RESEARCH AND DESIGN OF CRYPTOGRAPHY CLOUD FRAMEWORK

CONTENT

1.INTRODUCTION

At present, information technology with the rapid development promotes the rhythm and pace of society. With the assistance of characteristics of cloud computing that include high scalability, high reliability and flexibility, more and more application systems migrate to the cloud to deployed, for achieving the goal of centralized management of data and efficient use of resources. Cloud computing technology has been widely used in the information system of industry, finance and government, which greatly facilitates the work and life of people; at the same time, network information has become an important strategic resource, whose security can't be underestimated. To protect security of information data in the network environment, cryptography application mode under the cloud computing environment becomes particularly important. While the traditional cryptography technology is limited to fixed carrier and non-scalable cryptography computing resource, so that it can't satisfy the encryption requirements of massive cloud data. The conception of Crypto as a Service (CaaS) developed the concept of cloud computing from the aspect of information security, it finds a new way for the application of the cryptography technology in the cloud environment, also helps to innovate the new method. According to the report of cloud computing standard published by the NIST in 2011, the security of cloud computing can be divided into 3 parts, which are the security of cloud application, the security of cloud data and the security of cloud hardware with the virtualization.

2. ABSTRACT

Since the application mode of cryptography technology currently has different types in the cloud environment, a novel cryptography cloud framework was proposed, due to the non-expandability of cryptography resources. Through researching on the application models of the current encryption technology, the cryptography service demand under the cloud environment and the virtual structure of the cloud cryptography machine, this paper designed the framework of the cryptography cloud framework that provides cryptography services with the cloud computing mode. the design idea of the framework is expounded from two aspects include the function of modules and service flow of cryptography cloud, which resulted in the improvement of the flexibility of the application of cryptography technology in the cloud environment. Through the analysis of system function and management mode, it illustrated the availability and security of

cryptography cloud framework. It was proved that cryptography cloud has the characteristics of high-availability in the implementation and experiment, and it can satisfy cryptography service demand in the cloud environment existing calculations for the related makespan based numerous work process planning issue. Trial and measurable outcomes exhibit the viability and productivity of the proposed calculation.

3. Scope of the Project

The cryptography cloud framework that provides cryptography services with the cloud computing mode. The design idea of the framework is expounded from two aspects include the function of modules and service flow of cryptography cloud, which resulted in the improvement of the flexibility of the application of cryptography technology in the cloud environment. Through the analysis of system function and management mode, it illustrated the availability and security of cryptography cloud framework.

4. PROBLEM STATEMENT

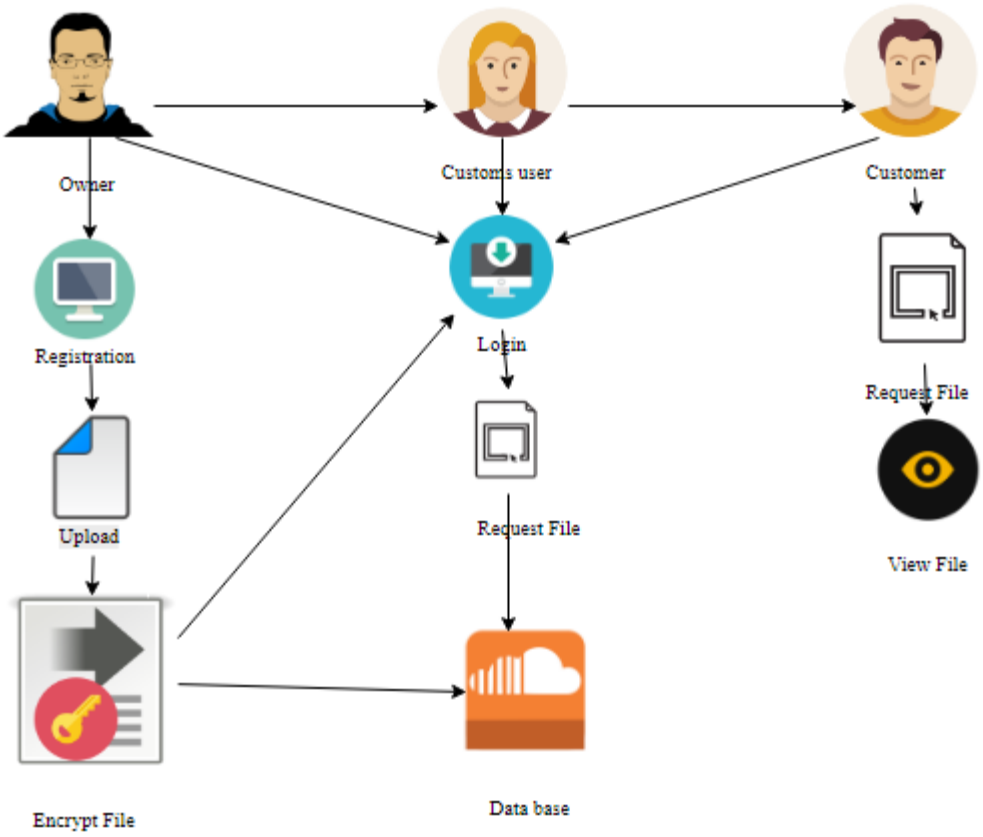
The application mode of cryptography technology currently has different types in the cloud environment, a novel cryptography cloud framework was proposed, due to the non-expandability of cryptography resources. Through researching on the application models of the current encryption technology, the cryptography service demand under the cloud environment and the virtual structure of the cloud cryptography machine.

5. EXISTING SYSTEM

5.1 Existing System:

Adapted algorithm is used to simulate resource provisioning and scheduling in a real public cloud. It is also extended to support periodical workflow applications.

5.2 Over all Diagram


Owner
Customs user
Customer
Registration
Login
Request File
Upload
Request File
View File
Encrypt File
Data base

5.3 EXISTING SYSTEM METHOD:

FHE Algorithm.

Definition:

It is the enhanced version of Fast Random Bit Encryption. After compression, the compressed data is converted into frames before encryption is applied.

EXISTING SYSTEM	PROPOSED SYSTEM
EXISTING CONCEPT:- • The illegal user accesses their own key informationaccordingtotheir requirements, but trust of the third party can't be measured objectively, so there are still existing security risks to a certain extent. • The application mode of cryptography technology currently has different types in the cloud environment, a novel cryptography cloud framework was proposed, due to the non-expandability of cryptography resources.	**PROPOSED CONCEPT:-** • It designed the framework of the cryptography cloud framework that provides cryptography services with the cloud computing mode. • It was proved that cryptography cloud has the characteristics of high-availability in the implementation and experiment, and it can satisfy cryptography service demand in the cloud environment.
EXISTING ALGORITHM:- • FHE Algorithm.	**PROPOSED ALGORITHM:** • Cryptography Algorithm.
ALGORITHM DEFINITION:- • It is the enhanced version of Fast Random Bit Encryption • After compression, the compressed data is converted into frames before encryption is applied.	**ALGORITHM DEFINITION:-** • Decryption is the reverse, in other words, moving from the unintelligible ciphertext back to plaintext. • A cipher (or cypher) is a pair of algorithms that create the encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and in each instance by a "key".

DRAWBACKS:-	ADVANTAGES:-
• It is very difficult or impossible to learn. • The data loss is high.	• Symmetric cryptography uses the same key to both encrypt and decrypt information. • That implies that both sender and receiver must possess the same key. Symmetric cryptography provided a great advantage over normal forms of communication but posed some new problems.

7.PROPOSED SYSTEM

7.1 Proposed System

The proposed Path Cluster Heuristic (PCH) supposes that each task can only be processed on a single processor and uses the clustering technique to generate a group of tasks.The Heterogeneous Earliest Finish Time (HEFT) is a popular scheduling heuristic for minimizing the makespan of a single workflow.

7.3Proposed System Model Explanation

Precedence Tree based Heuristic Algorithm

PTH consists of three phases: Workflows Combination and Parameters Initialization (WCPI), initial schedule Construction Methods (CM) and Schedule Improvement Procedure (SIP).

8.TECHNOLOGIES USING THIS PROJECT

In this Project

MVC

- Jsp
- Servlet
- Java Script
- Interfaces
- Bean Classes
- JDBC

TECHNOLOGIES USED IN THIS PROJECT:

In this project we are developing web Application and using technology such as

WEB APPLICATION:

A web application or web app is any program that runs in a web browser. It is created in a browser-supported programming language (such as the combination of JavaScript, HTML and CSS) and relies on a web browser to render the application.

MVC (Model, View, Controller):

MVC stands for Model View and Controller. It is a design pattern that separates the business logic, presentation logic and data. Controller acts as an interface between View and Model. Controller intercepts all the incoming requests. Model represents the state of the application i.e. data. It can also have business logic. View represents the presentation i.e. UI (User Interface).

JSP:

In our project we are using Jsp to design the application process. JSP pages are using to develop the form pages like login and user registration pages. It means it is mainly useful for user Interaction development. And some static content of html pages to jsp pages for dynamic content.

Servlet:

In our project we are using Servlet to control the application process. Servlet is the center of our application because all the controlling part will be monitoring by the Servlet only. It means Servlet takes requests and matches for suitable jsp's and it is also useful for database controlling.

Interfaces:

An interface is a collection of abstract methods. A class implements an interface, thereby inheriting the abstract methods of the interface.An interface is not a class. Writing an interface is similar to writing a class, but they are two different concepts. A class describes the attributes and behaviors of an object. An interface contains behaviors that a class implements.

Bean Classes

Inour project we are using Java Beans;JavaBeans are reusable software components for Java. They are classes that encapsulate many objects into a single object (the bean). They are serializable, have a 0-argument constructor, and allow access to properties using getter and setter methods.

Java Script:

JavaScript is a dynamic computer programming language. It is lightweight and most commonly used as a part of web pages, whose implementations allow client-side script to interact with the user and make dynamic pages. In this project we are using JavaScript validation purpose.

JDBC:

JDBC is a Java database connectivity technology (Java Standard Edition platform) from Oracle Corporation. This technology is an API for the Java programming language that defines how a client may access a database. It provides methods for querying and updating data in a database.

9. FUTURE ENHANCEMENT

- Few works have been carried out on the multiple workflows scheduling problem.
- The proposed schedule construction and improvement procedures can be easily adapted to other workflow based scheduling problems.

10. SOFTWARE REQUIREMENTS

In our Project we use **Front End** as Java (Eclipse) and **Back End** as a MY SQL.

Jdk 1.8:

In our project we are using java to design the application process. Java contains technologies such as JEE (Servlet, Jsp) that is used to design the view page easily. Since java is an open source and platform independent this makes the application more flexible.

MY SQL:

My SQL is a relational database management system developed by Sun Micro systems. As a database, it is a software product whose primary function is to store and retrieve data as requested by other software applications, be it those on the same computer or those running on another computer across a network (including the Internet). There are different workloads (ranging from small applications that store and retrieve data on the same computer, to millions of users and computers that access huge amounts of data from the Internet at the same time).

ALTERNATIVE TITTLE:

. Outline of Cryptography Cloud Framework

2. Research and Design of Cryptography Cloud Framework