Literature Review

Securing file storage using hybrid encryption and cryptology

Tushar Agarwal
1783910056
Agarwal.tushar2905@gmail.com

Shivendra Trivedi
1783910051
Shivendratrivedi2014@gmail.com

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. 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. With concern of security we should keep some points in mind like privacy, confidentiality, integrity and so on. And our novel research based on this.

Cloud computing is originated from earlier large-scale distributed computing technology. NIST defines Cloud computing as a model for enabling convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". In Cloud computing, both files and software are not fully contained on the user's computer. File security concerns arise because both user's application and program are residing in provider premises. The cloud provider can solve this problem by encrypting the files by using encryption algorithm. This paper presents a file security model to provide an efficient solution for the basic problem of security in cloud environment. In this model, hybrid

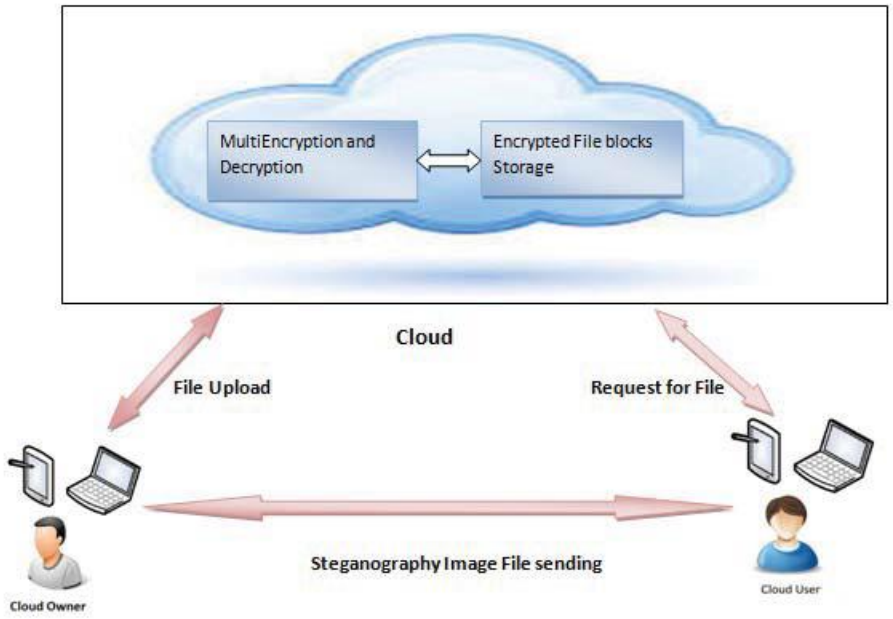
encryption is used where files are encrypted by blowfish coupled with file splitting and SRNN (modified RSA) is used for the secured communication between users and the servers

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 delivering the key to receiver into multi user application. These algorithms 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 providing security to text. Minimum space is essential for text steganography as compare to image steganography 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 providing better performance in terms of delay 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. 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 has capability of provide better performance as compare to DES and 3DES. 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 operates on single byte at a time. 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 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 providing security to text. Minimum space is essential for text steganography as compare to image steganography. 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. 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 advantages of symmetric key cryptography algorithms. 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. 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 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. 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. 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. 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. 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. 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.



Cloud owner and cloud user are included into system architecture as show in above figure 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.

Data Security Issues

Due to openness and multi-tenant characteristics of the cloud, the traditional security mechanisms are no longer suitable for applications and data in cloud. Some of the issues are as following:

- Due to dynamic scalability, service and location transparency features of cloud computing model, all kinds of application and data of the cloud platform have no fixed infrastructure and security boundaries. In the event of security breach, it is difficult to isolate a particular resource that has a threat or has been compromised.
- According to service delivery models of Cloud computing, resources and cloud services may be owned by multiple providers. As there is a conflict of interest, it is difficult to deploy a unified security measure.
- Due to the openness of cloud and sharing virtualized resources by multitenant, user data may be accessed by other unauthorized users.

HYBRID CRYPTOSYSTEM SCHEME

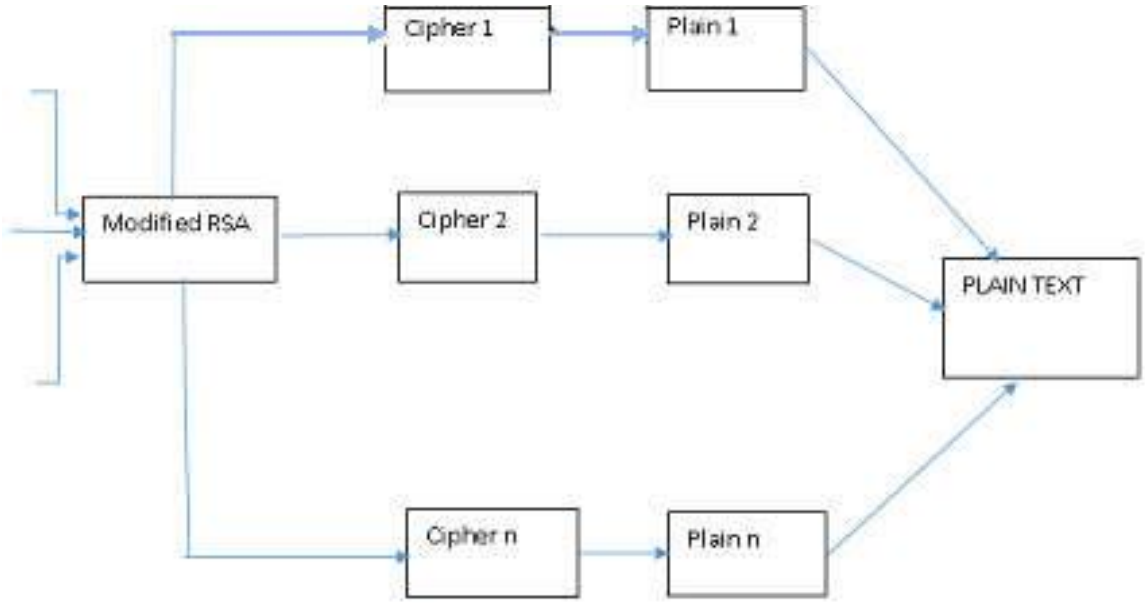
In order to ensure file security on cloud, hybrid cryptosystem is being used. We assume that the remote server is trusted, so files are encrypted by server and finally encrypted files are stored at the server end. The hybrid cryptosystem uses a combination of:

- Blowfish Algorithm coupled with File Splitting and Merging mechanism
- SRNN Algorithm

In a hybrid scheme, the performance of symmetric algorithm is integrated with security of asymmetric algorithm. The symmetric algorithm (Blowfish) used in hybrid cryptosystem has best practice to avoid data misuse when compared with other symmetric algorithms. Also, in terms of throughput, Blowfish has best performance. The SRNN used serves as a good balance between speed and security. In hybrid cryptosystem, firstly, files uploaded files are sliced and each slice is encrypted by the corresponding key Blowfish key provided by the user. Secondly, each of the n keys are encrypted using SRNN where n is the number of slices.

Blowfish

Blowfish is a symmetric block cipher which uses a Fiestal network, 16 rounds of iterative encryption and decryption functional design. The block size used is of 64-bits and key size can vary from any length to 448.Blowfish cipher uses 18 sub arrays each of 32-bit commonly known as P-boxes and four Substitution boxes each of 32-bit, each having 256 entries. The algorithm design is shown in figure. It consists of two phases: one is Key Expansion phase another is Data Encryption phase. In Key expansion phase, key is converted into several sub-keys and in Data Encryption phase, encryption occurs via 16-round networks. Each round consists of a key dependent permutation and a key and data dependent substitution.



SRNN

The SRNN algorithm is a public key cryptography algorithm similar to RSA with some improvement. In this algorithm, extremely large number having two prime factors (similar to RSA) is used. In addition to, this, two short range natural number in pair of keys are used. This improvement increases the security of cryptosystem. SRNN is used for secure communication between user and cloud servers.

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.

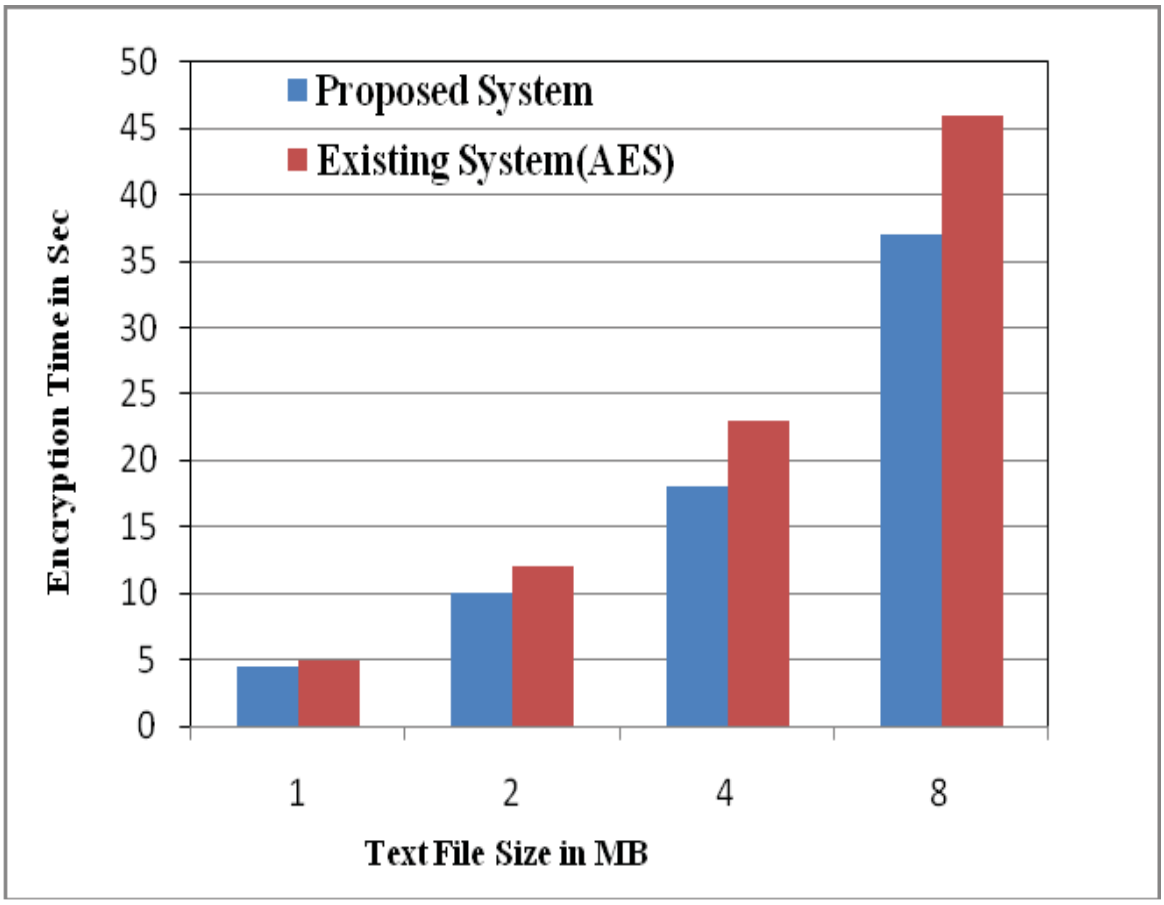
In security model symmetric algorithm uses chunk level encryption and decryption of data in cloud computing. Key size is 256 bit. Key is rotated to achieve high level security. For

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.

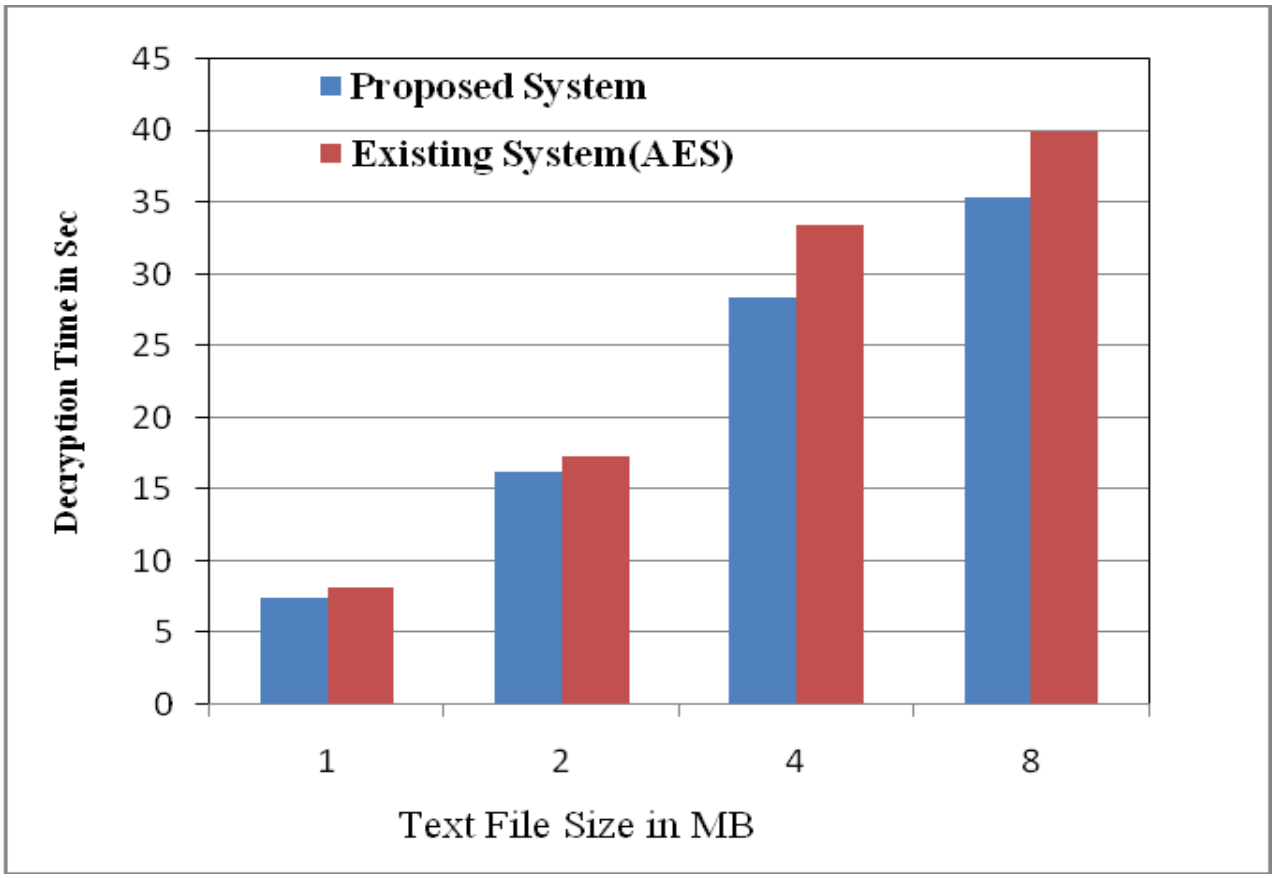
Three algorithms are used for implementation of hybrid algorithm. User authentication purpose digital signature is used. Blowfish algorithm is used to produce high data confidentiality. It is symmetric algorithm. It uses single key Blowfish algorithm need least amount of time for encode and decode. Sub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

RESULT ANALYSIS

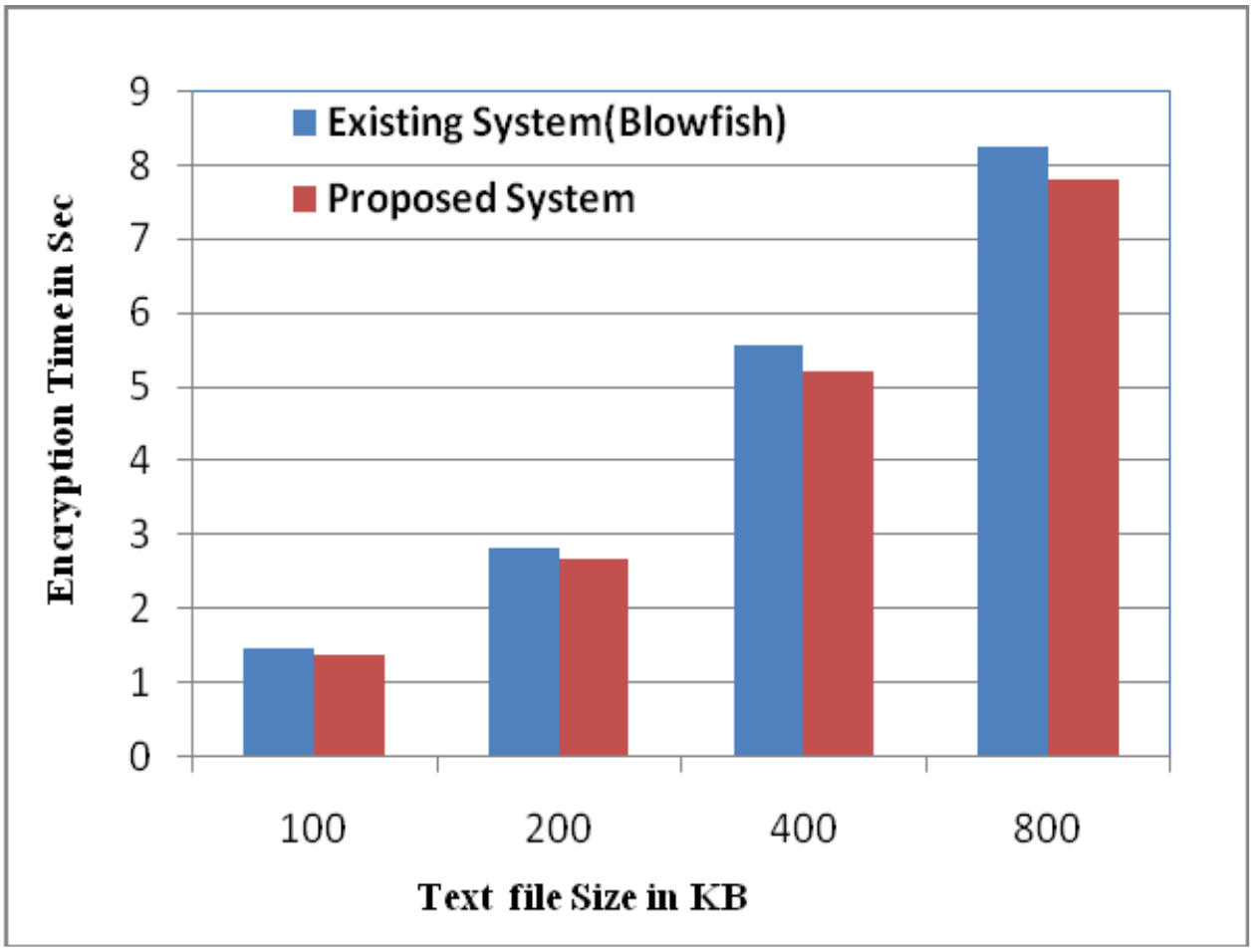
In this proposed system AES, RC6, Blowfish and BRA algorithms are used for block wise security to data. Proposed system is hybridization of AES, RC6, Blowfish and BRA. All algorithms are symmetric key cryptography. These algorithms uses a single key for file encode and decode purpose. All algorithms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



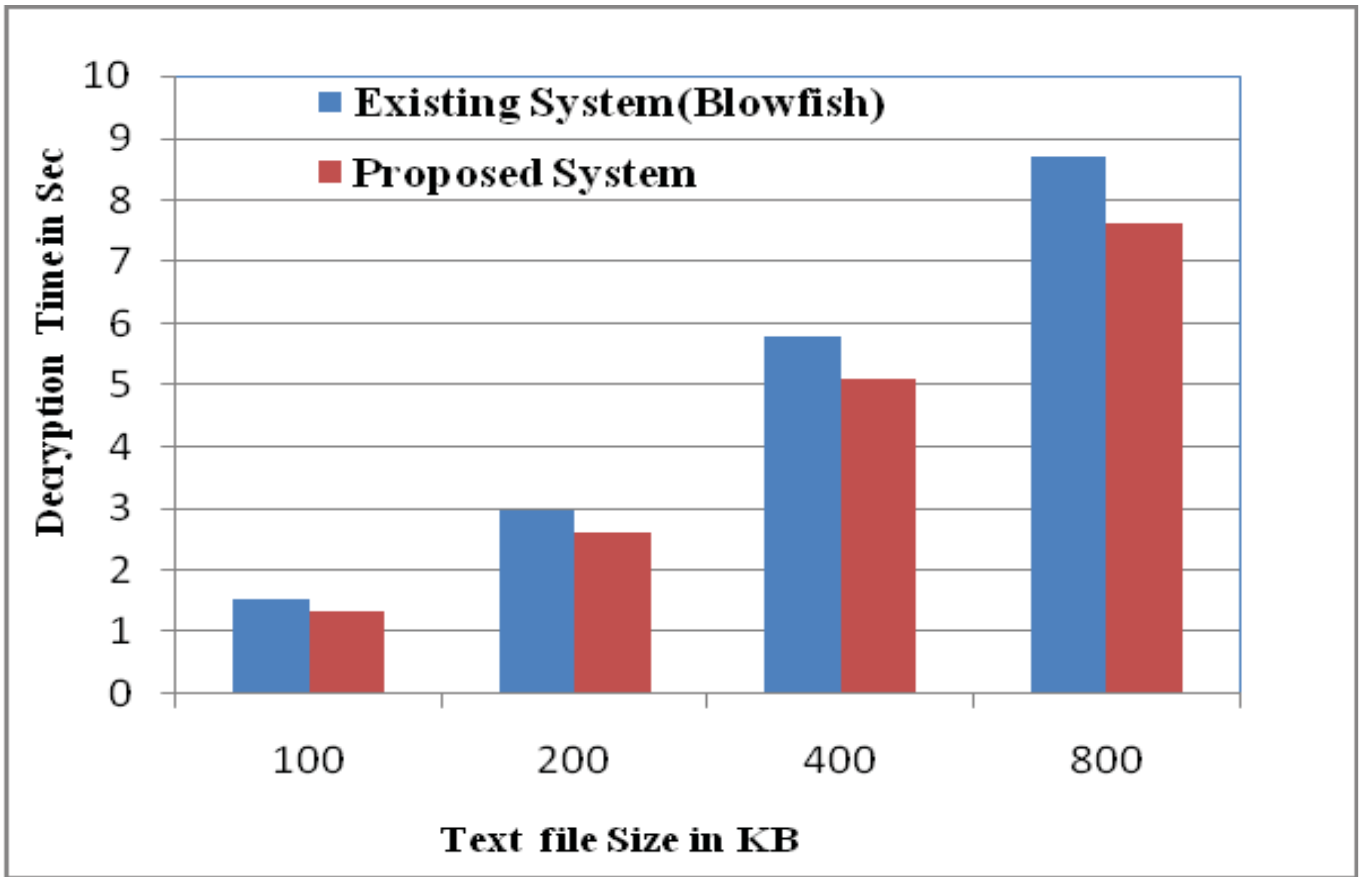
As shown in figure proposed system need least amount of time for file encode. Because in proposed system combination of symmetric key cryptography algorithms are run simultaneously. In Hybrid algorithm need 17% to 20% less time for text file as compare to Existing system. Use of single algorithm does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



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



Blowfish need least amount of time for file encode with compare to Advance Encryption Standard algorithm. As shown in above figure 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.



In proposed sysystem for text file decryption need 10% to 12% minimum time as compare to Blowfish as shown above figure 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.

HYBRID CRYPTOSYSTEM PHASES

.

The hybrid cryptosystem used to maintain security of the files has two phases:

- Encryption Phase
- Decryption Phase

A. Encryption Phase

At the encryption end,

- On the specification of user, the file being encrypted will be sliced into n slices. Each of the file slices is encrypted using Blowfish key provided by the user for each slice.
- The key will be encrypted using SRNN public key
- After encryption, we have encrypted files slices and the corresponding encrypted keys.

B. Decryption Phase

At the decryption end,

- The user will provide n SRNN private keys, according to the number of slices (n) created during the encryption phase. Blowfish key is decrypted at the server end using the SRNN private key specific to the slice.
- Using the corresponding decrypted Blowfish keys, file slices stored at server are decrypted.
- The decrypted slices will be merged to generate original file.

PROPOSED CLOUD COMPUTING SECURITY ARCHITECTURE

In order to ensure file security on cloud, the above hybrid cryptosystem is deployed on cloud. We assume cloud server as trusted but in order to prevent tampering/misuse of data by intruder or data leakage or other security concerns, the data is stored at server in the encrypted form. We broadly classify the scheme deployed on cloud in three phases:

- Registration Phase
- Uploading Phase
- Downloading Phase

We used Open Nebula toolkit to set up cloud environment. In Open Nebula, we have one front node and n cluster nodes. The VM's are deployed from front node to the corresponding cluster node. Open Nebula has been designed in such a way that it allows integration with many different hypervisors and environments. There is a front-end that executes all the process in Open-Nebula while the cluster nodes provide the resources that are needed by VM. There is at least one physical network joining all the cluster nodes with the frontend.

A. Registration Phase

In the Registration Phase, the client registers himself in order to upload and view his files to/from the cloud server. In the registration process, the client sends its request to front node and in return, front node assigns the VM of the cluster node, which has minimum load among other VM's on the network to the client. At the end of registration phase, the client is registered with IP address of corresponding VM. Whenever he again issues his request, the request is transferred to its corresponding VM. The encrypted files, encrypted blowfish keys, public SRNN keys are stored at his registered VM.

B. Uploading Phase

In the Uploading Phase, steps are as follows:

- Step: 1: The client will send request to front node to authenticate himself.
- Step 2: On successful authentication, the front end which send the corresponding IP address of the VM against which user was registered.
- Step 3: The files are uploaded by the client to the registered server (VM).
- Step 4: The encryption of uploaded files is done using the hybrid cryptosystem.
- Step 5: The encrypted slices and Blowfish encrypted keys remain stored in VM's data store.
- Step 6: The SRNN private keys are send to user and finally they are deleted form the server so that only the authenticated user is able to view his uploaded file.

C. Downloading Phase

In the downloading phase, the steps are as follows:

- Step 1: The client will send request to front node to authenticate himself.
- Step 2: On successful authentication, the front end which send the corresponding IP address of the VM against which user was registered
- Step 3: The client will upload n SRNN private keys for the corresponding n slices.
- Step 4: The SRNN private keys will decrypt the corresponding encrypted Blowfish keys and the encrypted slices are decrypted by Blowfish keys.
- Step 5: The decrypted files are merged to generate original file.
- Step 6: The decrypted file is downloaded and viewed at client end.

DESIGN AND IMPLEMENTATION

For the purpose of simulating the proposed cloud security model, we used Open Nebula open source toolkit. Here we created one front node and two cluster nodes. At each of the Cluster node 2 VM's are deployed. The allocation of VM at the time of registration is implemented in python which is well known for its platform independence. The hybrid cryptosystem is also implemented in python and deployed at each of the VM. Various libraries have been used like

python. crypto. security to implement hybrid encryption scheme. The cloud security model has been tested for various types of file: audio, image, text, word, pdf file.

BENEFITS OF PROPOSED MODEL

The proposed model is liable to meet the required security needs of data center of cloud. Blowfish used for the encryption of file slices takes minimum time and has maximum throughput for encryption and decryption from other symmetric algorithms. Modified RSA(SRNN) has increased security than RSA. The idea of splitting and merging adds on to meet the principle of data security. The hybrid approach when deployed in cloud environment makes the remote server more secure and thus, helps the cloud providers to fetch more trust of their users. For data security and privacy protection issues, the fundamental challenge of separation of sensitive data and access control is fulfilled. The various benefits are as summarized:

- The public key cryptography used helps to facilitate authorization of user for each file.
- The need of more light and secure encryption system for file information preserving system on cloud is satisfied.
- The file splitting and merging makes the model unfeasible to get attacked.

CONCLUSION AND FUTURE WORK

Cloud storage issues are solved using cryptography and stenography 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.

According to service delivery models and deployment models of cloud, data security and privacy protection are the primary problems that need to be solved. Data Security and privacy issues exist in all levels in SPI service delivery models. The above-mentioned model is fruitful in data as a service, which can be extended in other service models of cloud. Also, it is tested in cloud environment like Open Nebula, in future this can be deployed in other cloud environments and the best among of all can be chosen.