Chief Editor

Dr. A. Singaraj, M.A., M.Phil., Ph.D.

Editor

Mrs.M.Josephin Immaculate Ruba

EDITORIAL ADVISORS

1. Prof. Dr.Said I.Shalaby, MD,Ph.D.
   Professor & Vice President
   Tropical Medicine,
   Hepatology & Gastroenterology, NRC,
   Academy of Scientific Research and Technology,
   Cairo, Egypt.
2. Dr. Mussie T. Tessema,
   Associate Professor,
   Department of Business Administration,
   Winona State University, MN,
   United States of America,
3. Dr. Mengsteab Tesfayohannes,
   Associate Professor,
   Department of Management,
   Sigmund Weis School of Business,
   Susquehanna University,
   Selinsgrove, PENN,
   United States of America,
4. Dr. Ahmed Sebihi
   Associate Professor
   Islamic Culture and Social Sciences (ICSS),
   Department of General Education (DGE),
   Gulf Medical University (GMU),
   UAE.
5. Dr. Anne Maduka,
   Assistant Professor,
   Department of Economics,
   Anambra State University,
   Igbariam Campus,
   Nigeria.
6. Dr. D.K. Awasthi, M.SC., Ph.D.
   Associate Professor
   Department of Chemistry,
   Sri J.N.P.G. College,
   Charbagh, Lucknow,
   Uttar Pradesh. India
7. Dr. Tirtharaj Bhoi, M.A, Ph.D,
   Assistant Professor,
   School of Social Science,
   University of Jammu,
   Jammu, Jammu & Kashmir, India.
8. Dr. Pradeep Kumar Choudhury,
   Assistant Professor,
   Institute for Studies in Industrial Development,
   An ICSSR Research Institute,
   New Delhi- 110070, India.
9. Dr. Gyanendra Awasthi, M.Sc., Ph.D., NET
   Associate Professor & HOD
   Department of Biochemistry,
   Dolphin (PG) Institute of Biomedical & Natural Sciences,
   Dehradun, Uttarakhand, India.
10. Dr. C. Satapathy,
    Director,
    Amity Humanity Foundation,
    Amity Business School, Bhubaneswar,
    Orissa, India.

ISSN (Online): 2455-7838
SJIF Impact Factor : 6.093

EPRA International Journal of

Research & Development

(IJRD)

Monthly Peer Reviewed & Indexed International Online Journal

Volume: 4, Issue:2, February 2019

Published By
EPRA Publishing

CC License

BY NC ND

SJIF Impact Factor: 6.093 Volume: 4 | Issue: 2 | February | 2019 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Peer Reviewed Journal

AN APPROACH TO SECURE CLOUD COMPUTING USING CRYPTOGRAPHY BASED ALGORITHMS

Rajalakshmi S
Student, BCA, Department of Computer Science, M.O.P. Vaishnav College for Women, Chennai.

Deepa L
Student, BCA, Department of Computer Science,M.O.P. Vaishnav College for Women, Chennai.

Yuvashree B
Student, BCA, Department of Computer Science, M.O.P. Vaishnav College for Women, Chennai.

Nirmala G
Student, BCA, Department of Computer Science,M.O.P. Vaishnav College for Women, Chennai.

ABSTRACT
A broad range of services is provided by cloud computing which is delivered by a third-party service provider owning the cloud infrastructure. People tend to save data in cloud as it provides easy data access from anywhere and at anytime. This gives more flexibility to users and faster access to data. Because of all these advantages of cloud, each and every firm is moving its data to the cloud. While this pose as an advantage, the cloud service provider must also ensure for security to the data accumulated in the cloud. Data should be safeguarded against illegal access, alteration or DoS etc. This paper suggests a cryptographic algorithm based on symmetric key to encrypt the files before uploading in the cloud and to decrypt the files on downloading, in order to prevent intruders from accessing other cloud user's data and also provide end-to-end security when migrating within the data centers of the providers.

KEYWORDS: *Cloud Computing, Cloud Storage, Standardization, Cryptography, Protection, Network, Security, Encryptio, Decryption, Privacy, Data migration*

I. INTRODUCTION

Cloud computing is the deployment of evaluating utilities via the International Network (Internet). Services offered by cloud enable people as well as organizations for utilizing both hardware along with software which are handled by third party service providers located at distant centres. Storing files, social networking sites, enterprise applications are all examples of cloud services. Cloud computing technology allows access to information and computer resources from any place on the earth where a network connection is available. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications[1]. Cloud computing provides for provisioning on-demand access to a network in order to connect to a common storehouse of resources to be elastically supplied and delivered with minimal effort.

Cryptography helps in achieving data confidentiality in the cloud. Cryptography, is contemplated as a blend of three algorithms. They are (1) Symmetric-key algorithms (2) Asymmetric-key algorithms and (3) Hashing [1]. Data cryptography, can be defined as the scrabbling of the data content, in order to make it unreadable, meaningless or invisible during storage or transmission. This methodology is also coined as encryption. The foremost aim of

cryptography is to secure the data from attackers. The task of retrieving original data from the encrypted one is called decryption, which results in restoration of original data. Data encryption at cloud storage can make use of both symmetric key algorithms as well as asymmetric key algorithms. However, performance of asymmetric key algorithm works slower while accessing cloud storage which holds a huge set of databases, when compared to symmetric key algorithms. The problems that are encountered mostly in cloud computing are cyber attacks, government intrusion, lack of standardisation and outages [2][3]. Therefore, an efficient way to overcome most of the problems is to encrypt files before storing it in web based cloud storage service.

II. LITERATURE REVIEW

Data authentication, data integrity, querying and outsourcing the encrypted data were targeted by Brian Hay et. al [4]. At operational trust modes, resource sharing, new attack strategies arises risk because in operational trust modes, data centre used the communication channels which were encrypted and it performs computation on encrypted data which forms the homomorphic encryption [5]. Virtual Machine Introspection(VMI), a new attack strategy can be used at virtualization layer to process and alter the data.

"To provide on demand computing resources and services, distributed architecture of cloud computing centralizes server resources on a scalabe platform", was stated by Kevin Curran et.al [3].The cloud computing has begin to be a variable platform which allows the companies to build their foundations on it. Companies which are utilizing the benefits of cloud based system by using cloud storage to store their data will have to face with a duty of revaluating their current security tactics.

"Challenges that slow down the services in the cloud are privacy, security and lack of standards" was mentioned by Randeep Kaur et.al [6] as some of the significant challenges related to cloud.

Rashmi Nigoti et.al [7] mentions some security and privacy-related issues that seem to have long-term effect on cloud storage.

In order to choose where to run instances of workflow and to store data while providing audit data to verify policy compliance and avoid prosecution through an automated dynamic and policy-driven approach was proposed by John C. Mace et.al [8]. An automated tool was suggested by them to help form more financially beneficial and justifiable security policy decisions for policy-makers, they suggested an automated tool to quantify information security policy implications.

Summary on Literature Review:

The above review holds the explanations of cloud computing as stated by US National Institute of Standards and Technology[13]. The security challenges raised in cloud computing have been discussed by a number of researchers. It is undoubtedly clear that the security problems have played the most critical role in preventing the acquiring cloud computing. Different encryption techniques are analyzed by researchers for securing data storage in cloud. As examined in the review, many security procedures are registered to cloud storage at present. Also, many fields require further improvements where effective algorithms need to be produced to raise the security level in cloud storage.

III. EXISITING APPROACHES

Google Drive provides a service to store personal files on the cloud. Google Drive encrypts data using Transport Layer Security standard even before it leaves the device and then it is uploaded to the drive. Once the data reach Google it is unencrypted and then re encrypted using 256-bit Advanced Encryption Standard (AES). The AES encryption keys which are used for data encryption are further encrypted with rotating master keys to add an extra second layer of security, thus making the data more secure[9][10]. During data retrieval from Google Drive, the process is reversed.

Amazon S3 stores objects redundantly across multiple data centres. This redundancy helps is repairing data if there is a data corruption issue. Also, Amazon S3 also uses versioning techniques to preserve each and every version of all the objects in Amazon S3 bucket. Versioning allows us to recover data easily from application failures and unintended user actions[11]. The encryption used in the server side of Amazon is almost identical to that of Google (256-bit AES)[12]. Though most of the providers sustain high encryption standards, encryption during data migration still remains an issue.

Currently, security is the number one cloud challenge and is of most important concern.

IV. PROPOSED METHODOLOGY

In symmetric key cryptographic encryption, both the sending party and receiving party agree to own the same key and keep it secret. This method of encryption provides confidentiality when the sender and receiver communicate with each other using the keys. Before the message is transmitted from sender to receiver, the message is encrypted using the key in order to obtain a cipher text. This cipher text is then transferred over the network to the receiver who then performs decryption using the key that he possess. The cipher text is then converted to the real message on successful decryption. In symmetric key cryptography, since the key for encrypting and decrypting the message must be familiar between sender and receiver, giving out the key is a laborious task.

We have proposed an algorithm for symmetric key to encrypt the data at client side and then it gets uploaded to a web based cloud storage service. The data downloaded from the cloud storage is then sent for decryption using the encryption keys. The primary aim of this algorithm is to secure the data during transmission, although Secure Socket Layer is used to ensure data privacy during data transition between a web browser and a server through an encrypted link but encrypting the data before it is sent provides an extra layer of security. Many cloud service

providers(CSP) do not perform encryption when migrating data between their data centres which might open on to loss of data, privacy risks, intrusions into the system and so on. Also, many CSPs do not account for end-to-end encryption. Thereby, performing data encryption at the client side even before the file is uploaded on to the cloud storage can prove to be helpful in order to overcome such threats.

Encryption algorithm

1. Generate ASCII value for every character in a file
2. Convert the ASCII values into respective binary values for every character in the file
3. Determine whether the produced binary value has 8 bits
4. If it doesn't have 8 bits, then add preceding 0's in order to make it a 8-bit binary value.
5. Generate a reverse of the corresponding 8-bit binary value
6. Take out the first 4 bits from the reversed 8-bit binary value
7. Reverse the first 4 bits
8. In the same way, extract the final 4 bits and reverse them
9. Append the 4 bit binary values obtained in the steps 7 and 8 to form a 8-bit binary value, which is the cipher text
10. This cipher text(binary value) is then changed to its coresponding ASCII value to form the encrypted file
11. The key is generated by adding 10 to the ASCII value in step 10, and the generated value is written to a separate encryption key file

Decryption Algorithm

1. Extract each character from the encrypted file and generate ASCII value of each and every character
2. Subtract 10 from each character's ASCII value in the encryption key file
3. Check if the values obtained in steps 1 and 2 are identical
4. If they are different, then do not perform decryption
5. If they are identical, perform decryption by reversing the encryption algorithm, i.e., by converting encrypted character to corresponding ASCII value and then from converting ASCII value to a 8-bit binary value, breaking the binary value to 4 bits, reversing them individually and appending them and the reversing the appended binary value.
6. The decrypted message is written to a separate decryption file which should be same with the substance of the original file.

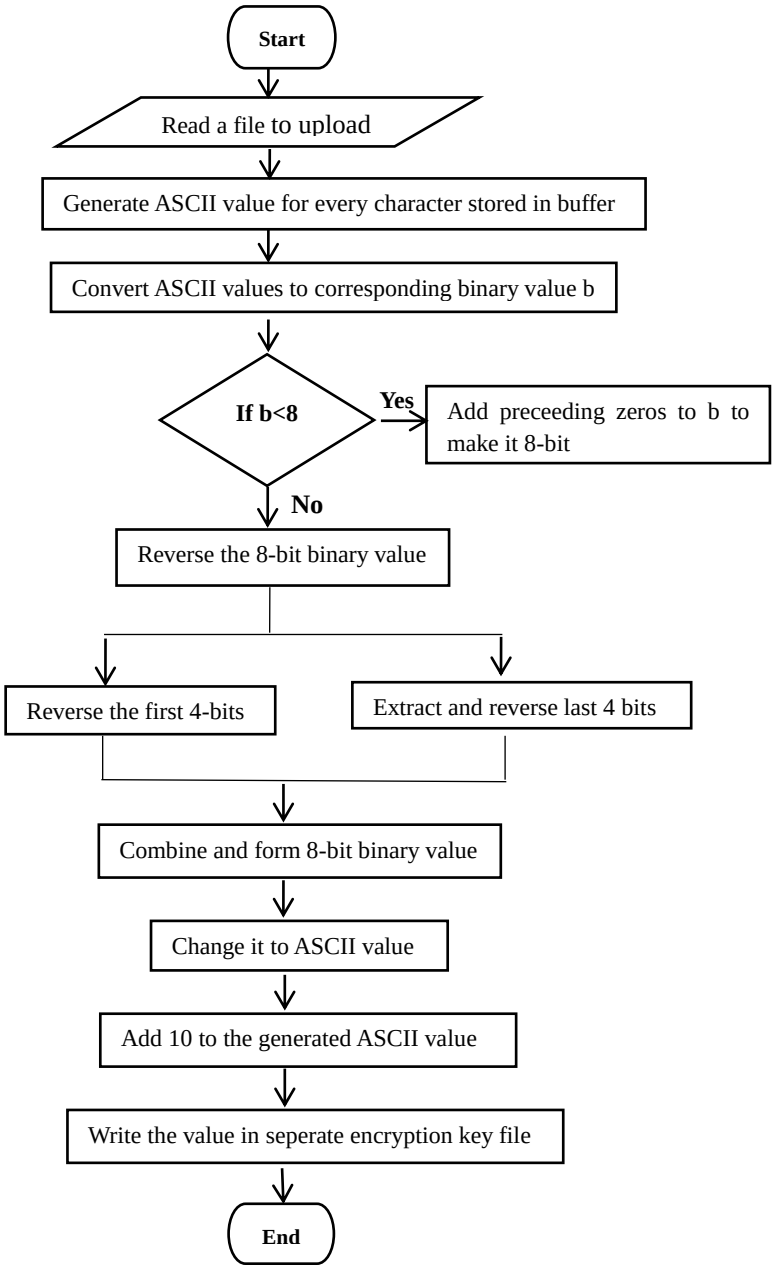

Fig. 1 Flowchart for Encryption Algorithm

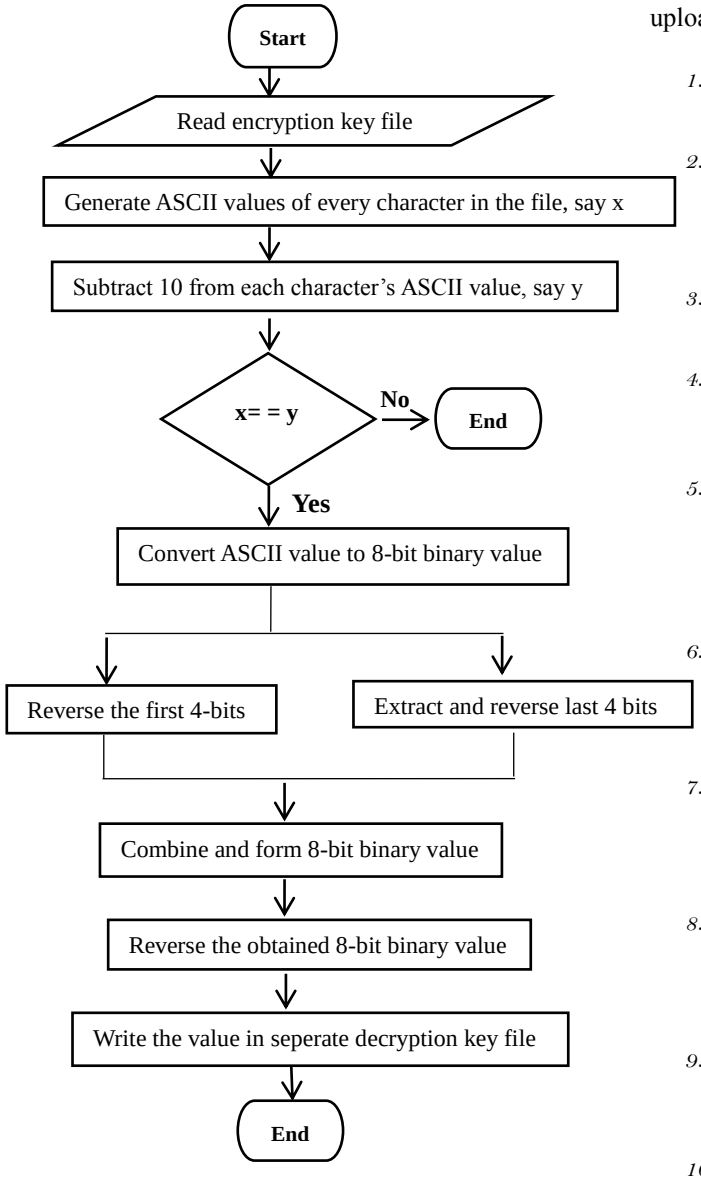

Fig. 2 Flowchart for Decryption Algorithm

V. Future work and Conclusion

In this paper we have suggested an algorithm for symmetric key to encrypt the data at client side and then it gets uploaded to a web based cloud storage service. The main aim of this algorithm is to provide an additional security layer (though SSL exists already), thereby minimising data theft during data transition,reducing data intrusion and spying during data migration between the data centres of the cloud service provider. This paper also focuses on solving the problem of lack of standardisation ,where end-to-end encryption is guaranteed by the service providers. This algorithm has been tested for text files especially, for which the encryption and decryption worked as expected. But, it could be further enhanced for encrypting other file formats or even audio and video files and even larger files could be encrypted at client side before uploading to the cloud.

VI. REFERENCES

1. *Shakeeba S. Khan, R.R. Tuteja, Security in Cloud Computing using Cryptographic Algorithms in IJIRCCE, Vol. 3, Issue 1, pp. 148-154, January 2015*
2. *Zhidong Shen, Li Li , Fei Yan, Xiaoping Wu , "Cloud Computing System Based on Trusted Computing Platform", International Conference on Intelligent Computation Technology and Automation, Volume 1, pp.942-945, 2010.*
3. *Kevin Curran, Sean Carlin and Mervyn Adams, "Security issues in cloud computing", Elixir Network Engg.38 (2011), pp.4069-4072, August 2011.*
4. *Brian Hay, Kara Nance, Matt Bishop, "Storm Clouds Rising: Security Challenges for IaaS Cloud Computing" Proceedings of the 44th Hawaii International Conference on System Sciences, pp.1-7, 2011.*
5. *Maha TEBAA, Saïd EL HAJJI, Abdellatif EL GHAZI, "Homomorphic Encryption Applied to the Cloud Computing Security", World Congress on Engineering, Volume I, ISBN: 978-988-19251-3-8; ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online) , 2012.*
6. *Randeep Kaur, Supriya Kinger, "Analysis of Security Algorithms in Cloud Computing" International Journal of Application or Innovation in Engineering & Management (ISSN 2319 - 4847),Volume 3 Issue 3, pp.171-176, March 2014.*
7. *Rashmi Nigoti, Manoj Jhuria and Dr.Shailendra Singh, "A Survey of Cryptographic Algorithms for Cloud Computing" International Journal of Emerging Technologies in Computational and Applied Sciences,Vol. 4, pp.141-146, March-May 2013.*
8. *Priyanka Arora, Arun Singh, Himanshu Tyagi, "Evaluation and Comparison of Security Issues on Cloud Computing Environment", World of Computer Science and Information Technology Journal, pp.179-183, 2012.*
9. *Encryption At Rest In Google Cloud Platform, an article available at https://cloud.google.com/security/encryption-at-rest/default-encryption/, April 2017.*
10. *Managing Data Encryption, an article at https://cloud.google.com/storage/docs/encryption#rotating-keys , January 2017.*
11. *Protecting Data Using Encryption, an article at http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html*
12. *Protecting Data Using Server-Side Encryption with Amazon S3-Managed Encryption Keys , an article at http://docs.aws.amazon.com/AmazonS3 /latest/dev/UsingServerSideEncryption.html*
13. *Pearson S., Benameur, A., Privacy, "Security and Trust Issues Arises from Cloud Computing", Cloud Computing Technology and Science (CloudCom), IEEE Second International Conference, pp.693-702, 2010*
14. *AL.Jeeva, Dr.V.Palanisamy And K.Kanagaram "Comparative Analysis Of Performance Efficiency And Security Measures Of Some Encryption Algorithms" International Journal Of Engineering Research And Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue 3, pp.3033-3037, May-Jun 2012.*
15. *Dr. Chander Kant and Yogesh Sharma, "Enhanced Security Architecture for Cloud Data Security" International Journal of Advanced Research in*

Computer Science and Software Engineering, Volume 3 Issue 5, pp.571-575, May 2013.

16. *Puneet Jai Kaur, Sakshi Kaushal, "Security Concerns in Cloud Computing", Communication in Computer and Information Science Volume 169, pp.103-112, 2011.*
17. *Rachna Arora, Anshu Parashar, "Secure User Data in Cloud Computing Using Encryption Algorithms", International Journal of Engineering Research and Applications (IJERA), Vol. 3, pp.1922-1926, Jul-Aug 2013.*
18. *Mandeep Kaur and Manish Mahajan, "Implementing Various Encryption Algorithms To Enhance The Data Security Of Cloud In Cloud Computing" VSRD International Journal of Computer Science & Information Technology, Vol. 2, pp.831-835, October 2012.*
19. *Wayne Jansen ,Timothy Grance, "Guidelines on Security and Privacy in Public Cloud Computing", NIST Special Publication,NIST SP - 800-144 ,80 pp., 2011.*
20. *L. M. Kaufman, "Data security in the world of cloud computing,"IEEE Security & Privacy Magazine, vol. 7, pp. 61-64, July2009.*