 'User Name:', 'Password:', 'Contact No:', 'Email Id:', and 'City:'. Below these fields is a 'Register' button. To the right of the form is a 'Menu' section with three links: 'Home', 'Client', and 'Cloud Database'. The browser's taskbar at the bottom shows various application icons and the system clock indicating 11:03 AM.

Fig 7.6: Client Registration (Empty)




Registration Form

localhost:39233/register.aspx

Registration

DISTRIBUTED, CONCURRENT, AND INDEPENDENT ACCESS TO ENCRYPTED CLOUD DATABASES



Registration

User Name:

Password:

Contact No:

Email Id:

City:

Menu

[Home](#)

[Client](#)

[Cloud Database](#)

Waiting for localhost...

11:14 AM

Fig 7.7: Client Registration (Full)

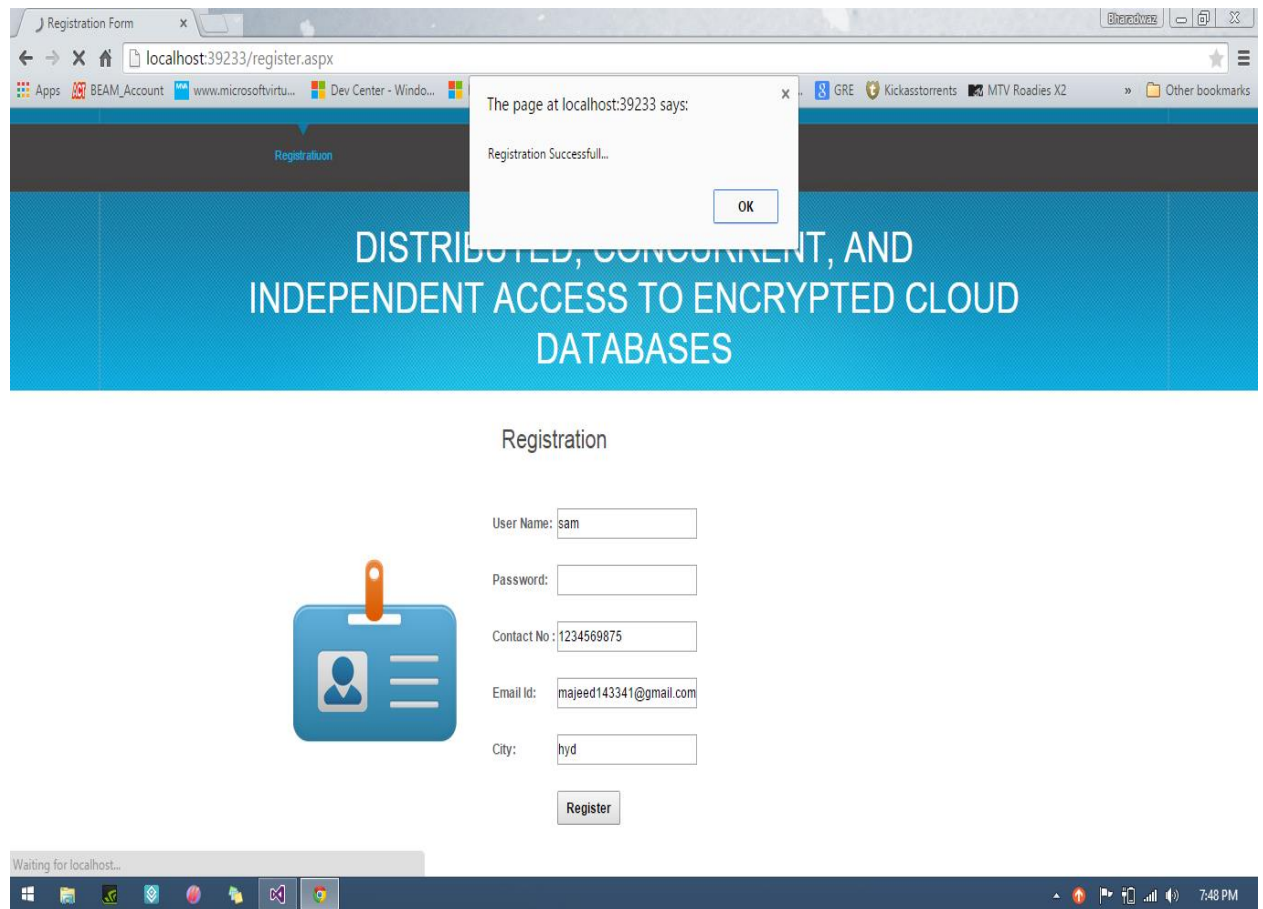


Fig 7.8: Client Registration (Success)

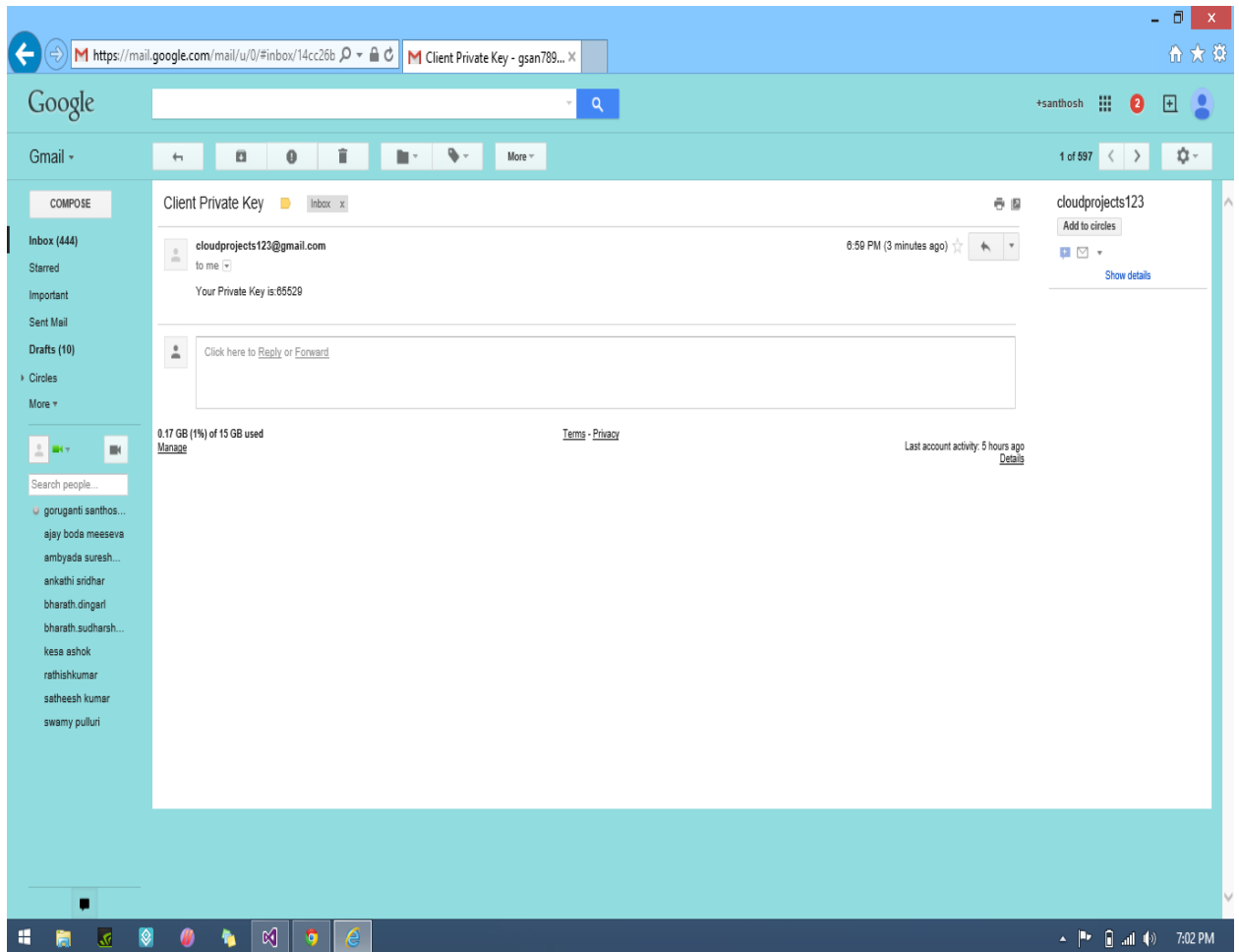


Fig 7.9: Client Registration Key (mail)

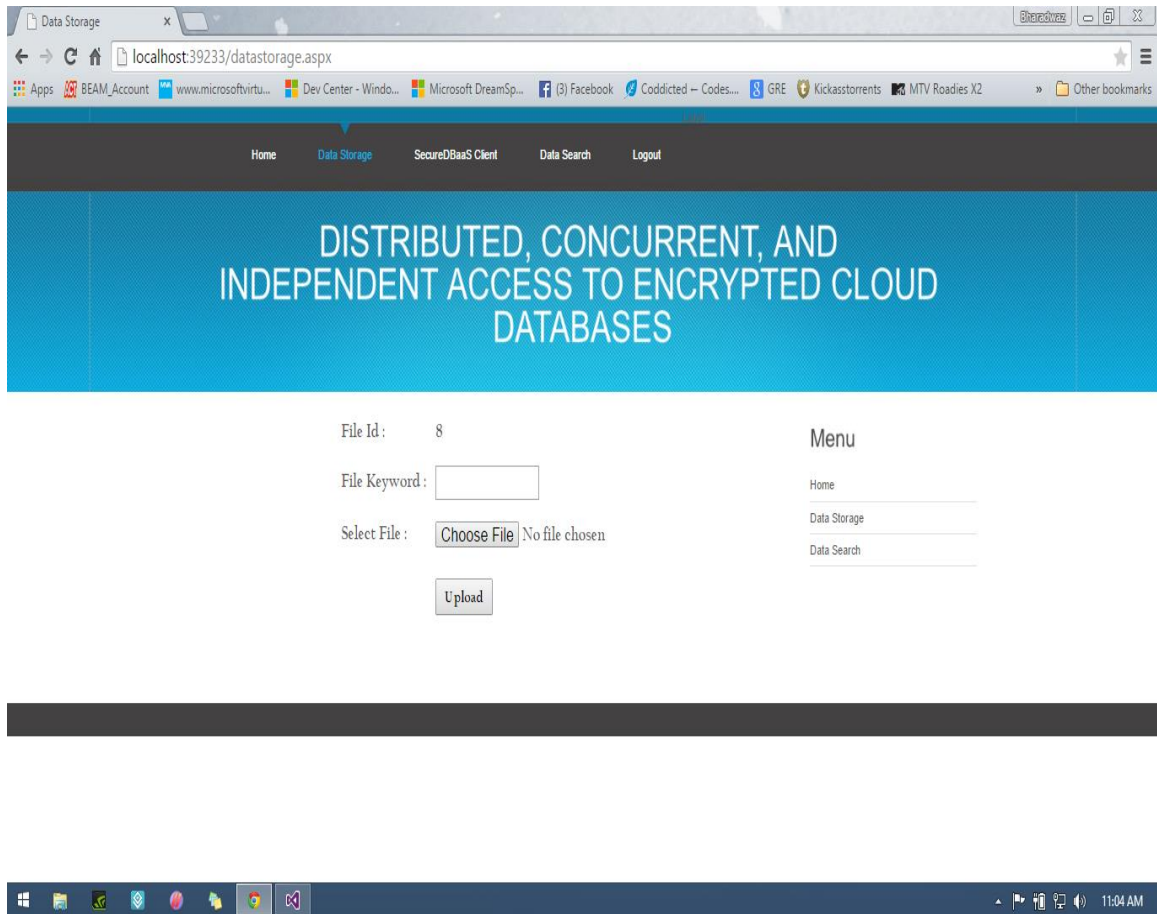


Fig 7.10: Client Upload (Empty)

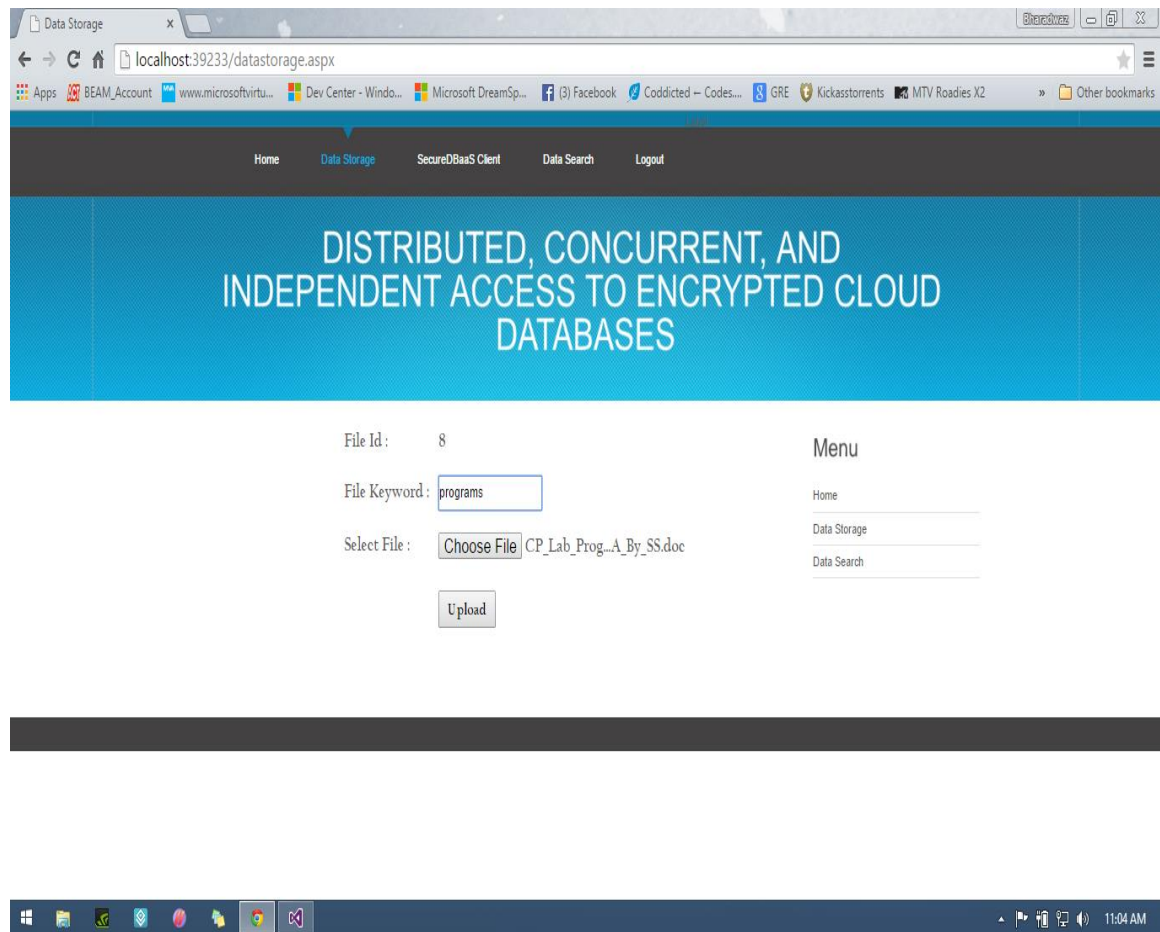


Fig 7.11: Client Upload (Full)

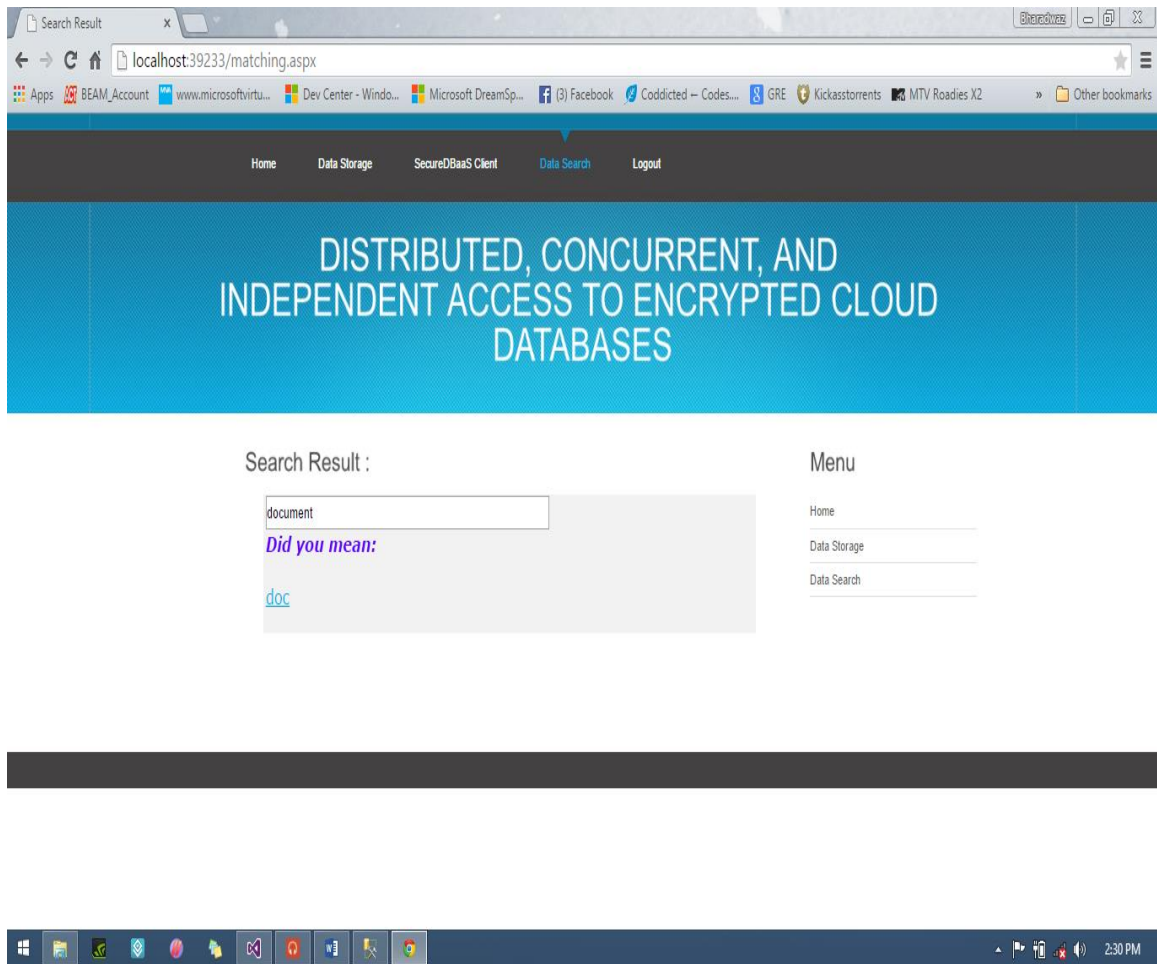


Fig 7.12: Client Search Page

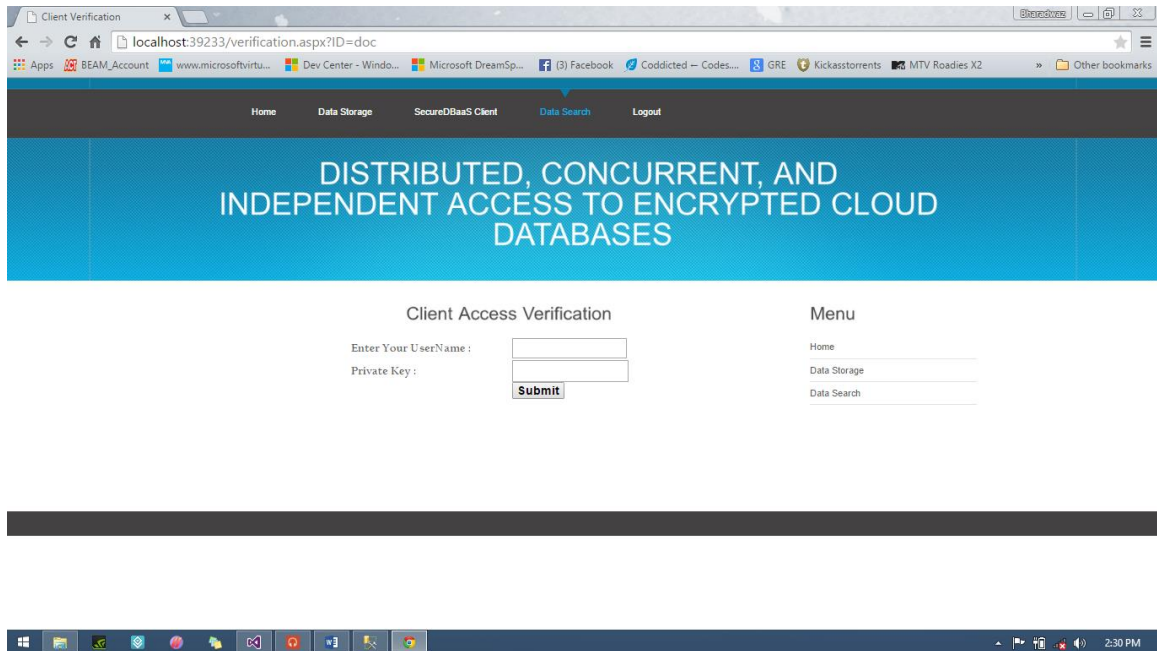


Fig 7.13: Client Download Page

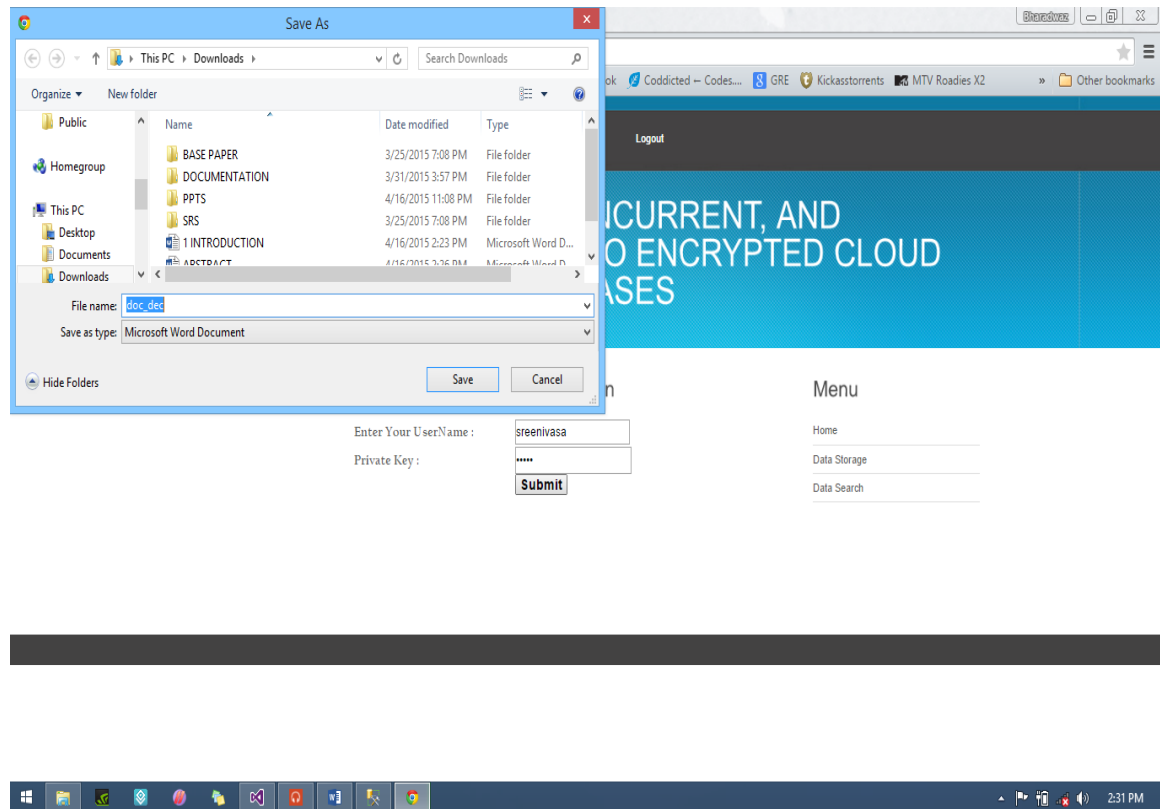


Fig 7.14: Client Search Page

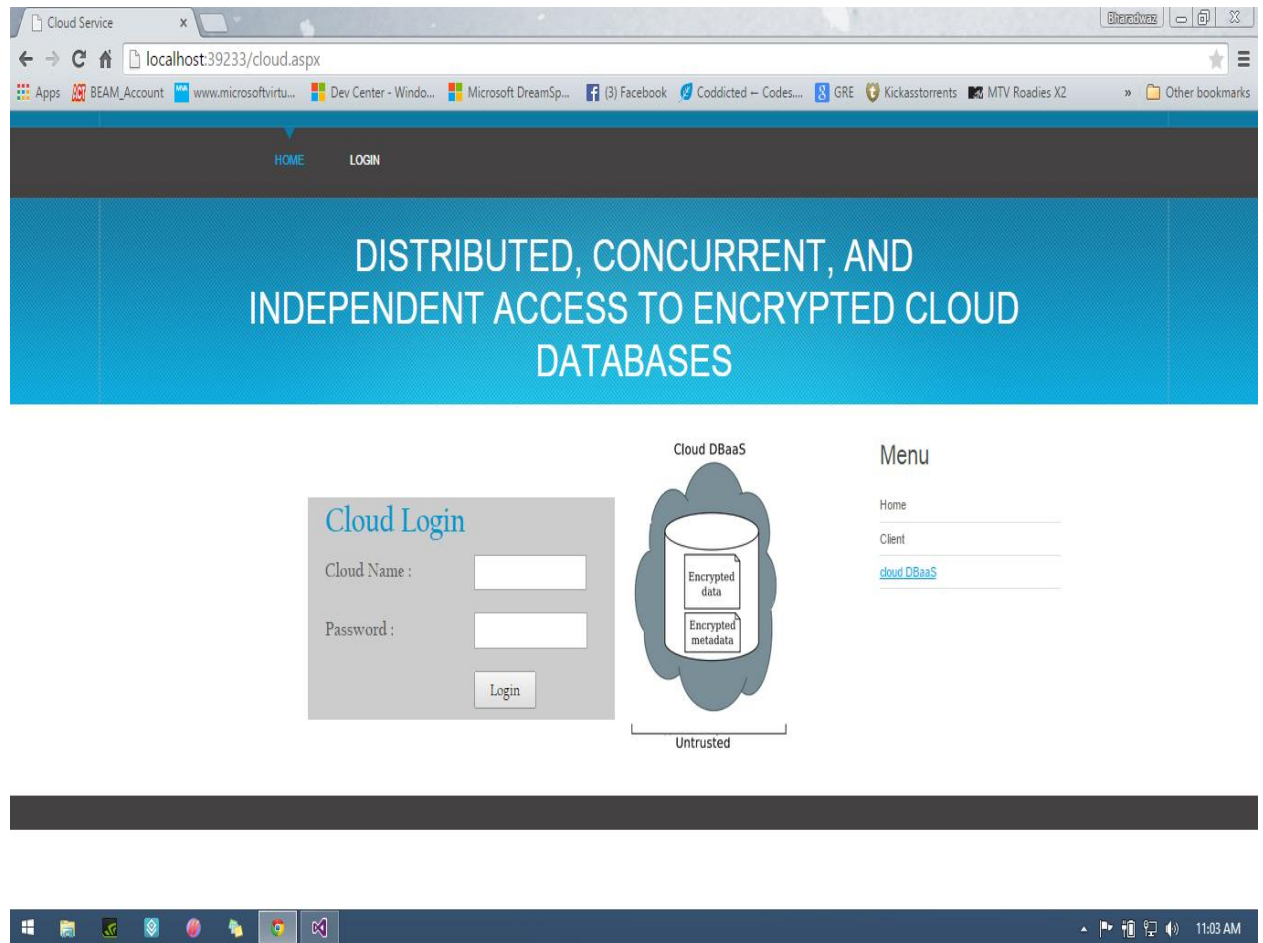


Fig 7.15: Admin Login (empty)

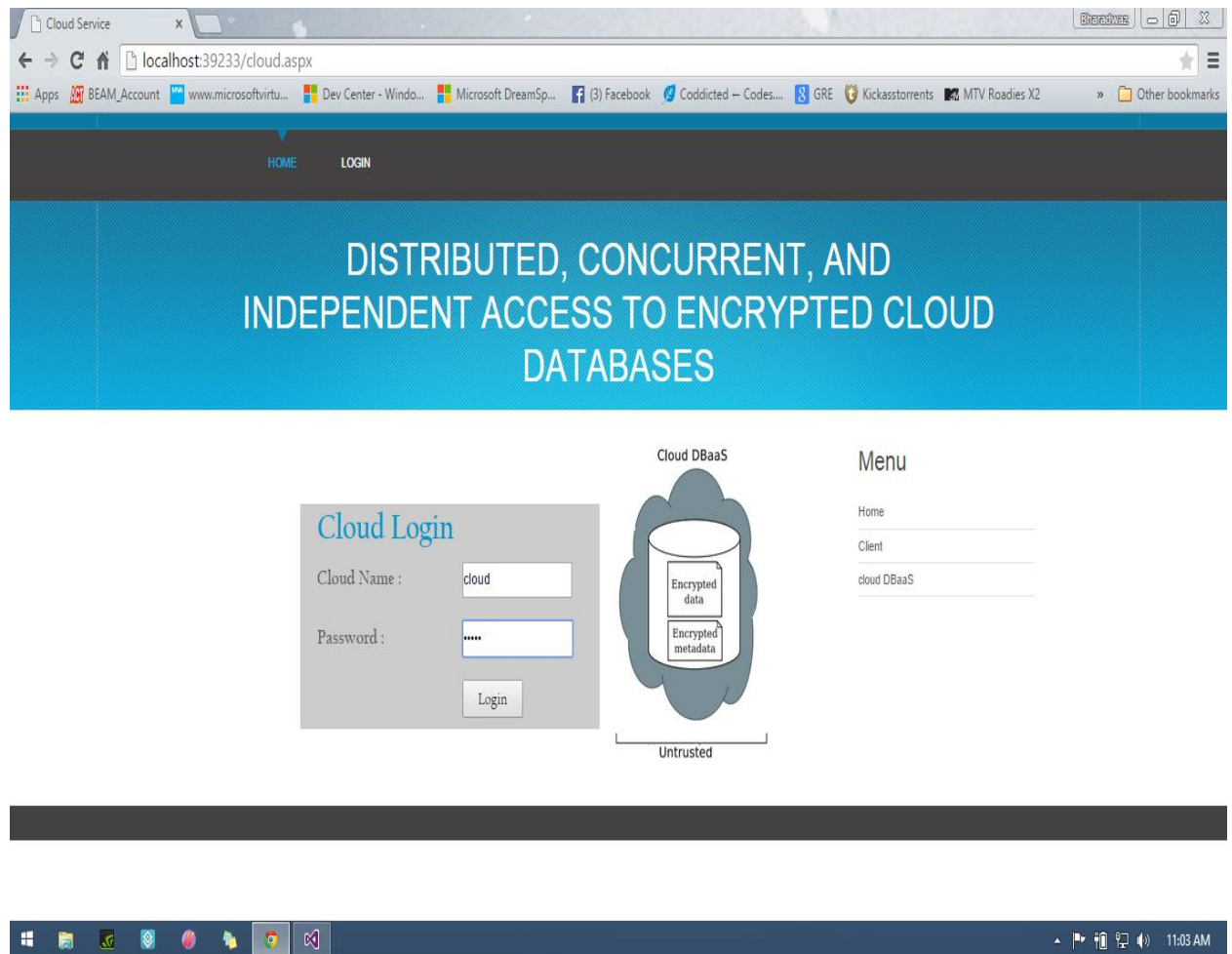


Fig 7.16: Admin Login (full)

cloud DBaaS

localhost:39233/cloudDBaaS.aspx

HOME CLIENT cloud DBaaS

DISTRIBUTED, CONCURRENT, AND INDEPENDENT ACCESS TO ENCRYPTED CLOUD DATABASES

View Cloud DBaaS Menu

ID	File Name	File	Meta Data
1	Avkv0C89p9rUTkE9zYbqHkGaInXcVclGwrp+ygdzwWc=	Test File 1_enc.txt	MvpRy37JHGDQRLXYkZ7
2	Avkv0C89p9rUTkE9zYbqHkGaInXcVclGwrp+ygdzwWc=	Test File3_enc.txt	MvpRy37JHGDQRLXYkZ7
3	h1vpvPMJHTsRfOJCS+U1kfixMqDAgp9ZQg4KATj4RZ4=	Id Generation_enc.txt	MvpRy37JHGDQRLXYkZ7
4	S/A0O3vmZludEfeO8uhTqBqWKjW1hDz5nu41/uV5gfA=	imp link_enc.txt	MvpRy37JHGDQRLXYkZ7
5	+rpM10WVuTHQ1Wsa4wCUYs9xnBuTYn8tqEFJWnbKip8=	validation_enc.txt	MvpRy37JHGDQRLXYkZ7
6	R7W2HULxGetFDAG8fkjGg==	Index_enc.docx	MvpRy37JHGDQRLXYkZ7
7	cjK3Jo2FsO+1YS97qT95lw==	doc_enc.docx	MvpRy37JHGDQRLXYkZ7

Home
Client
cloud DBaaS
About

11:04 AM

Fig 7.17: Admin View of Files

8. CONCLUSION AND FUTURE SCOPE

We propose an innovative architecture that guarantees confidentiality of data stored in public cloud databases. Unlike state-of-the-art approaches, our solution does not rely on an intermediate proxy that we consider a single point of failure and a bottleneck limiting availability and scalability of typical cloud database services. A large part of the research includes solutions to support concurrent SQL operations (including statements modifying the database structure) on encrypted data issued by heterogeneous and possibly geographically dispersed clients. The proposed architecture does not require modifications to the cloud database, and it is immediately applicable to existing cloud DBaaS, such as the experimented PostgreSQL Plus Cloud Database, Windows Azure, and Xeround. There are no theoretical and practical limits to extend our solution to other platforms and to include new encryption algorithms. It is worth observing that experimental results based on the TPC-C standard benchmark show that the performance impact of data encryption on response time becomes negligible because it is masked by network latencies that are typical of cloud scenarios. In particular, concurrent read and write operations that do not modify the structure of the encrypted database cause negligible overhead. Dynamic scenarios characterized by (possibly) concurrent modifications of the database structure are supported, but at the price of high computational costs. These performance results open the space to future improvements that we are investigating.

9. REFERENCES

- [1] M. Armbrust et al., “A View of Cloud Computing,” *Comm. of the ACM*, vol. 53, no. 4, pp. 50-58, 2010.

- [2] W. Jansen and T. Grance, “Guidelines on Security and Privacy in Public Cloud Computing,” *Technical Report Special Publication 800-144*, NIST, 2011.

- [3] A.J. Feldman, W.P. Zeller, M.J. Freedman, and E.W. Felten, “SPORC: Group Collaboration Using Untrusted Cloud Resources,” *Proc. Ninth USENIX Conf. Operating Systems Design and Implementation*, Oct. 2010.

- [4] J. Li, M. Krohn, D. Mazieres, and D. Shasha, “Secure Untrusted Data Repository (SUNDR),” *Proc. Sixth USENIX Conf. Operating Systems Design and Implementation*, Oct. 2004.

- [5] P. Mahajan, S. Setty, S. Lee, A. Clement, L. Alvisi, M. Dahlin, and M. Walfish, “Depot: Cloud Storage with Minimal Trust,” *ACM Trans. Computer Systems*, vol. 29, no. 4, article 12, 2011.

- [6] H. Haciguoglu, B. Iyer, and S. Mehrotra, “Providing Database as a Service,” *Proc. 18th IEEE Int’l Conf. Data Eng.*, Feb. 2002.

- [7] C. Gentry, “Fully Homomorphic Encryption Using Ideal Lattices,” *Proc. 41st Ann. ACM Symp. Theory of Computing*, May 2009.

- [8] R.A. Popa, C.M.S. Redfield, N. Zeldovich, and H. Balakrishnan, “CryptDB: Protecting Confidentiality with Encrypted Query Processing,” *Proc. 23rd ACM Symp. Operating Systems Principles*, Oct. 2011.

- [9] H. Hacigu"mu" s,, B. Iyer, C. Li, and S. Mehrotra, "Executing SQL over Encrypted Data in the Database-Service-Provider Model," Proc. ACM SIGMOD Int'l Conf. Management Data, June 2002.
- [10] J. Li and E. Omiecinski, "Efficiency and Security Trade-Off in Supporting Range Queries on Encrypted Databases," Proc. 19th Ann. IFIP WG 11.3 Working Conf. Data and Applications Security, Aug. 2005.
- [11] E. Mykletun and G. Tsudik, "Aggregation Queries in the Database-as-a-Service Model," Proc. 20th Ann. IFIP WG 11.3 Working Conf. Data and Applications Security, July/Aug. 2006.
- [12] D. Agrawal, A.E. Abbadi, F. Emekci, and A. Metwally, "Database Management as a Service: Challenges and Opportunities," Proc. 25th IEEE Int'l Conf. Data Eng., Mar.-Apr. 2009.
- [13] V. Ganapathy, D. Thomas, T. Feder, H. Garcia-Molina, and R. Motwani, "Distributing Data for Secure Database Services," Proc. Fourth ACM Int'l Workshop Privacy and Anonymity in the Information Soc., Mar. 2011.
- [14] A. Shamir, "How to Share a Secret," Comm. of the ACM, vol. 22, no. 11, pp. 612-613, 1979.
- [15] M. Hadavi, E. Damiani, R. Jalili, S. Cimato, and Z. Ganjei, "AS5: A Secure Searchable Secret Sharing Scheme for Privacy Preserving Database Outsourcing," Proc. Fifth Int'l Workshop Autonomous and Spontaneous Security, Sept. 2013.
- [16] "Oracle Advanced Security," Oracle Corporation,
<http://www.oracle.com/technetwork/database/options/advanced-security>, Apr. 2013.

- [17] G. Cattaneo, L. Catuogno, A.D. Sorbo, and P. Persiano, “The Design and Implementation of a Transparent Cryptographic File System For Unix,” Proc. FREENIX Track: 2001 USENIX Ann. Technical Conf., Apr. 2001.
- [18] E. Damiani, S.D.C. Vimercati, S. Jajodia, S. Paraboschi, and P. Samarati, “Balancing Confidentiality and Efficiency in Untrusted Relational Dbmss,” Proc. Tenth ACM Conf. Computer and Comm. Security, Oct. 2003.
- [19] L. Ferretti, M. Colajanni, and M. Marchetti, “Supporting Security and Consistency for Cloud Database,” Proc. Fourth Int’l Symp. Cyberspace Safety and Security, Dec. 2012.
- [20] “Transaction Processing Performance Council,” TPC-C, [http:// www.tpc.org](http://www.tpc.org), Apr. 2013.