OPEN ACCESS INTERNATIONAL JOURNAL OF SCIENCE & ENGINEERING

PROVIDE DATA SECURITY USING 3DES AND DATA SHARING MECHANISM OF THREE FACTORS FOR CLOUD STORAGE SYSTEM

Miss. Swati R.Vibhute[1], Prof. Karwande V.S.[2]

P.G. Student, Computer Science & Engineering, Everest Educational Society's Group of Institutions, Aurangabad, Maharashtra, India.[1]

Asst. Professor Computer Science & Engineering, Everest Educational Society's Group of Institutions, Aurangabad, Maharashtra, India.[2]

vjy725@gmail.com[1], svibhute18@gmail.com[2]

Abstract: **Cloud storage is an appositeness of clouds that absolve organizations from establishing data storage systems. However, cloud storage enhances the security concerns. In case of groups-shared data, the data face both issues like cloud-specific and decorous insider threats. Securely data sharing among a group that counters insider threats of apropos up to now malicious users is an important research issue. Cloud computing has been rapidly changing modern computing environment. The problem of how to keep the confidentiality of user data against malicious entities including a CSP (cloud service provider) has been recognized as a significant issue. This problem becomes even more complicated if a data is shared among multiple users. In addition to existing system here we introducing the new factor for data security on cloud storage and for data sharing is figure impression i.e. this is the alternative for mobile if mobile OTP fails then it works.Using 3DES(Data Encryption Standard) algorithm we provide high level of security for securely data transmission on cloud storage system. The 3 Factor Secure Data Sharing methodologies include 3 Factor Secure access to sharing mechanism. Whenever a group membership is changed, only a new condition value is distributed to the users via cloud server. As a result, the overhead of each user becomes significantly reduced at each membership change. As result this system is provide high level of security for data sharing and storage on cloud.**

Keywords: *Three factor, factor revocability, cloud security using 3 DES, cloud storage*

I INTRODUCTION

Now a day we all know about a new technology is Cloud Computing. ***What is Cloud?*** Cloud i.e. relate to internet or network. In other words cloud is nothing but present at remote location. Cloud provides services atop network i.e. on private networks, on public networks i.e. LAN, WAN.

Cloud computing means what?

In cloud computing, instead of yours computer hard drives with the help of cloud you can easily storing and accessing data and programs on the internet .The word cloud are used as metonymy for the internet. With the help of this concept of cloud computing users are competent to access applications and software from anywhere and anytime.

Before cloud computing, most of the business applications have been very expensive and complicated. The variety of software's and hardware's required for run the applications. Lots of problems are faced like you need to whole expert team to install software, configure, test then run and update them. So with the help of cloud computing ,you exterminate those problems over come with storing your own data ,reason behind is that you are not managing software and hardware –this is the responsibility of an experienced person.

In cloud computing it provides the shared infrastructure that means it works like a utility program. For this you just need to only pay as per user requirement, upgrades are automatically and scaling up or down is cushy.

Basic Concepts

There are some assured services and working models to make cloud computing viable and easily accessible to the users. Basically Cloud Computing is explained in two

ways. It is either based on the cloud type or on service type. So following are given some working models for cloud computing:

a) Deployment Models
b) Service Models

Cloud Storage:

Cloud storage it is model of cloud computing which stores data on the internet through a cloud computing provider who operate and manages data storage as services.Cloud storage also known as utility storage. It distributes on demand service with its capacity and costs. Using cloud storage you can manage your own data infrastructure and eliminate also. With this additional feature user can access data from anytime, anywhere. Cloud storage mange the capacity.

II LITERATURE SERVEY

In this section related existing research work is illustrated here and also explains how our proposed work is differing from it.

III RELATED WORK

This section is divided in to two parts:

1. Registration mechanisms
2. Data Sharing Mechanism

1. Registration mechanisms

Using this mechanism user can first registered with the system and after verification of user with his mail and mobile user can store data on cloud storage.

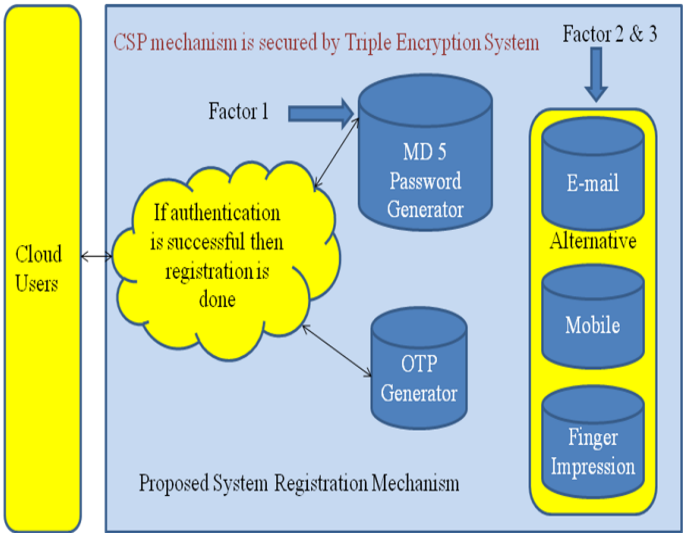


Figure 1 Proposed system registration mechanisms

2. Data Sharing Mechanism

After user successfully authenticated using data sharing mechanism user can share data from cloud storage which is stored or required.

Description:

Above figure 2 shows the graphical representation of data sharing mechanism. Majorly it consists of three sections. 1) Cloud users 2) authentication mechanism 3) sharing mechanism. Below is the brief of above system.

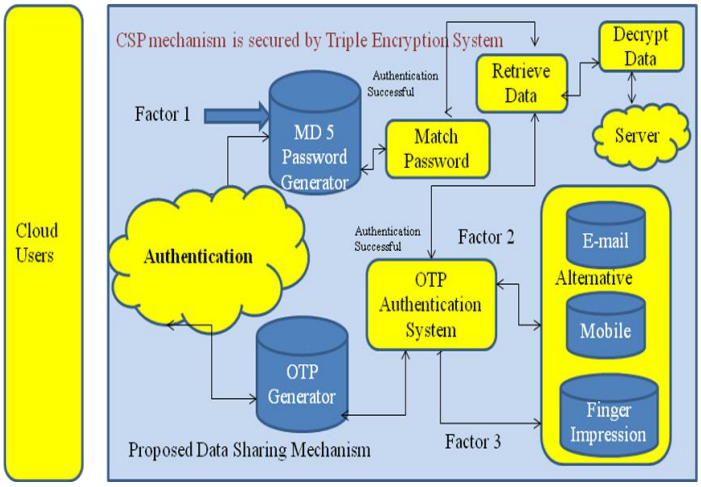


Figure 2 Proposed system data sharing mechanisms

The main concept behind this is to avail a secure system for cloud users to access data through cloud. The major threat using cloud is the malicious and fraud users. To avoid these attacks, above systems uses the secure way of data sharing. This included the first step to verify the registered user using 3-factor verification which includes user name and password, email id, mobile no.

Mainly when user is registered system verifies its username, password, email and mobile no. This is further used to verify the user when he requests the data from CSP. As data is stored in cloud when users demand the authorized data he is verified by the system and then he is given the access to that requested data. This can be mainly used in the infrastructures where large amount of data and resource sharing is done. Such as companies where all development work is done in cloud, or the Email machines which are used in private networks. Also this can used public sectors such as aadhar card verification, election card registration and PAN card registration.

When user is registered his password details are stored in MD5 format [2] and retrieved in same when it is verified. Users enter the details in plaintext or we can say decimal then is converted in system language. When users requests any data or resource from cloud, system asks for user name, password and generates a OTP on email and mob no. When user confirms the OTP then only user is allowed to access the data area or the resource area or data. The main motto behind this mechanism is to avoid an unauthorized user from accessing the CSP. Using 3 factors can also used as alternative authentications, such as set of 2's Username Pass and email or Username Pass and mob no. The mobile have alternative if mobile OTP is failed then use figure impression. This can be used as backup in case of unavailability of regular authentication method. But in this system it is only authorized in very rare cases such as system failure or any

non recovering disaster. It also shows the data sharing mechanism using 3-factor authentication system; user can share data only using 3DES technique.

IV RESULTS AND ANALYSIS

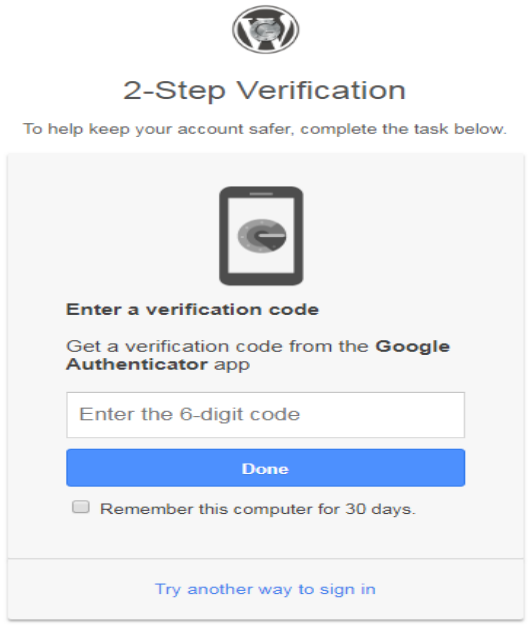


Figure 3: Performance of Three Factors

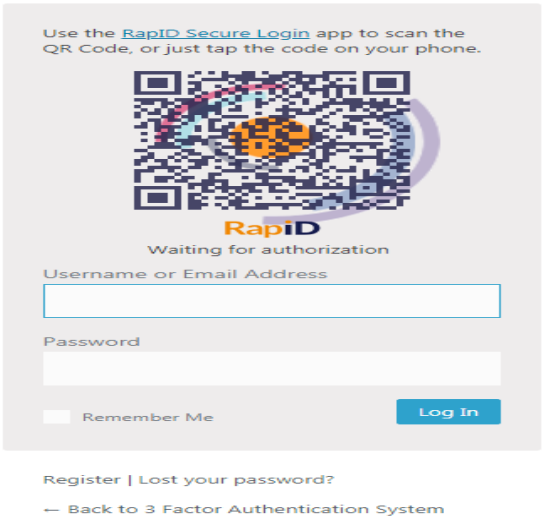


Figure 4 Login Screen

Above Figure 4 shows the staring process of getting log in to cloud panel, Here we propose the multi factor credential login for cloud storage system. In above figure we can see the basic method of username and password combination to log in to system, but in addition to this we have also added another factor QR code to simplify the process and at the same time making it more secure with medium of android phone and getting it register with internal system. User are enabled to log in with their android phones using QR code which is newly generated at every login and is only verified with registered mobile no using app.

Here now comes the second factor that is used make login harder for malicious users or unauthorized users. Here we are using OTP on mobile using Google Authenticator to move forward to next stage of login Screen.

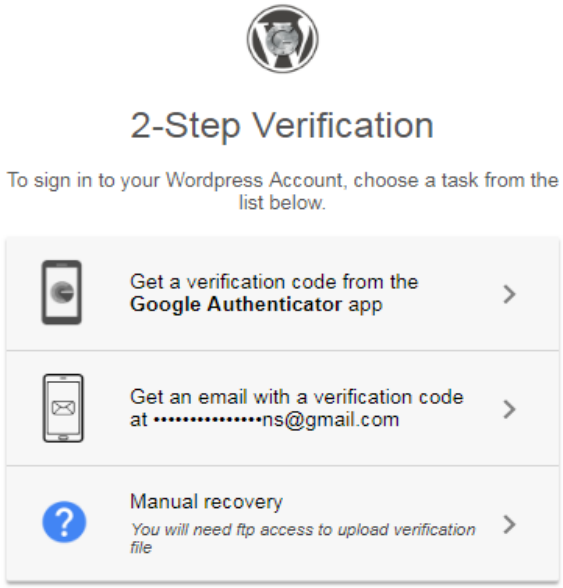


Figure 5 Login Screen

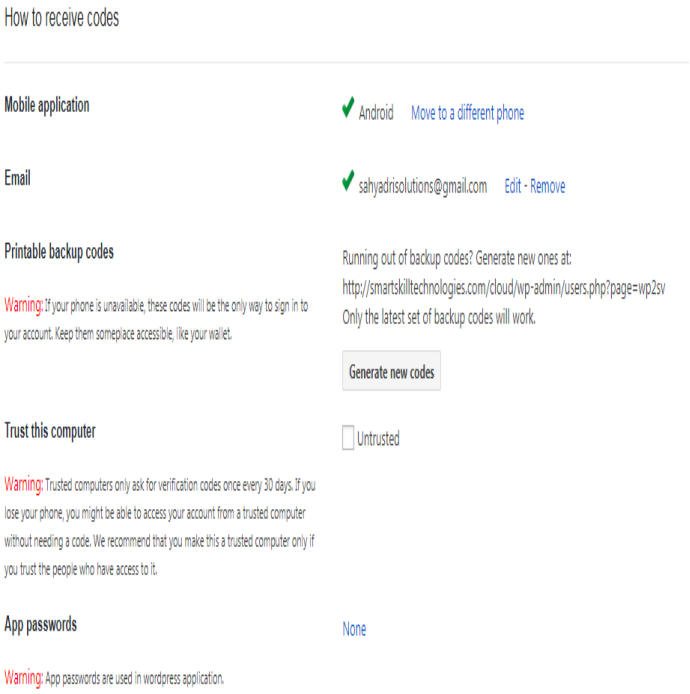
Typically, a user installs the Authenticator app on a smart phone. To log into a site using two-factor authentication, by providing user name and password of the user to the site and runs the Authenticator app. The app displays an additional six-digit one-time password. The same password is independently generated by the site, which asks the user for it. The user enters it, thus authenticating the user's identity.

Figure 5OTP on mobile with Google Authenticator App. For this type of set-up work, operation has to be performed onwards of time: the site provides a shared secret key to the user over a secure channel, to be stored in the Authenticator app. This secret key will be used for all the future logins to the site. Using two-factor authentication i.e. only you have to cognition about user name and password to break security of user account is not adequate. The attacker also needs knowledge of the shared secret key or which physical access to the device running the Authenticator app. OTP code alternative on Email or Mobile choose any one method

There is no need to consume the SMS charges to get the OTP or any kind of SMS gateway integration, we made it safe yet simple using Google Authenticator. Using this method we are moving next step forward for making the login and sharing process more secure. When a user comes to this step, simple he has make his Google authenticator app live in his mobile and enter the code that will be generated there. This OTP will be changing every 30 seconds and new

one is generated so user has make this in 30 seconds only, now this time bonding factor adds one more security to this system that is auto hacking tools or malicious robots can't make it done in 30 second so the fails to decrypt the OTP system. Now if user fails to reach its mobile phone then what? Next figure show the same.

Figure shows the alternate option for OTP on mobile, in case user fails to reach his mobile here we provide another option to get the OTP and that is OTP on pre-verified email id. User can choose this method and get login to panel. Here also the password expires after every 5 minutes which make it harder to reach using malicious techniques.



IV METHODOLOGY

Flow Chart for proposed system is shown in following Figure No.6 Following flow diagram represents the flow of the system in short. As we can see that user has to login into system to access or process and kind of information or to use system. As figure describes that login requires two attributes username and password. When username and password is entered by the user it is processed in details verification box. If the authentication is success then it is send to next level, where user can request the data from cloud. Here 2 and 3 rd factor authentication is requested to user.

This authentication includes OPT on email and OTP on mobile no. When user enters the OTP it is verified in OTP verification box. If the user satisfies this condition it is provided the information needed. Following figure No.6 shows the flowchart for proposed system.

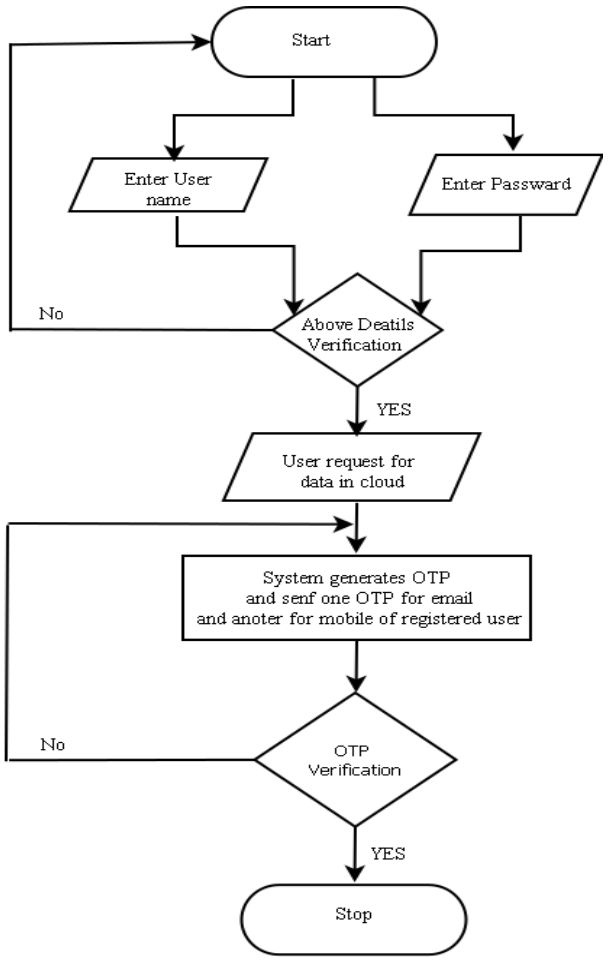


Figure 6 Flow Chart of the Proposed System

V RESULTS AND ANALYSIS

Three factor authentications effectively work and overcome the drawback of traditional approaches. These approaches are not effectively from the they work on small data and today's storages are huge amount of data need to stored, so they not effectively work of their limitations. So three factors work effective and excellence on these situations. Following figures shows the results produced by three factors authentication. The given graph shows the performance of single factor, two factors and three factors authentication with security scale, encryption, and rounds attributes. So our system performs better as it is very flexible with respect to others factors.

Sr.no	Authentication factors	Security scale	Encryption	Rounds
1	Single factor	1.5785	32	10
2	Two Factor	4.55879	128	12
3	Three Factors	8.638942	256	24

Table No.1 Comparison of Authentication factors for data security on cloud storage

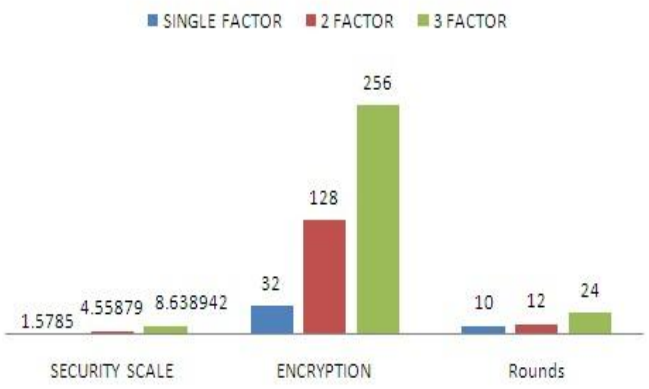


Figure 7 Comparison graph for Authentication factors

To evaluate the performance of our system, we take the three attributes Security scale, encryption and rounds. Security scale is used for scaling the security of data, Encryption is used for key size i.e. how many bits of key is used for encryption. And rounds attribute is used for depend on key size it rounds are arranged.

VI RESEARCH WORK

We can overcome the drawback of problem involves in two factor authentication system like no backup options in OTP, password recovery option not feasible and OTP on email is less secure than OTP on mobile devices. Using three factor authentication methods we can easily solve the problems arise in existing system. To increase the data security in cloud storage and securely data sharing mechanism on cloud is easily done with this method. Finding the best methods like triple DES Algorithm for cloud storage and provide high level of security.

VII CONCLUSION AND FUTURE SCOPE

Cloud computing is the present and futuristic resource pooling paradigm which converges with the Internet of Things (IoT). However, there are authentication and key management issues to be resolved. Identifying users is not an easy task in cloud. As a result in this article we proposed a provably secure multi-factors authentication scheme with trusted third party. In our approach, trustee distributes the authentication tokens on behalf of cloud service providers and allows the cloud servers just to verify the hashed key credential data. This approach also ensures the mutual authentication of the communication entities. We used multi-party station to station Diffie-Hellman key exchange protocol which overcomes many key management problems. Our proposed mechanism preserves the privacy of the remote authentication details in the cloud and significantly helps to protect the stakeholder's sensitive information from the inside and outside malicious attackers. Our work and many existing cloud-based authentication works are still centralized and are yet to be transformed to a distributed or collaborative cloud paradigm.

ACKNOWLEDGMENT

It is my great pleasure in expressing sincere and deep gratitude towards my guide Prof. B.K.Patil. I am also thankful to Head of Department of Computer Science and Engineering, Prof. B.K.Patil for providing me various resources and infrastructure facilities. I also offer my most sincere thanks to Principal of Everest College of Engineering, Aurangabad, my colleagues and staff members of computer science and Engineering department, Everest college of Engineering, Aurangabad for cooperation provided by them in many ways.

REFERENCES

[1] Joseph K. Liu, Kaitai Liang, Willy Susilo, Jianghua Liu, and Yang Xiang, Senior Member, IEEE. "Two-Factor Data Security Protection Mechanism for Cloud Storage System", June 2016.

[2] Y. Kale, A.Patankar, "Enhanced Data Security Mechanism on Cloud Using Two-factor Authentication, Data Encryption and Key Sharing Mechanism", IRF International Conference 15 June 2014 Pune.

[3] A. Akavia. S.Goldwasser, and V. Vaikuntanathan "Simultaneous Hardcore Bits and Cryptography against Memory Attacks" 2009.

[4] A.Boldyreva, V. Goyal, V.Kumar "Identity-based Encryption with Efficient Revocation " in 2008.

[5] Praveenkumar, Jyoti Patil, "Distributed, Concurrent, and Independent Access to Encrypted Cloud Databases".

[6] J.Shao & Z. Cao,"Multi-use unidirectional identity-based proxy re encryption from hierarchical identity-based encryption", Info.Sci. 2012.

[7] Vijay Varadharajan, Senior Member, IEEE, and Udaya Tupakula, Member, IEEE. IEEE Transactions on Network and Service Management," Security as a Service Model for Cloud Environment", Vol. 11, No. 1, March 2014.

[8] Cong Wang, Student Member, IEEE, Sherman S.-M.Chow, Qian Wang, Student Member, IEEE, Kui Ren, Member, IEEE, and Wenjing Lou, Member, IEEE." Privacy-Preserving Public Auditing for Secure Cloud Storage."

[9] Divya Saraswat, Dr. Pooja Tripathi, "Strengthen Cloud Computing Security with Enhanced Two Factor Authentication and Encryption."

[10] Yinchuan Sun , Junsheng Zhang, Yongping Xiong,Guangyu Zhu," Data Security and Privacy in Cloud Computing."

[11] Rabi Prasad Padhy ,Manas Ranjan Patra, Suresh Chandra Satapathy, " Cloud Computing: Security Issues and Research Challenges", IJCSITS, Vol. 1, No. 2, December 2011.

[12] Shaunak S. Ganorkar, "Achieve Date Integrity and Security on Cloud Storage using 3DES Encryption Algorithm"IJSRP, Vol. 4, Issue 8, August 2014 ISSN 2250-3153.

[13] Divya Pritam, Madhumita Chatterjee, "Enforcing Role-Based Access Control for Secure Data Storage in Cloud Using Authentication and Encryption Techniques", JNCET,Vol. 6, Issue 4, April 2016.

[14] Vijay Varadharajan, Senior Member, IEEE, and UdayaTupakula, Member, IEEE, "Security as a Service Model for Cloud Environment", IEEE Transactions on Network And Service Management, Vol. 11, No. 1,March 2014.

[15] Kan Yang, Xiaohua Jia, Kui Ren, "DAC-MACS: Effective Data Access Control for Multi-Authority Cloud Storage Systems".

[16] Anamika Sirohi1, Vishal Shrivastava2, "A Multi-Level Security Mechanism for Data Storage in Cloud Computing: A Review", IJRASET, Vol. 4, Issue II, February 2016, ISSN: 2321-9653.

[17] Ms.Vaishali Patil , Prof. Archana Lomte,"Implementation of Privacy-Preserving Public Auditing and Secure Searchable Data Cloud Storage", IJAIEM, Vol. 3, Issue 7, July 2014, ISSN 2319 - 4847

[18] Nikunj Kumar, Prof. Priti Sharma," Cloud Systems Security Threats And Prevention Mechanisms", IJARCSSE, Vol. 4, Issue 5, May 2014 ISSN: 2277 128X.

[19] Nandini Mishra , Kanchan khushwha, Ritu chasta, Er. Abhishek Choudhary, "Technologies of Cloud Computing - Architecture Concepts based on Security and its Challenges ", IJARCET,Vol. 2, Issue 3, March 2013, ISSN: 2278 – 1323.

[20] Amlan Jyoti Choudhury, Pardeep Kumar1,Mangal Sain1 Hyotaek Lim, Hoon Jae-Lee, "A Strong User Authentication Framework for Cloud Computing",2011 IEEE Asia -Pacific Services Computing Conference.

[21] Prof. (Ms.) Kim aya Ambekar , Prof. (Dr.) K amatchi R. ," Enhanced User Authentication Model in Cloud Computing Security".

[22] Ms. Swati R.Vibhute "Three Factor Data Sharing Mechanism for Cloud Storage System" in IJASRET, Vol. 2, Issue 12 July 2017 ISSN(online) 456-0774.