TRJ VOL. 2 ISSUE 4 JULY-AUG 2016 ISSN: 2454-7301 (PRINT) | ISSN: 2454-4930 (ONLINE)
DOI: 10.13140/RG.2.2.23618.38087

Multilayer File Encryption Scheme to Encrypt Multimedia Data in Cloud Computing

Tanu Dhiman[1], Er. Gurjot singh[2]
Student (M.Tech)[1], Assistant Professor[2]
Shahid Udham Singh College of Engineering and Technology Tangori (Mohali)

***Abstract*—**Cloud computing is the future of computing industry and it is believed to be the next generation of computing technology. Encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption is basically of two types: symmetric key encryption and public key encryption. In symmetric key, the encryption and decryption keys are same whereas in public key encryption, encryption key is published foe anyone to use and encrypt message. However, only the receiving party has access to the decryption key that enable message to read. This research wok is based on the hybrid algorithm made with the combination of Diffie-Hellman key exchange and serpent algorithm which is used to encrypt and decrypt multimedia files. The proposed work was evaluated using the parameters given by Encryption time, decryption time, probability value, accuracy per frame. The quantitative parameters prove that the proposed algorithm is highly efficient than existed one.

***Keywords*—**Cloud-computing, Multimedia-data encryption, Diffie-Hellman, Serpent algorithm,

I. INTRODUCTION

Cloud computing provides on-demand resources access from a shared pool of computing resources such as; hardware and software for efficient manage. Cloud computing services can be used from varied & prevalent property, slightly than distant servers or confined equipment. Since the user transit its confidential or sensitive data from local system to public cloud, it need to be protected from the unauthorized parties. Cryptography is the one of the way to protect data on cloud server. This involves the implementation of various encryption and decryption algorithms There are two type of encryption scheme are available: symmetric key and Public key encryption. Due to the present expansion in computer system knowledge, giving out of digital multimedia satisfied during the internet is massive.

In this research work, we vision the cautious encryption go forward for protective multimedia information. Computation workload essential for this encryption is extremely less. Encryption on the complete income to adjust the communiqué into code or vicious form, so that anyone who does not have entered to decode the code cannot view it. This is regularly done by means of a 'cipher'. A code is kinds of algorithm new in encryption that utilize certain explain method to combine up the data. The secret message can only be decipher with a 'key', that is what is branded as 'decryption'. At present much company's cloud comparable to Amazon EC2, Google Music, Drop Box, Skydive offer content organization system within the cloud system.

This research works upon the hybrid algorithm to encrypt or decrypt the multimedia using the Hellman Key Exchange algorithm which is asymmetric in nature and serpent algorithm which is symmetric. Using of multiple keys to encrypt is much more beneficial than using single key to encrypt any algorithm. As multiple key systems can increase the security even with short length of keys. That is why this research works upon hybrid algorithm. Compatibility factor of these two algorithms is far better than the other algorithms depending upon key size and accuracy.

Fig 1. Cloud computing

II. RELATED WORK

Junzuo Li et al. has proposed a model for data encryption and decryption. The encryption algorithm is designed, the information at highest factor by applying series of rotation on every block character and the key is rotated for every character and hence algorithm is called as key motor encryption algorithm. The key portion of algorithm is th CA inverter and CA shifter which is performed on every block character and finally on entire block. If file has N blocks and if every block has n characters then CAI and CAS is performed by N*n operations. And therefore this algorithm has complexity of O(N*n).

III. PROPOSED WORK

The proposed work use encryption algorithm like serpent and key exchange algorithm using diffie- hellman.

A. Diffie-Hellman Key Exchange

Asymmetric Encryption of data necessitates transfer of cryptographic isolated key. The most exciting part in this encryption is the transfer of the key from sender to receiver without anyone interrupting this key in between, this made possible by the Diffie-Hellman algorithm.

Diffie-Hellman agrees 2 users to swap a symmetric clandestine key from end to end an unsure wired or wireless conduit & devoid of any previous clandestine. DH works beneath the area of figure Zn where n=p.

P is a great main numeral & a is a manufacturer certain from the cyclic collection Zn. Two Heads A & B can use the DH algorithm to swap symmetric key.

- The center of population key of A is (pa, a') & the confidential key is a. A sends it's key to B.
- After reaction of A's community key, B chooses its own confidential key b, & multiply its community key (pa, ab). B sends it community key to A.
- Now A*B compute their symmetric key.
- Diffie-Hellman key discussion launches a joint secret among 2 merrymaking that can be used for clandestine communiqué for exchange data over a public system.

The following theoretical figure demonstrates the universal idea of key swap by using insignia in its place of very large books. The procedure initiates by having the 2 parties, Alice &Bob, concur on a chance preliminary shades that does not require to be kept secret; in this example the color is yellow. Every of them choose a clandestine colour-red & aqua in that order-which they keep to themselves. The significant part of procedure is that Alice and Bob at the present mix their clandestine colour jointly with their uniformley shared colour,as shown in fig.

B. Serpent Algorithm

The serpent algorithm was calculated by R.Anderson, E.Biham & L.Knudsen. the algorithm is a chunk code which code & decipher 128 bit blocks of information with a key of duration 128, 192, or 256. This algorithm occupy of three main machinery:

- First transformation IP
- Thirty-two rounds contain of around occupation perform key mash, S-box substitution & data celebrations via a linear alteration
- Final permutation

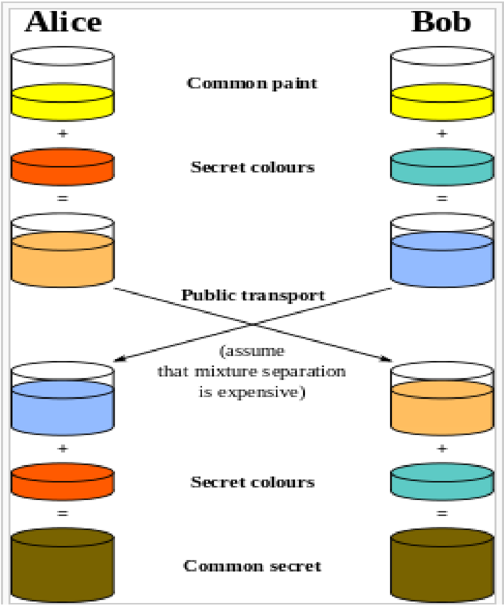


Fig 2 Diffie Hellman Key Exchange

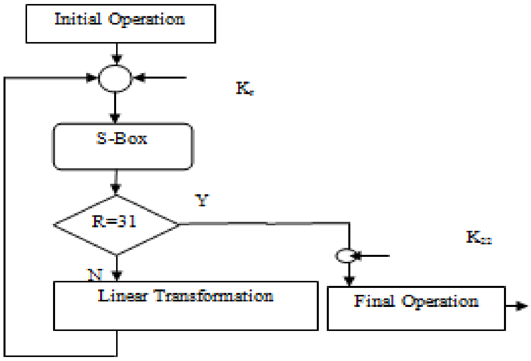
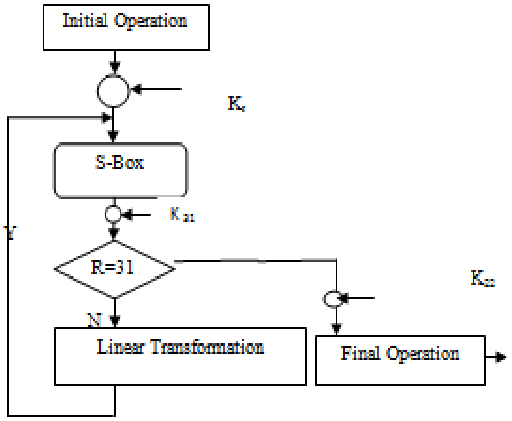


Fig 3 Encryption



DOI: 10.13140/RG.2.2.23618.38087

Fig 4 Decryption

C. *Methodology*

The implementation of the proposed algorithm is done on the private cloud. We have proposed a hybrid algorithm (Diffee- Hellman and Serpent Algorithm) which is used to encrypt the text file, image, audio and video file. First of all we encrypt the file using appropriate steps and get the file according to their perspective. After encrypting the file we will receive a mail through which we get our private key we have used mail-gun postmaster method to receive the key via mail.

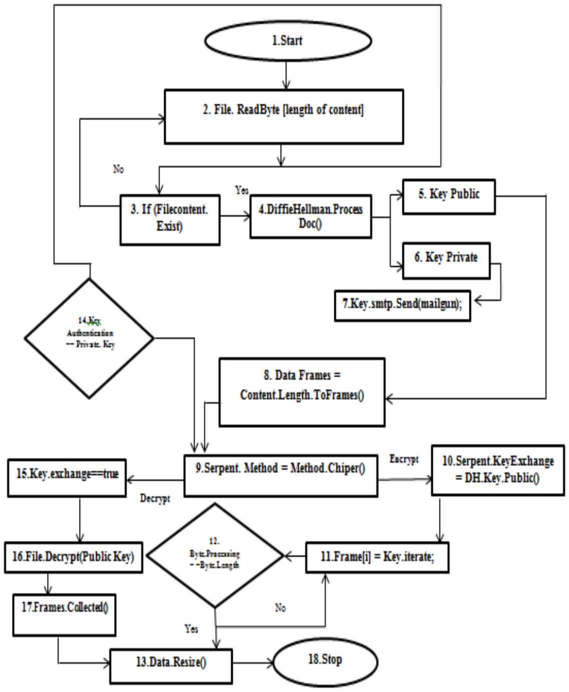

1.Start
2. File. ReadByte [length of content]
No
Yes
3. If (Filecontent. Exist)
4.DiffieHellman.Process Doc()
5. Key Public
6. Key Private
7.Key.smtp.Send(mailgun);
14.Key Authentication -- Private. Key
8. Data Frames = Content.Length.ToFrames()
15.Key.exchange==true
9.Serpent. Method = Method.Chiper()
Encrypt
10.Serpent.KeyExchange = DH.Key.Public()
Decrypt
16.File.Decrypt(Public Key)
12. Byte.Processing --Byte.Length
11.Frame[i] = Key.iterate;
17.Frames.Collected()
No
Yes
13.Data.Resize()
18.Stop

Fig 5 Flow chart

D. *Performance Analysis*

The result of proposed algorithm is compared with the existed one using various performance parameters like encryption time, decryption time, probability value, accuracy per frame. Using this hybrid algorithm time of encrypting and decrypting the multimedia get decreased as comparison to the existed algorithm. Probability of decrypting a file by unauthorized user is also less in this work whereas accuracy per frame is more as comparison the other so we get the accurate result using this hybrid algorithm. We can see results in following graph:

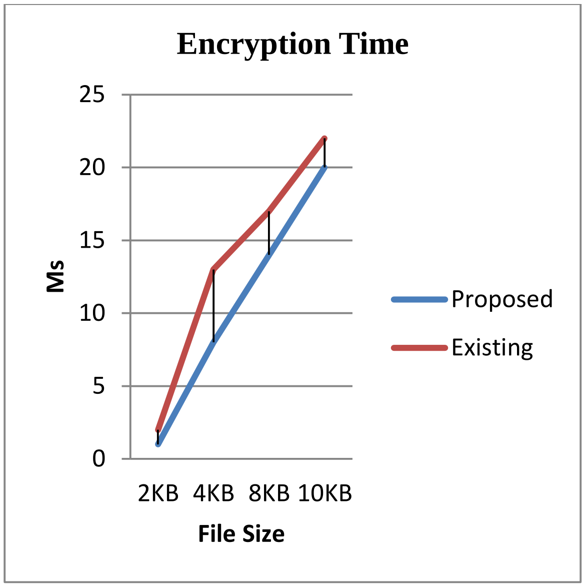


Fig 6 Encryption time

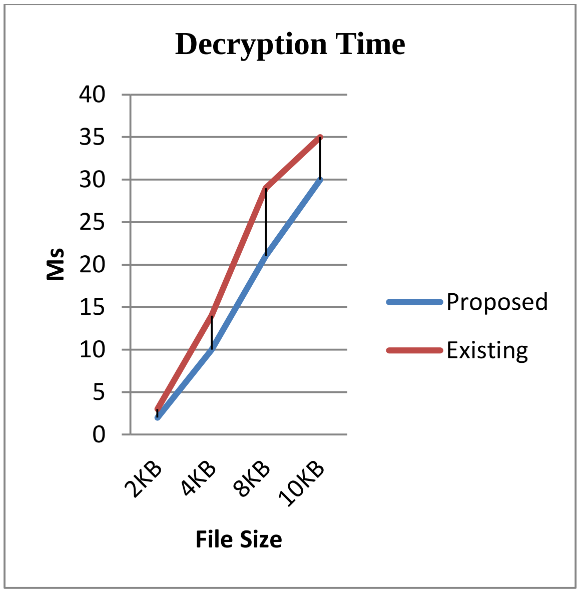


Fig 7 Decryption time

DOI: 10.13140/RG.2.2.23618.38087

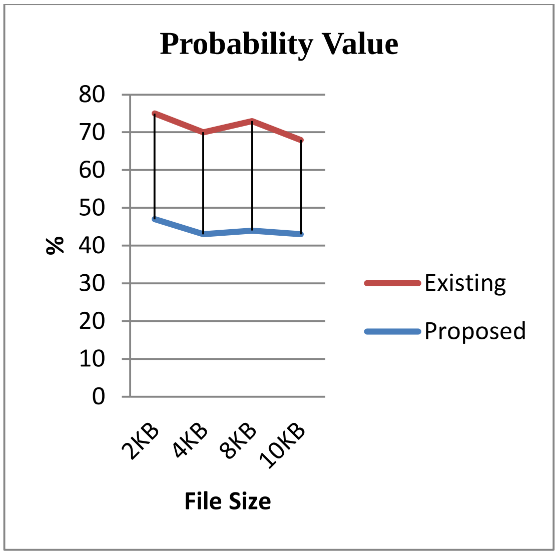


Fig 8 Probability Value

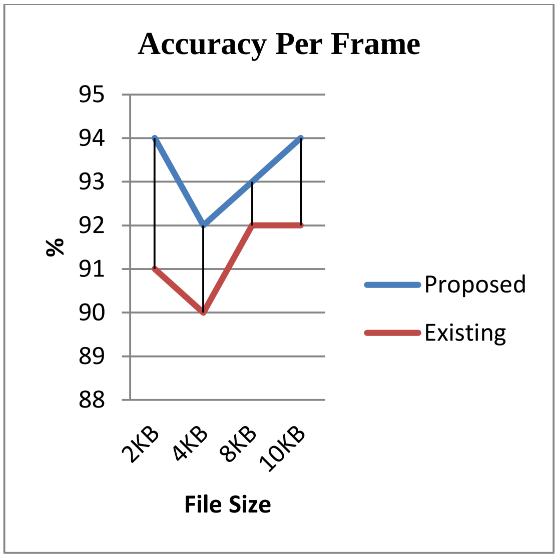


Fig 9 Accuracy per frame

IV. CONCLUSION AND FUTURE SCOPE

This presented a secure data exchange through key exchange algorithm using Diffie-Hellman & Serpent algorithm. We applied the scheme to secure data exchange. The projected SERPENT encryption comes up to for shielding information. This moves towards decrease the computational workload. Selective encryption is the procedure of encrypting only parts of a multimedia satisfied. Since the computational workload is fewer. This result in command of cloud computing. Other than, due to a variety of safety problems during sharing of data, some faults occur. Encryption technique reduce the probability of decryption over a cloud server but in future if any other optimization technique which optimize the information blocks for embedding and extraction than it might increase the security of this process with high accuracy rate as well.

V. REFRENCES

[1]. Adjeroh, Donald A., & Kingsley C. Nwosu. "Multimedia database management—requirements issues." IEEE multimedia 4.3 (1997): 24-33

[2]. Ahmed, Monjur, & Mohammad Ashraf Hossain. "Cloud computing & security issues in the cloud." *International Journal of Network Security & Its Applications* 6, no. 1 (2014): 25

[3]. Anderson, Ross, Eli Biham, & Lars Knudsen. "Serpent: A proposal for the advanced encryption standard." NIST AES Proposal 174 (1998).

[4]. Bhattacharya, Prabir, Mourad Debbabi, & Hadi Otrok. "Improving the Diffie-Hellman secure key exchange." Wireless Networks, Communications & Mobile Computing, 2005 International Conference on. Vol. 1. IEEE, 2005.

[5]. Ghebghoub, Y., S. Oukid, & O. Boussaid. "A Survey on Security Issues & the Existing SolutionsinCloud Computing." *International Journal of Computer & Electrical Engineering* 5, no. 6 (2013): 587

[6]. Kalaivani, K., & B. Sivakumar. "Survey on multimedia data security."International Journal of Modeling & Optimization 2.1 (2012): 36-41.

[7]. Kawle, Pravin, et al. "Modified Advanced Encryption Standard.", International Journal of Soft Computing & Engineering, Volume-4, Issue-1, March 2014

[8]. Prof. Radha.S.Shirbhate, 2Anushree A.Yerawar, 3Ankur M. Hingane," Features Preserving Data Encryption Used to Secure Multimedia Data", International Journal of Emerging Technology & Advanced Engineering, Volume 2, Issue .1, January 2012.

[9]. Singh, Ajit, & Swati Malik. "Securing Data by Using Cryptography with Steganography." International Journal of Advanced Research in Computer Science & Software Engineering (IJARCSSE) ISSN 2277 (2013).

[10]. Wolfgang, Raymond B., & Edward J. Delp III. "Overview of image security techniques with applications in multimedia systems." Voice, Video, Zhou, Minqi, Rong Zhang, Wei Xie, Weining Qian, & Aoying Zhou. "Security & privacy in cloud computing: A survey." In *Semantics Knowledge & Grid (SKG), 2010 Sixth International Conference on*, pp. 105-112. IEEE, 2010.

Tanu Dhiman, student of M.Tech (cse). My research area is cloud computing. I have done my research in multilayer file encryption scheme used to encrypt multimedia data using hybrid algorithm under the guidance of Er. Gurjot Singh, assistant professor at SUS Tangori Mohali.