iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** VI **Month of publication:** June 2018

DOI: http://doi.org/10.22214/ijraset.2018.6213

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue VI, June 2018- Available at www.ijraset.com

Transmission, Authentication and Compression Using Cloud Computing

Likitha G Gowda[1], Shubha S V[2], Siri P[3]
[1] *Student VIII Sem, Department of Information Science & Engineering, NIE, Mysuru*
[2] *Student VIII Sem, Department of Information Science & Engineering, NIE, Mysuru*
[3] *Student VIII Sem, Department of Information Science & Engineering, NIE, Mysuru*

Cloud computing environments are facing serious problem in security which are, Confidentiality of Data, Integrity of the Message and Authenticity of the users. Since user's personal data is being stored in an unencrypted format on a remote machine operated by third party vendors who provide various services, the impact of user's identity and unauthorized access or disclosure of files are very high. Hence user authentication in cloud computing plays a major role in handling cloud security issues. And the other major problem that has been faced by the cloud service providers is that transmission of huge data, be it in a form of text, audio, image or video which results in the major consumption of the resource. Hence data compression is a very useful technique that helps in reducing the size of text data and storing the same amount of data in relatively fewer bits resulting in reducing the data storage space, resource usage or transmission capacity.
Keywords: Authenticity, confidentiality, integrity, transmission, unencrypted format.

I. INTRODUCTION

Cloud provides users with storage space and makes user friendly and timely acquire data. However there is lack of very strong authentication and less storage space for the files to be stored. Since cloud has been majorly used by people to store, share their personal data. This forms a strong need to come up with system that could solve above problem.
We are achieving the same by providing a strong multifactor authentication while logging in as well as authentication check in homepage so that third party cannot access any data of the authorised user, this is achieved using Google Authenticator.
To make optimal utilization of given storage space the files to be uploaded are compressed in their size by approximately up to 60 percentage. This can be achieved by implementing G-Z algorithm namely Deflate compression.
To make data and password much secured we are encrypting them using AES Encryption.
In order to make this system more interactive a chat messenger feature has also been added where authorized users who are online can communicate with each other using this application. Here chat messenger is provided using SignalR.

II. METHODS AND MATERIAL

This system provides users facilities like authentication using Google authenticator, encryption of data and passwords using AES encryption, compression of files using Deflate compression, chat communication among authorized users using SignalR.
The system comprises of four module

A. Authentication Using Google Authenticator

This module is aimed towards providing multifactor authentication using Google Authenticator. Google Authenticator is a application that performs two-step verification utilizing the Time-based One-time Password Algorithm , for verifying users of their target device by Google. Authenticator provides a six digit OTP which users must provide along with their username and password to log into the system. Normally, a user installs this Google Authenticator app on a cell phone or tab or PC. To sign into the system user uses two-factor validation, the user gives username, password and confirm password to the system shown in fig 1.1 and runs this Authenticator app. The application shows an extra six-digit one-time password which keep changing for every 30 sec. The user needs to enter it, to validate his identity. For this to work, a set-up task must be performed early: the system generates a secret key , user here has to put secret key to generate respective QR code in the google authenticator as shown in fig 1.2 and 1.3 respectively. By scanning QR code six digit OTP is generated as shown in fig 1.4. Enter this OTP to login to system as shown in fig 1.5. With this two-factor authentication, by mere knowledge of username and secret key isn't adequate to break into a user record.

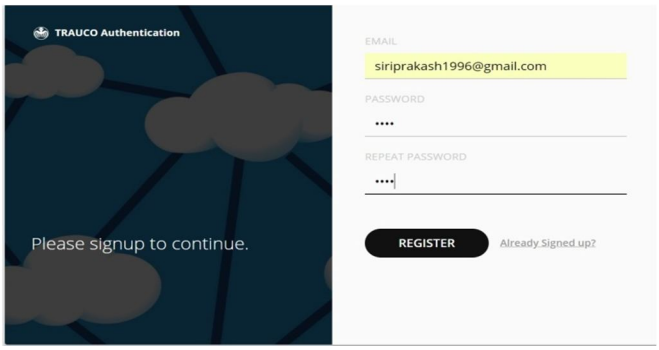


Fig 1.1 Collecting user details

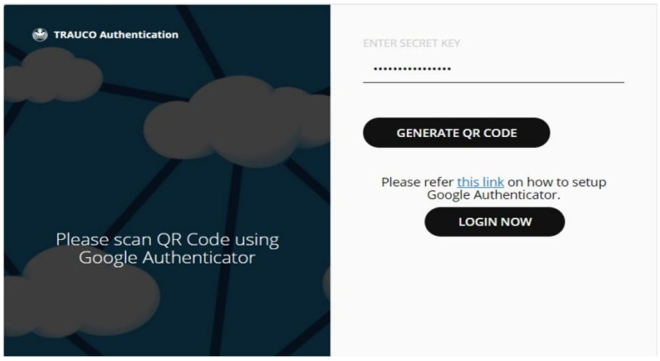


Fig 1.2 Use secret key to generate QR code

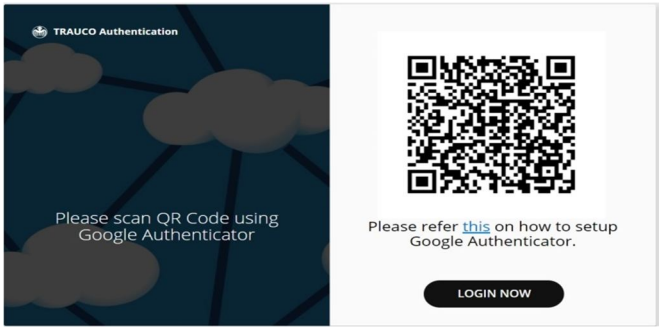


Fig 1.3 Generation of QR code

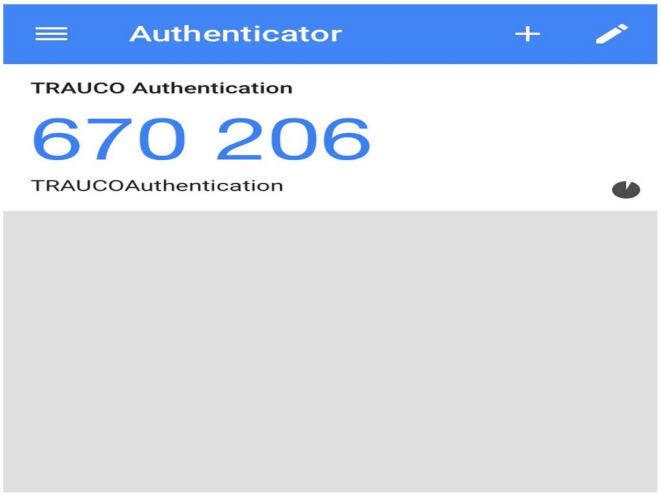


Fig 1.4 Generation of OTP

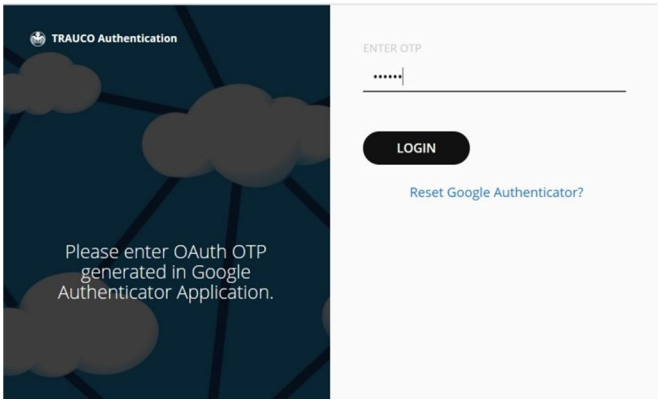


Fig 1.5 Enter OTP to login

B. Gzipalgorithm

The gzip algorithm also known as deflate algorithm uses lz77 and huffman coding. Computer programs have lot of redundant codes or data. The same code will be repeated may a time in a single context. Computer storage, on the other hand, is a valuable resource. It becomes less and less scarce every day, but every time capacity increases.

Conceptually, lz77 is pretty straightforward . When the word occurs for the second times it removes that and in that position it creates piointer to the word encountered for the first time. Lets take a glance at figure 1.6 and figure 1.7. Figure 1.6 contains some words and figure 1.7 shows all of the places wherever text from a previous purpose within the document is recurrent. Lz77 will a really smart job of exploiting that redundancy and creating economical use of accessible storage.

001:001 In the beginning God created the heaven and the earth.

001:002 And the earth was without form, and void; and darkness was upon the face of the deep. And the Spirit of God moved upon the face of the waters.

Figure 1.6 Uncompressed ASCII text

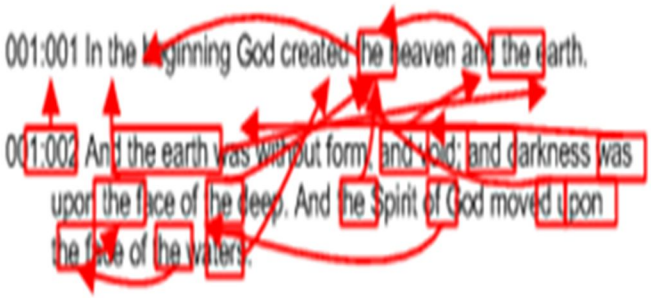


Figure 1.7 LZW compression

For example <25,5> indicates that, to uncompress the document, search backward 25 characters, and reproduce the five characters you find there. This relatively short document is compressed at just over 3:1 and the compression ratio increases as documents get longer.

C. SIGNAL R

SignalR in ASP.NET is a library that eases the method of adding time period net practicality to applications. SignalR permits two way communication between server and client. In 2 way communication, not only client can ask server for data, server could also ping its client with the set of data it has.

Signal R can be used to add any sort of problem solving functionality to your ASP.NET application. Any time a user reloads an internet page ,or the page waits for a long time to retrieve new data, it is a candidate for using Signal R. Examples embody dashboards and observation applications, cooperative applications, job progress updates, and time period forms

D. AES ALGORITHM

AES is an iterative approach. It depends on substitution– stage arrange. We are using this algorithm to encrypt data as well as password. Curiously, AES plays out every one of its calculations on bytes as opposed to bits. Henceforth, AES treats the 128 bits of a plaintext hinder as 16 bytes. AES utilizes 10 rounds for 128-piece keys, 12 rounds for 192-piece keys and 14 rounds for 256-piece keys. Every one of these rounds uses an alternate 128-piece round key, which is computed from the first AES key. In DES it also follows the same round but in reverse order.DES is used to decrypt data which was encrypted using AES in our case file uploaded on our system will be decrypted. The first round is shown in figure 1.8 −

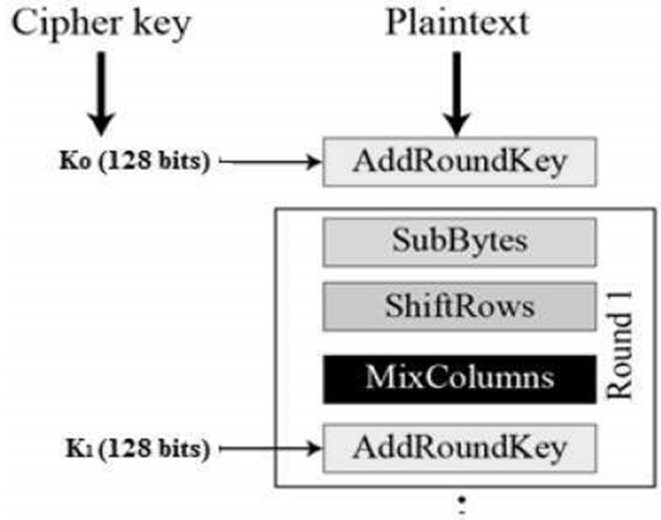


Figure 1.8 AES process

During Byte substitution the 16 input bytes are substituted by looking into a settled table (S-box) given in outline,result will be 4 rows and columns in matrix form. During Shift rows as shown in fig 1.8 each of the four rows of the matrix is shifted to the left. In MixColumns takes 4 bytes of one of the rows and one column and outputs four completely new bytes, which replace the original column. In Addround key the 16 bytes of the lattice are xored. On the off chance that this is the last round then the yield is the ciphertext. In a similar manner other rounds are followed.

III. RESULTS AND DISCUSSION

This system provides organisation a platform for internal upload of a file, internal sharing of a file and internal deletion of a file shown in fig 1.8. Here all above feature are provided with strong authentication, good rate of compression and provides file details like file name, file size, file type, file created date shown in fig 1.9. This system also provides internal chat communication among the authorized users shown in fig 1.10

Fig 1.9 Home Page

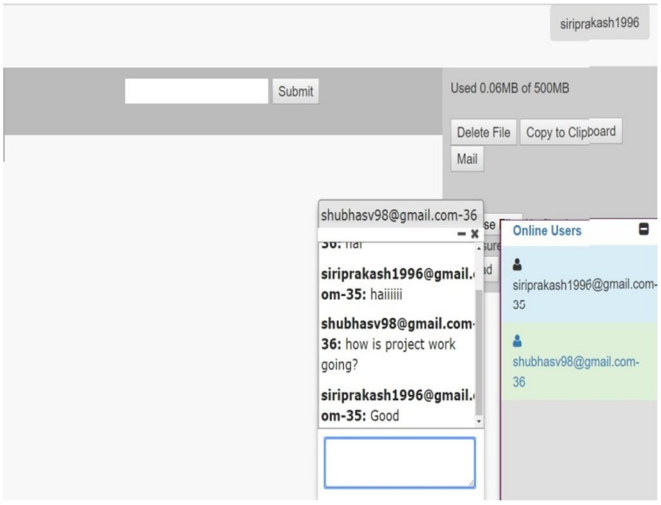


Fig 1.10 Chat messenger

IV. CONCLUSION

The proposed system provides good authentication , good percent of compression , internal upload, delete and sharing of files. It has a similar but better performance when compared to older techniques. Also, this new techniques provides integration of mentioned all above four modules ie transmission, authentication and compression ,encryption and chat communication under a single platform This system also provides intercommunication facility between the authorized users who are online using chat messenger. Authentication mentioned here is two factor Google Authenticator . Good percent of compression is achieved using Deflate compression . Chat messenger is implemented using SignalR library.

This system is majorly used among organizations since this provide good authentication , good percent of compression , internal upload, delete and sharing of files along with internal communication through chat messenger.

REFERENCES

[1] "Cloud security assessment and identity management" by A. Bhardwaj and V. Kumar. Published in: Computer and Information Technology (ICCIT), 14th International Conference on, dec. 2011, pp. 387 –392

[2] "A Block-sorting Lossless Data Compression Algorithm", by M. Burrows and D. J. Wheeler. Published in:Digital Systems Research Center Research Report 124, May 1994

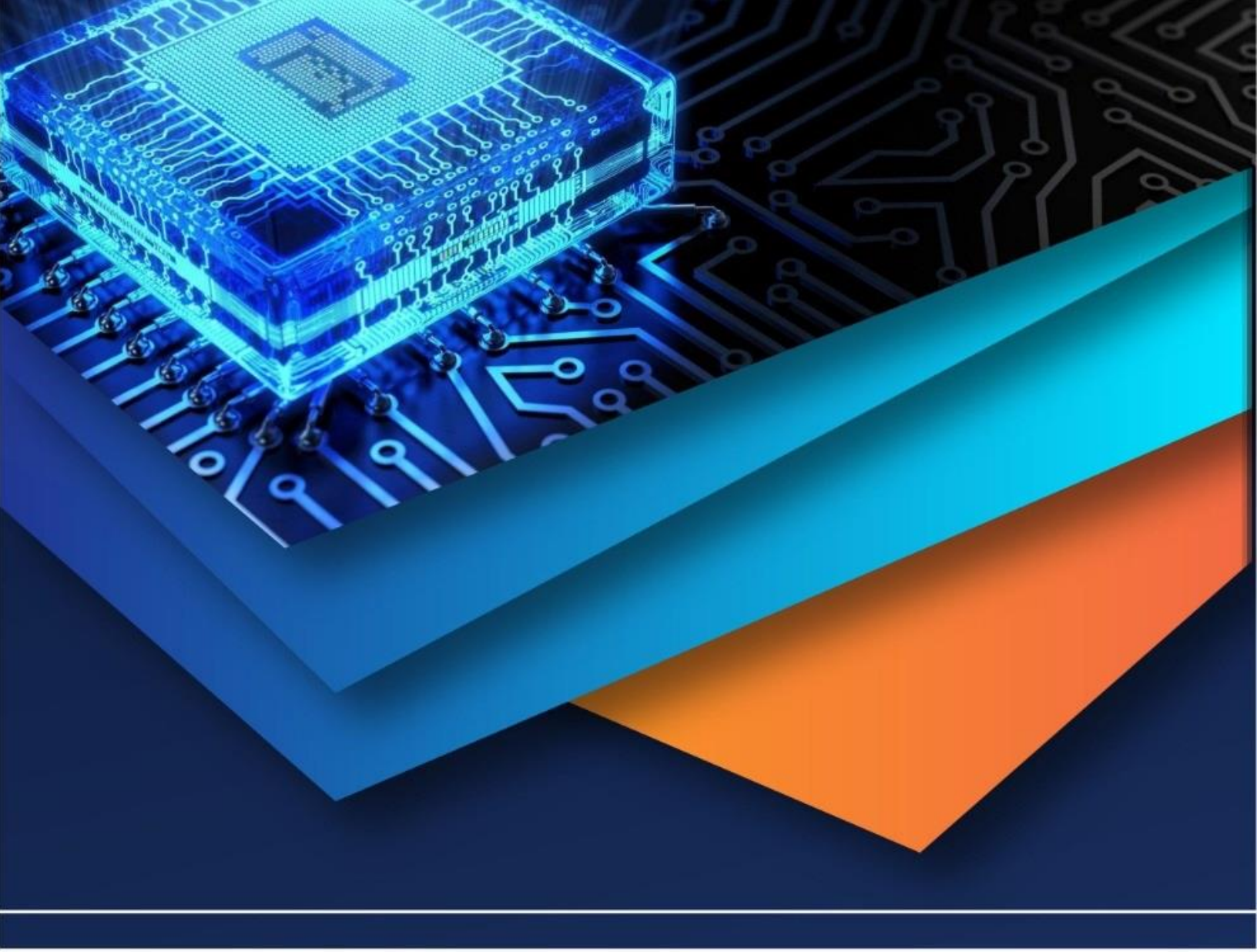
[3] "Data security and privacy protection issues in cloud computing," by D. Chen and H. Zhao. Published in Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on, vol. 1, march 2012, pp. 647 –651

[4] "A Semantic-Based Access Control for Ensuring Data Security in Cloud Computing", by M.Auxilia and K. Raja. Published in IEEE conference on Radar, Communication and Computing, 2012

[5] "Cloud Computing Security Management", by Sameera Abdulrahman Almulla, Chan Yeob Yeun, Published in Engineering systems management and its applications (2010), pp. 1-7.

[6] "Danger in Clouds", by Steve Mansfield-Devine, Published in Network Security (2008), 12, pp. 9-11

[7] "Security in the cloud" , by Gary Anthes. Published in :ACM Communications (2010), vol.53, Issue 11, pp. 16-18



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY