Implementation of Multifactor Authentication System for Accessing Cloud Service

Sumathi M[*], Sharvani G.S[**], Dinesha H A[**]

[*] MTech in Computer Science, R.V. College of Engineering, Bangalore
[**] Professor, R.V. College of Engineering, Bangalore
[***] PES Institute of Technology, Bangalore

Abstract- Authentication is an important process in any system to verify whether someone is in fact. In any type of computer network such as private or public, authentication needs username and password. Password is a secrete key to verify the person is authentic. When user wish to use a system, first thing is user has to register with the system, then unique code is assigned for that person. On each subsequent use, the user must know and use the previously declared password. Authentication and authorization plays a major role which accessing the cloud service from vendors. Cloud customers should be authenticating enough to use the cloud services. Cloud authentication could be done in many ways like textual password, biometrics and graphical etc. In this paper, we are presenting the implementation details for Multifactor Authentication System which authenticates the customer in multiple levels using multidimensional and multilevel password generation technique.

Index Terms- authentication, cloud computing, cloud security, multifactor authentication, password generation.

I. INTRODUCTION

Cloud computing technology is an open standard and service-based, Internet centric, safe, fast and convenient data storage and network computing services [1].

In these days each and every organization such as association, group, institute, union, business etc uses cloud computing. The benefits of cloud computing are vast. Cloud computing provides highly scalable data solutions to businesses, infrastructure cost is reduced [2], location independent, low cost. In cloud computing the data accessibility is increased and improved flexibility. So the security of cloud computing is reduced. Providing a security to cloud environment is a major issue. Cloud computing environment is not a place to store sensitive data. To provide security to cloud is also a challenge task. Dealing with "single cloud" providers is predicted to become less popular with customers due to risks of service availability failure and the possibility of malicious insiders in the single cloud.

One of the primary benefits of cloud computing is a vast amount of computing power, achieved from relatively low-cost personal computers and servers. When you tap into the power of the cloud, you get supercomputing power at personal computer prices. Figure 1 illustrates how individual users connect to the cloud from their own personal computers or portable devices, over the Internet. To these individual users, the cloud is seen as a single application, device, or document. The hardware in the cloud (and the operating system that manages the hardware connections) is invisible [3].

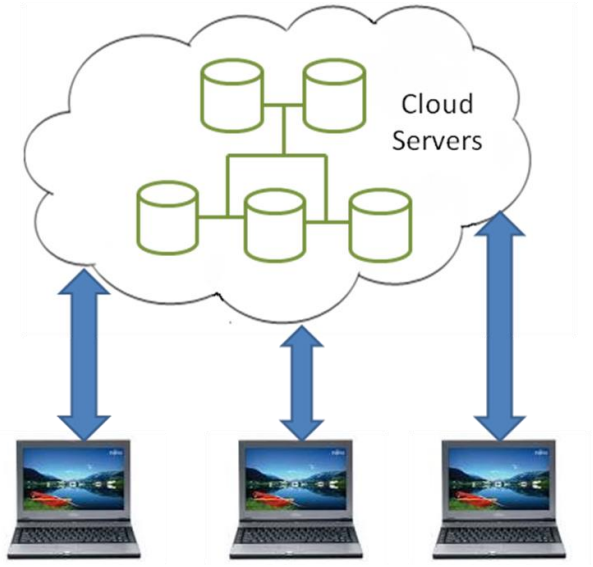

Figure 1: How users connect to the Cloud

Figure 2 portray the Architecture diagram for usage of cloud computing system. This is how users select a task or service. The user's request then gets passed to the system management, which finds the correct resources and then calls the system's appropriate provisioning services. These services carve out the necessary resources in the cloud, launch the appropriate web application and either creates or opens the requested document. After the web application is launched, the system's monitoring and metering functions track the usage of the cloud so that resources are apportioned and attributed to the proper users.

Cloud Computing Technologies are grouped into four different services as shown in Figure 3. They are SaaS (Software as a Service), DSaaS (Data Storage as a Service), IaaS (Infrastructure as a Service) and PaaS (Platform as a Service) [4].

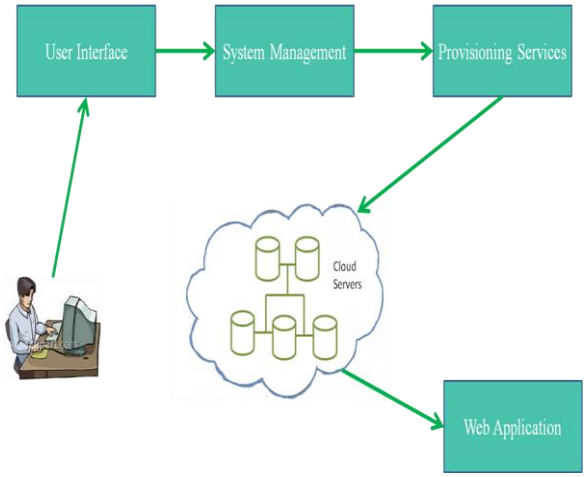

Figure 2: Architecture diagram for usage of cloud computing system

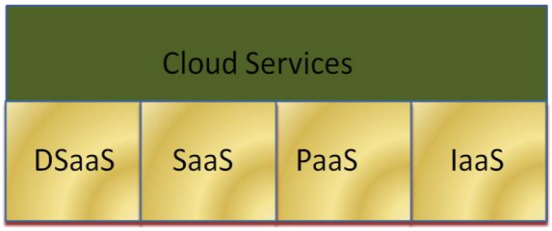

Figure 3: Services provided by Cloud Computing

Three types of models exist for providing services of cloud. These are referred are SPI models (Software, Platform and Infrastructure) [5]. At present cloud authentication systems are using methods: i) Simple text password ii) Third party authentication iii) Graphical password and iv) Biometric each technique has its own limitation. Another simple approach is to generate and authenticate the multidimensional password by considering many aspects of cloud paradigm.

The paper is organized in the following manner: Section 2 provides overview of Multifactor Authentication Technique along with the Architecture and Activity diagram. Section 3 provides the System Design along with Data Flow Design and Algorithms. Section 4 presents the Experimental details of the proposed system and interpretation of results. Finally, we conclude the paper with directions for further work in Section 6.

II. OVERVIEW OF MULTIFACTOR AUTHENTICATION TECHNIQUE

One of the most important issues related to cloud security risks is data integrity [6].The Multifactor Authentication technique generates multidimensional password in multiple levels, is a combination of Multidimensional [7] and Multilevel Technique [8]. Each level requires an authentication details. Based on the authenticated password, individuals can access the cloud services. Before generating password, user has to face the protocol user interface to enter the details. Based on the user interface inputs, password generates automatically and retains generated password to access the cloud data. Figure 4 shows, the architecture diagram of Multifactor Authentication System which has two separate entities

i) cloud service provider who provides the variety of cloud services and
ii) Authenticated client organization to use cloud services

There are three key areas of concern related to security and privacy of data. They are 1) location of your data 2) Control of your data 3) Secure transfer of your data [9]. Before using cloud services, company authentication confirms with service agreement from cloud vendors. This architecture helps in checking authentication against the services and privileges. It helps to ensure which customer has what kind of privileges to use cloud services. This is evaluated by multiple level authentications such as Service Authentication(SA), Team Authentication(TA) and Privilege Authentication(PA) with multidimensional password generation. The abstraction of a cloud hides the internal security details from clients [10].

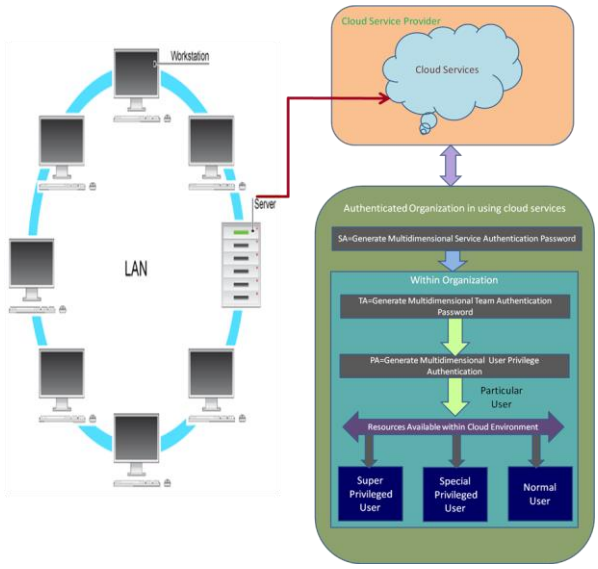

Figure 4: Architecture diagram Multifactor Authentication System

First level password generation: This level is organization level password generation to check against the particular cloud service. If unauthenticated organization or hackers tries to access the cloud services, they are terminated in this level itself. In this level, password generates based on many input parameters. For example to check organization authentication, one needs to enter organization name, private logo (which is different in size and dimensions compare to what organization published in internet/web) Company ID which is unique number is given by CSP (Corporate Service Provider) while registering to service agreement. Company signature which is scanned sign image of head of the company. These inputs processed with our algorithm and generated the multidimensional password. Algorithm adds the image and convert into number data, then concatenate with textual inputs. The resultant output will be SA (multidimensional Service Authentication) password.

Second level password generation: This level is a team level password generation to authenticate the team for particular service. Example team needs to enter the team name, team id, team thumb image and sign. First all images get added and convert into number data. This data gets concatenate with textual

inputs. The resultant output will be a TA (multidimensional team authentication) password.

Third level password generation: This level is a user level password generation. It authenticates the user privileges. User need to enter user name, age, phone number, id and DOB to generate his/her password. Algorithm will process these inputs and generate the PA(multidimensional privilege authentication) password. Organization password alone is not sufficient to access any cloud service. Organization password helps to move authentication into Intranet. Team password helps to move intra team and privilege password helps to access the cloud service for particular user. Figure 5 shows the Sequence diagram to generate Multidimensional Password.

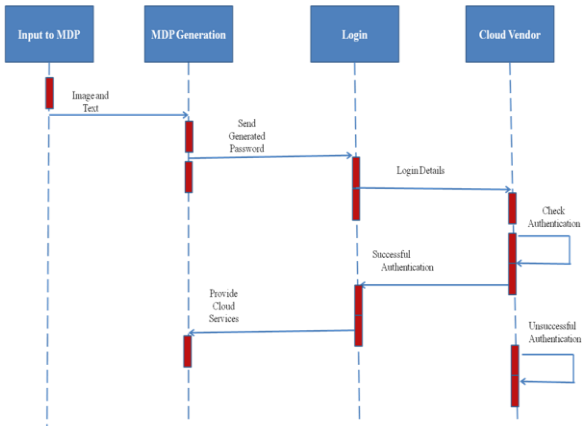

Figure 5: Sequence diagram to generate Multidimensional Password

Figure 6 shows the activity diagram for generation of password using Multifactor Authentication System. In this there are three levels to generate password such as Organization, Team, and User. In Organization level set of details are combined to generate password, these details contains image data, one text data called text1. This is also called password for corresponding user. The second level is the generation of administrator password is also called Team password. In this level image data and another text data called text2 are used to generate password. The third level also called last level image data and text3 data are combined to generate password.

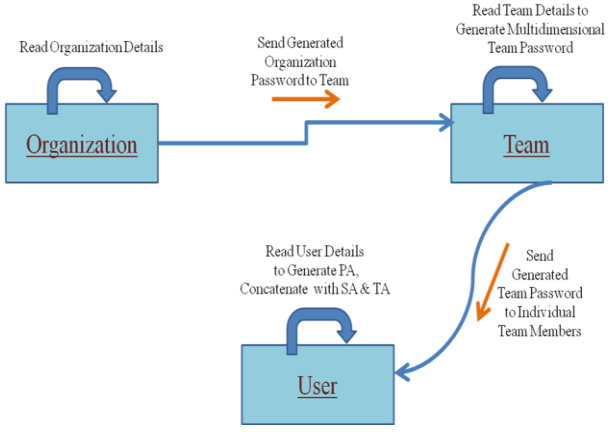

Figure 6: Activity diagram to generate multifactor authentication

This technique of password generation allows cloud environment to protect from Daniel of Service attack, Cloud Malware Injection Attack, Side channel Attack, Authentication Attack, Man-in-the-middle cryptographic attack[11], Network Sniffing [12] etc.. Authenticated client must know all levels details to use the cloud resources. Users are much concerned about the security of their private and confidential data [13].

III. System Design

A Data Flow Diagram (DFD) is a graphical representation of the "flow" of data through an information system. Data Flow models are used to show how data flows through a sequence of processing steps. The data is transformed at each step before moving on to the next stage. These processing steps transformations are program functions when Data Flow Diagrams are used to document a software design.

The Data Flow Diagram (DFD) can be decomposed into three levels such as level 0, level 1 and level 2. The level 0 is the initial level of Data Flow Diagram and it is generally called as the context level diagram. It is common practice for a designer to draw a context-level DFD first which shows the interaction between cloud and cloud vendor. The context level DFD is then exploded to show more details of the system being modeled.

The figure 7 shows the Level 0 Data Flow Diagram for Context Level. Context Level DFD shows the system boundaries, external entities that interact with the system, and major information flows between entities and the system. In this level 0 DFD, two entities have been indentified i.e. Strict Authentication System and strong Password Authentication. To check valid cloud vendor, he must provide valid authentication details such as, username and password. The complete Multifactor Authentication System is shown as a single process.

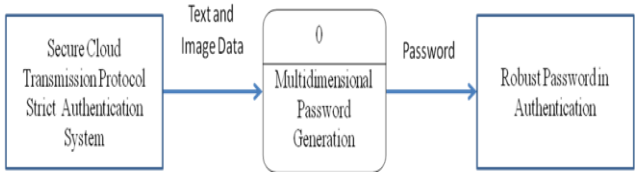

Figure 7: Level 0 Overview of Multi Dimensional password generation System

The first level DFD shows the main processes within the system. Each of these processes can be divided into further processes. The Level 1 diagram identifies the major processes at a high level and any of these processes can then be analyzed further rise to a corresponding Level 2 process diagram. This phase deals with the Cloud Environment Deployment.

Level 1 DFD for the Multifactor Authentication System using Multidimensional password technique is shown in figure 8. The main processes identified in Level 1 DFD are explained as follows.

1. Server initialization is the basic step to set up the cloud environment.
2. Before deploying the cloud environment in the Local Area Network, Server checks all details.

3. Server establishes a cloud environment, with available details such as which system's data is sharable in the cloud environment.
4. Using the Remote Method Invocation (RMI) Technique Server establishes a connection with all valid cloud clients
5. It is common practice for a designer to draw a context-level DFD which shows the interaction between cloud vendor and other cloud client. The context level DFD is exploded to show more details of the system being modeled.

All the processes executed gives back the result to the user interface nothing but System Administrator.

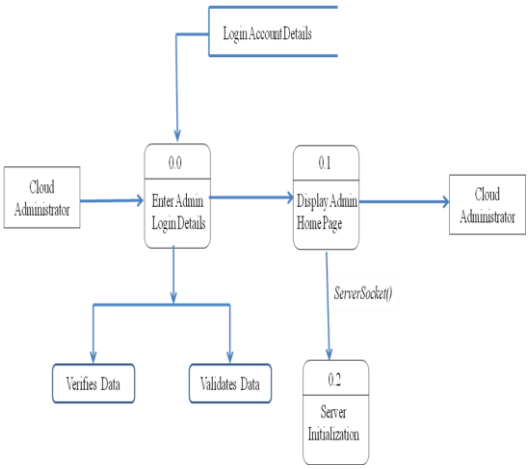

Figure 8: Level 1 DFD for Cloud Environment Server Node Applications

The Level 2 Data Flow Diagram gives more information than the Level 1 Data Flow Diagram. The Figure 9 shows Level 2 DFD for Cloud Environment Server Applications of IP addresses.

The Cloud Environment Server Application for IP Addresses is divided into three processes, viewing all valid IP addresses Cloud Environment Clients, process to remove any specific IP address from the Cloud Environment, process to add a new valid IP address to Cloud Environment.

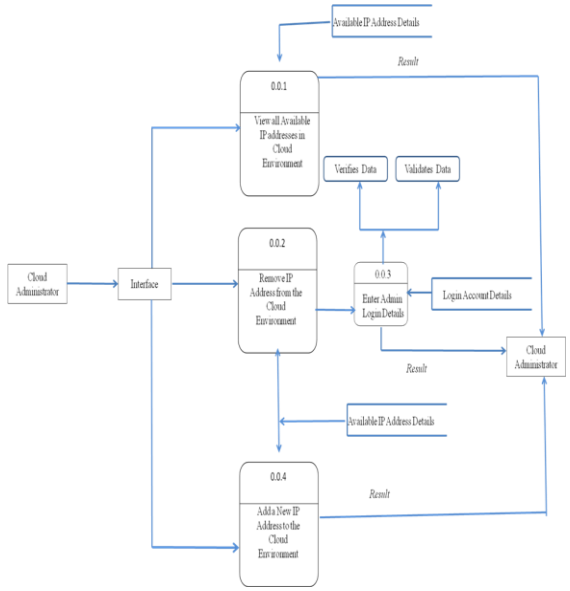

Figure 9: Level 2 DFD for Cloud Environment Server, Applications related to IP Addresses

The Figure 10 shows Level 2 DFD for Cloud Environment Server Applications of Cloud Resources.

The Cloud Environment Server Application for Cloud Resources is divided into three processes, viewing all cloud accessible resources by valid Cloud Environment Clients, process to remove any specific Cloud Resource from the Cloud Environment, process to add a new Resource to Cloud Environment.

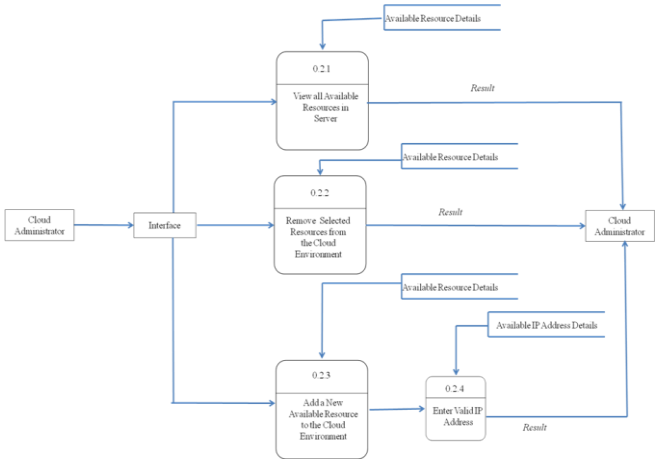

Figure 10: Level 2 DFD for Cloud Environment Server, Applications related to Cloud Resources

The Level 2 Data Flow Diagram for Multifactor Authentication System gives more information of Secure Authentication. The Figure 11 shows Level 2 DFD for Cloud Environment Multifactor Authentication System. In this level 2 DFD Cloud Environment Multifactor Authentication System, two entities have been indentified i.e. cloud vendor and cloud client. In this level Cloud Environment Server creates a new User. In this to create new user server node accepts details such as name, age, gender, address, phone number, department, mobile number. Multifactor Authentication Technique is applied

on these data to generate a username, password and key for new cloud client.

In the Level 2 DFD for Cloud Environment Multifactor Authentication System, explains the high level view of the project how the security in the cloud environment is established between the cloud vendor and other cloud clients. In this the combination of all the data given such as, name, age, gender, address, phone number, department, mobile number generates the result at the end and gives username, password and key.

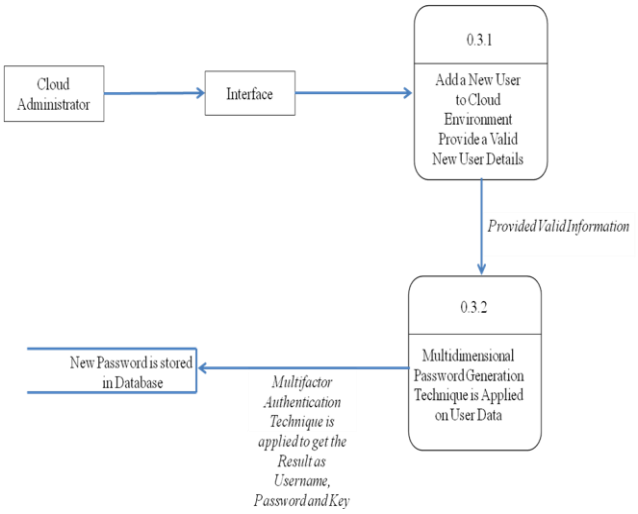

Figure 11: Level 2 DFD for Cloud Environment Multifactor Authentication System

Level 2 for Cloud Environment Client Applications contains the client interface, the user selects the event in the cloud, if the event is within the cloud environment range then the node processes the event and the client can download particular resource from the cloud environment server, and generates the event messages and passes the message to server to based on client request.

Algorithm:

- Algorithm: Multidimensional Password Generation

Step 1: Start
Step 2: Read input values such as Name, Age, Gender, Address, Phone Number, Department, Mobile Number
Step 4: Extract image feature
Step 5: Apply Encryption Algorithm
Step 6: Combine image features with input texts in a pre-defined sequence to generate Organization or Service Authentication (SA) Password
Step 7: Combine image features with input texts in a pre-defined sequence to generate Team Authentication (TA) Password
Step 8: Combine image features with input texts in a pre-defined sequence to generate User or privilege Authentication (PA) Password
Step 9: Authentication check : Multifactor Authentication Technique
If Service authentication is successful
Then
check Team level authentication
If Team Authentication is successful
Then
check Privilege level Authentication
If password for privilege level is successful then provide access to cloud environment.
else goto step 9
Step 9: Stop

IV. Experimental Details

For the implementation of this project flexible systems implementation language is needed. Compilation should be relatively straightforward compiler, provide low-level access to memory, provide language constructs that map efficiently to machine instructions, and require minimal run-time support. Program should be compiled for a very wide variety of computer platforms and Operating Systems with minimal change to its source code. For Graphical User Interface Programming, language chosen must be simple to use, secure, architecture neutral and portable. So Java is a best suited programming language, is used is to develop Multifactor Authentication System. Also features of such as Java Swing is used to design front end. Remote Method Invocation(RMI) is used provide a socket connection between nodes.

First thing we need to consider is the Initialization of server module. It has some set of procedures. In this, first step is to set the classpath, second is display the authentication screen in front end, third is start RMI registry, fourth is system administration verification and validation. Figure 12 illustrates the System Administrator Authentication Module. In this first step is to set the classpath, second is display the authentication screen in front end, third is start RMI registry in backend, fourth is system administration verification and validation.

System administrator has the following responsibilities:

- Setup and maintaining user accounts this is also called user administration
- Maintain system
- Verify that peripherals are working properly
- Monitor system performance
- Create file system
- Install software
- Create backup and recovery policy
- Monitor network communication
- Update system as soon as new version of OS and application software comes out
- Implement the policies for the use of the computer system and network
- Setup security policies for users.

Figure 12: System Administrator Authentication system

Once System administrator gets entry to cloud environment, then he can perform the following actions:

- Start server
- Available IP addresses
- Available Resources
- Add Newuser

Figure 13 shows the System Administrator Main Page which includes the above points. Start Server option is used to start RMI registry. RMI registry is used to setup a socket [14] between server and valid cloud clients. System Administrator has to click on this option to share data and message between server and clients. Once you click on Start Server option in backend RMI registry displays information as shown in Figure 14.

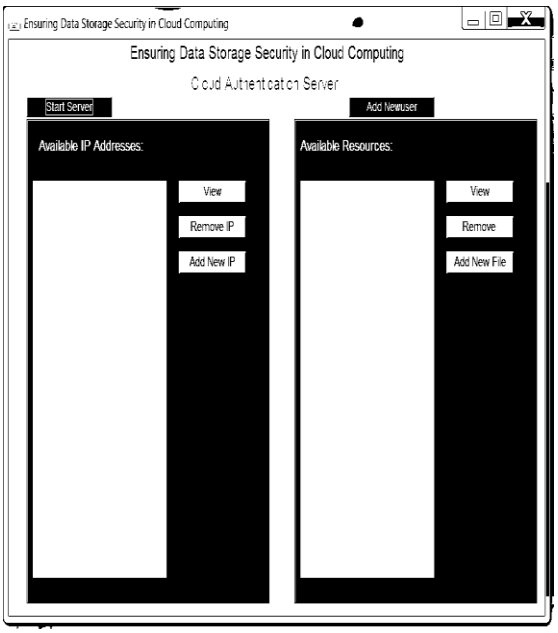

Figure 13: System Administrator Main Page

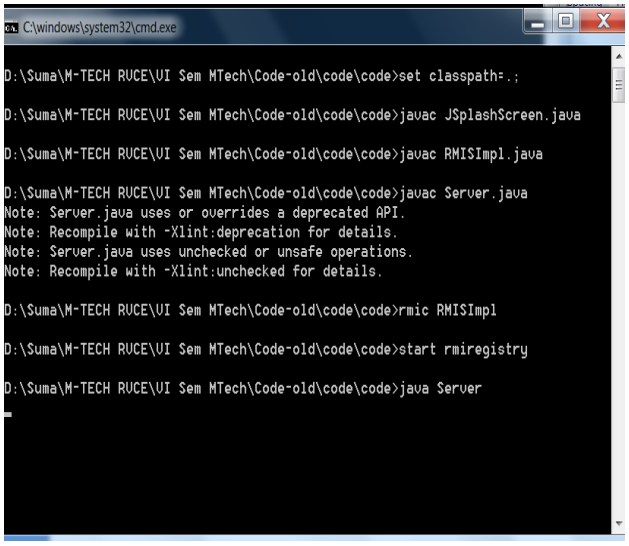

Figure 14: Initialization of server module

The next option is "Available IP addresses". This option contains the following sub sections:

- View
- Remove IP
- Add new IP

First thing is System administrator can view all IP addresses which are within cloud environment. Second option is if he wants remove any IP address from cloud environment he has to select that IP address then he has to provide the administrator key or password value. If it is a valid password then only the selected IP address will be removed else it will display an error message like "Invalid key word". Third option is to add a new IP address to cloud environment. In this system administrator has to provide a valid IP address to add that to cloud.

System Administrator next option is modifications of resources present in cloud. There are three sub options:

- View
- Remove
- Add New File

Administrator has full control over the data that is present in cloud. First thing is he can view all the data that is stored in cloud environment using "View" option. The second option is "Remove". This is simple, to remove any file from cloud if it no longer need for clients, first select the file and then click on Remove option. It will be removed interface but not from database. The third option is "Add New File". To add a new file Administrator has to provide the data for following option, and this is for security purpose.

- Enter the New Filename
- Enter the Fake Filename
- Enter the option of File Security
- Enter the IP Address

If the file is shared for a particular IP address, then only that node can access the file content from server not other nodes. While uploading a file to cloud environment system administrator has to provide more information that is for security

purpose such as, to protect data from unauthorized users. The shared file is available for client. From client node he can download that file.

System Administrator can add new user information. This is core of the Multifactor Authentication System. Multidimensional and multilevel authentication algorithms are applied on the data that is provided for the new user. The data include user name, age, gender, address, phone number, department, mobile number. All the data is encrypted and internal image is added to generate password, admin password and key for the new user. Text box validation is done in this and if you leave any textbox empty it will display error message. And in this age should be more than zero. And for Gender three options are given such as male, female, others. Figure 15 illustrates the New User Details.

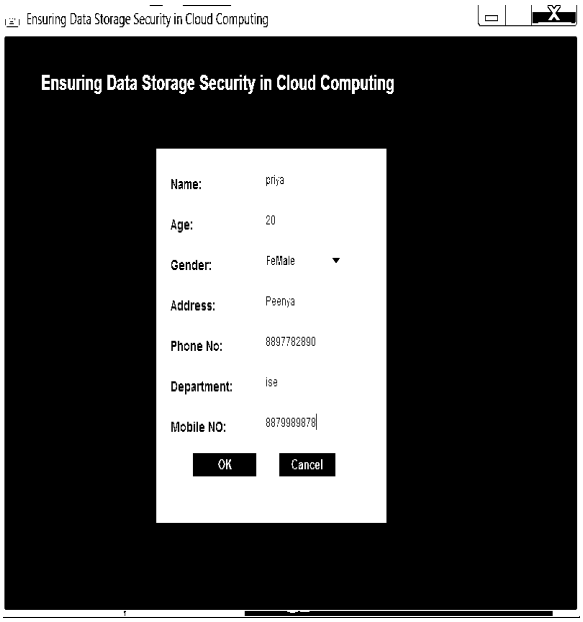

Figure 15: To Add new User

To access the cloud data client must login with valid credentials. First client has to set the classpath, second step is to start the socket connection with the server. Client has to provide valid authentication details to access the data.

Figure16 shows the Authentication module for client. Client has to provide the following data

- Username
- Password
- Admin password
- Key code

For the security reason all the above details has to filled by the client. Once all these details are correct then the client main page will be displayed else for each stage it will display error message. The steps are explained as follows.

- First step is Enter User Id and Password of valid client user
- If this is correct then enter Admin Password
- The last step is enter the key code

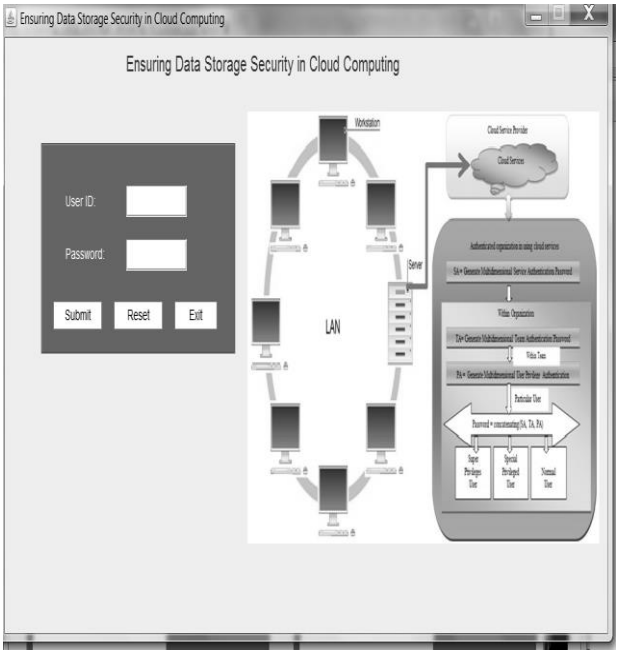

Figure 16: Client Authentication module

V. Conclusion and Future Work

The Multifactor Authentication System is the combination of Multilevel and Multidimensional Password generation Technique. The password generation technique proposed in this work relies on applying different authentication levels and dimensions. Using different authentication techniques protects especially sensitive data from Cloud Malware Injection Attack, Side channel Attack, Authentication Attack, Man-in-the-middle cryptographic attack, Network Sniffing etc. Cloud computing provides variety of Internet based on demand services like software, hardware, server, infrastructure and data storage. To provide privacy services to intended customer, it is better option to use multifactor authentication technique. This technique helps in generating the multidimensional password in many levels of organization so that the strict authentication and authorization could be possible against to the services as well as privilege. To provide privacy services to the intended customer, it is a better option to use Multifactor Authentication technique**.**

The project can be enhanced to use different encryption algorithms like Twofish, Blowfish [15] etc depending on user's choice to suite the application being protected. The project can be enhanced to address more number of attacks through mobile phone to get hackers information and other real world requirements. The performance evaluation of the project can include some more metrics like speed of data flow from server to client, memory usage, network throughput etc also overhead of each node to access the data from server.

Acknowledgement

Our sincere thanks to Dr. B. S. Satyanarayana, Principal, R.V.C.E, Bengaluru, and Dr. N. K. Srinath, Head Department of

Computer Science and Engineering, RVCE, Bangalore, for their valuable suggestions and expert advice.
Also we extend our sincere thanks to Prof. K.N.B.Murthy, Principal, and Prof. Shylaja S S, Head Department of Information Science and Engineering, PESIT, Bangalore,for their constant support and encouragement.

REFERENCES

[1] Dinesha H A, Dr. V. K Agrawal, "Framework Design of Secure Cloud Transmission Protocol", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 1, No 1, January 2013, ISSN (Print): 1694-0784 | ISSN (Online): 1694-0814,74-81.

[2] Nandini Mishara, Kanchan Khushwha, Ritu Chasta, Er. Abhishek Choudhary, "Technologies of Cloud Computing – Architecture Concepts based on Security and its Challenges, International Journa of Advanced Research in Computer Enginering and Technology (IJARCET), Volume 2, Issue 3, March 2013

[3] Michael Miller, "Cloud Computing, Web-Based Applications That Change the Way You Work and Collaborate Online", Pearson, Eight Impression, 2013.

[4] Atif Alamri, Wasai Shadab Ansari, Mohammad Mehedi Hassan, M.Shamim Hossain, Abdulhameed Alelaiwi, M.Anwar Hossain, "A Survey on Sensor-Cloud: architecture, Applications, and Approaches, Hindawi Publishing Corporation, International Journal of Distributed Sensor Networks, Volume 2013, Article ID 917923, 18 pages, 2013

[5] Anu Rathi, Yogech Kumar Anissh Talwar, "Aspects of Security in Cloud Computing", International Journal of Engineering and Computer Science ISSN: 2319-7242, Volume 2, Issue 4, April 2013, Page no. 1361-1363

[6] T. Neetha, CH. Sushma, "Security for Effective Data Storage in Multi Clouds", International Journal of Computer Applications Technology and Research, Volume 2, Issue 1, 16-17, 2013

[7] Dinesha H A, Dr. V. K Agrawal, "Multi-dimensional Password Generation Technique for accessing cloud services", Special Issue on: "Cloud Computing and Web Services", International Journal on Cloud Computing: Services and Architecture (IJCCSA), Vol.2, No.3, June 2012, 31-39.

[8] Dinesha H A, Dr.V.K.Agrawal, "Formal Modeling for Multi-Level Authentication in Sensor-Cloud Integration System", International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868, Foundation of Computer Science FCS, New York, USA Volume 2– No.1, May 2012 – www.ijais.org

[9] Bhavna Makhija, VinitKumar Gupta, Indrajit Rajput, "Enhanced Data Security in Cloud Computing with Third Party Auditor", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN : 2277 128X, Volume 3, Issue 2, February 2013

[10] Farhad Ahamed, Seyed Shahrestani and Athula Ginige, "Cloud Computing: Security and Reliability Issues", IBIMA Publishing, Communicaions of the IBIMA, Vol.2013, Article ID 655710, 12 pages, DOI: 10.5171/2013.655710, 2013

[11] A.M. Lonea, D.E.Popescu, H.Tianfield, "Detecting DDoS Attacks in Cloud Computing Environment", INT J COMPUT COMMUN, ISSN 1841-9836, 8(1):70-78, February, 2013

[12] Dr. A.Padmapriya, P.Subhasri, "Cloud Computing: Security Challenges and Encryption Practices", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 3, Issue 3, March 2013

[13] Azeem Sarwar, Muhammad Naeem Ahmed Khan, "A Review of Trust Aspects in Cloud Computing Security", International Jouranl of Cloud Computing and Services Science (IJ-CLOSER), Vol.2, No.2, April 2013, pp. 116~122, ISSN: 2089-3337

[14] Wei-Min Jeng, Hsieh-Che Tsai, "An Open MPI-based Cloud Computing Service Architecture", International Journal of Information Technology and Computer Science (IJTCS), ISSN no: 2091-1610, Volume 7, N0.4, Issue on January/February, 2013

[15] Leena Khanna, Prof. Anant Jaiswal, "Cloud Computing: Security Issues and Description of Encryption Based Algorithms to Overcome Them", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 3, Issue 3, March 2013

AUTHORS

First Author – Sumathi M, MTech in Computer Science, R.V. College of Engineering, Bangalore
Second Author – Sharvani G.S, Professor, R.V. College of Engineering, Bangalore
Third Author – Dinesha H A, PES Institute of, Technology, Bangalore