International Journal of Research
eISSN: 2348-6848 & pISSN: 2348-795X Vol-5 Special Issue-13
International Conference on Innovation and Research in Engineering, Science & Technology
Held on 23rd & 24th February 2018, Organized by Tulsiramji Gaikwad Patil College of Engineering & Technology, Nagpur, 441108, Maharastra, India.

Multicloud Security Using Binary Split Algorithm

Prajakta Devgade
Dept of Computer Science And Engineering
Tulsiramji Gaikwad Patil Collage Of Engineering And Technology
Nagpur, INDIA
Devgade123@gmail.com

Arati Jadhav
Dept of Computer Science And Engineering
Tulsiramji Gaikwad Patil Collage Of Engineering And Technology
Nagpur, INDIA
Aartujadhav@gmail.com

Saniya Ali
Dept of Computer Science And Engineering
Tulsiramji Gaikwad Patil Collage Of Engineering And Technology
Nagpur, INDIA
Saniyaali191@gmail.com

Snehal Gadre
Dept of Computer Science And Engineering
Tulsiramji Gaikwad Patil Collage Of Engineering And Technology
Nagpur, INDIA
snehalgadree@gmail.com

Laxmi Bharadbhunje
Dept of Computer Science And Engineering
Tulsiramji Gaikwad Patil Collage Of Engineering And Technology
Nagpur, INDIA
Laxmibharadbhuje65@gmail.com

Abstract

With the internet getting so popular data sharing and security of personal data has gain much more importance than before. Cloud provides and efficient way to outsource the data either online or offline but data security becomes one of the major issues in unreliable cloud environment. The proposed system addresses the security issues in cloud environment and also provides a way to provide better security in cloud environment. The proposed system uses cryptographic symmetric algorithm AES with key size of 256 for data encryption and Ultra Zip compression which provides a compression ratio up to 50% depending on the file type. After encryption and compression the data is splitted into multiple parts and each part is stored is separate data server. The proposed work can be used in many different application like social networking sites and file hosting websites.

Keywords

International journel of Research, Book Publisher, Cloud Computing, IaaS, SaaS, PaaS, Distributed, Security, Load Balancer, Ultra Zip, AES, Encryption.

1.Introduction

Cloud computing is architecture for providing computing service via the internet on demand and pay per use access to a pool of shared resources namely networks, storage, servers, services and applications, without physically acquiring them. So it saves managing cost and time for organizations. Many industries, such as banking, healthcare and education are moving towards the cloud due to the efficiency of services provided by the pay-per-use pattern based on the resources such as processing power used, transactions carried out, bandwidth consumed, data transferred, or storage space occupied etc. The main issues that are identified out in cloud IaaS services are load balancing in servers and data security provided to storage systems.

1.1 Cloud basics

Cloud computing, or "the cloud", concentrates on expanding the viability of the imparted assets. Cloud assets are typically imparted by numerous clients as well as progressively reallocated for every interest and pay for every utilization premise.

This can work for dispensing assets to clients. For instance, a cloud machine that serves Indian clients amid Indian business hours with an application (e.g., email) may reallocate the same assets to serve China clients

International Journal of Research
eISSN: 2348-6848 & pISSN: 2348-795X Vol-5 Special Issue-13
International Conference on Innovation and Research in Engineering, Science & Technology
Held on 23rd & 24th February 2018, Organized by Tulsiramji Gaikwad Patil College of Engineering & Technology, Nagpur, 441108, Maharastra, India.

1.2 Private Cloud

Private cloud give the capacity to all the more specifically oversee assets that oblige a larger amount of control than is typically accessible from people in general cloud.
Private cloud are typically utilized for a solitary business. For some associations considering distributed computing, private mists structures better beginning stage. They permit the association to have software's, situations, and databases in a cloud, while tending to concerns with respect to imparting and security and protection that can emerge in the general population the earth.

1.3 Infrastructure as a Service (IaaS)

Iaas conveys fittings assets, for example, CPU, plate space or system segments as an administration. These assets are generally conveyed as a virtualization stage by the Cloude supplier and might be gotten to over the Internet by the customer. The customer has full control of the virtualized stage and is not in charge of dealing with the underlying base.

1. Formulation Of Present Work

2.1 Existing System

Previously we used only AES algorithm for data encryption and decryption that increases in-house workload as well as it requires more memory space.

Because of the above mention loop whole previously speed for processing the system is low and we are not getting required functioning in less time.

Due to this reason to minimize in-house workload as well as complexity of existing system we proposed binary split algorithm which work on file splitting by dividing files into small chunks and stored it on different servers.

2.1.1 Dis-Advantages of Existing System

- Key size of AES which can be further extended to 256 bit.
- The system is very complex and the examine cause can be solved in different ways.

2.2 Proposed System

We are using binary split algorithm to provide security over multi-cloud, it is helpful to resist data theft.In this case data can be encrypted and decrypted by using AES algorithm.Using binary split algorithm file can be split into small chunk an then stored to servers.Space require to store a file on server is less by the use of ultra zip technique.

3.System Architecture

3.1 Technology Review

3.1.1 JAVA

Java is a set of several computer software and specifications developed by Sun Microsystems. Java is used in a wide variety of computing platforms from embedded devices and mobile phones to enterprise servers and supercomputers. While less common, Java applets run in secure, sandboxed environments to provide many features of native applications and can be embedded in HTML pages.

Writing in the Java programming language is the primary way to produce code that will be deployed as byte code in a Java Virtual Machine (JVM); byte code compilers are also available for other languages, including Ada, JavaScript, Python, and Ruby. In addition, several languages have been designed to run natively on the JVM, including Scala, Clojure and Groovy. Java syntax borrows heavily from C and C++, but object-oriented features are modeled after Smalltalk and Objective-C.

3.1.2 Use of Java in Web server and enterprise.

The Java platform has become a mainstay of enterprise IT development since the introduction of the Enterprise Edition in 1998, in two different ways:

Through the coupling of Java to the web server, the Java platform has become a leading platform for integrating the Web with enterprise backend systems. This has allowed companies to move part or all of their business to the Internet environment by way of highly interactive online environments (such as

highly dynamic websites) that allow the customer direct access to the business processes (e.g. online banking websites, airline booking systems and so on).

The Java platform has matured into an Enterprise Integration role in which legacy systems are unlocked to the outside world through bridges built on the Java platform. This trend has been supported for Java platform support for EAI standards like messaging and Web services and has fueled the inclusion of the Java platform as a development basis in such standards as SCA, XAM and others.

3.1.3 Apache Tomcat 7 Web Server

Apache Tomcat is an open-source web server and servlet container developed by the Apache Software Foundation (ASF). Tomcat implements several Java EE specifications including Java Servlet, Java Server Pages (JSP), Java EL, and Web Socket, and provides a "pure Java" HTTP web server environment for Java code to run in.

Tomcat is developed and maintained by an open community of developers under the auspices of the Apache Software Foundation, released under the Apache License 2.0 license, and is open-source software. It has also added user- as well as system-based web applications enhancement to add support for deployment across the variety of environments. It also tries to manage sessions as well as applications across the network. Tomcat is building additional components. A number of additional components may be

used with Apache Tomcat. These components may be built by users should they need them or they can be downloaded from one of the mirrors.

3.1.4 Mysql Server 5

MySQL is the world's second most widely used relational database management system (RDBMS) and most widely used open-source RDBMS. It is named after co-founder Michael Widenius's daughter, The SQL acronym stands for Structured Query Language. The MySQL development project has made its source code available under the terms of the GNU General Public License, as well as under a variety of proprietary agreements.

MySQL is a popular choice of database for use in web applications, and is a central component of the widely used LAMP open source web application software stack (and other 'AMP' stacks).

3.1.5 XHTML

Extensible Hypertext Markup Language (XHTML) is a family of XML markup languages that mirror or extend versions of the widely used Hypertext Markup Language (HTML), the language in which Web pages are formulated. While HTML, prior to HTML5, was defined as an application of Standard Generalized Markup Language (SGML), a flexible markup language framework, XHTML is an application of XML, a more restrictive subset of SGML. XHTML documents are well-formed and may therefore be parsed using standard XML parsers, unlike HTML, which requires a lenient HTML-specific parser.

3.2 Testing

This section describes the overall testing strategy and the project management issues that are required to properly execute effective tests.

3.2.1 Software to be tested

We are testing the project “Designing Multi-Cloud Server for Scalable and Secure Sharing over Web” which aims to provide security in cloud environment.

We are performing testing for different components.

- Authentication module
- File Upload
- File Download
- File Splitting

3.2.2 Testing Strategy

3.2.2.1 Unit Testing

Each component is tested separately. A bottom up approach is used for testing.

Components for unit testing

This involves testing of individual modules. Here we have tested individual modules written for various operations like:

- Authentication module
- File Upload
- File Download
- File Splitting

3.2.2.2 Integration Testing

The system as a whole is tested here. The system is said to be operating correctly if it passes these tests. After the different modules have been individually tested, we have to integrate them and tackle the issues during the integration.

3.3.2.3 Validation testing

The Validation testing is performed for all the components of the software. The accuracy of the result and the performance benchmarks are checked for all the components that are tested. The components are all stripped so that the testing can be done without the linking of other components.

3.2.3 Test Procedure

Table 1. Test case 1

Sr. No	1
Test Case Name	Login
Test Description	The website should not proceed further if username and password are not correct.
Steps	1. Visit Website. 2. Enter username and password. 3. Click on login button.
Expected Result	Website should display error if username and password are incorrect or else proceed.
Pass/Fail	Pass

Table 2 Test Case 2

Sr. No	2
Test Case Name	File Upload
Test Description	The web server should upload the file after encryption compression and splitting.
Steps	1. Start the website and login. 2. Select File Upload. 3. Select File to be uploaded
Expected Result	File should be upload after encryption compression and splitting.
Pass/Fail	Pass

Table 3. Test Case 3

Sr. No	**3**
Test Case Name	File Download
Test Description	The website should properly download the file
Steps	1. Start the website 2. Login 3. Select the file and click download
Expected Result	File should be downloaded in original format properly.
Pass/Fail	Pass

4.Formulation Of Modules

4.1 Problem Definition

To develop a system that provides data security in Cloud based IaaS services using encryption algorithm and compression algorithms.

4.1.1 Objectives

- To develop a website that will provide functionality to upload and download data.
- To encrypt data using AES algorithm (key size: 256).
- To compression data using ultra ZIP.
- To split data into multiple part and store it in different database servers.

4.2 Data Flow Diagram

Level 0:

Figure 1. DFD Level

Level 1:

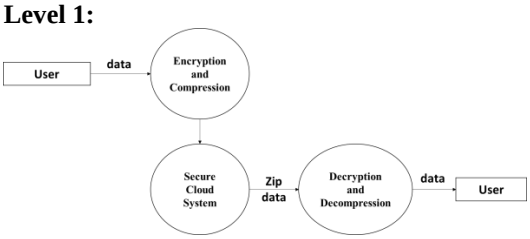


Figure 2. DFD Level 1

1.3 System Architecture

The proposed work is planned to be carried out in the following manner.

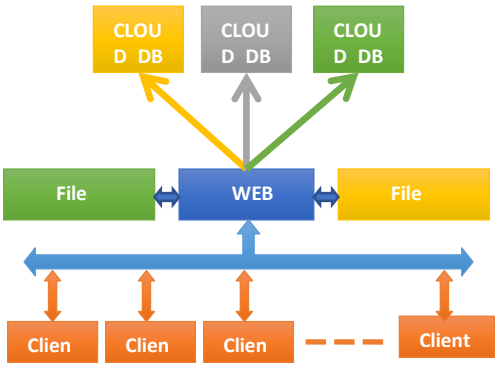


Figure 3. System Architecture

The system will provide load balancing both in terms of database and the file to be uploaded will be splitted into n parts and each part will be stored in a different cloud server. Consider an example where a file is splitted into two part out of which one is stored in Hotmail IaaS and other in Amazon IaaS.

4.3.1 Use Case Diagram

A use case diagram at its simplest is a representation of a user's interaction with the system that shows the relationship between the user and the different use cases in which the user is involved. A use case diagram can identify the different types of users of a system and the different use cases and will often be accompanied by other types of diagrams as well.

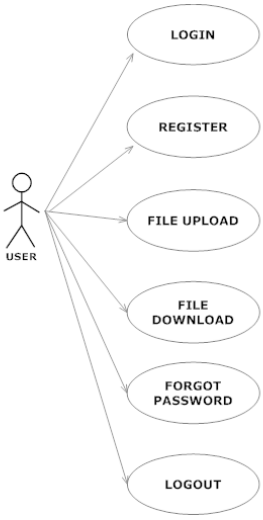


Figure 4. Use Case Diagram

4.3.2 Activity Diagram

Activity diagrams are graphical representations of workflows of stepwise activities and action with support for choice, iteration and concurrency. In the Unified Modeling Language, activity diagrams are intended to model both computational and organizational processes (i.e. workflows). Activity diagrams show the overall flow of control.

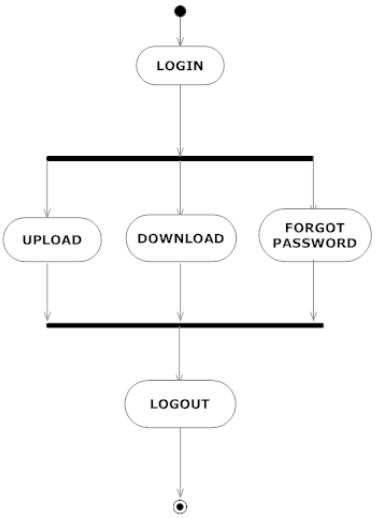


Figure 5. Activity Diagram

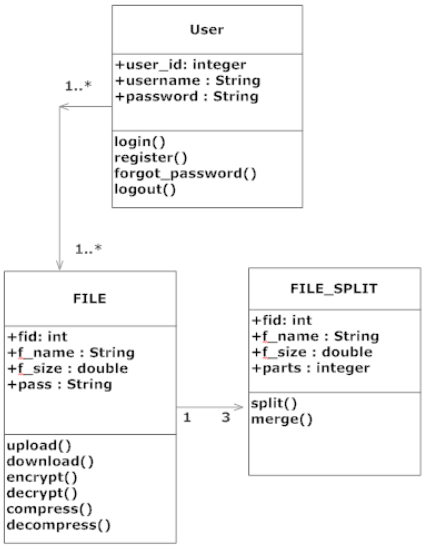


Figure 6.Code Sequence

4.3.3 Class Diagram

The class diagram is the main building block of object oriented modelling. It is used both for general conceptual modelling of the systematics of the application, and for detailed modelling translating the models into programming code. Class diagrams can also be used for data modeling. The classes in a class diagram represent both the main objects, interactions in the application and the classes to be programmed.

3.3.4 Sequence Diagram

A Sequence diagram is an interaction diagram that shows how processes operate with one another and what is their order. It is a construct of a Message Sequence Chart. A sequence diagram shows object interactions arranged in time sequence. It depicts the objects and classes involved in the scenario and the sequence of messages exchanged between the objects needed to carry out the functionality of the scenario. Sequence diagrams are typically associated with use case realizations in the Logical View of the system under development. Sequence diagrams are sometimes called event diagrams or event scenarios.

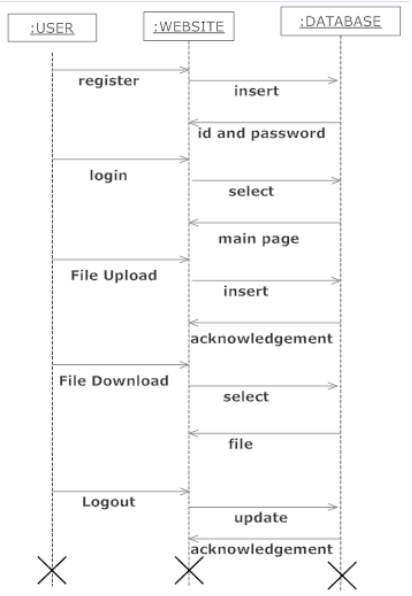


Figure 7. Sequence Diagram

3.3.5 Component Diagram

A component is something required to execute a stereotype function. Examples of stereotypes in components include executable, documents, database tables, files, and library files. Components are wired together by using an assembly connector to connect the required interface of one component with the provided interface of another component. This illustrates the service consumer - service provider relationship between the two components.

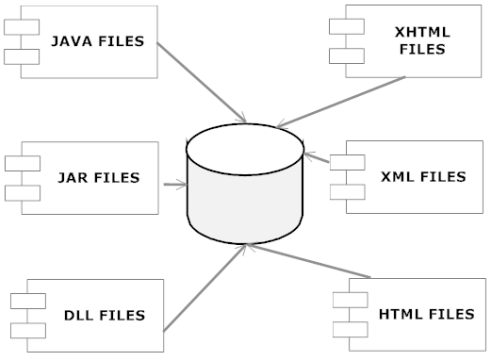


Figure 8. Component Diagram

3.4 Modules of Project

3.4.1 User Authentication

As a mandatory service we have provided an authentication module that checks the username and password before logging into the cloud. We have also provided service for forget /password and email notifications.

3.4.2 Data Security Using AES 256

In our proposed system the data security is provided using AES symmetric algorithm with a key size of 256. Again we have worked on reducing the size of encrypted message using ultra zipping which can compress data up to 50% depending on file type.

3.4.3 Data Balancing in Database Servers

In proposed system the data gets splitted in three equal parts and each part is saved in different database schema. This feature helps in maintaining the data balancing in database servers.

4. Methedology

4.1 Encryption Algorithms

4.1.1 AES algorithm

AES is based on a design principle known as a Substitution permutation network. It is fast in both software and hardware. Unlike its predecessor, DES, AES does not use a Feistel network. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits, whereas Rijndael's can be specified with block and key sizes in any multiple of 32 bits, with a minimum of 128 bits.

The block size has a maximum of 256 bits, but the key size has no theoretical maximum. AES operates on a 4×4 column-major order matrix of bytes, termed the state (versions of Rijndael's with a larger block size have additional columns in the state). Most AES calculations are done in a special finite field.

4.1.2 Working of AES

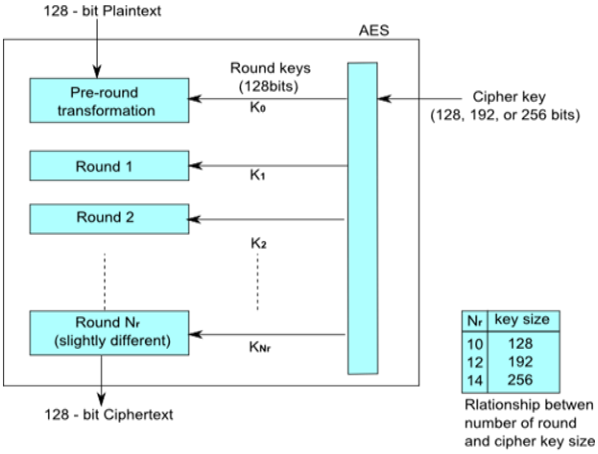
Advanced Encryption Standard or AES was invented by Joan Daemen and Vincent AES has

three approved key length: 128 bits, 192 bits, and 256 bits. To try to explain the process in simple terms, an algorithm starts with a random number, in which the key and data encrypted with it are scrambled though four rounds of mathematical processes. The key that is used to encrypt the number must also be used to decrypt it.

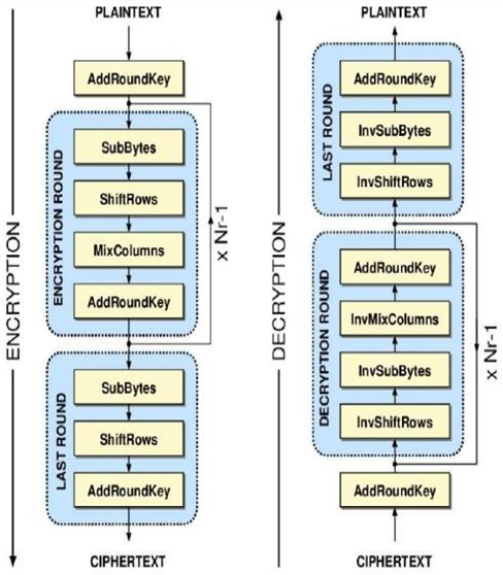
The four rounds are called Sub-Bytes, Shift-Rows, Mix Columns, and AddRoundKey. During Sub-Bytes, a lookup table is used to determine what each byte is replaced with. The Shift Rows step has a certain number of rows where each row of the state is shifted cyclically by a particular offset, while leaving the first row unchanged. Each byte of the second row is shifted to the left, by an offset of one, each byte in the third row by an offset of two, and the fourth row by an offset of three. This shifting is applied to all three key lengths, though there is a variance for the 256-bit block where the first row is unchanged, the second row offset by one, the third by three, and the fourth by four. The Mix Columns step is a mixing operation using an invertible linear transformation in order to combine the four bytes in each column. The four bytes are taken as input and generated as output.

In the fourth round, the AddRoundKey derives round keys from Rijndael's key schedule, and adds the round key to each byte of the state. Each round key gets added by combining each byte of the state with the corresponding byte from the round key. Lastly, these steps are repeated again for a fifth round, but do not include the Mix Columns step.

Rijmen, and accepted by the US federal government in 2001 for top secret approved encryption algorithms. It is also referred to as Rijndael's, as it is based off the Rijndael algorithm. Reportedly, this standard has never been cracked.



General design of AES encryption cipher

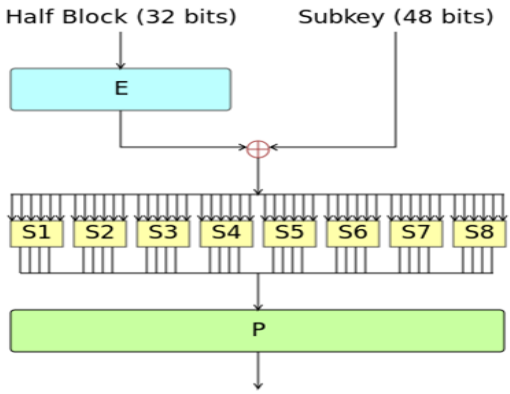


6.1.3 DES Algorithm

The Data Encryption Standard was once a predominant symmetric-key algorithm for the encryption of electronic data. It was highly influential in the advancement of modern cryptography in the academic world. Developed in the early 1970s at IBM and based on an earlier design by Horst Feistel, the algorithm was submitted to the National Bureau of Standards (NBS) following the agency's invitation to propose a candidate for the protection of sensitive, unclassified electronic

government data. In 1976, after consultation with the National Security Agency (NSA), the NBS eventually selected a slightly modified version (strengthened against differential cryptanalysis, but weakened against brute force attacks), which was published as an official Federal Information Processing Standard (FIPS) for the United States in 1977. The publication of an NSA-approved encryption standard simultaneously resulted in its quick international adoption and widespread academic scrutiny. Controversies arose out of classified design elements, a relatively short key length of the symmetric-key block cipher design, and the involvement of the NSA, nourishing suspicions about a backdoor.

DES is now considered to be insecure for many applications. This is mainly due to the 56-bit key size being too small; in January, 1999, distributed.net and the Electronic Frontier Foundation collaborated to publicly break a DES key in 22 hours and 15 minutes (see chronology). There are also some analytical results which demonstrate theoretical weaknesses in the cipher, although they are infeasible to mount in practice. The algorithm is believed to be practically secure in the form of Triple DES, although there are theoretical attacks.



Comparison between Symmetric Algorithms

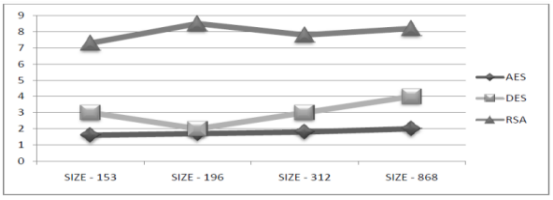


Figure 10. Encryption Time

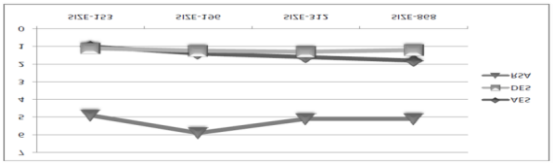


Figure 11. Decryption Time

4.3 Software Requirements

- JAVA 7
- JDK 1.7
- MYSQL 5
- Apache Tomcat Web Server 7
- Eclipse Juno

4.4 Hardware Requirements

- Client with minimum 1GB RAM 160GB HDD Dual Core Processor.
- Server with minimum 4GB Ram 500GB HDD i5 Processor.

LAN and Internet Connectivity.

4.5 Frontend and Backend

- XHTML as Frontend
- JAVA for Backend Connectivity
- SQL for Backend

2. Pictorial Representation

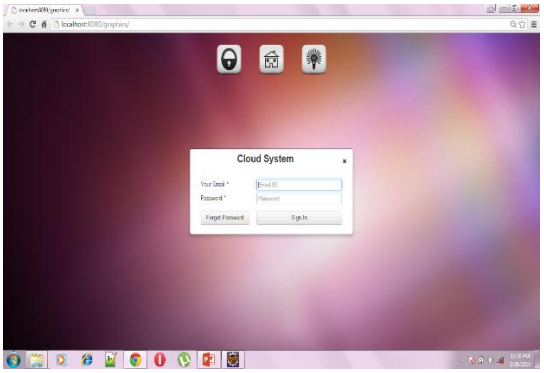


Figure 11. Login Page

Figure 12. Registration Page

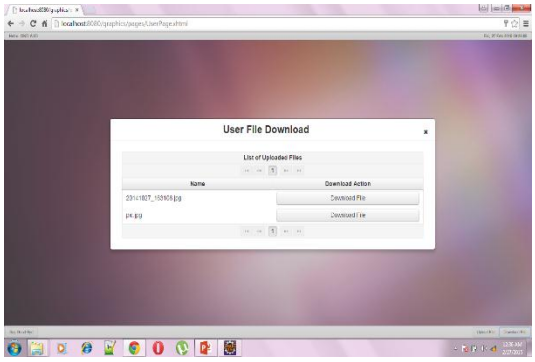


Figure 13. File download

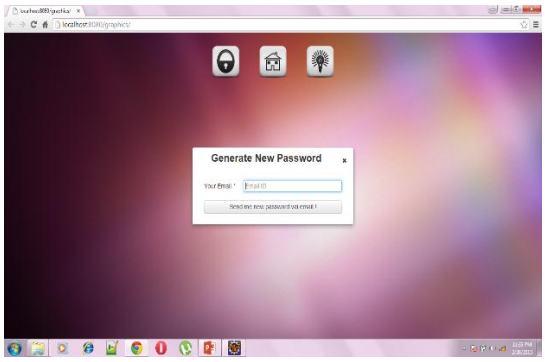


Figure 14. Forgot Password Page

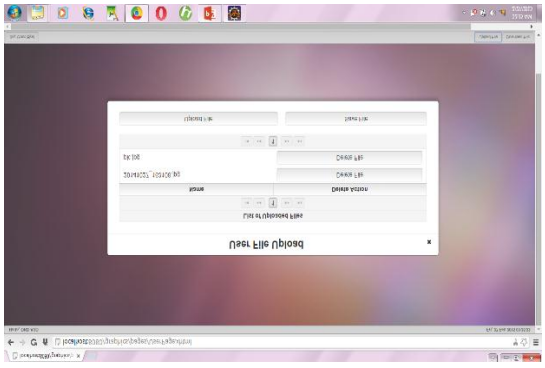


Figure 15. File Upload Page

5.Conclusion

IaaS is the establishment layer of the Cloud Computing conveyance demonstrate that comprises of numerous segments and innovations. Every segment in Cloud framework has its helplessness which may affect the entire Cloud's Computing security. Cloud computing business develops quickly notwithstanding security concerns, so coordinated efforts between Cloud gatherings would aid in overcoming security difficulties and push secure Cloud Computing administrations. In this project we have implemented a system that will provide better security in cloud environment. We have implemented a security architecture which provides strong security using AES algorithm.

6.REFERENCES

[1] Cloud Computing Security: From Single To Multi-Clouds Mohammed A. Alzain , Eric Pardede , Ben Soh , James A. Thom 2012 45th Hawaii International Conference On System Sciences.

[2] Ensuring Data Integrity And Security In Cloud Storage Olfa Nasraoui, Member, IEEE, Maha Soliman, Member, IEEE, Esin Saka, Member, IEEE, Antonio Badia, Member, IEEE, And Richard Germain IEEE TRANSACTIONS ON CLOUD AND DATA ENGINEERING, VOL. 20, No. 2, February 2013.

[3] Service-Oriented Cloud Computing Architecture Wei-Tek Tsai, Xin Sun, Janaka Balasooriya 2010 Seventh International Conference On Information Technology

[4] Key-Aggregate Cryptosystem For Scalable Data Sharing In Cloud Storage Cheng-Kang Chu, Sherman S. M. Chow, Wen-Guey Tzeng, Jianying Zhou, And Robert H. Deng, Senior Member, IEEE, IEEE Transactions On Parallel And Distributed Systems. Volume: 25, Issue: 2. Year: 2014.

[5] Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina And Eduardo B Fernandez An Analysis Of Security Issues For Cloud Computing Hashizume Et Al. Journal Of Internet Services And Applications 2013.

[6] Mukesh Singhal And Santosh Chandrasekhar Collaboration In Multicloud Computing Environments: Framework And Security Issues Published By The IEEE Computer Society 0018-9162/13/$31.00 © 2013 IEEE

[7] Sushmita Ruj, Milos Stojmenovic, Amiya Nayak Decentralized Access Control With Anonymous Authentication Of Data Stored In Clouds IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS VOL:25 NO:2 YEAR 2014.

[8] Lukas Malina and Jan Hajny Efficient Security Solution for Privacy-Preserving Cloud Services 6TH INTERNATIONAL CONFERENCE ON TELECOMMUNICATIONS SIGNAL PROCESSING YEAR 2013.

[9] Cheng-Kang Chu, Sherman S. M. Chow, Wen-Guey Tzeng, Jianying Zhou, And Robert H. Deng Key-Aggregate Cryptosystem For Scalable Data Sharing In Cloud Storage IEEE Transactions On Parallel And Distributed Systems. Volume: 25, Issue: 2. Year: 2014.