ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, Vol 8(23), DOI: 10.17485/ijst/2015/v8i23/79210, September 2015 ISSN (Online) : 0974-5645

Symmetric Encryption Algorithm to Secure Outsourced Data in Public Cloud Storage

Ramalingam Sugumar[1*] and Sharmila Banu Sheik Imam[2]

[1]Christhuraj Institute of Computer Application, Panjappur, Trichy, India;
rsp_sugu74@yahoo.co.in
[2]Department of CCSIT, King Faisal University, Al-Ahsa, Saudi Arabia;
sharmilasyed@gmail.com

Abstract

Background/Objectives: Cloud storage is an increasingly popular class of services for archiving, backup and sharing of data. Data security concern has been one of the major hurdles preventing its widespread adoption of cloud. This paper proposes a Symmetric Encryption Algorithm (SEA) for data security in the cloud. **Methods/Statistical Analysis:** Traditionally, Cryptography techniques are used for data security. Encryption is a cryptography technique used for securing the data. The proposed algorithm in this paper is a symmetric encryption technique. The proposed algorithm executes the ASCII code of each value in the original data. Encryption is done before the data are sent to the cloud. **Findings:** Proposed SEA is implemented in JAVA and procedure of encryption and decryption of the SEA is evaluated in cloud storage. SEA reduces the time taken for encryption and decryption. Data are frequently uploaded to cloud; proposed SEA should not make latency in data uploading. The proposed algorithm is easily fit into cloud storage environment. SEA helps cloud users and cloud service providers to maintain the security of data in cloud storage. Cloud provider should not access data stored in cloud storage server. Hence, the SEA provides secure data storage environment in cloud. **Application/Improvements:** Security is more essential to data in the cloud. The proposed SEA provides better security to the data stored in the cloud storage. This technique is suitable to education, medical and agriculture community to securely store their data in cloud storage.

Keywords: Cloud Storage, Cryptography, Data Security, Outsourced Data, Symmetric Encryption Algorithm

1. Introduction

Cloud provides on-demand computing services on the Internet[1]. Cloud operates huge numbers of high configured servers. Servers are connected each other via networks[2]. Computing resources are merged as one huge resource and shared among users[3]. Cloud storage is an accretion of storage servers that provide a location independent storage service[4]. Users can store and retrieve data from the cloud storage from anywhere at any time[5]. Enterprises are outsourced their data storage to a cloud[6]. Cloud storage not only provides the storage service as a purely virtual file system but also contribute too many service-based applications[7]. The advantage of using cloud storage instead of the local storage devices is significant. Users can universally enjoy the cloud storage service without the heavy burden of hardware or software maintenance[8]. In additional to low maintenance cost and ubiquitous use, cloud storage systems guarantee the data availability for a long period of time. Not only users but also the service providers gain advantage from the cloud storage[9]. The service providers can deliver quality of service to users non-interactively in real-time in the cloud storage[10].

Apart from the advantages of cloud, it has many security related issues[11]. The top most challenge in cloud is data security[12]. How the users' data are secured in cloud storage? This is the big concern about cloud storage[13].

* Author for correspondence

There are more possibilities that the data are accessed by the other users of cloud storage or a staff from cloud storage provider accesses the data[14]. Data security must be addressed in the cloud storage. Cryptography is most known technique for secure the data by encryption[15]. It is necessary to propose an encryption technique which is suitable for cloud storage. Cryptography techniques are categorized into two that are symmetric encryption and asymmetric encryption techniques[16]. Symmetric encryption technique is more suitable to cloud storage, because it encrypts large volume data in minimum time duration[17]. This paper proposes a Symmetric Encryption Algorithm (SEA) for cloud storage. The proposed SEA provides maximum security to the data in cloud storage.

A security Service Algorithm (SSA) is proposed for data security called AROcrypt SSA[18]. The proposed AROcrypt SSA is a service from a Cloud Service Provider (CSP). This is a symmetric encryption technique. Four keys are used for encryption and decryption. The original data are formed in a square matrix. Finally, the ASCII code values are converted into character value to produce the ciphertext. The outsourced data are efficiently protected by this SSA. The hybrid encryption algorithm and digital signature scheme[19] is developed and it uses both symmetric key algorithm and asymmetric key algorithm in order to transfer and save the data in the network. The encryption process has the private key. Using the SHA1 algorithm, can achieve the integrity by producing the brief message. Users encrypt data and provide the privacy by using the AES algorithm and verify the users' identity by using RSA algorithm. At first, information is converted to Encrypt message by the application of AES algorithm and generated key for the cryptography of proposed model. Then, Encrypted Message (EM) is delivered to the part of signature generation. RSA algorithm is continuously produced EK2 and RSA public key by the use of generated AES. A digital signature is an electronic tool with authenticity which results in authenticity of an electronic record through cryptography with public key.

A security mechanism[20] is designed to maintain security of text files only. It uses DES and RSA algorithm to generate encryption when user uploaded the text files in Cloud Storage and inverse DES and RSA algorithm to generate decryption when user download file from Cloud Storage, for increasing security. A user can upload Text file in Personal Cloud Storage. When uploading file, DES and RSA Encoding schemes are used to encrypt data. In this system, implementation of the DES algorithm takes place to generate first level encryption, and then apply the RSA algorithm on the encrypted output of DES algorithm to generate second level encryption. Same process takes place for decryption using inverse DES and RSA algorithms. Means they are applied multilevel encryption and decryption to provide security for cloud storage data. An encryption technique[21] is developed to hide the sensitive data before they are forwarded to cloud. In addition, data users can reconstruct the requested data from cloud server using shared secret key. The file is divided into blocks and confidentiality is emphasized on every character level of a block. The binary equivalent of block character is stored in circular array and number of moves the circular array is rotated is decided by the Circular Array Shifter. Where every rotation divides the data by 2 and this will optimize the data to its least value and hence the privacy of data is ensured.

A method[22] is proposed for providing the inverse of Caesar cipher that supports more security for the data compared with the earliest Caesar cipher. It can also be used simply encode the message for preserving privacy. The key value range is from 0 to 256. The proposed method encrypts the value using addition of key into plaintext. Subtract 256 from encrypted value. Finally the value of the corresponding symbol is encrypted text. It is complicated to understand the cipher text compared with the other methods. The organization of the paper is as follows, section 2 describes about the problem definition and motivation, section 3 describes the methodology of the proposed SEA, section 4 details the experimental result of proposed SEA, section 5 is conclusion of the paper.

2. Problem Definition and Motivation

Cloud storage is a model of networked enterprise storage[23] where data are stored in virtualized pool of storage which is generally hosted by cloud providers. Hosting companies operate large data centres, and people who require their data to be hosted buy or lease storage capacity from them. The data centre operators, in the background, virtualized the resources according to the requirements of the users and expose them as storage pool, which the users can themselves use to store files or data objects. Physically, the resource may span across multiple servers[24]. Cloud provides many benefits to users at the same time it has big concern about security of data. More numbers of research are carried out for securing the cloud environment. But,

still cloud security is top most challenge in the cloud environment. Followings are list of security problem derived from the literature.

- Outsourced data are not controlled or monitored by the users.
- Users are not able know the locations where are the data stored.
- Key management is very crucial to CSPs, so they maintain a single key for all users' data
- Some CSPs are not encrypted the data. Data may be stored in as original form.
- In most of the security framework, users have more work burden to maintain the components of the framework, encryption process and key generation.
- CSPs are the authorized people to access the data without users' knowledge.

The study of existing work helps to motivate to propose SEA for securing data in cloud environment.

3. Methodology

SEA encrypts the data before they are sent to the cloud storage. SEA is cloud service and keys generation is also a cloud service. SEA uses two keys for both encryption and decryption. Keys used for encryption are not communicated to CSPs who provides storage. Keys are confidentiality stored in the users' side for decrypting the data. CSPs have only the encrypted data. The proposed encryption algorithm is provided as a security service from a CSP. It is a symmetric encryption algorithm. It uses same keys for encryption and decryption. Procedures of proposed SEA are as follows:

- Cloud users submit the plaintext (PT) for encryption.
- Count the number of values in the PT.
- Convert each character in PT into corresponding ASCII code values.
- Divide the PT into two blocks by fetching alternate text in the PT .
- PT1=Text from odd position
- PT2= Text from even position
- Form a square Matrix MAT[R][C] for total number of values in PT.
- Fill the PT1 and PT2 into the matrix one by one from left to right.
- Fetch the data from odd indexed row from MAT[R] C[] to CT1
- Fetch the data from even indexed row from MAT[R] [C] to CT2
- Apply K1 and K2 keys on the CT1 and CT2 respectively.
- Convert the ASCII values into character data to produce the CT.

Users' data are in Plaintext (PT), it is to be submitted for encryption. Initially, SEA counts the number of characters in the PT and divides the PT into PT1 and PT2. PT1 and PT2 are converted into ASCII code values. A square matrix MAT[R][C] is formed for total numbers of character in PT. From MAT[R][C], CT1 and CT2 are derived. The keys K1 and K2 are applied on the CT1 and CT2 respectively. Finally, convert the CT1 and CT2 into ASCII code to produce the Cipher Text (CT).

Pseudo Code of SEA Algorithm:

- Start
- PT← Plaintext
- N← Total number character in PT //Divide the PT in PT1 and PT2 by fetching alternate character
- for i← 1 to N
  PT1←ascii(i)
  next i
- end for
- for i ← 1 to N
  PT1←charAt(i)
  i=i+1
  PT2←charAt(i)
  next i
- end for
- Based on the value of N, Form a square matrix MAT [R][C], $R_X C>N$,
  // $R_X C$-order of matrix, R=C
- Fill the Matrix MAT[R]{C] by PT1 and PT2 one by one from left to right
- Read the values from matrix by rows
  CT1← MAT[i][j] i←0 2...R
  CT2← MAT[i][j]i←1 3...R
- Apply the K1 and K2 on CT1 and CT2 respectively
  CT1← K1
  CT2←K2
- Convert the CT1 and CT2 into ASCII character code
  //Merge CT1 and CT2
- CT←merge(CT1,CT2)
  // CT=CipherText
- End

4. Experimental Results

The proposed SEA is implemented in JAVA. The SEA efficiently produces cipher for given plaintext. The SEA

and Keys are received as a service from the cloud. Consider a sample plaintext for experiment the proposed SEA.

Plaintext is "cloud provides on-demand computing".

PT = cloud provides on-demand computing

Step 1 → Count the number of values in the PT with space.

N = 34

Step 2 → Converts characters in PT into corresponding ASCII code values.

PT of ASCII code=

99	*108*	*111*	*117*	*100*	*32*	*112*
114	*111*	*117*	*105*	*100*	*101*	*49*
32	*111*	*110*	*45*	*100*	*101*	*109*
97	*110*	*100*	*32*	*99*	*111*	*109*
112	*117*	*116*	*105*	*110*	*103*	

Step 3 → Divide the PT into two blocks by fetching alternate text in the PT.

PT1=	99	111	100	112	111	105
	101	32	110	100	109	110
	32	111	112	116	110	
PT2=	108	117	32	114	117	100
	49	111	45	101	97	100
	99	109	117	105	103	

Step 4 → Form a square Matrix MAT[][] for total number of values in PT. N = 34,

MAT[R][C], where R = 6,C = 6, N<=RXC

Step 5 → Fill the PT1 and PT2 into the matrix one by one from left to right.

99	111	100	112	111	105
101	32	110	100	109	110
32	111	112	116	110	108
117	32	114	117	100	49
111	45	101	97	100	99
109	117	105	103	97	98

Step 6 → Fetch the data from even indexed row from MAT[][] to CT1

CT1 =	99	111	100	112	111	105
	32	111	112	116	110	108
	111	45	101	97	100	99

Step 7 → Fetch the data from odd indexed row from MAT[][] to CT2

CT2 =	101	32	110	100	109	110
	117	32	114	117	100	49
	109	117	105	103	97	98

Step 8 → Apply K_1 and K_2 keys on the CT1 and CT2 respectively.

Keys K1 = 5, K2 = 9

CT1 =	104	116	105	117	116	110
	37	116	117	121	115	112
	116	51	106	102	105	104
CT2 =	110	41	119	109	118	119
	126	41	123	126	109	123
	118	126	114	112	106	107

Step 9 → Convert the ASCII values into character data to produce the CT.

Cipher text:

htiutn%tuyspt3jfihn)wmvw~){~m{v~rpjk

4.1 Decryption Procedure

Decryption is the reverse process of encryption. When users apply decryption for the above ciphertext the same keys K1 and K2 will produce the plaintext.

4.1.1 Cipher Text

htiutn%tuyspt3jfihn)wmvw~){~m{v~rpjk

Apply the same keys K1 and K2 with reverse procedure of encryption will produce the plaintext as below,

4.1.2 Plaintext

Cloud provides on-demand computing

The proposed SEA efficiently executes the users' data to improve the security. Data are encrypted before they are uploaded to the cloud storage. Keys are securely kept by users for encryption and decryption. The keys used for SEA are not known to CSP. Even through, they have the rights to access the data but they can't get the original data which are stored in cloud storage. Process SEA encryption or decryption is not produces any latency in uploading the data to cloud storage. This SEA encrypts whole data to be stored in the cloud storage; instead, in future this algorithm is enhanced by encrypting only the sensitive data. Encrypting sensitive data still more reduces time taken for encryption and decryption and also save computation overheads. This SEA definitely helps users as well as CSP to trust and improve usage of cloud computing environment.

5. Conclusion

Cloud computing is more reliable for storage. It has more issue related to security. Security is the main concern in the cloud data storage. This paper is proposed a symmetric encryption algorithm for securing the data stored in the cloud storage. SEA converts original text into ASCII code to process the data during process of the encryption. Two symmetric keys are used for encryption and decryption. These keys are maintained in the cloud users' side. Authorized people from a CSP or a user of the cloud should not access the data in the cloud. The SEA minimizes time for encryption and decryption. It also produces maximum security to the data stored in the cloud. Hence, the proposed SEA helps CSPs and cloud users to maintain the security in cloud environment.

6. References

1. Arockiam L, Monikandan S. AROMO security framework to enhance security of data in public cloud. Int J Appl Eng Res. 2015; 10(9):6740–6.
2. Branco EC, de Castro Machado J, da Silva Monteiro Filho JM. A strategy to preserve data confidentiality in cloud storage services. 2014. p. 257–65.
3. Mell P, Grance T. The NIST definition of cloud computing. Gaithersburg, MD, United States: National Institute of Standards and Technology. 2014. Technical Report-800-145.
4. Rajasudhan S, Nallusamy R. A study on cryptographic methods in cloud storage. International Journal of Communication and Computer Technologies. 2014; 2(2):1–5.
5. Pitchay SA, Alhiagem WAA, Ridzuan F, Saudi MM. A proposed system concept on enhancing the encryption and decryption method for cloud computing. IEEE International Conference on Modelling and Simulation; 2015. p. 201–5.
6. Kamara S, Lauter K. Cryptographic cloud storage. Financial Cryptography and Data Security. Berlin Heidelberg: Springer; 2010. p. 136–49.
7. Lin HY. Data confidentiality and robustness in decentralized cloud storage systems. National Chiao Tung University. 2010.
8. Armbrust M, Fox A, Griffith R, et al. Above the clouds: A Berkeley View of cloud computing. Berkeley:EECS Department, University of California. 2009. p. 1–23.
9. Furht B. Cloud computing fundamentals. Handbook of cloud computing. Springer Science; 2010. p. 1–17.
10. Gong C, Liu J, Zhang Q, Chen H. The characteristics of cloud computing. International Conference on Parallel Processing Workshops Proceedings of IEEE. 2010. p. 275–9.
11. John H, Kaufman LM, Bruce P. Data security in the world of cloud computing. IEEE Journal of Security and Privacy. 2009; 7(4):61–4.
12. Rajathi A, Saravanan N. A survey on secure storage in cloud computing. Indian Journal of Science and Technology. 2013; 6(4):4396–401.
13. Onwubiko C. Security issues to cloud computing, cloud computing: Principles, systems and applications, computer communications and networks. London: Springer Verlag; 2010. p. 271–88.
14. Arockiam L, Monikandan S. Security framework to ensure the confidentiality of outsourced data in public cloud storage. International Journal of Current Engineering and Technology. 2014; 4(3):1265–70.
15. Arockiam L, Monikandan S. Data security and privacy in cloud storage using hybrid symmetric encryption algorithm. International Journal of Advanced Research in Computer and Communication Engineering. 2013; 2(8):3064–70.
16. William S. Cryptography and network security: Principles and practices. 5th ed. Prentice Hall; 2005. p. 6–56.
17. Mather T, Kumaraswamy S, Shahed L. Cloud security and privacy. USA: O'Reilly Media, Inc; 2009. p. 61–71.
18. Arockiam L, Monikandan S. AROcrypt: A confidentiality technique for securing enterprise's data in cloud. Int J Eng Tech. 2015; 7(1):245–53.
19. Shakeeba SK, Tuteja RR. Security in cloud computing using cryptographic algorithms. Int J Comput Sci Mobile Comput. 2015; 3(1):148–154.
20. Shiralizadeh A, Hatamlou A, Masdari M. Presenting a new data security solution in cloud computing. Journal of Scientific Research and Development. 2015; 2(2):30–6.
21. Prakash GL, Prateek M, Singh I. Data encryption and decryption algorithms using key rotations for data security in cloud system. International Conference on Signal Propagation and Computer Technology (ICPST); 2014. p. 624–9.
22. Padmapriya A, Subhasri P. Cloud computing: Reverse caesar cipher algorithm to increase data security. Int J Eng Trends Tech. 2013; 4(4):1067–71.
23. Kaur R, Kinger S. Analysis of security algorithms in cloud computing. International Journal of Application or Innovation in Engineering and Management. 2014; 3(3):171–6.
24. Chen D, Zhao H. Data security and privacy protection issues in cloud computing. IEEE Proceedings of International Conference on Computer Science and Electronics Engineering 2012; p. 647–51.