Global Journal of Engineering Science and Research Management

DEPENDABLE STORAGE FOR VEHICLE INSURANCE MANAGEMENT THROUGH SECURED ENCRYPTION IN CLOUD COMPUTING

Prof.Abhijeet A.Chincholkar [*1], Ms.Najuka Todekar [2]
[*1]M.E. Digital Electronics, JCOET Yavatmal, India.
[2] UG Student, B.E.Computer Engg. Dept .JDIET, Yavatmal, India.
*Correspondence Author: chincholkarabhijeet@gmail.com

Keywords: Elastic Compute Cloud, cloud service provider, Vehicle Insurance Management, Software as a Service.

Abstract

This project aims for automating information system for VIMS on which data is stored on cloud in encrypted form. This project also develops a suitable information system to coordinate Activities of Vehicle insurance management, insurance claim and corresponding reports on the same. The technology adopted is Distributed Computing Networking. The database is created with the help of MYSQL. The client part aims at producing different forms and reports in order to provide case and satisfaction of the Vehicle insurance management.

Introduction

Several trends are opening up the era of Cloud Computing, which is an Internet-based development and use of computer technology. The ever cheaper and more powerful processors, together with the software as a service (Saas) computing architecture, are transforming data centers into pools of computing service on a huge scale. The increasing network bandwidth and reliable yet flexible network connections make it even possible that users can now subscribe high quality services from data and software that reside solely on remote data centers.

Moving data into the cloud offers great convenience to users since they don’t have to care about the complexities of direct hardware management. The pioneer of Cloud Computing vendors, Amazon Simple Storage Service (S3) and Amazon Elastic Compute Cloud (EC2) are both well-known examples. While these internet-based online services do provide huge amounts of storage space and customizable computing resources, this computing platform shift, however, is eliminating the responsibility of local machines for data maintenance at the same time. As a result, users are at the mercy of their cloud service providers for the availability and integrity of their data. On the one hand, although the cloud infrastructures are much more powerful and reliable than personal computing devices, broad range of both internal and external threats for data integrity still exist. Examples of outages and data loss incidents of noteworthy cloud storage services appear from time to time. On the other hand, since users may not retain a local copy of outsourced data, there exist various incentives for cloud service providers (CSP) to behave unfaithfully towards the cloud users regarding the status of their outsourced data. For example, to increase the profit margin by reducing cost, it is possible for CSP to discard rarely accessed data without being detected in a timely fashion. Similarly, CSP may even attempt to hide data loss incidents so as to maintain a reputation. Therefore, although outsourcing data into the cloud is economically attractive for the cost and complexity of long-term large-scale data storage, it’s lacking of offering strong assurance of data integrity and availability may impede its wide adoption of enterprise and individual cloud users.

The data stored in the cloud may not only be accessed but also be frequently updated by the users, including insertion, deletion, modification, appending, etc. Thus, it is also imperative to support the integration of this dynamic feature into the cloud storage correctness assurance, which makes the system design even more challenging. Last but not the least, the deployment of Cloud data storage is powered by data centers running in a simultaneous, cooperated and distributed manner. It is more advantages for individual users to store their data redundantly across multiple physical servers so as to reduce the data integrity and availability threats. Thus, distributed protocols for storage correctness assurance will be of most importance in achieving robust and secure cloud storage systems. Before storing data on Cloud we used to secure it by using Encryption algorithm there are many algorithm for it i.e RSA, AES, DES etc Here we are using AES algorithm to make text encrypted so that no one can access it only those have that key only access it.

Literature Review

Cryptography is a process which is associated with scrambling plaintext (ordinary text, or clear text) into cipher text (a process called encryption), then back again to plain text (known as decryption). The key feature of asymmetric cryptography system is encryption and decryption procedure are done with two different keys - public key and private key. Private Key cannot be derived with help of public key that provides much strength to security of cryptography. This is one main difference between symmetric and asymmetric cryptography, but that difference makes whole process different. This difference is small but it is enough that it has implications throughout the security. Mainly, symmetric cryptography is seen as faster, more lightweight.

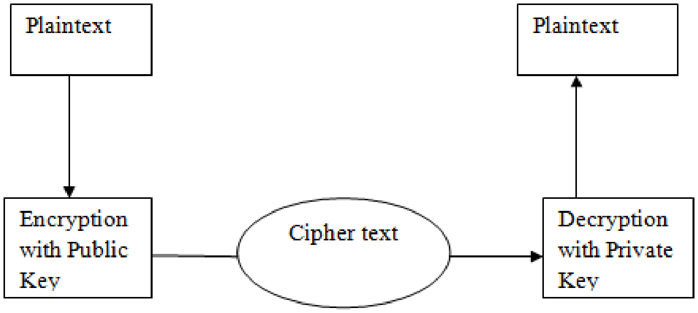


Figure 1 Encryption-Decryption using Public and private key

AES Algorithm is a symmetric block cipher. This means that it uses the same key for both encryption and decryption. AES standard states that the algorithm can only accept a block size of 128 bits and a choice of three keys - 128, 192, 256 bits. Depending on which version is used, the name of the standard is modified to AES-128, AES-192 or AES- 256 respectively. Encryption consists of 10 rounds of processing for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. Except for the last round in each case, all other rounds are identical. The four rounds are called Sub Bytes, Shift Rows, Mix Columns, and Add Round Key. 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.

Global Journal of Engineering Science and Research Management

System Overview

In this project, In Requirement analysis process user determining expectation for new or modified product. The features, called requirement, must be relevant and detailed. In software engineering aspects are often called functional specification. Requirement analysis involves frequent communication with system users to determine specific feature expectations, resolution of conflicts or ambiguity in requirement as demanded by various users, avoidance of features creep and documentation of all aspects of the project development process from start to finish. Energy should be directed towards ensuring the final system or product conforms to client needs rather than attempting to user expectation to fit requirements. It is divided into five areas of efforts like problem recognition, evolution, Synthesis, modeling, Specification and review.

System Design

In this project, the database used is MySQL where all the data user will be kept in it. To guarantee user's safety during the registering the details about him/her and used where the user will have to insert username, password. Design includes the diagrammatic representation of the system.

1. DFD
2. Sequence Diagram
3. Activity Diagram
4. Class Diagram

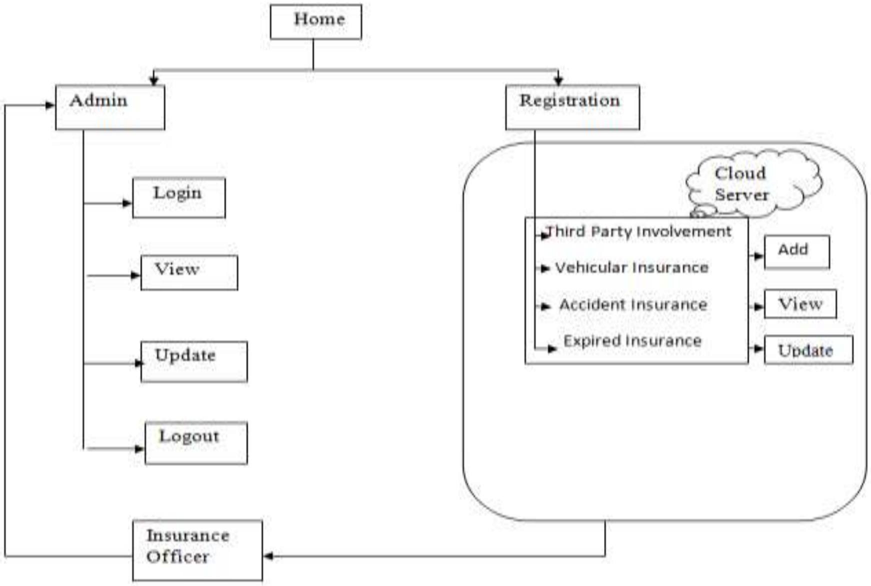


Figure 2. Overall working of project

System Analysis

In this phase the designs are translated into code. Computer programs are written using a conventional programming language or an application generator. Modules of the project is as Vehicle Insurance Schemes, Agent Login, Customer Login, Administrator Login, About us, Contact us.

Vehicular Insurance Module Description

The insurance company needs to keep track of details of its target companies, agents, policyholders, their premium payments and the various products that are available with it. Hence it is under tremendous pressure maintaining their day-to-day activities, which is currently Entire records have to be updated timely, even a slight mistake could complicate things. It is very difficult to handle bulk data since human memory is weaker than electronic counter part. It is time consuming to summarize these details to produce the reports.

Agent Login

The agent login form links to-

1. Basic agent information like contact details and address which will be shown in customer insurance information window.
2. All the information related to insurances which he has made to his clients.
3. Commission received by him for insurance made by him.
4. Option to create a new policy to any existing/new client.
5. Option to edit the contact information of its client.
6. Option to delete a policy of any client in case of policy lapse.

Customer Session

1. Collection of User Details
2. Customer Login
3. Insurance Entries
4. Insurance Claims
5. Mailing Options (Inbox, Compose, Sent Items)
6. View insurance Payment Details
7. View, Edit, Update Customer Details

Managerial Session

1. Collection of User Details
2. Admin Login
3. Collection of Customer Insurance Entries
4. Collection of Customer Insurance Claims
5. Manager Mailing Options (Inbox, Compose, Sent Items)
6. Insurance Payment Entry
7. View Customer Details, Insurance Details and Claim Details

Administrator login

Administrator has rights to-

1. Create new agent
2. Edit agent's information and its commission percentage.

Delete an agent's database and all its policies respectively.

Data Encryption Module

1. This module is maintaining data security by encryption techniques.
2. Using this module we can apply different encryption methodology (like AES) for different database schemas.
3. This module is also taking care of stored data must be in encrypted format.
4. This module functionality must be in generalized which mean that it easy to use for as developer perspective.

Data Storage Module

1. This module is responsible for taking care about data must be store in proper way.
2. This module should take care about avoid the data redundancy.
3. Integrity can be regarded as the opposite of duplicity, in that it regards internal consistency as a good feature.
4. About us:- It contains information about the organization's history and its achievements.
5. Contact us:-It contains the contact details of the organization's various branches located in different parts of a country.

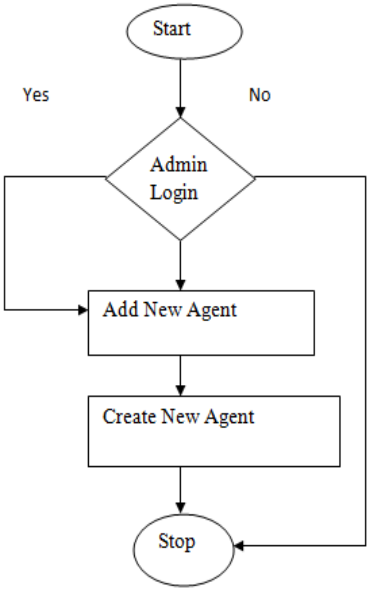


Figure 3.Agent Registration

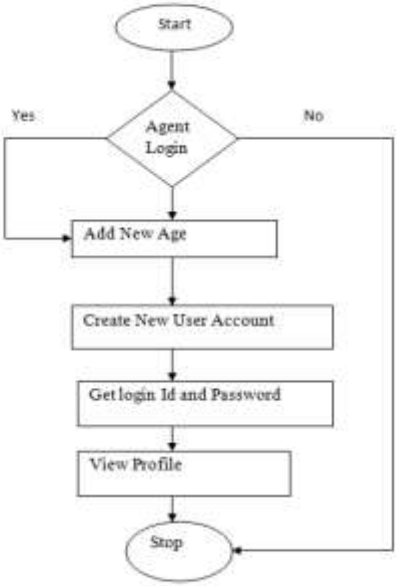


Figure 4. Flowchart For Add New User Module

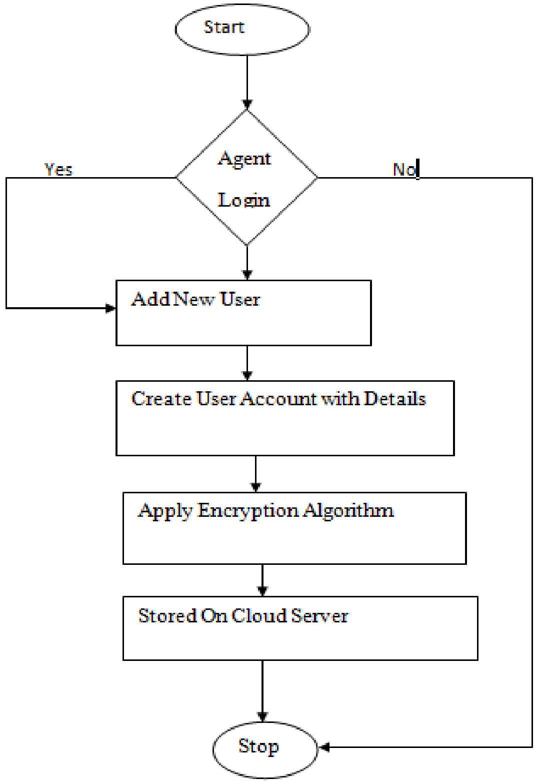


Figure 5. Flowchart For Data Storage on cloud using Encryption Algorithm

Implementation of Algorithm

AES is a block cipher with a block length of 128 bits. It allows three different key lengths: 128, 192, or 256 bits. We propose AES with 128 bit key length. The encryption process consists of 10 rounds of processing for 128-bit keys. Except for the last round in each case, all other rounds are identical. The 16 byte encryption key, in the form of 4-byte words is expanded into a key schedule consisting of 44 4-byte words. The 4 x 4 matrix of bytes made from 128-bit input block is referred to as the state array. Before any round-based processing for encryption can begin, input state is XORed with the first four words of the schedule.

For encryption, each round consists of the following four steps:

a. Sub Bytes – a non-linear substitution step where each byte is replaced with another according to a lookup table (S-box).

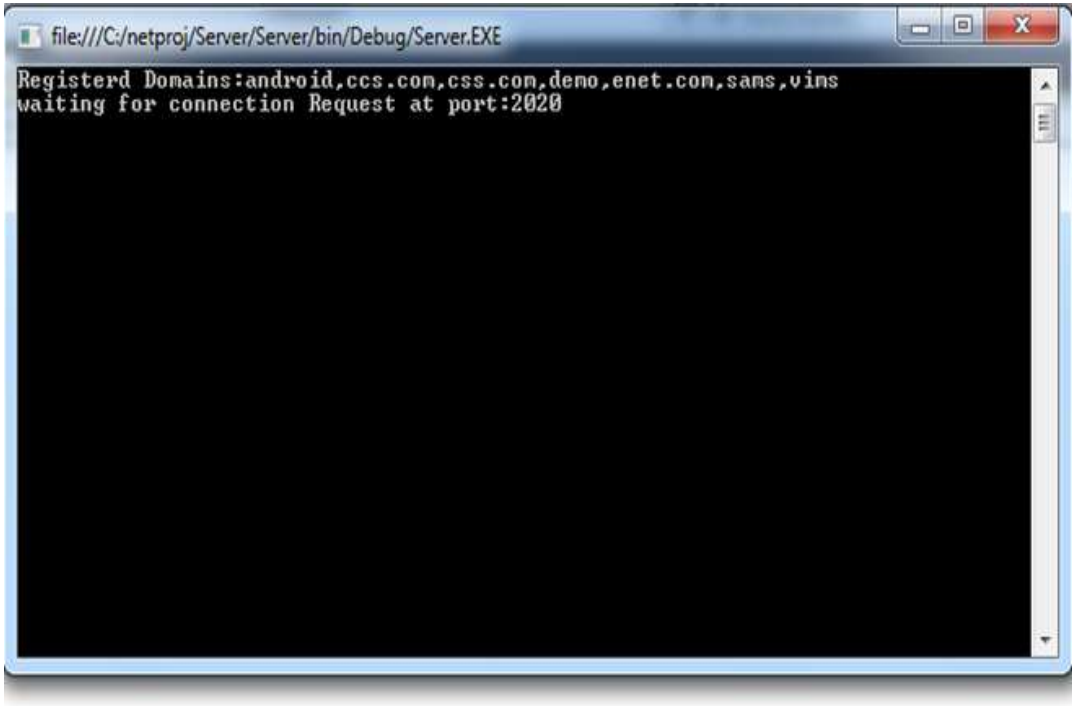
b. Shift Rows – a transposition step where each row of the state is shifted cyclically a certain number of times
c. Mix Columns – a mixing operation which operates on the columns of the state, combining the four bytes in each column.
d. Add Round Key – each byte of the state is combined with the round key; each round key is derived from the cipher key using a key schedule.

Modules

Following modules helps to get precise module of project

1. ***Server Cloud***

Cloud server is shown here. If any client send request it gives valid response.



file:///C:/netproj/Server/Server/bin/Debug/Server.EXE

```
Registerd Domains:android,ccs.com,css.com,demo,enet.com,sams,vims
waiting for connection Request at port:2020
```

Figure 6. Server Cloud

2. *Homepage of Web site*

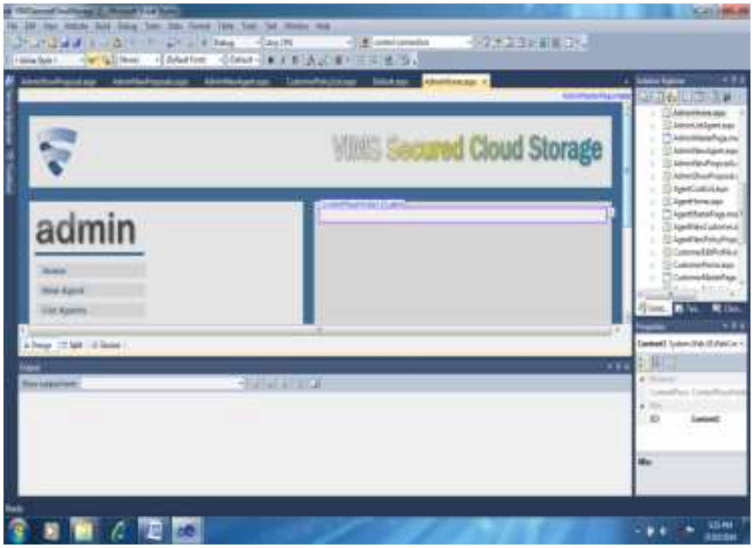


Figure 7. Homepage of Web Site

3. *Homepage*

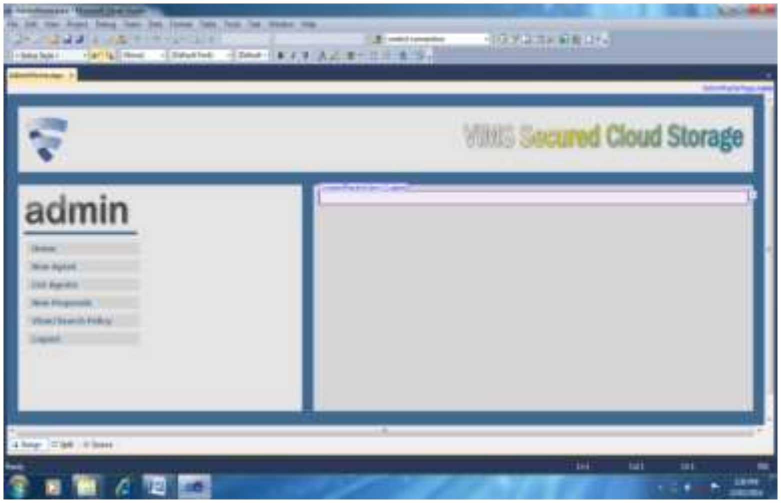


Figure 8. Homepage of Web Site

This the Front View of Admin Home Page which contain link for add new agent, show the list of Agent, New Proposals and View various Policies.

4. Administrator Login

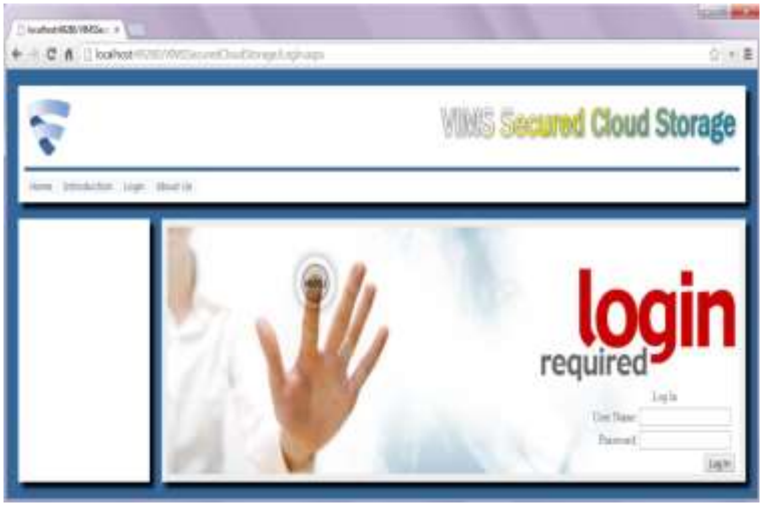

localhost:4526/VIMSSecuredCloudStorage/Login.aspx
VIMS Secured Cloud Storage
Home
Introduction
Login
About Us
login
required
Log In
User Name:
Password:
Log In

Figure 9. Administrator Login

It is login page of administrator; he has all system control Add agent, view list of agent, handle policy.

5. Add New Agent

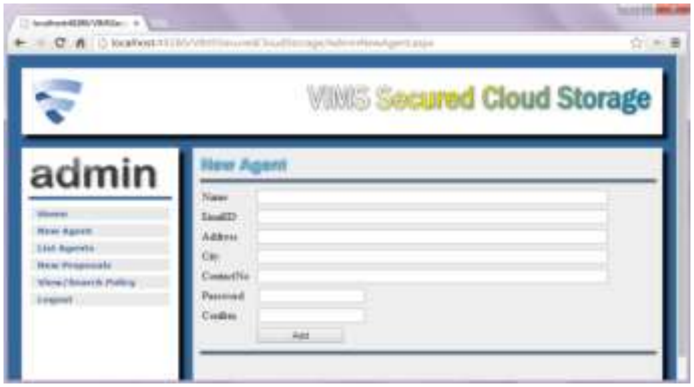


Figure 10. Add New Agent

The role of Administrator is to add the New Agent by filling their details. After adding any Agent in an list of agent under administrator he get certain identity number.

6. Agent Homepage

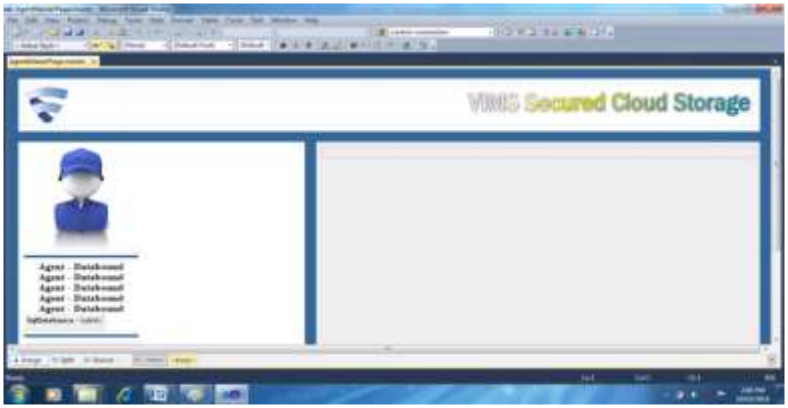


Figure 11. Agent Homepage

7. Add New User

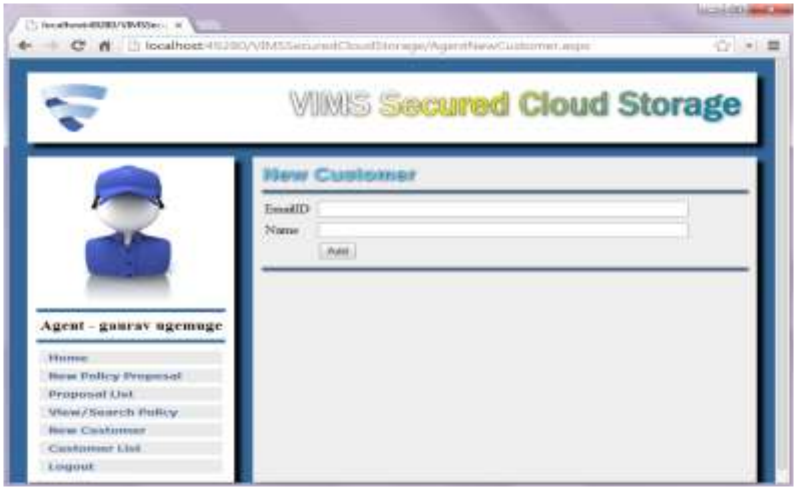
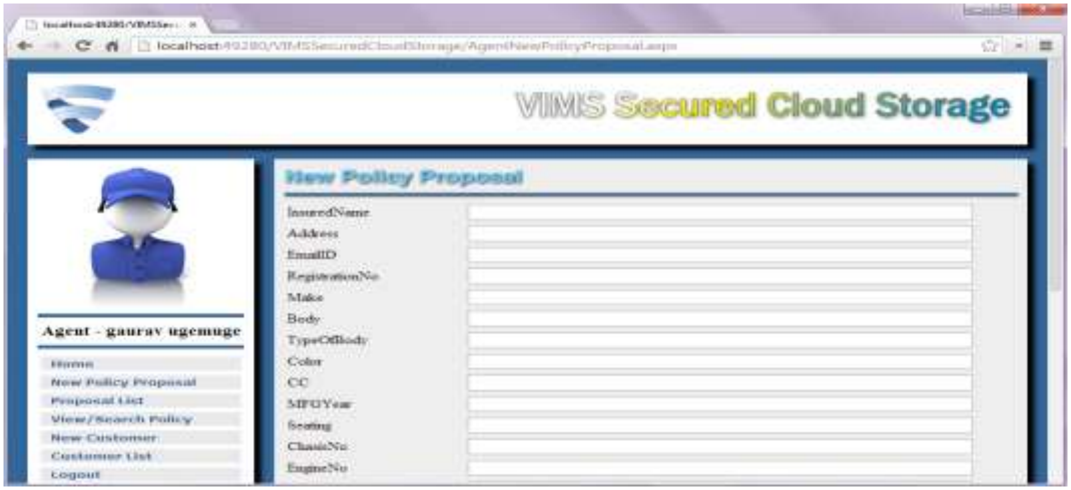


Figure 12. Add New User

Here we can add new user by their own credentials i.e. E-mail and password.

8. *Agent New Policy Proposal*



localhost:49280/VIMSSecuredCloudStorage/AgentNewPolicyProposal.aspx

New Policy Proposal

InsuredName

Address

EmailID

RegistrationNo

Make

Body

TypeOfBody

Color

CC

MFGYear

Seating

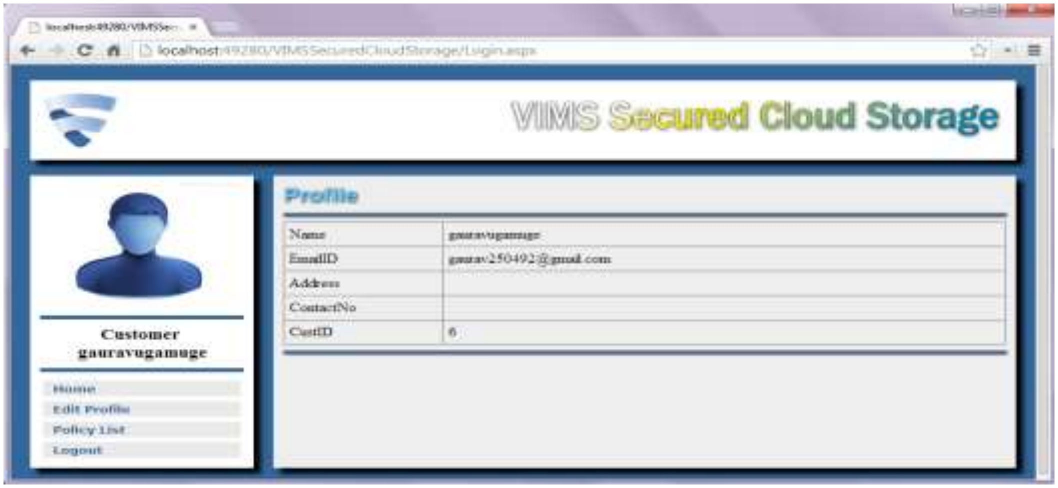
ChasisNo

EngineNo

Figure 13. Agent New Policy Proposal

The new policy is implemented by adding details as given in figure it is implemented by Agent.

9. *Customer Homepage*



localhost:49280/VIMSSecuredCloudStorage/Login.aspx

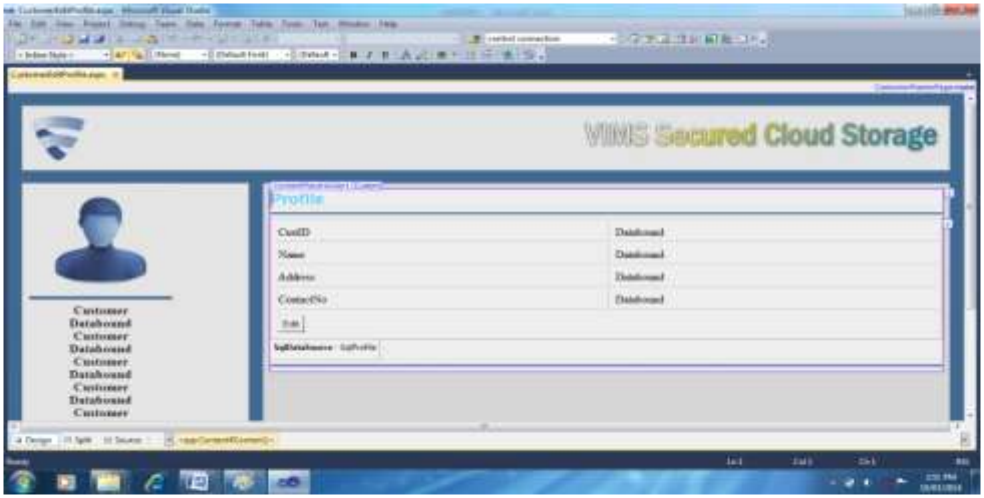
Profile

Name	gauravugamuge
EmailID	gaurav250492@gmail.com
Address	
ContactNo	
CustID	6

Figure 14. Customer Homepage

It is the Front look of Customer Homepage which contains their E-mail id, Name, Address, contact details and Customer ID.

10. Edit User Profile



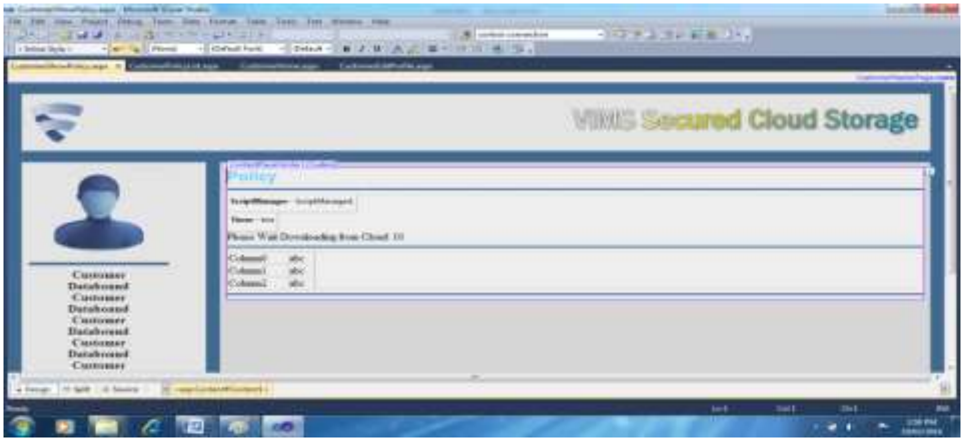
CustID	Databound
Name	Databound
Address	Databound
ContactNo	Databound

SqlDataSource - SqlProfile

Fig 5.10 Edit User Profile

Agent can edit user's profile by adding new credentials.

11. Show Policy



ScriptManager - ScriptManager1

Timer - tmr

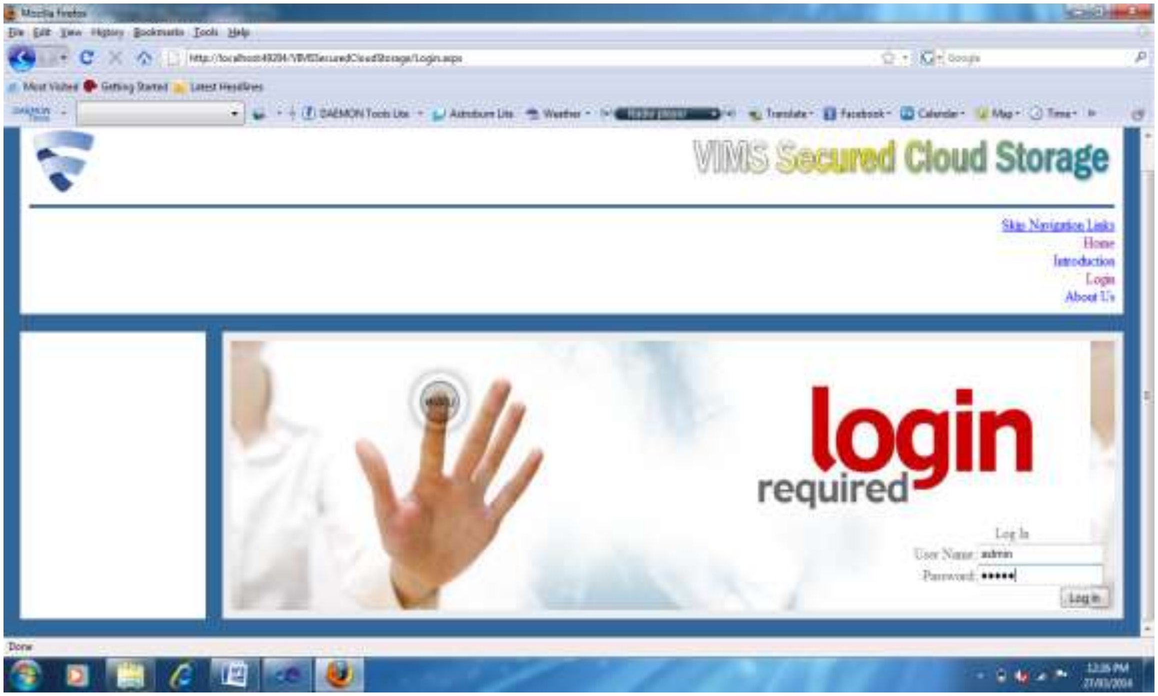
Please Wait Downloading from Cloud 10

Column0	abc
Column1	abc
Column2	abc

Figure 15. Show policy It shows the individual policy details.

Empirical technical investigations conducted for our project are self explained with respective snapshots:

Step1: This is the starting window for login of Administration Department.



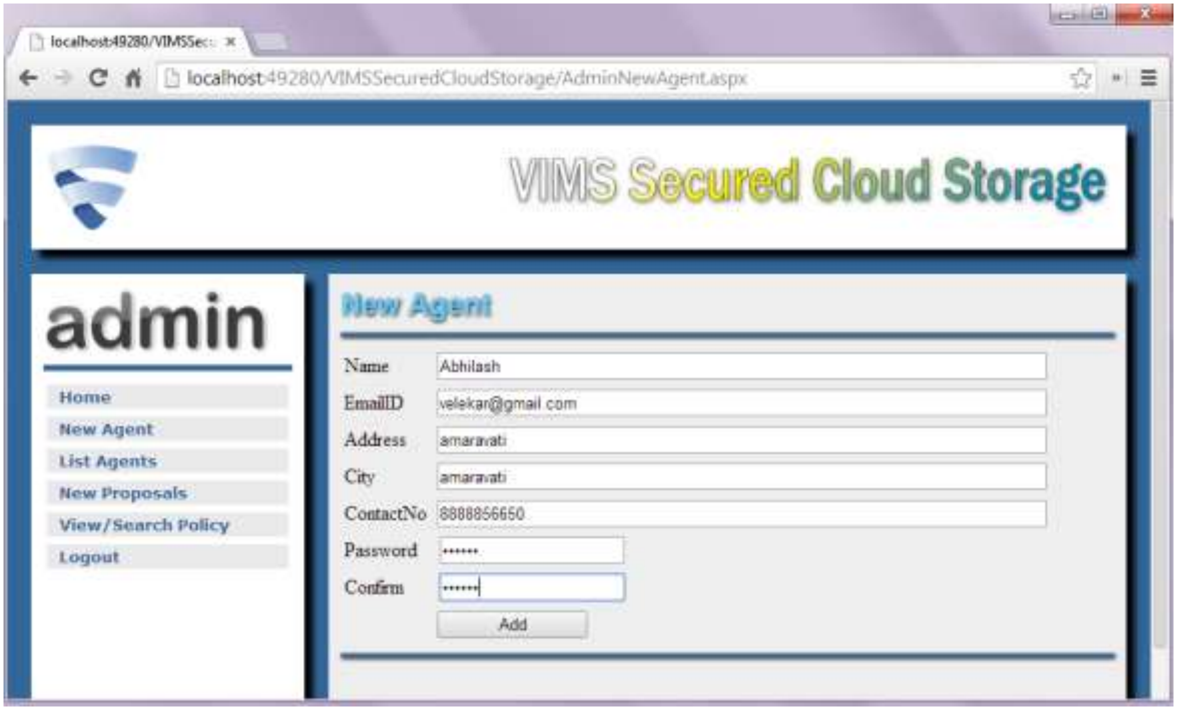
Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://localhost:49284/VIMSSecuredCloudStorage/Login.aspx
Most Visited Getting Started Latest Headlines
DAEMON Tools Lite Astroburn Lite Weather Translate Facebook Calendar Map Time
VIMS Secured Cloud Storage
Skip Navigation Links
Home
Introduction
Login
About Us
login
required
Log In
Log In
Done
12:35 PM
27/03/2014

User Name: admin

Password: •••••

Figure 16. Admin Login

Step 2: In Administration Department we can add New Agent the form for Add New Agent is as shown below

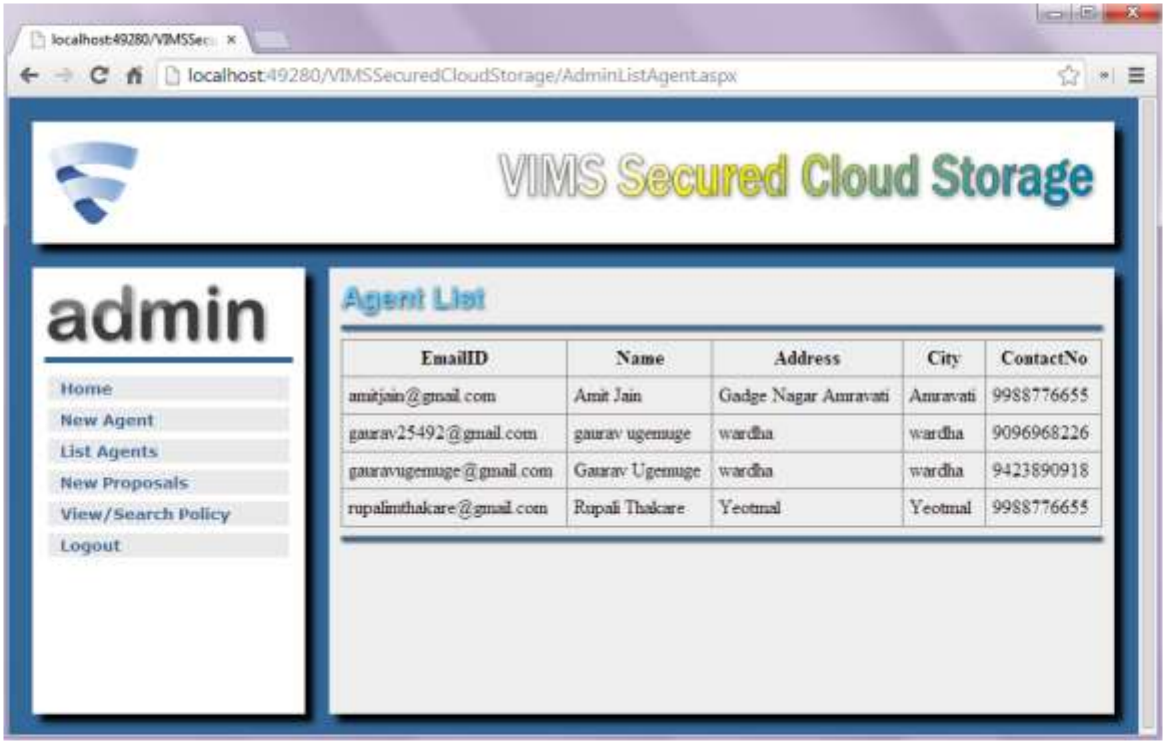


New Agent

Name	Abhilash
EmailID	velekar@gmail com
Address	amaravati
City	amaravati
ContactNo	8888856650
Password	•••••••
Confirm	•••••••

Figure 17. Add New Agent

Step 3: List of Agent is shown in shown

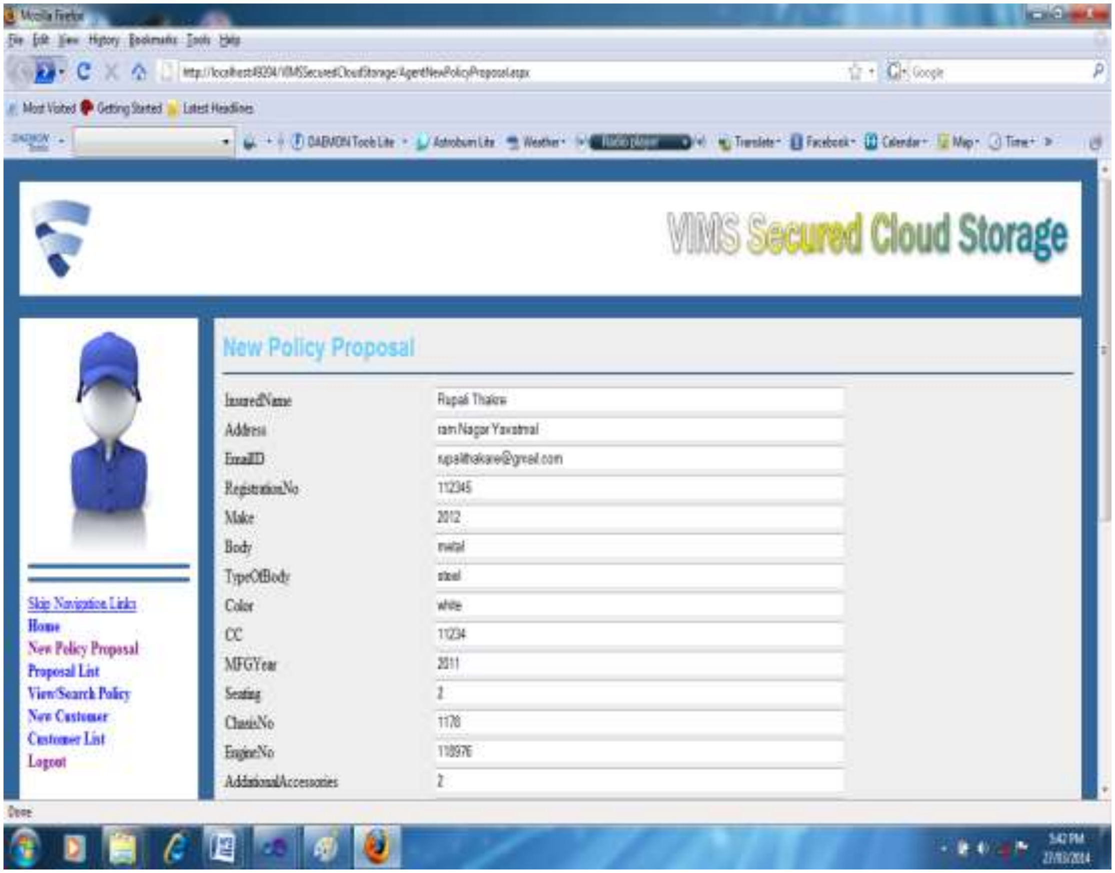


Agent List

EmailID	Name	Address	City	ContactNo
amitjain@gmail.com	Amit Jain	Gadge Nagar Amravati	Amravati	9988776655
gaurav25492@gmail.com	gaurav ugemuge	wardha	wardha	9096968226
gauravugemuge@gmail.com	Gaurav Ugemuge	wardha	wardha	9423890918
rupalimthakare@gmail.com	Rupali Thakare	Yeotmal	Yeotmal	9988776655

Figure 18. List of Agent

Step 4: New Policy Proposal Details



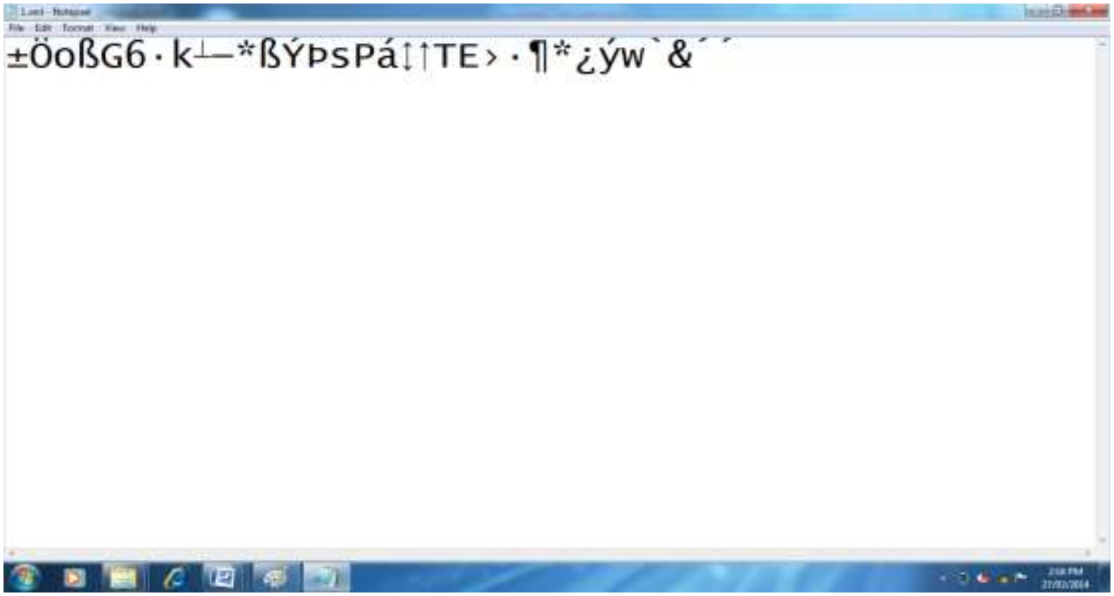
New Policy Proposal

InsuredName	Rupali Thakre
Address	ram Nagar Yavatmal
EmailID	rupalithakare@gmail.com
RegistrationNo	112345
Make	2012
Body	metal
TypeOfBody	steel
Color	white
CC	11234
MFGYear	2011
Seating	2
ChasisNo	1178
EngineNo	118976
AdditionalAccessories	2

Figure 19. New Policy Proposal

Step 5: Outcomes of the Project

A padded or encrypted message of a readable message is obtained thereby, securing there readable message between the communicating path of sender and receiver. Parallelisms been applied appropriately at some instances and program-code generates padded message successfully. The difficulty level of generation of cipher-text of the message has also been learnt by means a implementer, thereby demonstrating the importance of the algorithm which is dominating the field of cryptography for last 35 years.



```
±ÖoßG6·k┴─*ßÝÞsPá↕↑TE›·¶*¿ýw`&´´
```

Figure 20. Data Stored on Cloud In Encrypted Format

Conclusion and Future Scope

A computerized Vehicle Insurance Management System has been developed and the system was tested with sample data. Data are stored on cloud in encrypted format for providing more security. The system can be used to make better management described at appropriate time.

1. The present algorithms for calculating message digests are susceptible to brute force and rainbow table based attacks. We can further improve these classes of algorithms such that they can’t be decrypted by any ordinary means practically.
2. We can also work more on these algorithms so as to improve the space and time complexity further.
3. The algorithm we have proposed and implemented shows a randomness efficiency of around 70 percent. We can further improve these efficiency in the future works.

4. The use of MD5 in some websites' URLs means that any search engine (Google) can also sometimes function as a limited tool for reverse lookup of MD5 hashes. We can design tools like the modified version of present day salts to improve these.

References

1. *Sachdev Abha,and Mohit Bhansali"Enhancing cloud computing security using AES algorithm",IJCA,volume 67 No-09,April 2013.*
2. *Zlnidong Shen and Qiang Tong,"The security of cloud computing system enable by trusted computing technology",ICSPS,volume 976-1-4244-6893.*
3. *Sanjoli Singla and Jasmeet Singh"Cloud data security using authentication and encryption technique"IJARCSE volume 2, Issue 7, July 2013.*
4. *S.W.Wasankar, Dr. P.R.Deshmukh,"Implementation of Data Storage Security in private Cloud" volume 2, Isssue 4, April 2013, ISSN 2278-733X.*
5. *Leena Khanna, Prof Anant Jaiswal,"Cloud Computing: Security Issues & Description of Encryption Based Algorithm To overcome Then" volume 3, Issue 3, March 2013.*
6. *Bhavna Makhija, Vinitkumar Gupta,Indrajit Rajput,"Enhanced Data Security in Cloud Computing without party Auditor,"Volume, Issue 2 Februvary 2013.*