DOI: http://dx.doi.org/10.26483/ijarcs.v9i2.5916

ISSN No. 0976-5697

Volume 9, No. 2, March-April 2018

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

SECURE FILE STORAGE IN CLOUD COMPUTING USING HYBRID CRYPTOGRAPHY ALGORITHM

Bindu Bala
Department of Computer Application
Department of Computer Science and Engineering
Shaheed Bhaghat Singh State Technical Campus,
Firozpur, India

Lovejeet Kamboj*
Department of Computer Application
Department of Computer Science and Engineering
Shaheed Bhaghat Singh State Technical Campus,
Firozpur, India

Pawan Luthra
Department of Computer Application
Department of Computer Science and Engineering
Shaheed Bhaghat Singh State Technical Campus,
Firozpur, India

***Abstract*:** Now a day's cloud computing is used in many areas like industry, military colleges etc to storing huge amount of data. We can retrieve data from cloud on request of user. To store data on cloud we have to face many issues .To provide the solution to these issues there are n number of ways . Cryptography and steganography techniques are more popular now a day's for data security. Use of a single algorithm is not effective for high level security to data in cloud computing. In this paper we have introduced new security mechanism using symmetric key cryptography algorithm and steganography .In this proposed system AES, blowfish, RC6 and BRA algorithms are used to provide block wise security to data. All algorithm key size is 128 bit.LSB steganography technique is introduced for key information security. Key information contains which part of file is encrypted using by which algorithm and key .File is splited into eight parts. Each and every part of file is encrypted using different algorithm. All parts of file are encrypted simultaneously with the help of multithreading technique. Data encryption Keys are inserted into cover image using LSB technique. Stego image is send to valid receiver using email .For file decryption purpose reverse process of encryption is applied. Cloud security is defensive method to protect data and there are various method to protect data like Deterrent controls, Preventive controls , corrective controls and detective controls. Wih concern of security we should keep some points in mind like privacy , confidentiality, integrity and so on .And our novel research based on this.

Keywords: Cloud service provider(CSP), ,cloud server(CS), Encode, Decode, Delay, Integrity

I. INTRODUCTION

Cryptography technique translates original data into unreadable form. Cryptography technique is divided into symmetric key cryptography and public key cryptography. This technique uses keys for translate data into unreadable form. So only authorized person can access data from cloud server. Cipher text data is visible for all people.

Symmetric key cryptography algorithms are AES,DES,3DES,IDEA ,BRA and blowfish. The main issue is deliver the key to receiver into multi user application. These algorithm require low delay for data encode decode but provides low security. Public key cryptography algorithm is RSA and ECC algorithm. Public and private keys are manipulated into public key cryptography algorithms. These algorithms accomplished high level security but increase delay for data encode and decode. Steganography hide the secret data existence into envelope. In this technique existence of data is not visible to all people. Only valid receiver knows about the data existence. Text steganography technique is used to produce high security for data. Secret data of user hide into
text cover file. After adding text into text cover file it looks like normal text file. If text file found by illegitimate user than also cannot get sensitive data. If illegitimate user try to recover original data than large amount of time is essential.DES algorithm is used for text encode and decode. Advantage of text steganography technique is provide security to text. Minimum space is essential for text steganography as compare to image steganoraphy.[2]

Three bit LSB technique used for image steganography. This system is suggested by author R.T.Patil .Sensitive data of user hide into cover image. We can hide huge amount of into image using LSB steganography technique .The author Klaus Hafmann has implemented high throughput architecture for cryptography algorithm.AES is symmetric key cryptography algorithm. It supports three types of keys. For 128 bit key require 10 rounds,192 bit key require 12 rounds and 256 bit key require 14 rounds. In improved AES algorithm encryption and decryption time is reduced .Advantage of modified AES algorithm is provides better performance in terms of delay.[3][4]

New symmetric key cryptography algorithm is presented by author M. Nagle. It applies a single key for texts encode and decode. Size of key is 128 bit. In this algorithm many steps are executed randomly so illegitimate user can even guess the steps of algorithm. Provide high throughput is one of the advantage of symmetric key cryptography algorithms. [5] Improved DES algorithm uses 112 bit key size for data encode and decode. For data encode purpose two keys are used.128 bit input of DES algorithm is divided into two parts .That two parts are executed at a same time.DES algorithm has one weakness. That is less key size.3DES algorithm essential large amount of time for encryption and

decryption .Improved DES algorithm have capability of provide better performance as compare to DES and 3DES.[6]Name Based Encryption Algorithm is work on one byte at a time. It uses secret key for encryption and decryption .Key generation process is done using random key generation technique. It provides security to data. Disadvantage of this algorithm is essential maximum time for converting data into cipher text because it operate on single byte at a time [7]To solve data storage and security issues author has new security model .In this model private and public cloud storage areas are used for increase security level of data. On private cloud secure data is stored and unnecessary data is stored on public cloud. Because public cloud any one can access. The main reason behind this system is reduce storage cost .Private cloud is more secure than the public cloud.[10]To enhance security of file in cloud computing .Source file is break into different into different part. Every part of file is encrypted and stored on more than one cloud. Information about file is stored on cloud server for decryption purpose. If attacker try to recover original file than he will get only a single part of file.[11]Elliptic Curve cryptography algorithm is used to accomplish high level security .Key managing complications are removed using access management and identity.ECC algorithm need maximum amount of time for file encode and decode. [12]File is converted into unreadable format using AES algorithm. Encrypted file is stored on cloud.AES algorithm is less secure than public key cryptography algorithms.[13]

AES and 3DES algorithms are merge into hybrid algorithm to accomplish confidentiality. It is harder for attacker to recover secret file of user.It consumes maximum amount of delay to translate data into decode and encode form.[14]

In existing system single algorithm is used for data encode and decode purpose. But use of single algorithm is not accomplish high level security. If we use single symmetric key cryptography algorithm than we have to face security problem because in this type of algorithm applies a single key for data encode and decode. So key transmission problem occur while sharing key into multiuser environment. Public key cryptography algorithms accomplish high security but maximum delay is needed for data encode and decode. To solve above issues we have introduced new security mechanism.

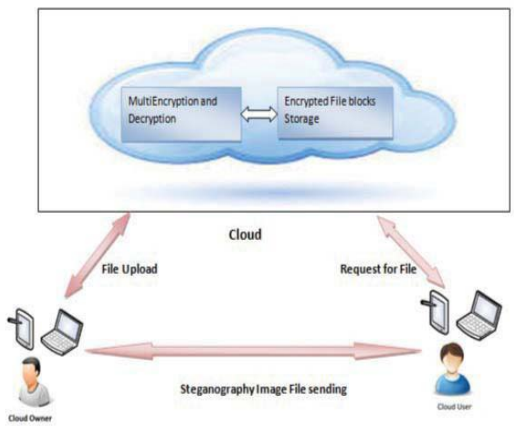

Figure 1. System Architecture.

Cloud owner and cloud user are included into system architecture as show in above fig 1.Cloud owner upload the data on cloud server. File is split into octet. Every part of file is encoded simultaneously using multithreading technique. Encoded file is stored on cloud server. Keys used for encryption are stored into cover image. Cloud computing is the multi user environment .In this more than one user can access file from cloud server. Cloud user request for file.On request of file user also get stego image using email which consist of key information. Reverse process is used for decode the file.

II. RELATED WORK

Hybrid cryptography algorithm present by author A. Shahade. AES and RSA algorithms are used into hybrid algorithm.AES algorithm require a single key. In hybrid algorithm three keys are used. For data upload on cloud mandatory keys are AES secret key and RSA public key. Private key of RSA and AES secret key are essential to download data from cloud. Whenever use makes an effort to upload data on cloud first that file stored onto directory for short time. In encryption process first AES algorithm is applied on file after that RSA algorithm is applied on encrypted data. Reverse process is followed for decryption. After applying keys that file covert into encoded form and stored on cloud server. Advantages of hybrid algorithm are data integrity, security, confidentiality and availability. Disadvantage of RSA algorithm is large amount time essential for data encode and decode.[1]

In security model symmetric algorithm uses chunk level encryption and decryption of data in cloud computing. Key size is 256 bit .Key is rotated to achieve high level security .For data integrity purpose hash value is generated. Hash values are garneted after encryption and before decryption. If both hash values matches than that data is in correct form. In this security model only valid user can access data from cloud. Advantages of security model are integrity, security and confidentiality.[8]

Three algorithms are used for implementation of hybrid algorithm. User authentication purpose digital signature is used. Blowfish algorithm is used to produce high data confidentiality .It is symmetric algorithm .It uses single key .Blowfish algorithm need least amount of time for encode and decode. Sub key array concept is used into blowfish algorithm. It is block level encryption algorithm. The main aim of this hybrid algorithm is achieve high security to data for upload and download from cloud. Hybrid algorithm solves the security, confidentiality and authentication issues of cloud. [9]

III. RESULT ANALYSIS

In this proposed system AES, RC6, Blowfish and BRA algorithms are used for block wise security to data. Proposed system is hybridization of AES,RC6,Blowfish and BRA. All algorithms are symmetric key cryptography. These algorithms uses a single key for file encode and decode purpose. All algorithms key size is 128 bit. To hide key information into cover image using LSB technique. Implementation of proposed system is done using java language. File encoding and decoding time is calculated with the help of java programming. File encode and decode

time is calculated for only text file with comparison of existing AES and Blowfish algorithms. File size is given in MB for AES algorithm. That is 1MB, 2MB, 4MB and 8MB.For Encode and decode time calculation of blowfish algorithm given file size is 100KB,200KB,400KB and 800KB.Encoding and decoding time is calculated in sec.

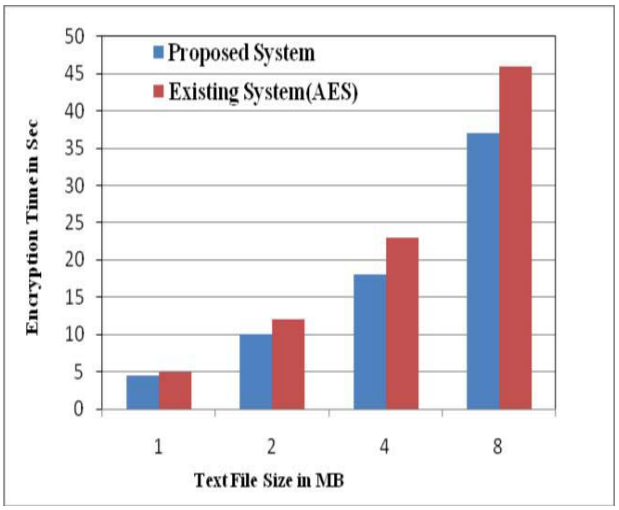

Figure 2. Encryption time Comparison with AES and Proposed System

As shown in fig 2 proposed system need least amount of time for file encode. Because in proposed system combination of symmetric key cryptography algorithms are run simultaneously. In Hybrid algorithm need 17% to 20% less time for text file as compare to Existing system. Use of single algorithm does not provide high level security to data in cloud computing.

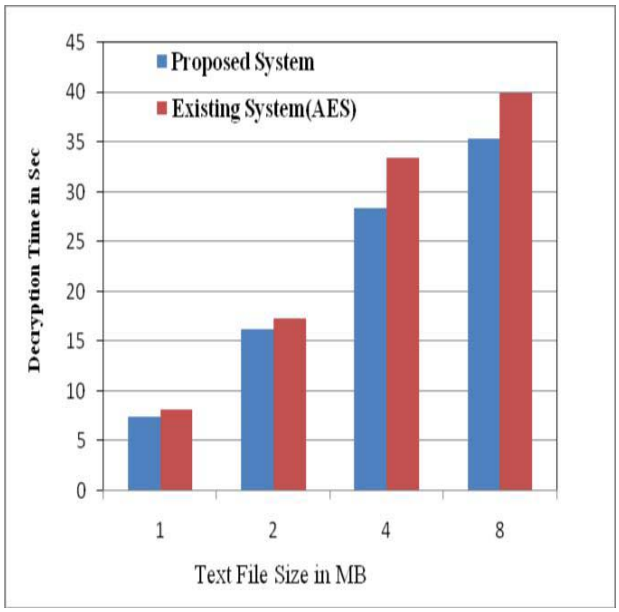

Figure 3. Decryption time Comparison with AES and Proposed System

As shown in figure 3 existing system need 15% to 17% maximum time need for file decryption purpose as compare to hybrid algorithm. AES algorithm is accomplish least amount of time for decryption.But provides less security to data.In AES if key size increases automaticaly number of rounds increases than encode and decode time also increases.

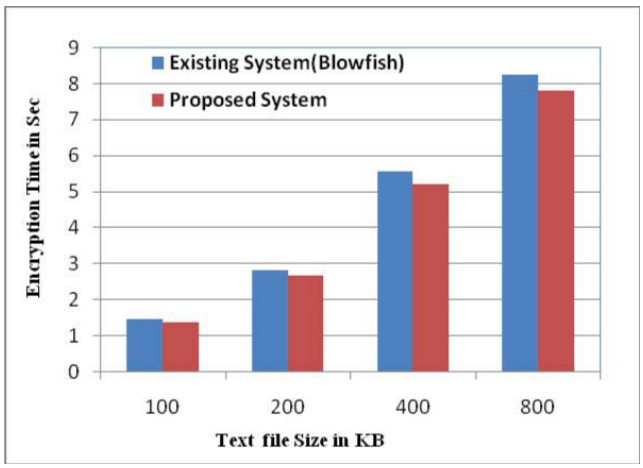

Figure 4. Encryption Time Comparison with Blowfish and Proposed System

Blowfish need least amount of time for file encode with compare to Advance Encryption Standard algorithm. As shown in fig.4 proposed system 12% to 15% less time need for file encode as compare to Blowfish. In proposed hybrid algorithm uses a single key for data encode and decode.

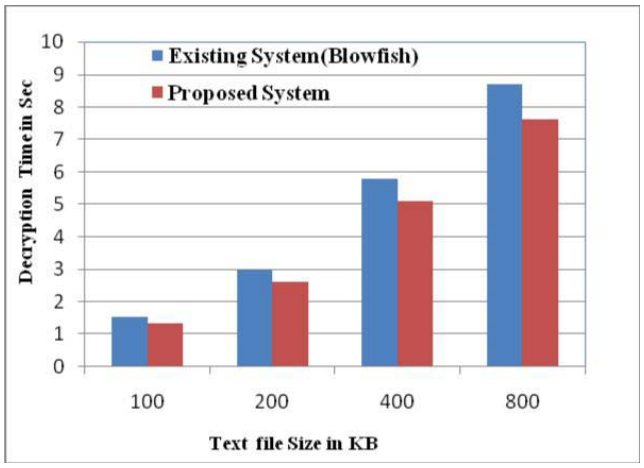

Figure 5.Decryption Time Comparison with Blowfish and Proposed

In proposed sysystem for text file decryption need 10% to 12% minimum time as compare to Blowfish as shown fig 5. In hybrid algorithm for file decryption needed maximum time as compare to encryption.But Blowfish algorithm need minimum time for text file decode as compare to AES algorithm.For text file deceyption needed maximum time in Blowfish algorithm as compare to encryption.

IV. CONCLUSION AND FUTURE WORK

Cloud storage issues are solved using cryptography and steganogarphy techniques.. Block wise Data security is achieved using AES, RC6, Blowfish and BRA algorithms. Key information security is accomplished using LSB technique. Data integrity is accomplished using SHA1 hash algorithm. Low delay parameter is achieved using

multithreading technique. With the help of proposed security mechanism data integrity, high security, low delay, authentication and confidentiality parameters are accomplished. Using proposed Text file encryption need 17% to 20% less time as compare to AES algorithm. For AES text decryption needs 15% to 17% maximum time as compare to proposed system. In Blowfish for encryption need 12% to 15% maximum time as compare to proposed hybrid algorithm. Text file decryption using hybrid algorithm need 10% to 12% less time with respect to Blowfish algorithm. In future, try to accomplish high level security using hybridization of public key cryptography algorithms. Steganography hide the secret data existence into envelope. In this technique existence of data is not visible to all people. Only valid receiver knows about the data existence. Text steganography technique is used to produce high security for data. Secret data of user hide intotext cover file. After adding text into text cover file it looks like normal text file. If text file found by illegitimate user than also cannot get sensitive data. If illegitimate user try to recover original data than large amount of time is essential.

REFERENCES

[1] V.S. Mahalle , A. K. Shahade, "Enhancing the Data Security in Cloud by Implementing Hybrid (Rsa & Aes) Encryption Algorithm", IEEE , INPAC,pp 146-149,Oct .2014.

[2] Abu Marjan, Palash Uddin, "Developing Efficient Solution to Information Hiding through text steganography along with cryptography",IEEE, IFOST,pages 14-17, October 2014.

[3] P. S. Bhendwade and R. T. Patil, "Steganographic Secure Data Communication",IEEE, International Conference on Communication and Signal Processing, pages 953-956,April 2014.

[4] S. Hesham and Klaus Hofmann , "High Throughput Architecture for the Advanced Encryption Standard Algorithm" IEEE,International Symposium on Design and Diagnostics of Electronic Circuits & Systems, pages 167-170,April 2014.

[5] M. Nagle, D. Nilesh, "The New Cryptography Algorithm with High Throughput",IEEE, ICCCI ,pages 1-5,January 2014.

[6] ZhouYingbing, LI Yongzhen, "The Design and Implementation of a Symmetric Encryption Algorithm Based on DES", IEEE,ICSESS,pages 517-520,June 2014.

[7] N. Sharma ,A.Hasan, "A New Method Towards Encryption Schemes (Name-Based-Encryption Algorithm)",IEEE, International Conference on Reliability, Optimization and Information Technology,pages 310-313,Feb 2014.

[8] Inder Singh, M. Prateek," "Data Encryption and Decryption Algorithms using Key Rotations N. Sharma ,A.Hasan, "A New Method Towards Encryption Schemes (Name-Based-Encryption Algorithm)",IEEE, International Conference on Reliability, Optimization and Information Technology,pages 310-313,Feb 2014.

[9] Jasleen K., S.Garg[,"Security in Cloud Computing using Hybrid of Algorithms",IJERJS, Volume 3, Issue 5, ISSN 2091-2730,pages 300-305, September-October, 2015.

[10] Jasleen K., S.Garg[,"Security in Cloud Computing using Hybrid of Algorithms",IJERJS, Volume 3, Issue 5, ISSN 2091-2730,pages 300-305, September-October, 2015.

[11] S. Munjal1, S. Garg, "Enhancing Data Security and Storage in Cloud Computing Environment", IJCSIT, Vol. 6, ISSN 0975-9646, pages 2623-2626,2015

[12] U.Veeresh,S.P.Kumar, " Multi Cloud Architecture to Provide Data Privacy and Inegrity" IJCERT, Vol. 2, Issue 9, PP 558-564, ISSN 2349-7084 , September 2015

[13] S. Ali Abbas, " Enhancing the Security of Identity and AccessManagement in Cloud Computing using Elliptic Curve Cryptography", IJERMT , Volume-4, Issue-7,ISSN: 2278-9359 ,pages 8-15,2015.

[14] Kiruthika.R,Jeena.R , " Enhancing Cloud Computing Security using AES Algorithm", IJARCSSE, Volume 5, Issue 3, ISSN 2277 128X,pp 630-635, March 2015.

[15] P. Kanchan, " Use of Digital Signature with Diffie Hellman Key Exchange and Hybrid Cryptographic algorithm to Enhance Data Security in Cloud Computing", Volume 5, Issue 6, ISSN 2250-3153 ,pp 1-4, June 2015

