A Trusted new method for Authentication and Security for Web Applications in Cloud using RSA Algorithm

K V V Satya Trinadh Naidu [1], Dr. A Radha Krishna [2], G Kumari [3]

P.G. STUDENT, DEPARTMENT OF CSE, PRAGATI ENGINEERING COLLEGE, SURAMPALEM, AP [1] Associate Professor, DEPARTMENT OF CSE, PRAGATI ENGINEERING COLLEGE, SURAMPALEM, A.P [2] Assistant Professor, DEPARTMENT OF CSE, PRAGATI ENGINEERING COLLEGE, SURAMPALEM, A.P [3]

***Abstract* -** Cloud stands for Common Location independent Online Utility on Demand services (or) Communities Libraries, Online Union Database which is abbreviated from AT&T (American Telephone & Telegraph) corporation. Now a day's cloud computing is one of the outstanding generation to provide wide form of services consisting of Software-as-a-Service, Infrastructureas-a-Service, Platform-as-a-Service, Data-as-aService and Voice-as-a-Service and many others. Cloud computing is a brand new innovated technology which offers various competencies to the users on call for foundation. In cloud computing facts storage is one of the famous offerings which stores records at remote servers and decreases cost at client aspect. Apart from the blessings cloud also lagging in presenting authentication, safety, integrity, availability to the person's information due to information isn't always beneath control of end user. Secret word and short message based validation strategies are at present the most famous ones to confirm portable clients. Be that as it may, there is numerous security dangers associated with these verification techniques.In this paper, proposed a Novel verification based on multifactor parameters strategy.

Keywords: Authentication, Cloud Computing,
Hashing, Server, Client, Security issues.

I.INTRODUCTION

With the fast boom of garage era and the achievement of the Internet, laptop sources have grow to be cheaper and more effective than earlier than and they'll be determined everywhere. This fashion gave upward push to a new subject matter, specifically cloud computing, where the assets (e.g. CPU and Memory) may be utilized by users and the Internet as a public tool, considering the necessities, and they'll later receive again. In a cloud computing environment, the traditional role of carrier companies may be divided into two parts: infrastructure providers that control the cloud platform and rent and retrieve assets given the value version according to the use, and provider companies that lease assets from one infrastructure issuer or more to deliver to give up clients. The emergence of cloud computing has substantially affected IT subjects in current years. In fact, cloud computing provides job proprietors with attractive advantages which include decreased realistic expenses, high scalability, clean accessibility, and reduced commercial enterprise hazard and preservation expenses.

Considering the ever-growing boom within the use of cloud offerings and the tendency of users to adopt this service, the hackers also commenced to focus in this provider simultaneously. The phrase cloud to start with implied the garage of consumer data in area supplied by way of a 3rd celebration. That is, information turned into no longer stored at the user's pc difficult drive and it become stored someplace else which changed into reachable at all times and in each area. The person changed into able to get entry to the records at any area. Despite its numerous benefits, this technique also has risks. For instance, how might a corporation comply with shop its touchy facts at a vicinity other than its very own garage gadgets, wherein the agency does now not recognize who can get right of entry to the aforesaid data? That is why distinct threats and protection mechanisms have been developed. As you realize, in the general public of cases wherein security is breached, the aim is to break the confidentiality of data, records accuracy, and facts accessibility. Given brute pressure attacks, the username and password mechanism turned into proven to be bad extra than ever.

Organizations and people expect distinct security parameters to be employed for growing the safety of gets right of entry to their sensitive records. With all the reasons provided, the primary and most critical step inside the design of a system is its safety. Cloud computing customers ought to be authenticated if you want to use the assets. It is noteworthy that a superb number of assaults arise at this front gate. Hence, the layout of a ease mechanism to authenticate users is a massive aid to multiplied security of the entire system.

II. Cloud Service Models

Cloud is the architecture and a set of services that allow access resources on demand. It is a dynamically scalable, on-demand, multi-tenant and often virtualized resources which might be provided as a self-service over the Internet/Intranet; Public, Private and Hybrid Models. Cloud gives you the flexibility to deal with rapid paced customer requirements and also provide a dependable solution in your applications, which could have an option to scale incrementally without having a downtime. However, one desires to have a clear expertise on what unique effects are preferred before considering the cloud platform.[2]

Software as a Service (SaaS):

Software as a provider (SaaS) is a cloud computing presenting that offers customers with get entry to to a vendor's cloud-based totally software. Users do not install applications on their devices. Instead, the applications live on a far off cloud network accessed through the web or an API. Through the application, customers can keep and examine facts and collaborate on projects.

Platform as a service (PaaS)

Platform as a provider (PaaS) is a cloud computing presenting that provides users with a cloud environment wherein they can increase, manipulate and supply packages. In addition to storage and different computing resources, users are able to use a collection of prebuilt equipment to develop, customize and check their own programs.

Infrastructure as a service (IaaS) is a cloud computing providing in which a vendor offers users access to computing assets including servers, garage and networking. Organizations use their own systems and applications inside a service provider's infrastructure.

Security issues in cloud computing

Cloud computing isn't always a great deal cozy through nature. Cloud protection isn't precisely tangible hence there a false sense of protection and tension about what cloud information is without a doubt secured and controlled. There are worries associated with the integrity and confidentiality of information. There have to suitable safety features for cloud clients to acquire their perception. Although a few security features have been implemented to cloud infrastructure still the customers are waiting for greater security aspects for his or her statistics in clouds. The cloud data is vulnerable to various varieties of assaults. Theseare following attacks which can affect the cloud security [3]

1. **Password Guessing Attack:** This consists of various attacks which may be achieved for obtaining the person password.

2. **Replay Attack:** This assault consists of tracking the authentication packet and reproduces the information to the unauthorized customers.

3. Man-in-the-middle Attack: Here the attacker poses to be a user and attempts to accumulate the password from theserver.

4. Masquerade Attack: The attacker pretends to be a verifier and authentication keys from the user.

5. Insider Attack: Here the attacker deliberately steals the private facts of the user.

6. Phishing Attack: Social Engineering sites such as fake emails, web sites call for the person screen his password or authentication keys.

7. Shoulder Surfing Attack: Social engineering assaults specific to password systems where the attacker secretly directs looking at the password when the person enters it. [3]

The extra security can be achieved best through total transparency. We can put into effect security with the aid of taking into account following points:

i. Cloud computing structure ii. Portability and interoperability iii. Data centre operations iv. Notification and remediation v. Application Security vi. Encryption and Key management vii. Identity and get admission to control.[3]

Related Work

Techniques used in user Authentication:

The valuable idea in the back of the Security provision is to avoid the undesirable intrusion of unauthorized customers and right at the entry point. That is all of the customers whether new of present are not allowed to get admission to the facts or assets without proving their identification. The request from the customers are first

secret key play a completely crucial position in DES

encrypted after which sent to the cloud files. The algorithms used to encryption procedure are mentioned as follows:

Data Encryption Standard Algorithm:

protection, in order that a terrific key generation unit required. Using Dynamic key generator, the generated key has characteristics of unpredictability and unrepeatability. Using this approach the

Data Encryption Standard algorithm is a type of symmetric-key encipherment algorithms. Symmetric- key encryption is a sort of cryptosystem in which encryption and decryption are carried out using an unmarried (mystery) key. As we are able to see, procedure is also carried out approximately the person password requests, even as logging inside the system later. After receiving an encrypted record from the gadget the user's browser will decrypt it with RSA algorithm the use of the user's personal key. Similarly whilst the device receives an encrypted document from the person it will right now decrypt it the use of its private key. As a result the communication turns into secured among the consumer and the gadget. [4, 5]

AES Algorithm & MD5 Hashing Algorithm:

When a report is uploaded by means of an consumer the system server encrypts the document the usage of AES encryption algorithm. In this 128, 192, 256 bit key can be used. The key's generated randomly by way of the system server. A unmarried secret's used handiest once. That precise key is used for encrypting and decrypting a report of a user for that instance. This key is not further utilized in any example later. The key's kept within the database

with the consumer account is stored and maintained within the database desk on the storage server. Here user call is

OTP Password Algorithm:

used for synchronization among the database tables of important system server and the garage server. The encrypted files on the storage server are inserted now not serially. [10,11,12]

dynamic key generator can achieve the high speed and can be reduce logic complexity.

RSA Algorithm:

RSA encryption set of rules is used for making the communiqué safe. Usually the users' requests are encrypted even as sending to the cloud service provider machine. RSA set of rules the usage of the gadget's public key is used for the encryption. Whenever the user requests for a record the device sends it through encrypting it thru RSA encryption set of rules the use of the user's public key. Same desk of the system server along with the person account call. Before inserting the user account call it's also hashed the usage of md5 hashing. This insures that unauthorized person cannot retrieve the key to decrypt a particular

file for a specific user by means of genuinely gaining get admission to and watching the database desk of the machine server. As a result the key for a specific file turns into hidden and safe. Again while the encrypted file is uploaded for storing to the garage server, the course of the encrypted report together In this algorithm one time password has been used for authenticating the user. The password is used to keep the user account comfortable and secret from the unauthorized person. But the user described password can be compromised. To triumph over this difficulty one time password is used inside the

proposed safety model. Thus every time a person "SHA-1" produces a one hundred sixty-bit output logs within the machine, he can be supplied with a referred to as a message digest. brand new password for the use of it in the next login. This is typically supplied by means of the Syntax: system itself. This password could be generated Stringsha1 (stringsrc[,bool_raw_output]); randomly. Each time a brand new password is String source- defines the enter string. created for a person, the preceding password for Raw_output

that person will be erased from the device. New The raw_output is like a Boolean function this is: If password can be up to date for that precise person. FALSE (default) then it units raw 40-individual hex A single password might be used for login most quantity layout. If TRUE , it units raw 20-person effective once. The password will be sent to the binary layout.

customers authorized mail account. Therefore at a

identical time a check to decide the validity of the **III. PROPOSED SYSTEM** user is also accomplished. As an end result handiest authorized user with a valid mail account can be The proposed scheme presents multifactor capable to connect to the cloud system. authentication and encrypting user records with

different algorithms in line with user preference.

Blowfish

MULTI FACTOR AUTHENTICATION

Blowfish is yet another algorithm designed to replace

DES. This symmetric cipher splits messages into blocks Authentication is a mechanism which verifies users of sixty four bits and encrypts them in my view. Blowfish are legal or not to get entry to the sources. The basic is understood for each it's awesome velocity and authentication mechanism is login and password. It universal effectiveness as many claim that it has by no is two factor authentication mechanisms. In our means been defeated. Meanwhile, vendors have taken proposed system, we don't forget a couple of factors full gain of its unfastened availability in the public for authentication username, password and colour domain. Blowfish can be discovered in software classes value for authenticating person. The authentication starting from e-trade platforms for securing bills to manner is completed in two phases. 1. Registration password control gear, wherein it used to defend (Sign Up) Process and 2.Login Process. In passwords. It's actually one of the more flexible registration the process can be done in two ways. encryption techniques available. user is registered with enterprise server by means of presenting the non-public details, username, **Rijndael encryption Algorithm:** password, color and personal details. Once the registration completed, login to the web application Rijndael is the usual symmetric key encryption algorithm with the valid login details. Now Step 2 Registration for use to encrypt sensitive information. Rijndael is an form opened and their user can give the NONCE iterated block cipher, the encryption or decryption of a (Number that can be used once) Value, after that block of facts is done by way of the generation (a choose the appropriate Algorithm and public key, spherical) of a selected transformation (a round feature). these values are encrypted by using RSA Algorithm As input, Rijndael accepts one- dimensional eight-bit and send to the cloud server, the sever admin byte arrays that create information blocks. The plaintext decrypted these values and confirmed the is enter after which mapped onto nation bytes. The cipher registration by verifying their details, once register key is likewise a one-dimensional 8-bit byte array. With user genuine then the server admin give the an iterated block cipher, the extraordinary variations CLOUD Security

operate in sequence on intermediate cipher consequences Certificate to the register user. The password (states). **Secure Hash Algorithm 1 (Sha1):** and

The sha1 string feature is used to calculate the SHA-1 (Secure Hash Algorithm 1) hash of a string value. color details are saved inside the database in hash format. It is specially used for converting a string into 40- bit hexadecimal wide variety, that's so secured.

2. Compute n = a * b. **EXPERIMENTAL RESULTS**
3. Compute Euler's totient feature, Ø(n) = (a-1) * We implemented our consequences in (b-1). HTML, JS, AJAX and PHP, phpmyadmin and Xamp
4. Chose an integer e, such that 1 < e < Ø(n) and server, which presents exclusive classes and best commonplace divisor of e , Ø(n) is 1. functions for imposing encryption and hashing Now e is released as Public-Key exponent. algorithms. The evaluated results are shown below.
5. Now decide d as follows: d = e-1 (mod Ø(n))

Here, sha-1 (Secure Hash Algorithm 1) hash feature is implemented to transform password and coloration facts into hash format string into 40-bit hexadecimal wide variety, that's so secured. SHA-1" produces a one hundred sixty-bit output referred to as a message digest. The proposed approach provides strong security with the assist of color variable. Color is a value that's having the important thing space of [255,255,255] of RGB values. Generally user credentials are saved in cloud server and authentication is likewise achieved by way of cloud the server. In our proposed system, the user credentials are saved in business cloud server in hash format and encrypted format for a few sensitive values and verification is accomplished through cloud server without storing credentials at cloud server. Assume that business server is protected in a excessive comfortable way with the aid of the organization. The principal components included in this framework are

Authentication server, Preserving Privacy. To describe our approach, first user registered with business server by using presenting personal information, color facts generated with the aid of the client facet. Once registration is efficaciously completed the password along color value is stored in hash format. Here color is taken into consideration as mystery (secret) key.

RSA:

RSA set of rules is maximum widely a well-known cause technique to public-key encryption. It is an encryptiondecryption approach. It consists of plaintext and cipher textual content inside the shape of integers among 0 to n1. This simple text is encrypted in blocks; every and each block has a binary cost which needs to be less than n.

This set of rules is processed in 3 steps:

KEY GENRATION Before the statistics (information) is encryption key era need to be completed. This approach is done some of the cloud issuer and the user (client person).

1. Choose definite prime numbers a and b. For security features, the integers a and b should be selected at random and have to be of comparable bit length.

i.e., d is multiplicative inverse of e mod Ø(n).

6. d is saved as Private-Key component, So that d * e = 1 mod Ø(n).
7. The Public-Key consists of modulus n and the general public exponent e i.e., (e, n).
8. The Private-Key includes modulus n and the private exponent (private key) d, which should be saved secret i.e, (d, n).

CONCLUSION

In this paper, we applied multifactor authentication with much less computation by way of considering identification, password and color values as multifactor's which presents sturdy security examine to conventional authentication. We additionally implemented more than one encryption algorithms for encrypting messages and documents. The desire of encryption algorithm is achieved through the user .We also created a simple password generator with random class. All these offerings provide better safety to the data that is stored inside the cloud. The evaluated results show our frame work is combination of multiple services.

REFERENCES

[1] Chow R, Jakobsson M, Davis UC, Shi E (2010) Authentication in the Clouds: A Framework and its Application to Mobile Users. CCSW10, Chicago.

[2] Rajarshi Roy Chowdhury, Sylhet International University (2014) Security in Cloud Computing

[3] Mrs. S. M. Barhate, Dr. M. P. Dhore "User Authentication Issues In Cloud Computing"IOSR Journal of Computer Engineering (IOSR-JCE)e-ISSN: 2278-0661,p-ISSN: 2278-8727PP 30-35

[4] "Cloud Data Security Using Authentication And Encryption technique, Sanjoli single, Jasmeet Singh, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET). Volume2, Issue 7, July 2013.

[5] R.L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Laboratory for Computer Science, Massachusetts Institute of Technology, Cam-bridge, November, 1977

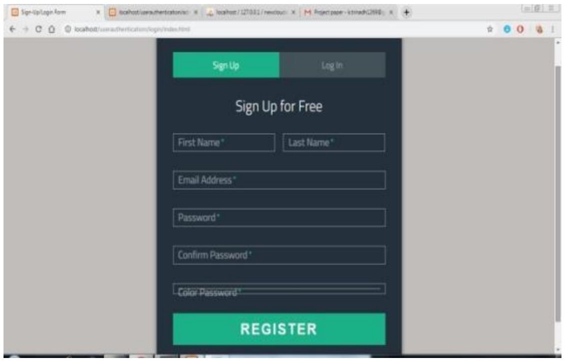
[6] RR Nadikattu, 2016 THE EMERGING ROLE OF ARTIFICIAL INTELLIGENCE IN MODERN SOCIETY. International Journal of Creative Research Thoughts. 4, 4 ,906-911.

[7] Sikender Mohsienuddin Mohammad, **"IMPROVE SOFTWARE QUALITY THROUGH PRACTICING DEVOPS AUTOMATION"**, International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume.6, Issue 1, pp.251-256, March 2018, Available at :http://www.ijcrt.org/papers/IJCRT1133482.pdf

[8] Rahul Reddy Nadikattu, "FUNDAMENTAL APPLICATIONS OF MACHINE LEARNING ACROSS THE GLOBE", International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume.6, Issue 1, pp.31-40, January 2018, Available at :http://www.ijcrt.org/papers/IJCRT1133453.pdf

[9] Sikender Mohsienuddin Mohammad, **"CONTINUOUS INTEGRATION AND AUTOMATION"**, International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume.4, Issue 3, pp.938-945, July 2016, Available at :http://www.ijcrt.org/papers/IJCRT1133440.pdf

Registration Page:



Sign Up for Free

First Name*

Last Name*

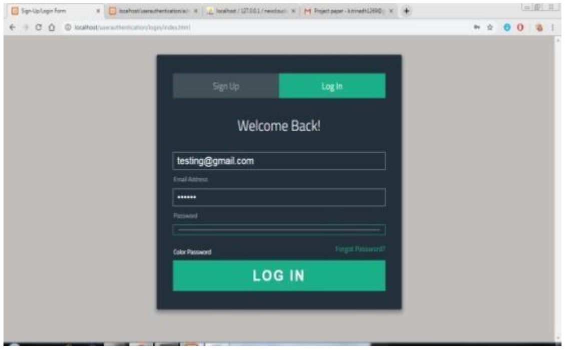
Email Address*

Password*

Confirm Password*

Color Password*

LoginPage:



Welcome Back!

testing@gmail.com

Email Address

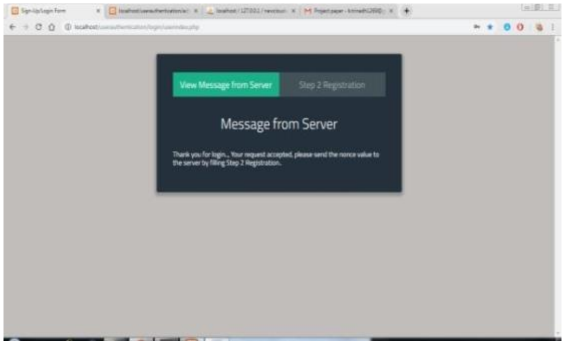
••••••

Password

Color Password

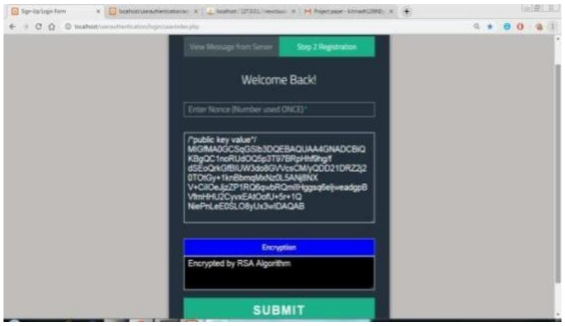
Forgot Password?

First Time Login by the user:



Message from Server

Thank you for login.., Your request accepted, please send the nonce value to the server by filling Step 2 Registration..

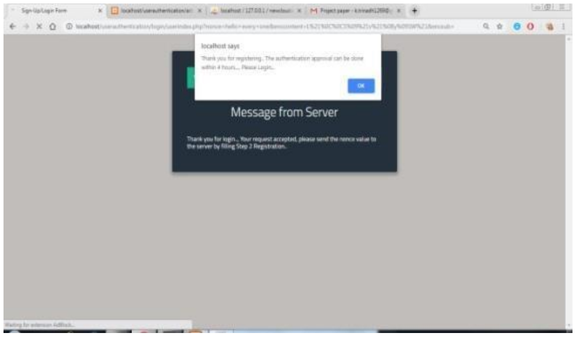


Welcome Back!

Enter Nonce (Number used ONCE)*

```
/*public key value*/
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQ
KBgQC1noRUdOQ5p3T97BRpHhf9hg/f
dSEoQrkGfBIUW3do8GVVcsCMlyQDD21DRZ2j2
0TOtGy+1knBbmqMxNz0L5ANj8NX
V+CilOeJjzZP1RQ6qwbRQmlIHggsq6eljweadgpB
VfmHHU2CyvxEAtOofU+5r+1Q
NiePnLeE0SLO8yUx3wIDAQAB
```

Encrypted by RSA Algorithm



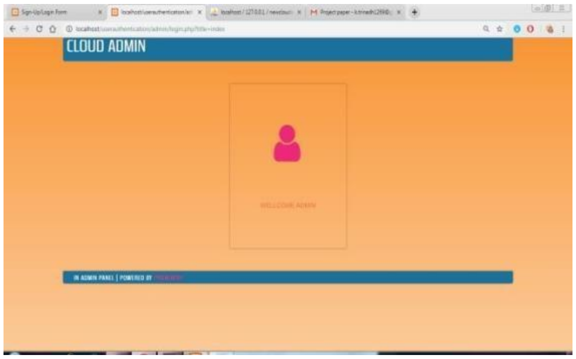
localhost says

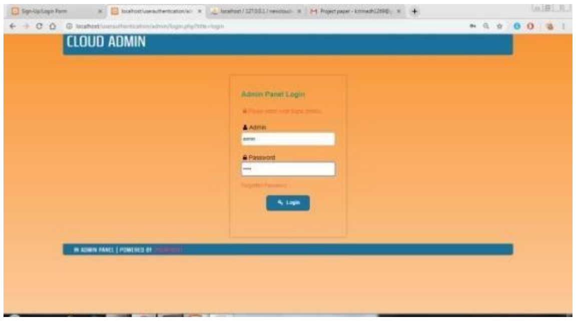
Thank you for registering.. The authentication approval can be done within 4 hours..., Please Login..

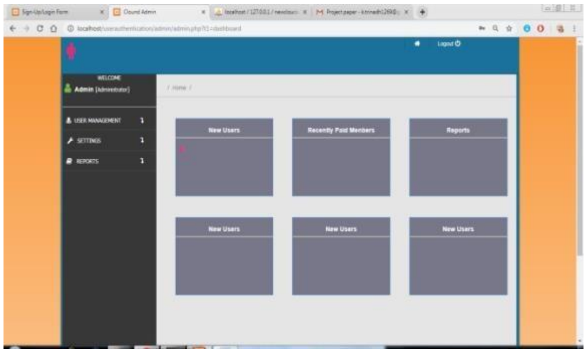
Message from Server

Thank you for login.., Your request accepted, please send the nonce value to the server by filling Step 2 Registration..

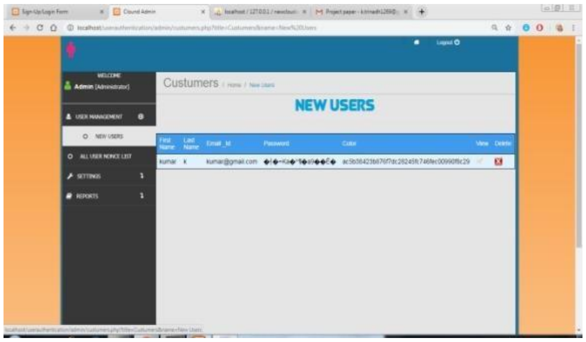
Admin Page:







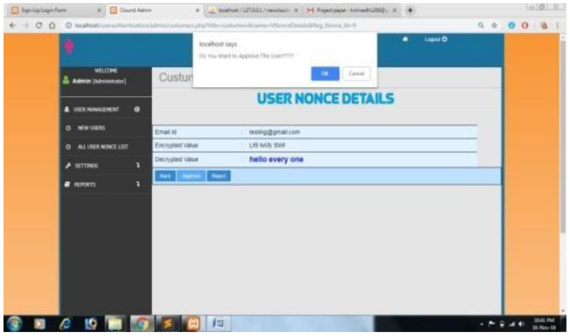
New Users:



NEW USERS

First Name	Last Name	Email_Id	Password	Code	View	Delete
kumar	k	kumar@gmail.com	◆!◆~Ka◆^¶◆a9◆◆É◆	ac5b38423b876f7dc28245ft746fec00990f8c29	✓	☒

All Users Nonce List:



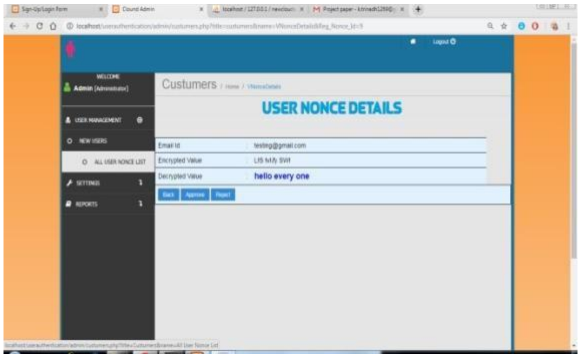
localhost says

Do You Want to Approve This User?????

USER NONCE DETAILS

Email Id	:	testing@gmail.com
Encrypted Value	:	LIS MJy SWI
Decrypted Value	:	hello every one

Click on the View Button:

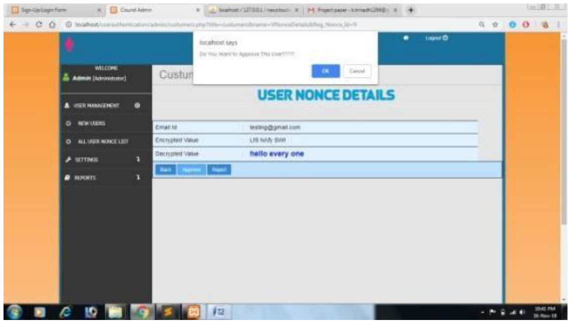


USER NONCE DETAILS

Email Id	:	testing@gmail.com
Encrypted Value	:	LIS MJy SWI
Decrypted Value	:	hello every one

The admin check the newly register user details, if there are valid details then admin will be approve, otherwise Reject the user account.

Click on the Approve Button:

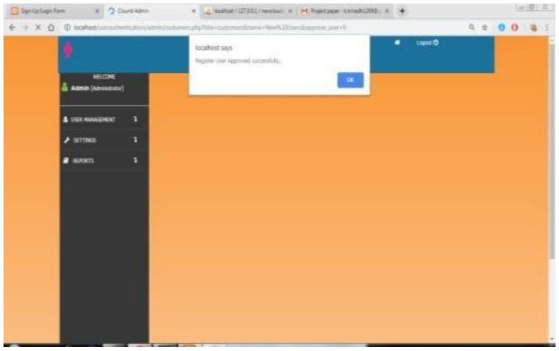


localhost says

Do You Want to Approve This User?????

USER NONCE DETAILS

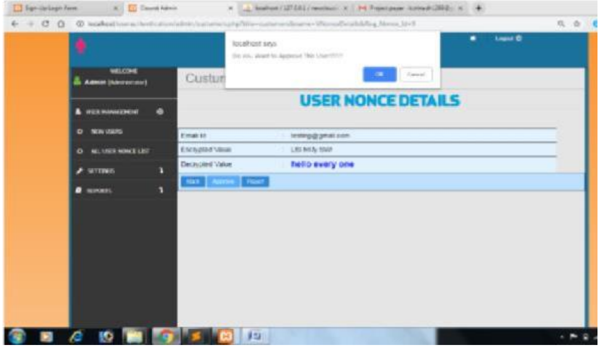
Email Id	:	testing@gmail.com
Encrypted Value	:	LIS MJy SWI
Decrypted Value	:	hello every one



localhost says

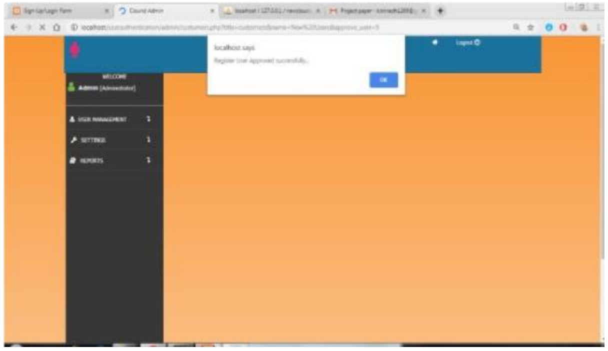
Register User Approved succesfully..

If Admin press the Reject Button

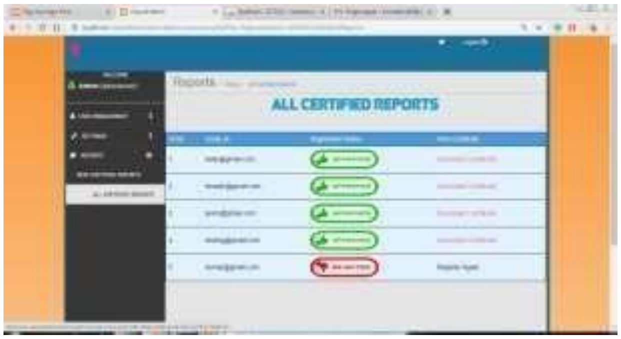

localhost says

Do you want to Approve This User????

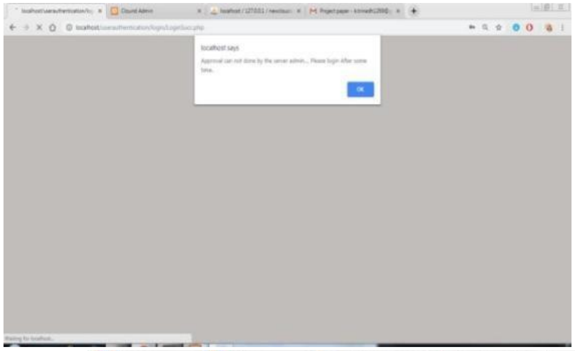
Email Id	testing@gmail.com
Encrypted Value	[illegible]
Decrypted Value	hello every one


localhost says

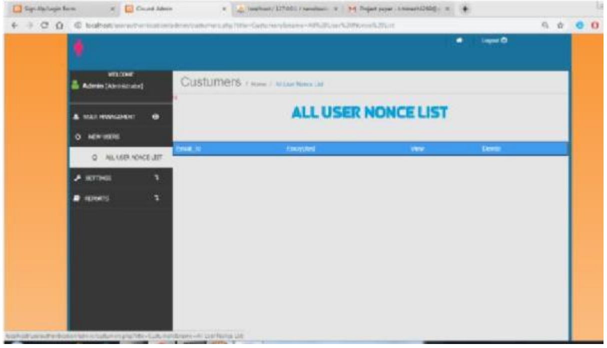
Register User Approved successfully..



If the user account has approved then user able to login otherwise it shows the following screen.


localhost says

Approval can not done by the server admin.... Please login After some time..



User’s Approved or Rejected List:

If the user account has approved then user can successfully login.

Mr. K V V S Trinadh Naidu is a student of Pragati Engineering College, Surampalem. Present he is pursuing his M.Tech from this college and he received his B.Tech from Sai Aditya Institute of Science and Technology, Surempalem, affiliated to JNTUK University, in the year 2012. His area of interest includes Cloud Computing and its objectives including Object Oriented Programming Languages, all current trends and techniques in Computer Science.

Dr. A Radha Krishna working as a Associate Professor in Pragati Engineering College. He has 19+ years of experience in teaching undergraduate students and post graduate students. His research interests are in the areas of Operating System, Computer Networks, Advanced Computer Networks, Artificial Intelligence and Neural Networks.

Mrs. G Kumari working as a Assistant Professor in Pragati Engineering College. She has 10+ years of experience in teaching undergraduate students and post graduate students. Her research interests are in the areas of Computer Networks, Wireless Sensor Network and Image Processing.