DOI : 10.15613/sijrs/2015/v2i2/114285
ISSN (Print): 2349–8919
SciеXplore: International Journal of Research in Science, *Vol 2(2), 24–30, July–December 2015* *ISSN (Online): 2350–0999*

Impregnable Cloud Storage using Surrogate Twofold Encryption Technique (STET) in Cloud

D. Seethalakshmi[1]* and G. M. Nasira[2]

[1]Research Scholar, Research & Development Centre, Bharathiar University, Coimbatore, Tamil Nadu, India
[2]Professor, Department of Computer Applications, Chikkanna Government Arts College, Tirupur, Tamil Nadu, India

Abstract

Privacy and security in cloud computing has becoming a challenging task where several techniques used by existing security based only on perimeter level. When an obtrude tries to hack the formatted encryption scheme protected by service provider they could not be hacked. However the data insecurity has no solution to the large extent though the entire process provided by the service provider may not always as right as cloud is a public entity. In our proposed, we enhance several algorithmic techniques chosen randomly applied for the cloud efficient storage and security. There are different service model and distribution model the organization use in cloud and they report the efficiency and correctness of data. The techniques emphasizing authorization models are Surrogate Twofold Encryption Technique (STET). The data from main database (owner's data) stored in cloud by transferring data contents into a substitute system and encrypting the original data in surrogate system, and then data is re-encrypted inside the cloud thus forming a triple layer protection for the database stored in cloud. Moreover, in arbitrary access control the security enhanced can randomly choose any two encryption technique from four cryptographic algorithms. Those two algorithms selected will be known only to their corresponding system encrypting it. Thus it passes twofold encryption methods and for decrypting it also it needs to pass this twofold decryption method. A flag set synchronized for accessing arbitrary choice of algorithms which promotes a secured algorithmic encryption. To make it more complex, the ciphered information stored in cloud is visible and known only to their corresponding system or well-known authorized user can view or use the data.

Keywords: Arbitrary Access Control, Encrypting Algorithm, Flag Set, Identity Based, Service Provider, Surrogate Twofold Encryption Technique (STET), Triple Layer Protection

1. Introduction

Cloud, a computational layout implies common storage and may change rapidly. Cloud being a technical era restrains intensive ranging effects in IT industry, software and information storing [1]. Cloud delivers computing resources over internet so that the clients can store their data over internet instead of storing in a hard drive or by uploading applications. Cloud is more efficient to store data, update applications and all over to view and use it [2]. While there are this much assets in cloud, in other hand the major drawback relating privacy implication also resist in cloud computing. Though privacy issue is not an obstacle but it takes in consideration and counter measures always evaluated. Some of the cloud services which affect security for storing files online, storing private data, social sites and some business (online) application [3]. Cloud equips information storage space, power processing in computer and executing application of user for better placement of data. Cloud computing allows third-party data centre to store and process data because of data corruption, data redundancy, lacking information, interchange between data and overflow of information permitted [4]. When the data endures over the organizational bound the user lose control on data and therefore hikes concern related to security in cloud. In existing system encryption technique used is not that much efficient to store data in cloud storage server. The ciphered text generated with basic modules allowing it easy for the intruder to hack the data from server. For instance, consider peer1 and peer2 as

*Author for correspondence

user A and third-party [5]. Here P1 stores data in inter cloud with simple specification that the encryption done using the user attribute or his\her details then it is clear for P2- the third party\intruder to crack the data of P1 by collecting P1's personal details [6]. So the attribute based encryption or the role based encryption is not at all the only choice for data security. Moreover, the data stored in the cloud storage server needs more protection and consideration and complex encryption techniques have been evaluated. In proposed cloud computing implies an intellectual task by providing security executing complex encryption techniques. However the data in cloud server need more protection, so single and simple encryption is not much enough. Computing techniques of data stored in cloud is not easy to keep its harder place for intruder even to view data. Thus in the first section we discuss about the encryption in cloud deployment model. In the second section algorithms used for encryption explained clearly. In the third section the technique for twofold encryption in surrogate system and cloud storage briefed how it gets over. At last the experimental and result analysis is explained in detail.

2. Cloud Encryption Deployment Model

Cloud delivers the data through certain delivery models. They are private, public, community and hybrid. In Public the uploaded user data delivered in public form of the service is possible owned by the organization. Example: Amazon cloud service which is a common provider [7, 8]. In private the service are individually provided managed by the organization or alternate party. Private comes beneath off site. In community several organization processes share the cloud service supporting particular community having concerns (security requirements, compliance consideration etc...). Cloud indicated as special case of cloud mostly provided by government agencies. Hybrid is the combination of all three computing infrastructure [9, 10]. Example: the data stored in private cloud indicating an agency with a process running in public and in as cloud [11]. The information stored under these models needchecked often and secured in prospective aspect [12]. The negligence in cloud storage may cause eventual risk to data owners thereby more chances for external hacker's attempts to threat, to cut data from the service provider. To avoid the circumstances various techniques formulated in providing cloud service [13]. Eventually data stored in third-party system cause issues on information security. As providing confidentiality for data in server, a client encrypts data by using cryptographic techniques [14]. The process handled by setting flag with managed configuration embedded with 6 cryptographic algorithm of cloud for encryption process. After completion of encryption then re-encryption takes place for better security. Through this double time encryption the data in cloud uploaded and hence the data protected.

Considering n as a distributed storage servers and n+1 as key server in storage system a specific message segregated into several blocks which represented as vectors. A secure cloud storage system is supporting a set of secure data uphold using a Surrogate System Encryption(SSE) scheme. This encryption technique supports flag set choosing cryptographic algorithm over ciphered data and supporting operations over encrypted messages[15]. The format is highly distributed to encode and pass message through servers. The storage capacity in every single server may not increase as the server stores a ciphered output indicating the collection of encrypted data symbols.

3. Algorithmic Techniques used in Encrypting

Cloud used for encryption based encryption used before providing less security in proposed several cryptographic algorithms. In cloud security, algorithms may differ as symmetric and asymmetric algorithm each defines its own criteria and characteristics. Symmetric algorithm (DES, blowfish, AES): In symmetric algorithms only a single key used to encrypt and decrypt the information. Asymmetric algorithm (RSA): in asymmetric two keys implemented both public and private key. Public Key used for encryption purpose and private key for decrypting data. As primary step it selects from these cryptographic algorithms any four of the algorithm and promoted for encrypting data.

The cloud executes any of the algorithms from symmetric section or asymmetric section arranged in a set of flag. In the flag the algorithms completed by segregating them in order so verifying the size, key length, security and speed of each single algorithm after it completes the sequencing the flag prepares to choose algorithm. The flag requests for choosing algorithm executed at once specifying the combination and features of algorithm.

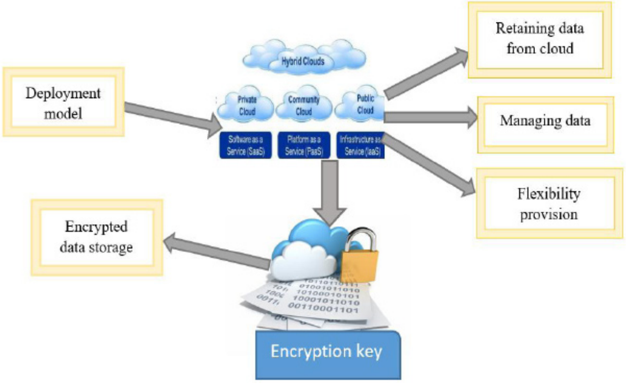

Figure 1. Providing encryption in deployment model.

The algorithm must give proper size, proper key length accurate encryption in all it should offer efficient security. Any two crypto algorithms are randomly selected for further execution and those chosen algorithms pinned algorithms selected randomly which denotes arbitrary access control.

3.1 Arbitrary Algorithm Selection Executing Flag Set

Arbitrary access control is an accessing technique that ensures what algorithm to choose? How can it be chosen? Arbitrary access control selects algorithm randomly and matches algorithm accordingly for further execution. Any two algorithms selected for encryption purpose the selection is made by calculating the specifications of each algorithm which includes length, block size, security and speed arranged in a flag set. The operation takes place initiating the combination-check algorithms are selected the first algorithm used must be suitable for encrypting and harder for decrypting. The cipher text produced by encryption being a critical one to find or evaluate must be processed in the way difficult to trap/decipher the information stored in the cloud storage server. Only the authorized user or the owner of the data has permission to access the data from cloud. To decipher the text a user must have knowledge about the algorithmic encryption and the user should guess what algorithm is been evaluated in this particular data. Though algorithmic techniques are used for encryption security, drip may occur, intruders may tend to attack the data, to handle this several other security measures are criticized.

Table 1. Algorithmic measurements and its usage

Flag set	DES	Blowfish	RSA	AES
Size	64	64	128, 245	128, 192 or 256
Security	inadequate	secure	Secure	Secure
Key length	56	32-448	1024 to 4096 bit	128, 192 or 256
Speed	Very slow	Fast	Fast	Very fast

In cryptographic algorithm four effective algorithms assigned for encryption technique for each algorithm a flag set is arranged by initiating particular name indicating the algorithm (F1, F2, F3, F4). This technique is operated as random process any two flag is called randomly for encryption purpose. For instance, F1 and F4 flag set is selected then the algorithm indicated in F1 is RSA (asymmetric key) which performs first level encryption in RSA method that uses two prime module numbers for encrypting data providing a fast and secured encryption. F4 executing DESede (symmetrickey) chosen next effecting re-encryption performed after compressing data. Here encrypts data by expanding the random key 2(r+1) into word performing both encryption and decryption.

In a surrogate system two encryptions will be undertaken and while passing through cloud there also two encryptions passed. If Flag 2 and 3 are selected in surrogate system the basic encryption done by using AES (F2) mechanisms encrypting data adding round key by shifting rows, mixing columns and by replacing sub bytes accordingly. For F3 blowfish algorithm is operated performing re-encryption using blowfish methodologies that uses large key relying for encrypting the original data where S-boxes are used for placing sub key arrays formulated for encrypting data. Various Encryption and Decryption algorithms will be deployed as below codes implementation model.

Here we deploy the pseudocode for blowfish

```
PUBLIC BLOWFISH() {
 TRY {
  /**
  * CREATE A BLOWFISH KEY
  */
  KEYGENERATOR = KEYGENERATOR.
GETINSTANCE("BLOWFISH");
  SECRETKEY = KEYGENERATOR.
GENERATEKEY();
```

```
    /**
    *CREATEANINSTANCEOFCIPHERMENTIONING THE NAME OF ALGORITHM
    * - BLOWFISH
    */
    CIPHER = CIPHER.GETINSTANCE("BLOWFISH");
  } CATCH (NOSUCHPADDINGEXCEPTION EX) {
    SYSTEM.OUT.PRINTLN(EX);
  } CATCH (NOSUCHALGORITHMEXCEPTION EX) {
    SYSTEM.OUT.PRINTLN(EX);
  }
}
```

The DES Pseudocode deployment is as follows

```
PUBLIC STRING ENCRYPT(STRING UNENCRYPTEDSTRING) {
  STRING ENCRYPTEDSTRING = NULL;
  TRY {
    CIPHER.INIT(CIPHER.ENCRYPT_MODE, KEY);
    BYTE[] PLAINTEXT = UNENCRYPTEDSTRING.GETBYTES(UNICODE_FORMAT);
    BYTE[] ENCRYPTEDTEXT = CIPHER.DOFINAL(PLAINTEXT);
    BASE64ENCODER BASE64ENCODER = NEW BASE64ENCODER();
    ENCRYPTEDSTRING = BASE64ENCODER.ENCODE(ENCRYPTEDTEXT);
  } CATCH (EXCEPTION E) {
    // E.PRINTSTACKTRACE();
    SYSTEM.OUT.PRINTLN("DES"+E);
  }
  RETURN ENCRYPTEDSTRING;
}
/**
* METHOD TO DECRYPT AN ECRYPTED STRING
*/
PUBLIC STRING DECRYPT(STRING ENCRYPTEDSTRING) {
  STRING DECRYPTEDTEXT=NULL;
  TRY {
    CIPHER.INIT(CIPHER.DECRYPT_MODE, KEY);
    BASE64DECODER BASE64DECODER = NEW BASE64DECODER();
    BYTE[] ENCRYPTEDTEXT = BASE64DECODER.DECODEBUFFER(ENCRYPTEDSTRING);
    BYTE[] PLAINTEXT = CIPHER.DOFINAL(ENCRYPTEDTEXT);
    DECRYPTEDTEXT = BYTES2STRING(PLAINTEXT);
  } CATCH (EXCEPTION E) {
    E.PRINTSTACKTRACE();
  }
  RETURN DECRYPTEDTEXT;
}
```

The AES encryption and decryption pseudocode deployment is as follows

```
PUBLIC STATIC STRING ENCRYPT(STRING PLAINTEXT, SECRETKEY SECRETKEY)
    THROWS EXCEPTION {
  BYTE[] PLAINTEXTBYTE = PLAINTEXT.GETBYTES();
  CIPHER.INIT(CIPHER.ENCRYPT_MODE, SECRETKEY);
  BYTE[] ENCRYPTEDBYTE = CIPHER.DOFINAL(PLAINTEXTBYTE);
  BASE64.ENCODER ENCODER = BASE64.GETENCODER();
  STRING ENCRYPTEDTEXT = ENCODER.ENCODETOSTRING(ENCRYPTEDBYTE);
  RETURN ENCRYPTEDTEXT;
}
PUBLIC STATIC STRING DECRYPT(STRING ENCRYPTEDTEXT, SECRETKEY SECRETKEY)
    THROWS EXCEPTION {
  BASE64.DECODER DECODER = BASE64.GETDECODER();
  BYTE[] ENCRYPTEDTEXTBYTE = DECODER.DECODE(ENCRYPTEDTEXT);
  CIPHER.INIT(CIPHER.DECRYPT_MODE, SECRETKEY);
  BYTE[] DECRYPTEDBYTE = CIPHER.DOFINAL(ENCRYPTEDTEXTBYTE);
  STRING DECRYPTEDTEXT = NEW STRING(DECRYPTEDBYTE);
  RETURN DECRYPTEDTEXT;
}
```

The RSA algorithm implemented as follows

```
PUBLIC STRING RSAENC(STRING ENC) THROWS NOSUCHPADDINGEXCEPTION, INVALIDKEYEXCEPTION, ILLEGALBLOCKSIZEEXCEPTION, BADPADDINGEXCEPTION {
  INITKEYPAIR();
  STRING DECRYPTEDSTRING = NULL;
```

```
 TRY {
  SYSTEM.OUT.PRINTLN(“\N RSA”);
  FINAL CIPHER CIPHER = CIPHER.GETINSTANCE(“RSA”);
  FINAL STRING PLAINTEXT = NEW STRING(ENC);
  // ENCRYPT USING THE PUBLIC KEY
  CIPHER.INIT(CIPHER.ENCRYPT_MODE, KEYPAIR.GETPUBLIC());
  BYTE[] ENCRYPTEDBYTES = CIPHER.DOFINAL(PLAINTEXT.GETBYTES());
  STRING CHIPERTEXT = NEW STRING(BASE64.GETENCODER().ENCODE(ENCRYPTEDBYTES));
  SYSTEM.OUT.PRINTLN(“ENCRYPTED (CHIPERTEXT) = “ + CHIPERTEXT);
  STRING CHIPERTEXT1 = NEW BLOWFISH().BLOW(CHIPERTEXT);
  // DECRYPT USING THE PRIVATE KEY
  CIPHER.INIT(CIPHER.DECRYPT_MODE, KEYPAIR.GETPRIVATE());
  BYTE[] CIPHERTEXTBYTES = BASE64.GETDECODER().DECODE(CHIPERTEXT1.GETBYTES());
  BYTE[] DECRYPTEDBYTES = CIPHER.DOFINAL(CIPHERTEXTBYTES);
  DECRYPTEDSTRING = NEW STRING(DECRYPTEDBYTES);
  SYSTEM.OUT.PRINTLN(“DECRYPTED (PLAINTEXT) = “ + DECRYPTEDSTRING);
}
```

Considering the arbitrary chosen flag as F3 and F4 ensuring the algorithms DES and DSA in cloud storage. DES performs encryption by comprising 3 keys (K1, K2, and K3) with 56 bits each, as base encryption with first key K1 is done then K2 decrypts the encrypted data then again K3 performs basic encryption finally triple encryption encrypts 64 block bits of data. For F3 DSA algorithm is carried out encryption is done in form of evaluating digital signatures using hashing technique for passing signatures. Likewise by chosing the alternative algorithm encrypting data is done and stored in cloud protecting the data performing arbitrary access control for selection and execution purpose.

4. Surrogate Twofold Encryption Technique (STET)

To offer extended security to cloud storage and to do the process of decryption more critical for the intruder a re-encryption technique used known as Surrogate Twofold Encryption Technique (STET). In surrogate Twofold Encryption Technique (STET) an alternate server have authority to send an encrypted text under a private key (P (a)) to a new one under alternative public key (P (b)). While the transformation is held the server does not know the plaintext. At first the data in the surrogate system encrypted with symmetric encryption key and that generated key will be again encrypted. Then the cloud storage stores the encrypted key and double encrypts it for secured storage. The cloud server use re-encryption algorithm to transfer encrypted results to a format assuming the recipient’s private key that may get decrypted. The recipient can upload the encrypted data from cloud and use data for decryption.

In every encrypted key set in any place parameters appended which inculcate the type of encryption used in that particular set. It acts as a pass code which can find only by that system or cloud storage. The surrogate key steps forward from information owner’s private key and recipient public key. Hence the owner may share different files with different client groups. Hence the other user might not able to read or copy data for a group which does not belong to the group. On other hand cloud act as common proxy that may display even personal data in public that causes major destruction to the user personal data. To avoid data corruption we use Surrogate Twofold Encryption Technique (STET) model to protect the public data and inter cloud data suited in cloud storage server. Surrogate Twofold Encryption Technique (STET) is a proxy encryption technique that performs double encryption.

4.1 Cloud Data Re-Encryption

When in the surrogate system data encrypted and the encrypted cipher text will pass through another encryption method and before that pass through another set of encryption. Here in the cloud it will be re-encrypted before storing in cloud. Again same arbitrary access control process can be followed for the random selection of data for re-encryption purposes any one of the cryptographic algorithm selected and the compressed cipher data is re-encrypted initializing the alternatives. This also inculcates parameters in the encrypted key thus to show the type of encryption selected. Here each data from the original data source shifted to surrogate system and there it encrypts using randomly selected cryptographic algorithm and the enciphered text sent to cloud storage.

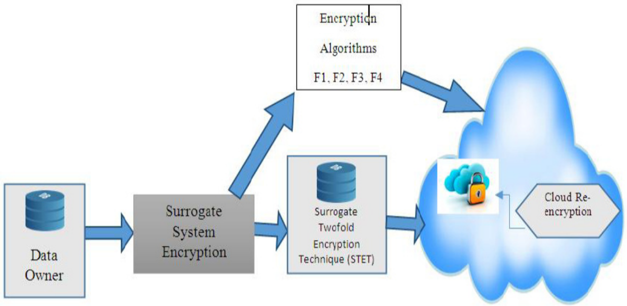

Figure 2. Encryption execution processed in inter cloud storage.

There again an encryption algorithm from the four is selected and again encrypted then stored.

It deciphered after the vice-versa rules. Finally the data that encrypted and again re-encrypted using the specific constraints retained in inter cloud with full-fledged security avoiding occurrence intrusion. Here only the cloud storage knows the encryption technique used and only the surrogate system have the information about encryption technique used there. Only authorized user can authenticate the ciphered text who knows the detail about the encryption technique otherwise the data stored cannot be retrieved by any other user, third-party or intruder even by the service provider.

5. Experiment and Result Analysis

Using several cryptographic algorithms the estimated secured storage of user data encrypted and compressed achieved by promoting layered flag set technique. Arbitrary choice executes and considering the specified bits and ciphered data is again encrypted successfully. Thus the cloud storage with cipher text helps the results to low bytes allotting extended space for storage. The processing of secured equation in cloud system which enhances encrypting process as major securing technique accomplishing data and re-encryption to store data may increase cloud computing ability to great extent. As we are encrypting it again and again infusing four different types of symmetric and asymmetric algorithms strong security provides for our STET model.

Comparing to existing system proposed results are comparatively efficient. In existing only normal encryption handles there occurs inefficiency in securing data and the encryption occupies more space lacking the provision of data from database storage. Whereas in proposed it enhances security both in inter cloud and exterior, efficiency, data protection. It provides secured data without any leakage and provides storage space. The main advantage in proposed is that it provides triple layer protection using surrogate system encryption and compression re-encryption technique. In Figure 3 the difference between existing and proposed will be easily plotted analysing uses of the both.

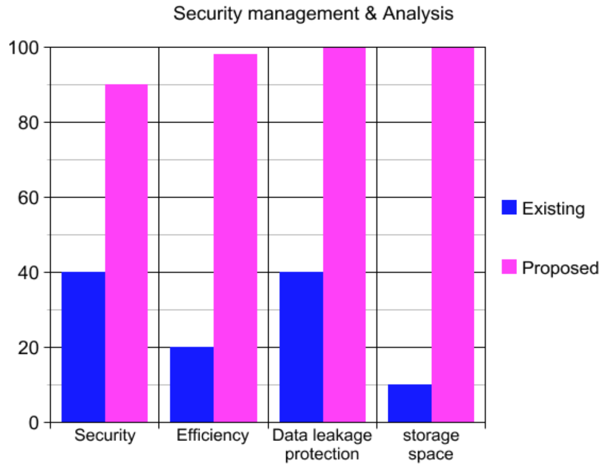

Figure 3. Differentiating and analysing Existing system and proposed system.

6. Conclusion

In cloud the encryption standards have increased security cloud storage. In existing techniques only base level encrypting methods formulation that too inside the cloud or from the data holder side. Whereas in proposed alternative solution used for back and back twofold secure user data encryption that encrypts data and again encrypt the ciphertext in two different places and store it safely in the inter cloud storage. Surrogate Twofold Encryption Technique (STET) adds efficiency to security and its different stage encryption obstructs intruder efficiently. When an intruder traps the data they need to decipher the data used in cloud and again re-decrypt the data from surrogate system which is harder and impossible. So the technique used in our proposed is helpful for security purpose, hence secured data from the cloud storage retrieved by the owner.

7. References

1. Sahai A., Waters B., “Fuzzy identity-based encryption”, *Eurocrypt*, 2005.

2. Goyal V., Pandey O., Sahai A., Waters B., "Attribute-based encryption for fine-grained access control of encrypted data", ACM Conference on Computer and Communications Security, 2006.
3. Bethencourt J., Sahai A., Waters B., "Ciphertext-policy attribute-based encryption", IEEE Symposium on Security and Privacy, 2007.
4. Waters B., "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization", *Public Key Cryptography*, 2011.
5. Sahai A., Seyalioglu H., Waters B.,"Dynamic credentials and ciphertext delegation for attribute-based encryption", *Crypto*, 2012.
6. Hohenberger S., Waters B., "Attribute-based encryption with fast decryption", *Public Key Cryptography*, 2013.
7. Tysowski P.K., Hasan M.A., "Hybrid attribute- and reencryption-based key management for secure and scalable mobile applications in clouds", *IEEE T. Cloud Computing*, p. 172–186, 2013.
8. Wired., Spam suspect uses google docs; fbi happy. 2014. Available: http://www.wired.com/2010/04/cloud-warrant/.
9. Wikiped-ia. Global surveillance disclosures. 2014. Available: http://en.wikipedia.org/wiki/Global surveillance disclosures (2013-present)
10. Snowden E., Available: http://en. wikipedia.org/wiki/ Edward Snowden
11. Lavabit. Available: http://en.wikipedia. org/wiki/Lavabit
12. Canetti R., Dwork C., Naor M., Ostrovsky R., "Deniable encryption", *Crypto*, 1997.
13. Lewko A.B., Okamoto T., Sahai A., Takashima K., Waters B., "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption", *Eurocrypt*, 2010.
14. Attrapadung N., Herranz J., Laguillaumie F., Libert B., Panafieu E De, Afols C.R., "Attribute-based encryption schemes with constant-size ciphertexts", *Theor Comput. Sci.*, vol. 422, 2012.
15. Murmuth M.D.,Freeman D.M., "Deniable encryption with negligible detection probability: An interactive construction", *Eurocrypt*, 2011.