International Journal of Science and Research (IJSR)
ISSN: 2319-7064
ResearchGate Impact Factor (2018): 0.28 | SJIF (2019): 7.583

Secure File Storage in Cloud Computing

Hrithik Dhakrey

School of Computer Science Engineering, Galgotias University, Greater Noida, India

Abstract: ***In the present and future cloud computing was used in several fields like military, business, colleges, IT industry, etc for storing large amounts of data. To provide security of data security problems there are many number of ways. Steganography with cryptography techniques are most useful and popular for data security. We aim to provide cloud security for securely store information into the cloud, By splitting all the data into sub-data or chunks, we provide data confidentiality, integrity and ensures availability. In present days cloud computing is increasing uses by almost every organization and IT industries. Cloud computing is a benefit in terms of low cost and availability of data through the Internet.***

Keywords: Secure file Storage, cloud computing

1. Introduction

Cryptography is closely related to the disciplines of cryptology and cryptanalysis. Cryptography is mechanism that convert original data into not readable form for human. The cryptography technique are two type one is symmetric-key cryptography and another one is asymmetric key cryptography. Encrypted text data is visible and not readable for all people[1].

In private key cryptography techniques, there are different algorithm like DES, RC2, AES and 3DES. The main problems is deliver encryption key to receiver. Private key cryptography algorithms takes least time for data encoding and data decoding. But private key cryptography algorithm are less secure or low security of data. In public key cryptography techniques, there are different algorithm like is Diffie Hellman, ECC and RSA. Private keys and Public keys create ecosystem of public key cryptography algorithms. Public key cryptography technique provides high security of data but it increase time of encryption and decryption.

Steganography is a useful technique for hide important data in existing file such as image, text, video etc. In steganography, hide messages is not checkable to unknown person. Only a valid software or receiver know about the data exist in file. For advanced level of security of data we use text Steganography mechanism. The secret messages of users hidden into cover text files. When padding some messages in the original message file it seems like a normal message text file. If unknown person found messages nut but it cannot read and get hide data. Text-encode and decode did by the AES algorithm. The main advantage and useful advantage of the steganography mechanism is to provide and fulfill high security to text data. As comparison of image steganography, minimum space are require in text steganography.

Existing system and proposed system are used for differentiate security of data and consumed time. In existing system we use single algorithm for data encryption and data decryption. But A single encryption algorithms is not achieve and provide high security of data. When if we use single algorithm then we faced data security issue because in this existing system we use single algorithm applies for data encoding and data decryption. And suppose that key transmission is medium is not secure. So problems occur when we share key into valid person. Public key cryptography algorithms provide high data security but these algorithm are takes time for data encryptom and data decryption. So we provide much simple and secure mechanism for solve problems of like encryption and decryption take less time and provide high data security

2. Related Work

In cloud computing, resources and application are share all of the individual person, business and servers. For data security, it not simple for the cloud service provides to provide an ensuring data and file security. Creating a high data security system are not easy or not difficult process. As a result of low security, it is easy like a gift for a hacker to full misuse access and destroy or delete the original of data. if any way compromises cloud security at any price; untrusting or that type of cloud are no use. A need for robust to technique becomes useful for secure data. In the proposed system introduced the data security model that used concept of hybrid encryption scheme to meet high security needs. Modified version of AES, RSA and DES algorithms are used in cloud servers for encryption and decryption.[2]

In hybrid algorithms we combine three different algorithm these algorithm are AES, DES and blowfish algorithms. AES algorithms required a single 8 bit key for encryption or decryption. In the hybrid cryptography algorithm, for data encryption and decryption three different length keys are use and then uploads on cloud servers. For download data from cloud Public key of DES Blowfish or RC6 and AES being use. Whenever file upload on server for few microseconds file is not encrypted because of without file upload encryption is not done. When file upload on server it divide into three parts. These part are encrypted using three different algorithm(AES, DES and RC6 or Blowfish). AES algorithm encrypt first part of file and DES encrypt second part of file and RC6 or Blowfish encrypt last part of file. After all process done encrypted data store on cloud and servers automatically delete the temporary file. All encryption keys shows on server where user can copy key in our system. The advantages of cryptography algorithms is provides data security, confidentiality integrity and availability.[3] chunk level data encryption and data decryption used by the security model of symmetric algorithm in cloud computing. For achieve high level of data security we use Keys rotation technique. Hashes use for data integrity purpose. Hash values

show before encryption and after encryption and same before decryption and after decryption . If both file hash values same, then it show data otherwise that data is corrupt. In that procedure, cloud server only allows authentic users can access and download data. Advantages of proposed system security models are securely configure for provides data security, confidentiality and integrity.[4] Hybrid algorithms are combination of three algorithms. For providing high data confidentiality we use Blowfish algorithm. The main aim of this hybrid cryptographic algorithms is to achieve and provide advanced level of security for users to data for download and upload from cloud server. On cloud server, Hybrid algorithm solves the security measures , confidentiality and authentication issues . [5]

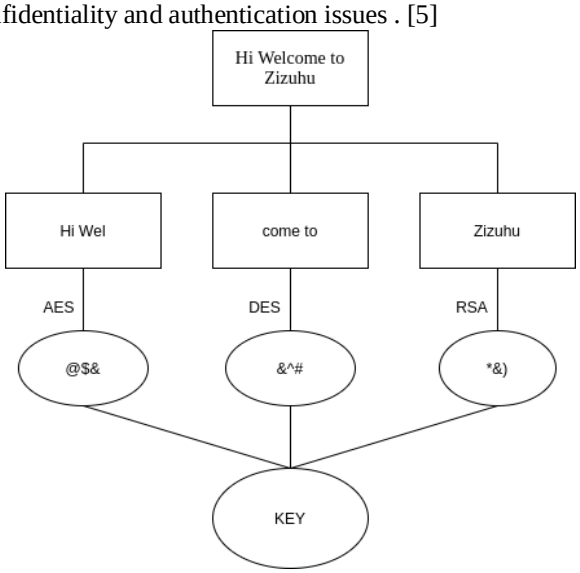

Figure 1: Data Encryption and Key Generation steps

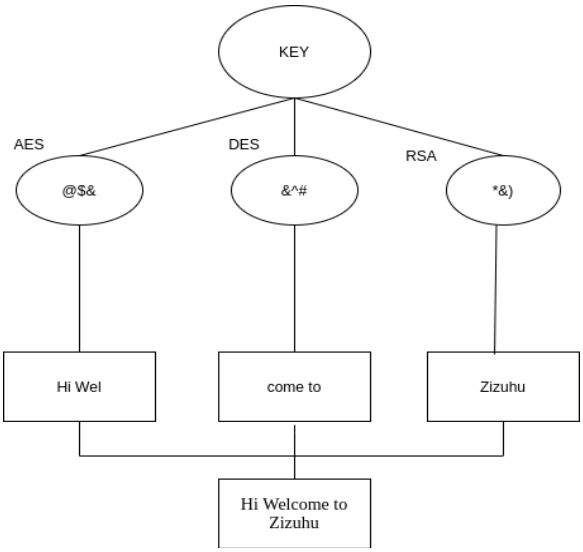

Figure 2: Data Decryption steps

Image steaganography user for hide sensitive data in a single images. In image steganography we use three bit Least Significant Bit (LSB) technique. All Important data hides in user target cover image. Using LSB steganography technique our approach to hide sensitive data in large amount of a single image. AES (Advanced Encryption Standard) is one of the secure symmetric key cryptography algorithm. AES algorithm supports three different size of key. For specific key size require specific round For example 256 bits key requires 14 rounds, 192 bits key requires 12 rounds and 128 bits key requires 10 rounds.[3][4]

3. Result Analysis

In Proposed system, we use AES, DES, and Blowfish algorithms are an example of block-wise security to data. The proposed system is combination of AES, DES and Blowfish or Hybrid algorithms. All algorithms are symmetric-key cryptography. the single key use for file encodes and decode. All algorithms' key size is different like For AES 256 bits key, DES 64 bits key and Blowfish 256 bits key use for encryption. LSB technique use to hide key information into user selected target image. The target proposed system implementation is done using python programming language. File encryption and decryption time is record using DateTime package name in python programming. We record encryption and decryption time for comparison between existing system and target system. We process encryption and decryption process on various file sizes that are 1MB, 2MB, 4MB, and 8MB. Encoding and decoding time is calculated in see

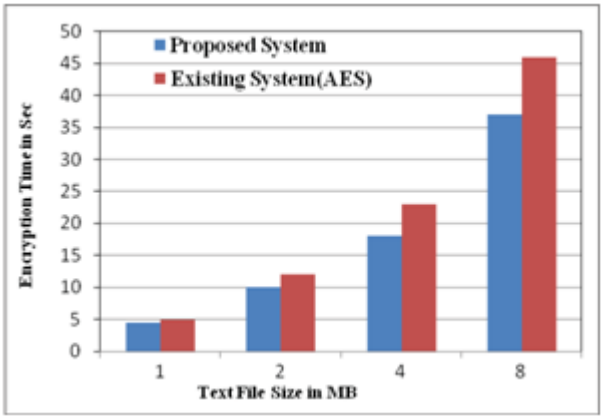

Figure 3: Encryption Time Comparison between AES and Proposed System

As we see in figure 3 less time require in proposed system for file encode. Target proposed system combination of AES, DES and Blowfish algorithms. In target proposed system all algorithm are not dependable to other algorithms. In proposed system 18% to 21% less time as comparison with Existing system for text file. We already says single encryption is not provide advanced level data security in cloud computing.

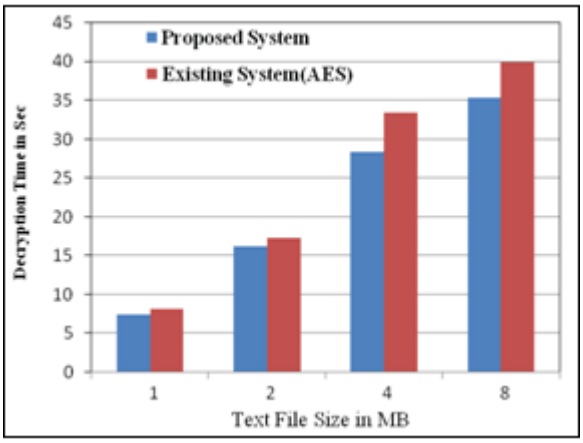

Figure 4: Decryption Time comparison between AES and Proposed System

As we see in figure 4 decryption process in existing system takes 15% to 17% more time as comparison between hybrid algorithm. AES is completion with more time for decryption and it is also provides less data security. If we increasing key size of AES algorithm's than automatically number of rotation round increased. And the result encryption and decryption time also increased.

Blowfish algorithm as comparison with AES algorithm take more time for file encryption. As we see in figure 5 as compare with file proposed system take 11% to 14% less time for file encryption. In proposed system we use three keys for file encode and decode.

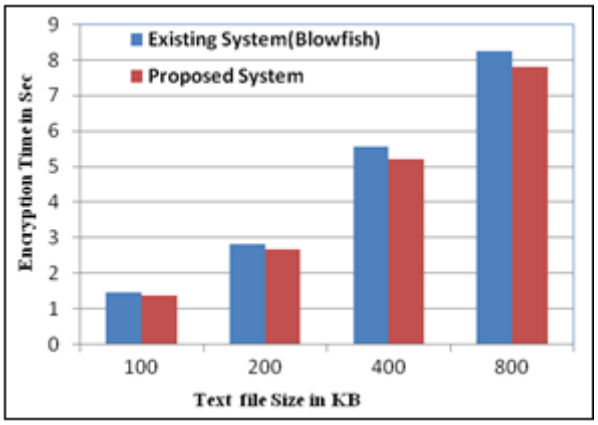

Figure 5: Encryption Time Comparison with Blowfish and Proposed System

Text file decoding needs 10% to 12% less time in the proposed system as compared to the Blowfish algorithm as shown in figure 6. As compare to encryption File decryption using hybrid algorithm required more time. But AES algorithm require less time for file decryption in comparison with Blowfish algorithm. In Blowfish algorithm text data decryption need more time as compared to Blowfish encryption

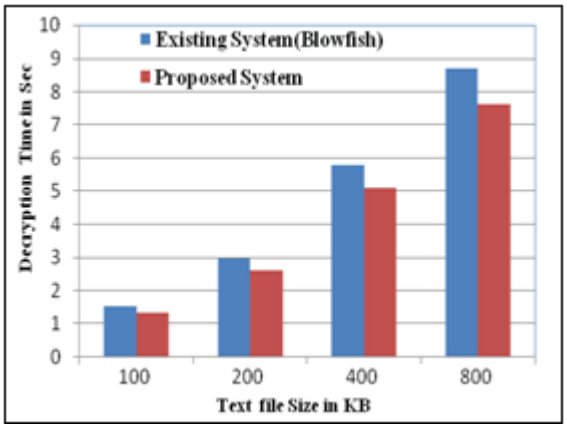

Figure 6: Decryption Time Comparison with Blowfish and Proposed

4. Conclusion and Future Work

Cryptography and Steganography techniques are helping to solve cloud storage security issues. AES, Blowfish and RC6 algorithm provides Block wise data security. The LSB (Lease Significant Bit) techniques are used to complete key information security. For low delay of parameter pass we use multithreading techniques. Data integrity, low delay, and high security and confidentiality are applied with the help to the proposed system. Text data encryption needs 18-21% less time in proposed system as comparison with AES algorithm. in AES algorithm, text data decryption take 16-18% more time comparison with target proposed system. Blowfish algorithm as compare to proposed hybrid system need 12-15% more time for data encryption.

References

[1] S Ramgovind, MM Eloff, E Smith, "The Management of Security in Cloud Computing", IEEE, ISSA,Sep .2010.
[2] Sherif El-etriby, Emam M. Mohamad, Hatem S. Abdul-kader, "Modern Encryption Techniques for Cloud Computing",IEEE, ICCCI,pages 800-805, Jun 2012.
[3] Tahira Mahboob, Maryam Zahid Gulnoor ahmad, "Adoptiong Information security techniques for cloud computing",IEEE,ICITISEE, pages 7-11,Jan 2017.
[4] M. Nagle, D. Nilesh, "The New Cryptography Algorithm with High Throughput",IEEE, ICCCI ,pages 1-5,January 2014.
[5] Manpreet Kaur, Rajbir Singh, "Implementaion Encryption Algorithms to Enchance Data security of cloud in cloud computing",IEEE, IJCA ,pages 16-21,May 2013.
[6] Andrzejak.2010, Exploiting Non-Dedicated Resources for Cloud Computing,In Proceedings of 12th IEEE/IFIP Network Operations & Management Symposium(NOMS 2010),Osaka Japan
[7] Shilpi Gupta, Jaya Sharma, "A Hybrif Eryption Algorithm Based on RSA and Diffie-Hellman",IEEE, IEEE International Conference on Computational Intelligence and Computing Research,Feb 2014.
[8] 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.
[9] Lili Yu, Zhijuan Wang, Weifeng Wang, "The Application of Hybrid Encryption Algorithm in Software Security", IEEE, International Conference on Computational Intelligence and Communication Networks,pages 762-765, Nov, 2012