ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017

User Authentication and File Encryption Technique for achieving high Cloud Computing Security

Sandeep Kumar Pandey, Sujeet Kumar Tiwari

M.Tech Scholar, Department of Computer Science and Engineering, Lakshmi Narain College of Technology Jabalpur, (M.P.), India

Asst. Professor, Department of Computer Science and Engineering, Lakshmi Narain College of Technology Jabalpur,(M.P.), India

ABSTRACT: Cloud Computing is the most promising technology which increases rapidly as increasing years. In Cloud Computing environment, the data of the user is stored in the server and security of the data be blame to service providers of the company. The service provider taken care of the security for the data of the customers. In the cloud computing system, the problem is that the service providers treating all the data in the same manner means they provide common security to all the data for the particular user without considering that whether that required that security or not. So as a solution for this problem, we proposed the concept of data classification. In our proposed work, we categorize the data into categories based on the secrecy of the data and particular category of the data is secured with respective level of security. By using this concept we can reduce the overhead and increased the processing time. Also it can increase the performance of the cloud environment.

KEYWORDS: Cloud Computing, Data Security.

I. Introduction

Now a day’s Cloud Computing Technology is the most promising technology comes in the real world. Users are more aware of the advantages of the cloud computing and they start using it. Cloud Computing is the next generation system which provides an easy and customizable way of managing data in the Internet. It provides the user various services of accessing and work with the application of Cloud. Users can upload their data in the Cloud Storage and can access through anywhere through any devices like laptop, mobile, desktop etc. Whenever the discussion of data comes some of the properties of data emerges and some of them are as follows Accuracy, Completeness and Consistency.

In cloud computing data is mainly deal with 3 security issues Confidentiality, Integrity and Availability. Data Confidentiality means data should be confidential to others, no unauthorized access to the data is allowed. Data Integrity means content of the data should not be violated. Availability means whenever the user wants to access their data the data is available to them.

DOI: 10.15680/IJIRCCE.2017. 0509035

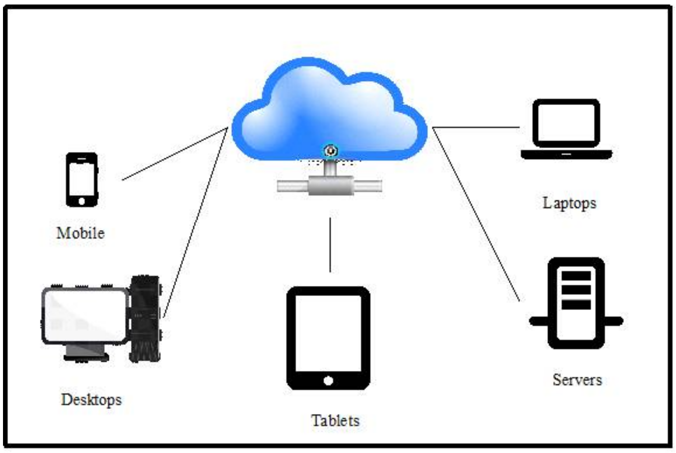


Figure.1: Cloud Computing

After the user upload the data in the cloud environment, it is the responsibility of the CSP (Cloud Service Providers) for the protection of the data in the cloud.

II. Literature Review

We all know that cloud storage provides various advantages like better accessibility means make data to access from anywhere using internet. No need for the users to depends upon the physical storage for carry and retrieving of data.

Ji Hu, Andreas Klein [1]**,** focuses on the security of the data in the place of use of data. Here they make a Benchmark which analyze the basic requirement of applications in the cloud for the security of the e-commerce data. In this different approach of the encryption is discussed for securing the data during transactions as the data in the transaction is critical.

In Cloud computing preserving integrity of the data is the most important challenge, method for checking the integrity of the data without download the data. In normal the user has to download the data and check after that they get the doubt of the illegally modification of the data. But they doesn't have any evidence to proof for the same. An approach is made which know the integrity of the data without downloading the data [2].

Ashish Singh, Kakali Chatterjee [3]**,** according to the characteristics of the cloud, the user should not to know the location of the data and which security is used for securing the data. Not only the outer attacks, insider attacks are also be taken care. For avoiding the insider attack, CSP uses authentication scheme. Here in this paper new Two-Tier Authentication is made which is more secure and provide advancement in the security in cloud.

Cloud Security Alliance (CSA) prepared a document in 2010, [5] in which they discuss the threats which are harmful to the data present in the cloud. Some of the issues they figure out are Corrupt and Abuse use of Cloud Computing, Insecure Programming Interface, Insider Attacks, Vulnerabilities in shared environment, Data Loss and Leakage and so on. In the Cloud Storage environment, all the data present in the cloud storage are get encrypted with single security algorithms without considering the whether it requires or not. So Rizwana Shaikh, Dr. M. Sasikumar, [7] proposed a technology which classifies the data into different category based upon the properties of the data like Access Control, Content, Storage etc. After the classification they provide the security accordingly, by using permissions to data like Restricted, Moderate and Mandatory.

While implementing the Cloud environment, the Service providers faces many issues regarding the security and other aspects. R. Velumadhava Raoa, K. Selvamani [8],shows the major security challenges which the services providers has to

DOI: 10.15680/IJIRCCE.2017. 0509035

face during the implementation of the cloud computing platform are Integrity of Data, Security, Locality, Access, Breaches, Segregation and also some solutions for the issues like Encryption, Calculation of Hash Value etc.

Microsoft Trustworthy Computing, Frank Simorjay [9], the document which declared only for the information regarding Cloud computing. In this document it is discussed that the data in the cloud exists in 3 states: at Rest, at Process and at Transmit. And according to the document the data should remain status in all three states. Security to the data also depends on the states of data.
In cloud computing there are many challenges the providers face, 2 important challenges are Confidentiality and Privacy. In [10], the author provide the solution for the above two problems, a framework proposed by the author where different tasks are executing before the actual use of the data by the user. Task like Key Management, Encryption Mechanism, Verification Mechanism at client side and at server side tasks are Authorization Mechanism and Integrity Mechanism.

Efficient Cloud Storage Confidentiality to Ensure Data Security: L. Arockiam et al[11], we know, for the protection of the data in the cloud Encryption is used but sometimes only encryption doesn't provide high security so, author proposed new technique for providing more security. Here in this paper, two technique used Encryption and Obfuscation. Encryption converts the readable text to unreadable form while Obfuscation makes the numeric content confusing.

High-Throughput Encryption for Cloud Computing Storage System: Yaser Jararweh et al[12]**,** various methods and algorithms were proposed to make the data secure efficiently. In this paper a Symmetric Block Algorithm (CHiS-256) proposed which encrypt the which encrypt the cloud data efficiently and metadata based Cloud Storage which stores the data into small parts. There are various security algorithm presents but only few are used for the high security. Some of the security algorithms are as follow [13] RSA, SHA1 and MD5. In cloud computing data first get encrypted with security algorithms and then uploaded in the cloud storage. In cloud storage the encrypted data is stored and here author compares three algorithms in terms of security, efficiency and other factors like using different key size to judge the performance of the algorithm in best key size.

A Secure Cloud Computing Model based on Data Classification: Lo'ai Tawalbeh et al[14], here they find out the problem that treating all the data in the same manner and providing same level of security. As a solution for the above problem they proposed a framework which classify the data into different categories like Basic, Confidential and High Confidential and providing the different security techniques according the requirement they provide that type of security to that category.

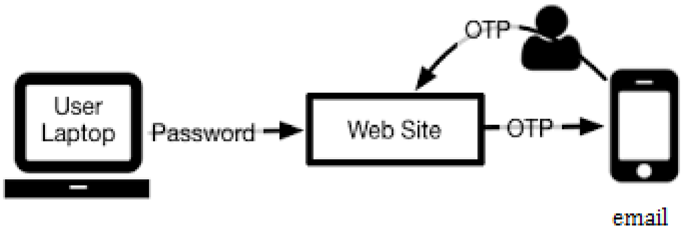
Security Issues in Cloud Computing: A Survey, Rizwana Shaikh et al[15], this paper is the survey paper which surveyed the security issues in cloud computing. They proposed the different security concerns, what is the security issues the Client and the Providers facing in the Cloud Computing. For some of the issues they also focus on the solutions to be taken.
Anup Mathew [16], proposes a survey paper focus on the various Security, Data Privacy and Data Confidentiality Issues. Here in the safety and privacy concern covers like Location Independent Services, Communication and Infrastructure etc. also classify the security issues into two category: Access Security and Service Security.

Trust Model for Measuring Security of Cloud Computing Service: Dr. M. Sasikumar et al[17], due to increase in the Cloud Computing Technology, now a day's there are various CSP's in the market. There are some of the tools and measurements presents which the providers are using for measuring the security of their services. This paper presents a measurement for cloud service. This measurement is based on the trust model. The trust model calculates a value called Trust Value and this value comprises of many parameters like Identity, Management, Authentication, Authorization etc.

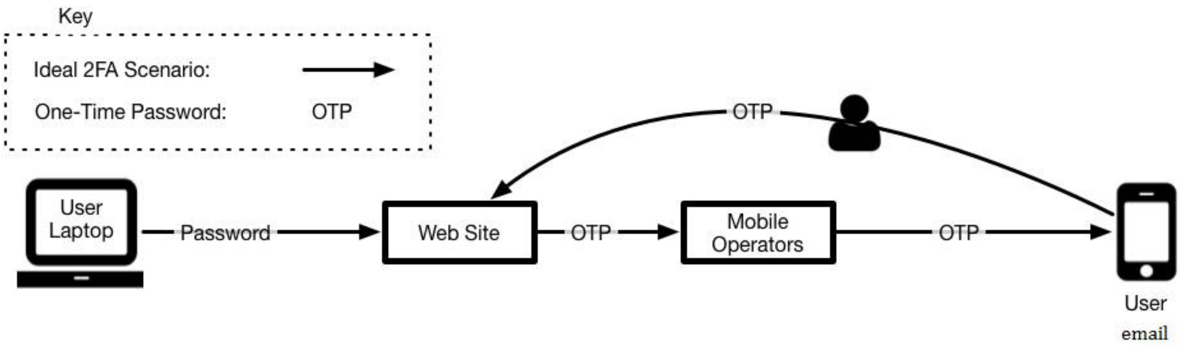
III. PROPOSED WORK

In the cloud computing there is a problem of treating all the data in same manner which is infeasible. The infeasibility of encrypting all the data with single security algorithm without considering whether that data actually required high security or not. Let us consider an example, suppose we have 10gb of total data and using old mechanism of encrypting with single method it is encrypted. Now let's examine, out of 10gb only 2gb of data require high level security other 8gb can be secured with moderate or less security. Using old mechanism, unnecessary 8gb data encrypted with high security which is not feasible wasting of time and memory.

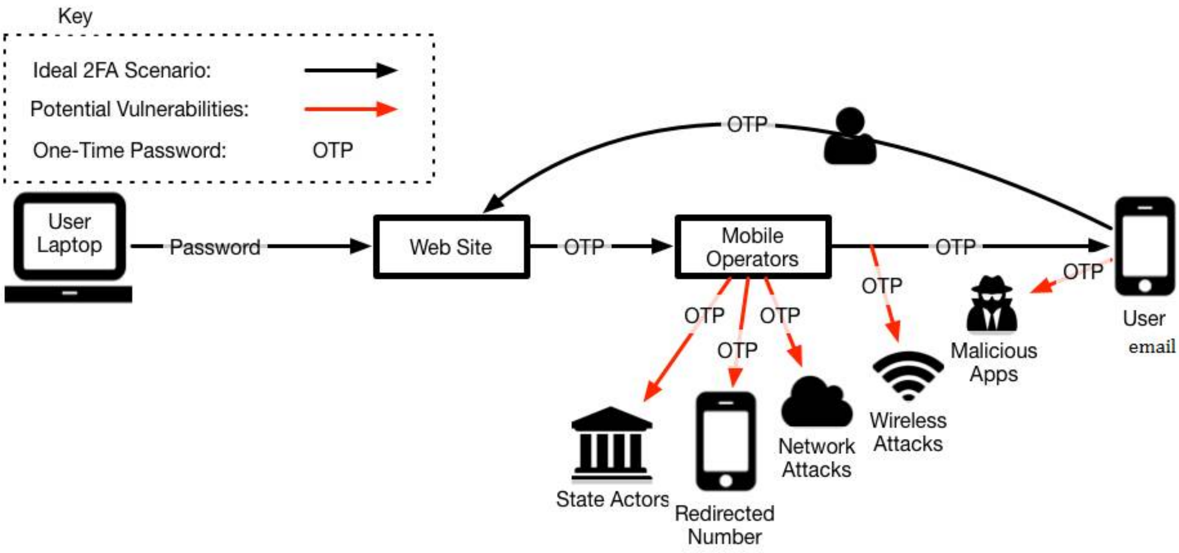
To keep away from aforementioned thing we have proposed the accompanying model for secure login and confirmation. In our proposed show new client needs to give their own portable number while doing enlistment and it must be confirmed by the supplier. So that same portable number is utilized to send OTP (one time secret key) with encoded plan of 256 piece message digest framework AES-256.



Proposed Model Step 1



Proposed Model Step 2



Proposed Model Step 3

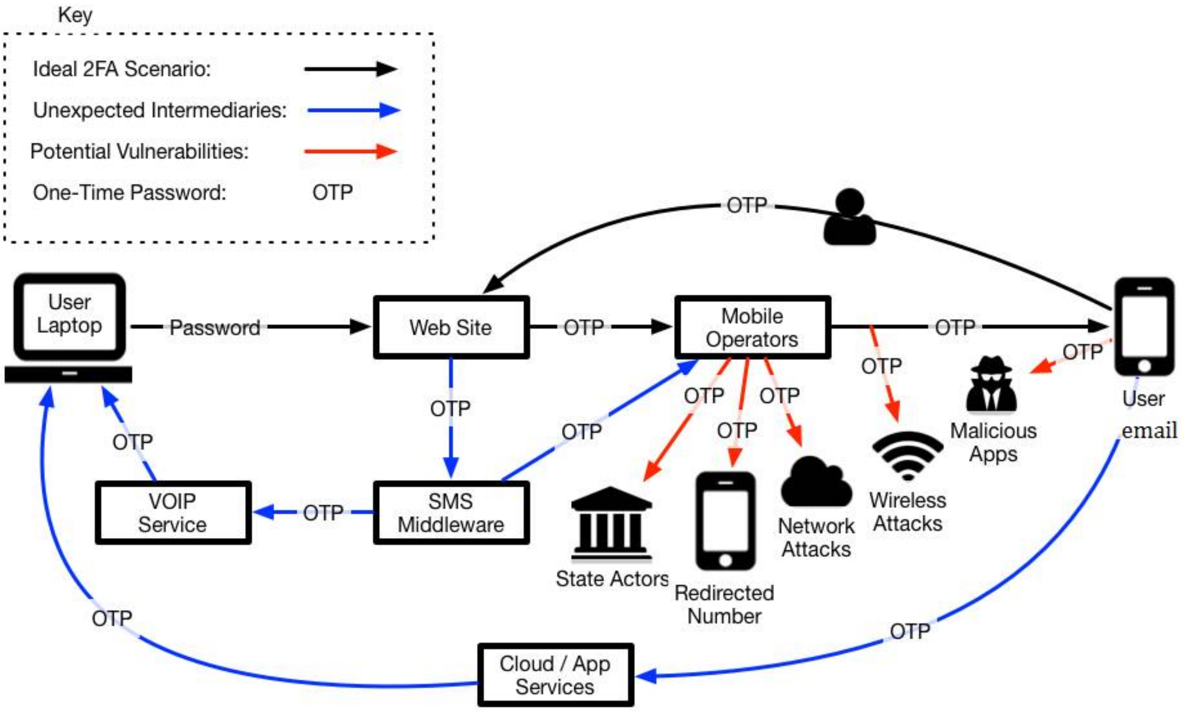


Fig.3.1 Proposed Model

The proposed structure for verifying the client in cloud stage. In this model, an idea of giving a Digital Signature (DS) at the client story and a Trusted Authenticator (TA) for giving high security is exhibited.

IV. RESULTS & ANALYSIS

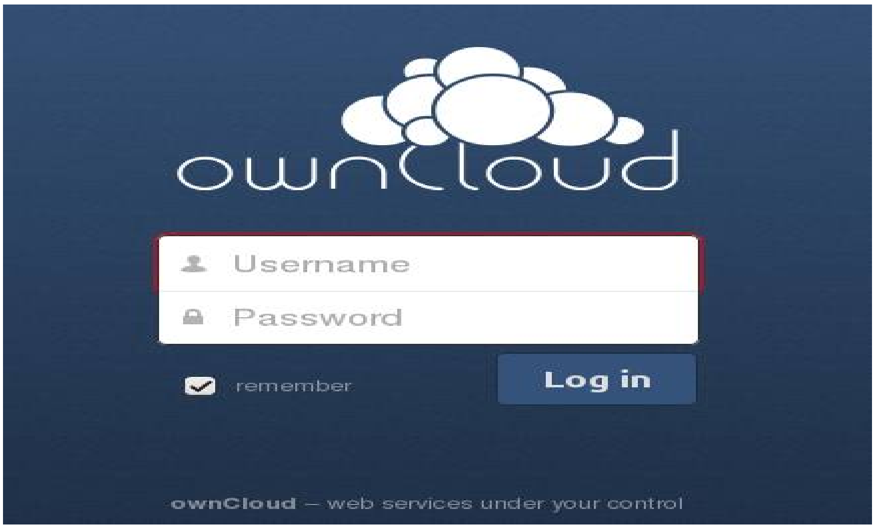
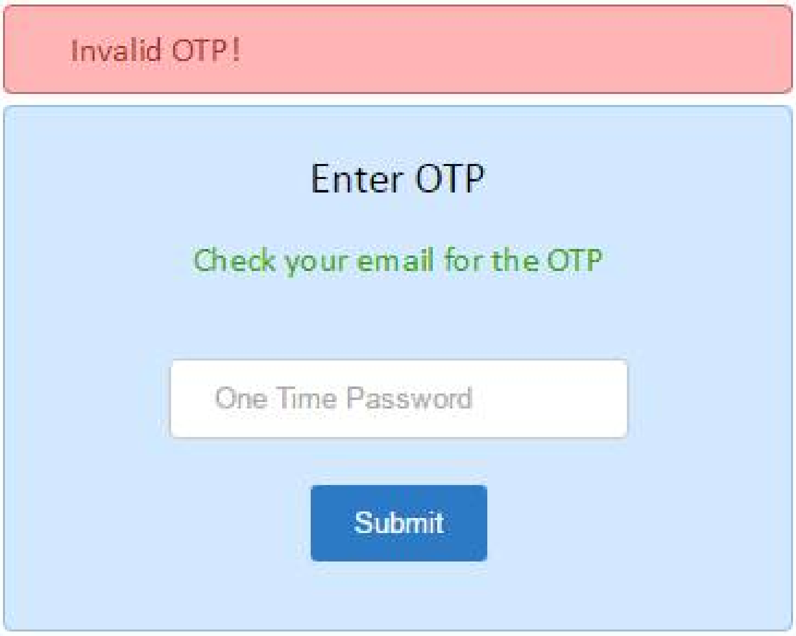


Figure 5.1 Login Page for User Panel

In computer security, logging in (or logging on or signing in or signing on) is the process by which an individual gains access to a computer system by identifying and authenticating themselves. The user credentials are typically some form of "username" and a matching "password", and these credentials themselves are sometimes referred to as a login, (or a logon or a sign-in or a sign-on). In practice, modern secure systems also often require a second factor for extra security.



Invalid OTP!

Enter OTP

Check your email for the OTP

Figure 5.2 Login Page with OTP for User Panel

In a typical two-factor authentication application, user authentication proceeds as follows: a user enters username and password into a website or other server, generates a one-time password for the server using TOTP running locally on a smartphone or other device, and types that password into the server as well. The server then also runs TOTP to verify the entered one-time password. For this to work, the clocks of the user's device and the server need to be roughly synchronized (the server will typically accept one-time passwords generated from timestamps that differ by ±1 time interval from the client's timestamp). A single secret key, to be used for all subsequent authentication sessions, must have been shared between the server and the user's device over a secure channel ahead of time. If some more steps are carried out, the user can also authenticate the server using TOTP.

TOTP is based on HOTP with a timestamp replacing the incrementing counter.

The current timestamp is turned into an integer time-counter (TC) by defining the start of an epoch (T0) and counting in units of a time step (TS). For example:

TC = floor((unixtime(now) − unixtime(T0)) / TS),

TOTP = HOTP(SecretKey, TC),

TOTP-Value = TOTP mod 10d, where d is the desired number of digits of the one-time password.

V. CONCLUSION & FUTURE WORK

The proposed work is carried out to analyze and to provide better security to the data present in the Cloud Storage Environment. In our work we have classified the data into three categories and each category is secured with different security algorithms. Also for the high security to data we have introduced new algorithm which divides the data into small parts called as 'Chunks' and process is called as File Splitting. These chunks are then encrypted with different-different security algorithm is a specific order. In addition, our work can be enhanced with better security algorithms like Asymmetric Algorithms with better execution time, New Techniques and methods can be made for providing better security to the information. Also new classification way can be made and Soft Computing technique can be used which provide Automatic Data Classification and for maintaining confidentiality and integrity of the data.

REFERENCES

[1] Ji Hu, Andreas Klein, "A Benchmark of Transparent Data Encryption for Migration of Web Applications in the Cloud", 8th IEEE International Conference on Dependable, Autonomic and Secure Computing, 2009.

[2] Thanh Cuong Nguyen, Wenfeng Shen, Zhou Lei, Weimin Xu, Wencong Yuan, Chenwei Song, "A Probabilistic Integrity Checking Approach for Dynamic Data in Untrusted Cloud Storage", 978-1-4799-0174-6/13/$31.00 2013 IEEE.

[3] Ashish Singh, Kakali Chatterjee, "A Secure Multi-tier Authentication Scheme in Cloud Computing Environment", 2015 International Conference on Circuit, Power and Computing Technologies [ICCPCT].

[4] Abidalrahman Moh'd, Yaser Jararweh, Lo'ai Tawalbeh, "AES-512: 512-bit Advanced Encryption Standard Algorithm Design and Evaluation", 7th International Conference on Information Assurance and Security (IAS), 2011.

[5] Rishabh Jain, Rahul Jejurk ar, Shrikrishna Chopde, Someshwar Vaidya, Mahesh Sanap, "AES Algorithm using 512 bit key Implementation for Secure Communication", International Journal of Innovative Research in Computer and Communication Engineering, vol. 2, Issue 3, March 2014.

[6] CSA, "Top Threats to Cloud Computing", V1.0, 2010.

[7] Rizwana Shaikh, Dr. M. Sasikumar, "Data Classification for achieving Security in Cloud Computing", International Conference on Advanced Computing Technologies and Applications (ICACTA-2015).

[8] R. Velumadhava Rao, K. Sevamani, "Data Security Challenges and Its Solution in Cloud Computing", International Conference on Intelligent Computing, Communication & Convergence (ICCC-2015).

[9] Frank Simorjay, "Data Classification for Cloud Readiness", Microsoft Trustworthy Computing Doc. 2014.

[10] Yang Wei, Zhao Jianpeng, Zhu Junmao, Zhong Wei, Yao Xinlei, "Design and Implementation of Security Cloud Storage Framework", 2nd International Conference on Intrument & Measurement, Computer, Communication and Control, 2012.

[11] Dr. L. Arockiam, S. Monikandan, "Efficient Cloud Storage Confidentiality to Ensure Data Security", International Confernece on Computer, Communication and Informatics (ICCCI-2014).

[12] Yaser Jararweh, Ola Al-Sharqawi, Nawaf Abdulla, Lo'ai Tawalbeh, Mohammad Alhammouri, "High-Throughput Encryption for Cloud Computing Storage System", International Journal of Cloud Application and Computing, 2014.

[13] V. Sreenivas, C. Narasimham, K. Subrahmanyam, P. Yellamma, "Performance Evaluation of Encryption Techniques and Uploading of Encrypted Data in Cloud", 4th ICCCNT-2013.

[14] Lo'ai Tawalbeh, Nour S. Darwazeh, Raad S. Al-Qassas, Fahd AlDosari, "A Secure Cloud Computing Model based on Data Classification", 1st International Workshop on Mobile Cloud Computing Systems, Management and Security (MCSMS-2015).

[15] Rizwana Shaikh, M. Sasikumar, "Security Issues in Cloud Computing", International Journal of Computer Applications, 2012.

[16] Anup Mathew, "Survey Paper on Security & Privacy Issues in Cloud Storage Systems", EECE 571B, TERM SURVEY PAPER, APRIL 2012.

[17] Rizwana Shaikh, Dr. M. Sasikumar, "Trust Model for Measuring Security Strength of Cloud Computing Service", International Conference on Advanced Computing Technologies and Applications (ICACTA-2015).