ISSN: 2366-1313

EFFICIENT AND SECURE FILE TRANSFER IN CLOUD THROUGH DOUBLE ENCRYPTION USING AES AND RSA ALGORITHM

[1]Mrs K. Prathyusha, [2]Pogaku Tarun, [3]Mokila Satwik Reddy, [4]Mannem Sai Ganesh

[1]Assistant Professor, Dept.of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad,

kemaprathyusha@gmail.com

[2]BTech student, Dept.of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad,

tarunpogaku21@gmail.com

[3]BTech student, Dept.of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad,

satwikreddymokila@gmail.com

[4]BTech student, Dept.of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad,

mannemsaiganesh@gmail.com

Abstract: *With recent advances in Cloud computing, information is being contracted by cloud services. Dropbox and Google Drive provide cloud services to users with low-cost storage. Here we present a protection method by encrypting and decrypting the files which offer an enhanced level of protection. To encrypt the file that we upload in cloud, we make use of Double Encryption technique. The file is being encrypted twice using the two algorithms one after the other. The file is first encrypted using AES algorithm and then by RSA algorithm. The corresponding keys are being generated during the execution of the algorithm. This technique increases the security level.*

Keywords: *Double Encryption, Security in Cloud storage, Security analysis, AES, RSA*.

I. INTRODUCTION

Cloud computing is a very vast and rapidly emerging technology. It may have different meanings for different individuals but the common characteristic that brings different individuals together is the high availability of data at any time and at any place. Cloud computing not only reduces the role of local computers but also makes computing more integrated. In addition, Software as a Service is a software delivery model in which a third party provides host applications to the organizations and makes them accessible over the internet. Also, SaaS reduces the need for organizations to individually install and run applications on their own computers [1]. This property of SaaS eliminates the cost of installation and support, software licensing, maintenance,

ISSN: 2366-1313

and hardware installation. For instance: The old-style approach of storing documents was to write them in MS Word but that might be substituted by Cloud Computing. It is a more effective way of doing that task as the user can just log into his account and use the Google Document Service provided by Google. On the other hand, storing the data on cloud can make it more prone to threats and attacks. Thus, the concern of security and privacy of data is of utmost importance. The word 'Cloud' computing comes from two words, that is Cloud which refers to the internet and 'Computing' which means technology based on computers. Here, Internet is storage or warehouse where the virtualized resources are stored which then are provided as services. From building through initial concepts to the actual deployment, cloud computing has been expanding. These days there are many organizations from small to medium are getting to realize the advantages of having their application and their data on the cloud. By adapting to the cloud computing techniques, the growth in business development will be more efficient and data more secure[2].

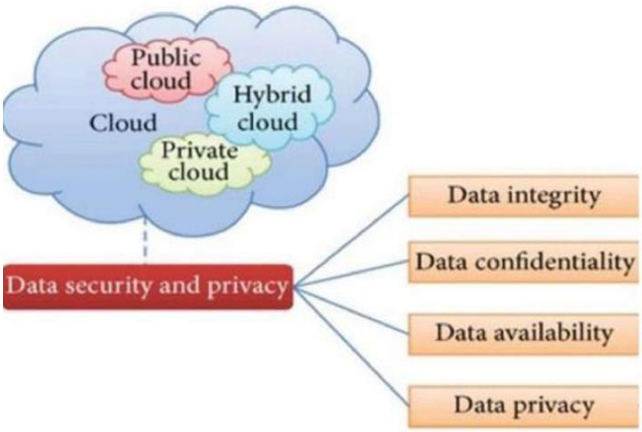

Fig.1 Cloud architecture

II. LITERATURE SURVEY

RELATED WORKS Yibin Li et.al[3], focused on the data over collection problem.They tried to put all customer details into a cloud the security of customer details could be increased They have explored various experiments and the output shows the effectiveness of their approach. Their most direct improvement was reducing the storage in customer smartphone Pictures, videos and other storage information or data occupy more storage space so these are vacated which enable users to install new applications. They showcased an active approach. Whenever an application requires customer data it needs to access request in cloud.

Liwei Kuang et.al[4], implemented a method that could process large scale heterogeneous data that safely decompose a tensor. Tensor is used in applications that

ISSN: 2366-1313

are rich in data or information. Required number of orthogonal bases is multiplied along with the core tensor. Fully homomorphic encryption is used to encrypt the data, after which decomposition is performed by an algorithm. It could secure data processing on the cloud. A security scheme for cluster management detailed by Jun Wu et.al provides high security

Krikor et.al[5], in presented a selective encryption method by using high frequency DCT coefficients that contain more visual information. Security is added to the encrypted block by making use of shuffling method. The use of DCT transform helps in data reduction. It is well known that multimedia data are compressed using DCT. At the receiver end, Han Qui et.al estimated the DC coefficients, which help to reduce the transmission error. Andreas Pommer et.al in designed a scheme to protect content and provide security for a specific multimedia application. This scheme which made use of classical ciphers on the multimedia proved to be inefficient as it required high computation.

Med Karim Abdmouleh et.al[6] encrypted the LL band after performing DWT on the image. This method proved to be fast, robust, and efficient. Keke Gai et.al, in proposed CRN it is widely used in wireless networking. CRN make use of WSGNs. Their proposed approach was examined and the outputs were positive. A method of data storage from end-users to clouds was presented by Han Qiu et.al. Zafar Shahid et.al presented a selective encryption idea that satisfies all real time constraints. In spite of Data integrity being an essential factor, it was not considered in earlier SE methods Image quality and Integrity are not assured in fractional wavelet-based SE methods idea that satisfies all real time constraints. In spite of Data integrity being an essential factor, it was not considered in earlier SE methods Image quality and Integrity are not assured in fractional wavelet-based SE methods.

In another method, data packets are checked if required to be split during operation period. It provides security and can guard threats from clouds.

Han Qiu et al[7] did DCT on bitmap images and tried to reduce rounding errors and recovery from non-selected DCT coefficients. Another encryption algorithm uses a secret key, a map to change positions of image pixels and a second map to modify intensity of image pixels. This method could enhance security to a large level. Han Qiu Et.al in proposed an image protection with shorter calculation resources but with larger image input. The traditional encryption method is very slow.

ISSN: 2366-1313

As it is not fast it consumes a lot of CPU calculation resource. For this issue they came up with a combined selective encryption along with the current GPGPU acceleration.

Yulen Sadourny et al[8] proposed selective encryption and impact of signalling information. When the signaling was taken into account there was lot of problems, so they tried to resolve by applying the selective encryption scheme. This was implemented because the image code stream provided extra information to the transcoding application.

W.Puech et al[9] incorporated AES cipher to encrypt JPEG images. A major advantage of this method is the reduction of calculation resources for big sized data. Ayoub Massoudi et al proposed a cost-effective encryption method for JPEG2000. Harshitha.Y et.al in proposed a study which is based on keyword and multi-keyword. this compares the term efficiency. Here the performance is calculated based on the speed of search done over the encrypted data. They also tried to improve the time for multi keyword search over the RSA.

Andreas Pommer et.al in [10] designed a scheme to protect content and provide security for a specific multimedia application. This scheme which made use of classical ciphers on the multimedia proved to be inefficient as it required high computation.

A more secure algorithm implemented in VHDL used a digital signature. The usage of both cryptography and steganography at the same time improved security to a large extent. Naga Hemanth et.al in [11] proposed an RSA algorithm for the purpose of security of the information and the key which is used for encrypting the information or data. This methodology is implemented in three steps. In the first step text is been encrypted using playfair cipher which make use of 9x6 matrices. The second step deals with XOR operation carried out between key and encrypted text. At the last step of encryption, the key was made using the RSA algorithm and further XOR operation was continued. Finally, the encrypted information along with key is received and decrypted to read the message. This algorithm provided by them provides extra security among the existing algorithms. A hybrid encryption algorithm that could protect data in Cloud used three encryption keys

III. PROPOSED WORK

We propose a method that provides high security. Here, we use the Double Encryption Technique. Here we first encrypt the private fragment containing the

ISSN: 2366-1313

important information with AES128. After the first encryption is over the corresponding key is generated. This encrypted file is again subjected to encryption with RSA algorithm. The various parameters that we have considered here are security level, speed, data confidentiality, data integrity and cipher text size

SYSTEM DESIGN

We propose a method that provides high security. The user uploads a file into the cloud which has public and private fragments. The private fragment is supposed to securely protect. As said before we have proposed to use the Double Encryption Technique. For Double Encryption the algorithms that we have used are AES and RSA. Here we first encrypt the private fragment containing the important information with AES128. After the first encryption is over the corresponding key is generated. This encrypted file is again subjected to encryption with another algorithm.

IV. IMPLEMENTATION

Figure 2 shows the process of how a file is being uploaded. Initially the user first registers and then logs into the profile. The user then selects the file which he wanted to upload into the cloud to keep it safe. After choosing the file some internal process is undergone by the file before it gets uploaded. First the file is being encrypted using the AES algorithm and then by RSA algorithm. Double Encryption is done for security purposes.

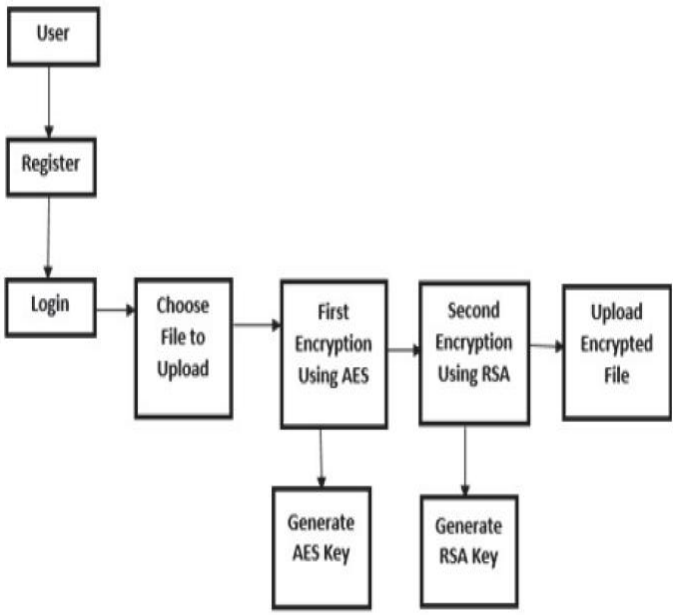

Fig.2 File upload process

File Download Process

Figure 3 shows the system architecture for file download purpose. The user again logs into account. The user views the cloud to check out the files that are being uploaded by others. The user requests the file that he wishes for. This file request is sent to the owner of the file. If the owner of the file wishes to grant access he accepts the request otherwise he deletes it. If the request is accepted, send the key to the user through Email to open the file. The requested user shall make the user of the key to download the file to view or read it.

ISSN: 2366-1313

The downloaded file gets stored in the requested user's system.

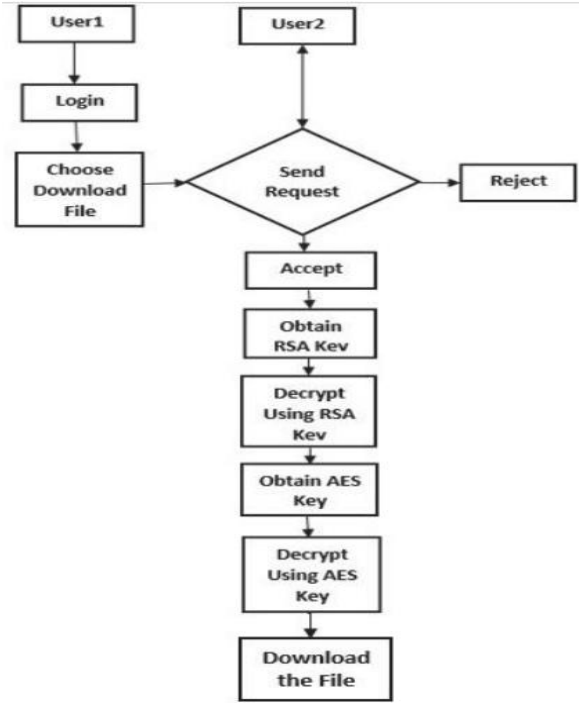

Fig.3 File Download Process

Algorithm:

The system has been implemented using AES and RSA algorithms. Both the algorithms are explained here.

A. Working of AES Algorithm

1. Obtain the key from cipher key.

2. Assign the plain text to state array.

3. Prefix state array with initial round key.

4. Perform manipulation nine times.

5. Carry out the tenth and last manipulation.

6. Copy cipher text the working of AES algorithm.

AES is an iterative cipher. It is symmetrical block cipher algorithm.

It is capable of encrypting 128 bits of plain text. The various keys used by this algorithm are 128,192,256 bits.It is considered as the most secured algorithm

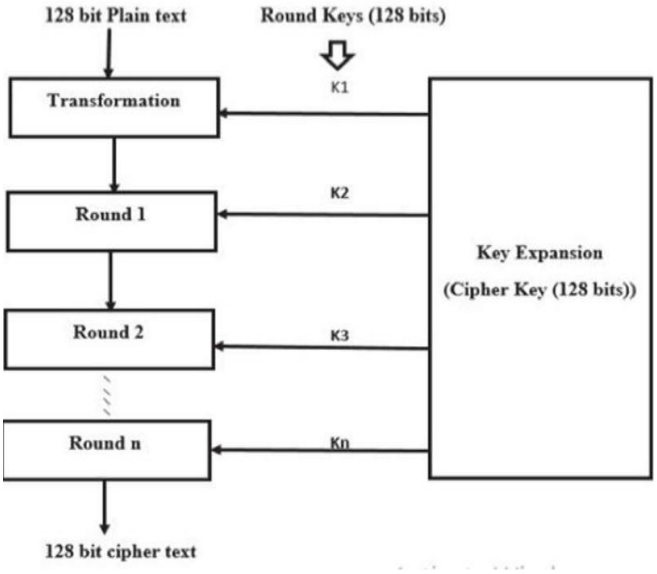

Fig.4 AES Architecture

B. Working of RSA Algorithm

Step 1: Generating Public Key: Select two prime numbers.

Suppose p=53 and q=59 Now we have to compute the public key which is done as follows We require n and e n is computed as n = p*q (3127) e is an integer but not a factor of n. e should be like 1< e < (n). So the value of e is taken as 3. Now our public key is created using n and e.

Step 2: Generating Private Key: Here we need to calculate (n) in such a way that (n) = (p

ISSN: 2366-1313

-1) (q-1). Here, (n)=3016. Now we calculate private key d as d = (k*(n) + 1) / e for some integer k If we take k as 2 then d is 2011. Now we are ready with our Public Key (n = 3127 and e = 3) and Private Key (d = 2011)

Encryption and Decryption Now we can encrypt and decrypt using an example. Let the example be “HI” Convert the letters to numbers: H=8 and I=9 The encryption formula is c = 89e mod n (1394 for the example) The decryption formula is m = cd mod n (the encrypted data comes out as 89 which is nothing but “HI”).

V. RESULTS

SYSTEM ARCHITECTURE

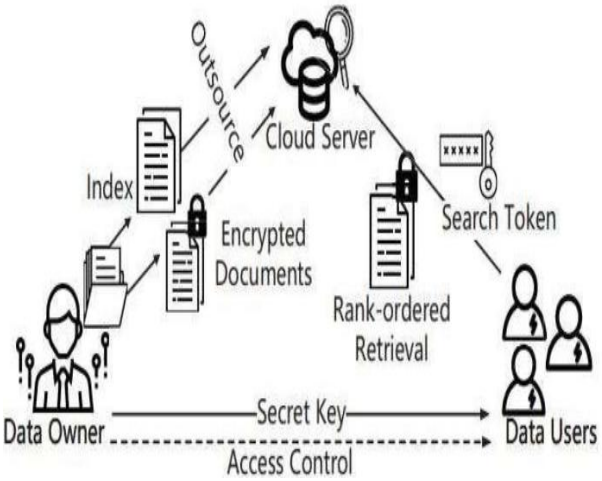

Fig.5 System architecture

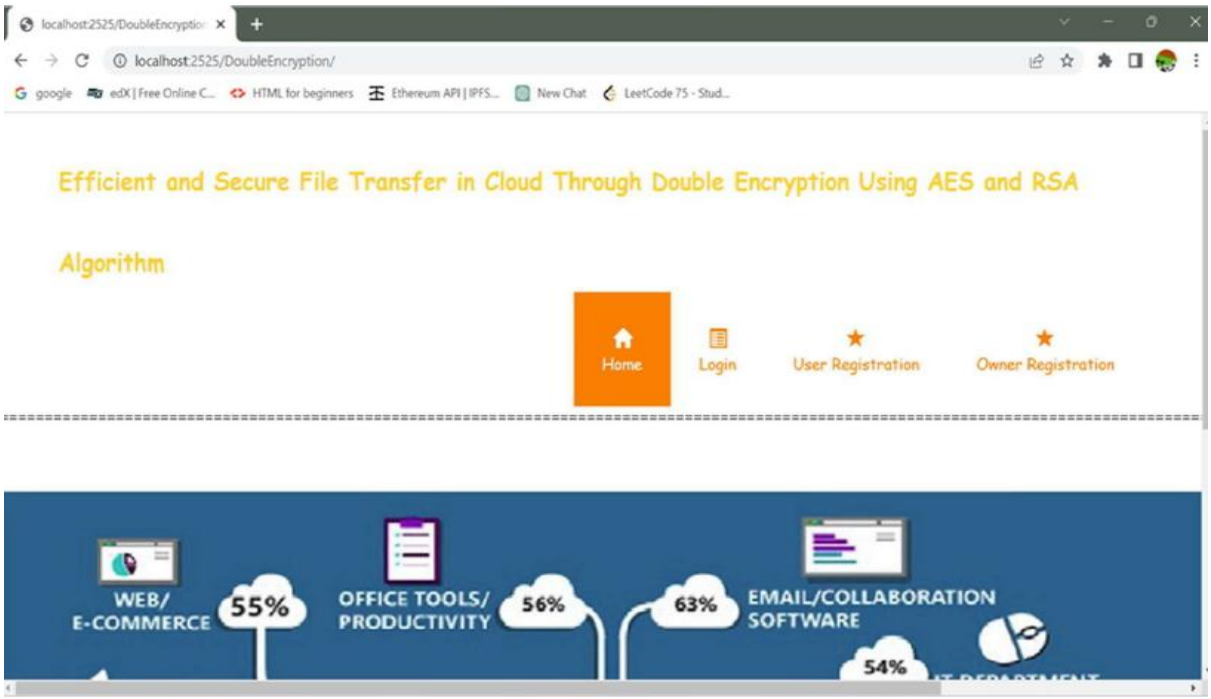

Fig.6 Cloudme Homepage

ISSN: 2366-1313

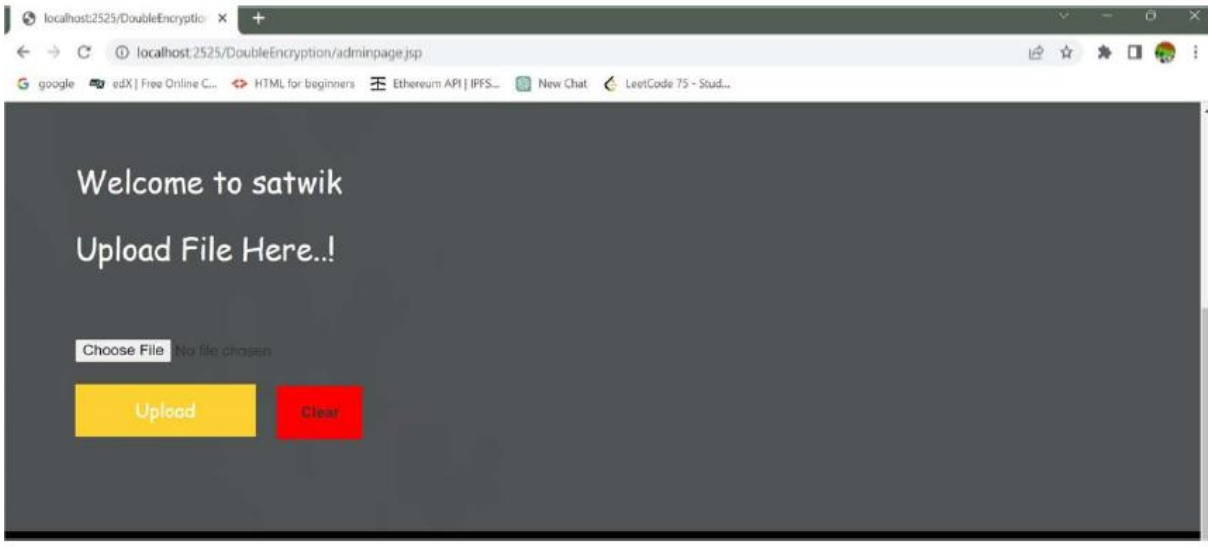

Fig.7 File upload page

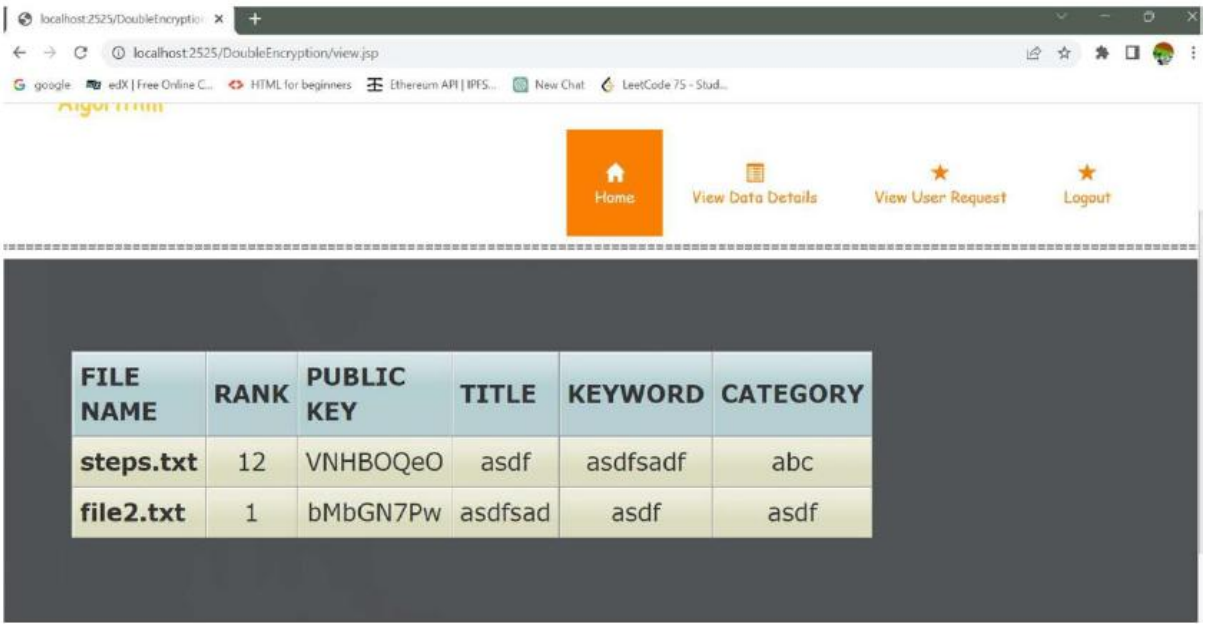

Fig.8 File Encryption Page

ISSN: 2366-1313

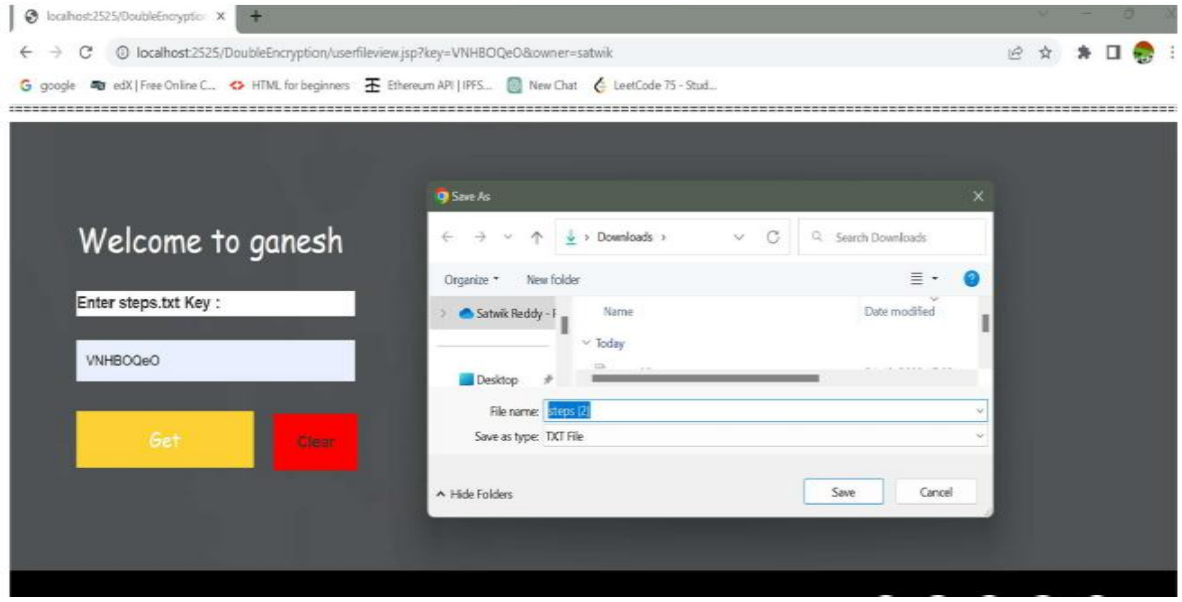

Fig.9 File Save Page

VI. CONCLUSION

From the results obtained, our method provides high security with resistance against propagation errors. The runtime of our algorithm is less compared to the existing algorithms; hence it is fast. Therefore, we propose a secure and cost-effective data protection method for cloud service end-users. Our system efficiency in terms of runtime with secure protection of text data over cloud compared with existing encryption and decryption methodologies like DES, Blowfish, RC5,3-DES. Our proposed methodology produces the best result compared with existing methods.

REFERENCES

[1] Li, Yibin, et al. "Privacy protection for preventing data over-collection in smart city." IEEE Transactions on Computers 65.5 (2015): 1339-1350.

[2] Wu, Jun, et al. "Big data analysis-based secure cluster management for optimized control plane in software-defined networks." IEEE Transactions on Network and Service Management 15.1 (2018): 27-38.

[3] Kuang, Liwei, et al. "Secure tensor decomposition using fully homomorphic encryption scheme." IEEE Transactions on Cloud Computing 6.3 (2015) 868-878.

[4] Krikor, Lala, et al. "Image encryption using DCT and stream cipher." European Journal of Scientific Research 32.1 (2009): 47-57.

ISSN: 2366-1313

[5] H.Qiu,G.Memmi,X.Chen,andJ.Xiong,"DC coefficientrecovery for JPEG images in ubiquitous communication systems," Future Generation Computer Systems,2019.

[6] Pommer, Andreas, and Andreas Uhl. "Selective encryption of wavelet-packet encoded image data: efficiency and security." Multimedia Systems 9.3 (2003): 279-287.

[7] Abdmouleh, Med Karim, Ali Khalfallah, and Med Salim Bouhlel. "A novel selective encryption DWT-based algorithm for medical images." 2017 14th International Conference on Computer Graphics, Imaging and Visualization. IEEE, 2017.

[8] Gai, Keke, et al. "Spoofing-jamming attack strategy using optimal power distributions in wireless smart grid networks." IEEE Transactions on Smart Grid 8.5 (2017): 2431-2439.

[9] Qiu, Han, and Gerard Memmi. "Fast selective encryption methods for bitmap images." International Journal of Multimedia Data Engineering and Management (IJMDEM) 6.3 (2015): 51-69.

[10] Shahid, Zafar, and William Puech. "Visual protection of HEVC video by selective encryption of CABAC binstrings." Ieee transactions on multimedia 16.1 (2013): 24-36.

[11] Xiang, Tao, Chenyun Yu, and Fei Chen. "Secure MQ coder: An efficient way to protect JPEG 2000 images in wireless multimedia sensor networks." Signal Processing: Image Communication 29.9 (2014): 1015-1027.

[12] Prasadu Peddi (2019), "Data Pull out and facts unearthing in biological Databases", International Journal of Techno-Engineering, Vol. 11, issue 1, pp: 25-32.