iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** X **Month of publication:** October 2019

DOI: http://doi.org/10.22214/ijraset.2019.10028

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue X, Oct 2019- Available at www.ijraset.com

Dual Layer Data Security in Cloud Computing

Mr. Himanshu Taiwade[1], Mr. Devendra Raut[2], Mr. Zeeshan Sabir[3], Miss. Pragati Meshram[4], Miss. Janhavi Dixit[5]
[1]*Prof. Priyadarshini Institute Of Engineering And Technology, Nagpur*
[2, 3, 4, 5]*Priyadarshini Institute Of Engineering And Technology, Nagpur*

Abstract:** One of the major advantage of cloud computing is that data can be shared among various organizations. However, this advantage itself have a risk to data. In order to negate potential risk to the data, it is necessary to protect data. Encryption is a hugely important tool when it comes to protecting data. This paper propose a new era of cryptographic dual layer encryption to make the data store in cloud more secure and trustworthy. There are readily available many multiple encryption techniques that are available in present time but unable to provide sufficient security. This paper aim to suggest the new encryption technique named as dual encryption. It is based on popular encryption algorithm AES which is symmetric-key algorithm. We are going to propose an additional layer of rabbit algorithm around encrypted data which will help to provide more security against Brute-force and other type of attacks. Therefore, if an intruder detects a single key of cryptosystem even then it is not possible to decrypt the original message. This paper aims to suggest a perspective which is a double layer encryption method to ensure security in cloud. In this proposed double layers encryption schemes, the data will be extremely secured while protecting and sharing in cloud environment. This scheme not only makes full use of the great processing skill of cloud computing but also can efficiently ensure cloud data privacy and security.

I. INTRODUCTION

In the cloud, the data is transferred between the server and client. High speed is the significant of service, cryptography offers numerous option to not only secure the transfer of information from the cloud but also to house it within. Data encryption is a security procedure where information is encoded and can only be accessed or decoded by a user with the correct encryption key. Encrypted data, also called as cipher text it appears scrambled or unreadable to a person or entity who is accessing without permission. Data Encryption is used to protect from malicious parties from accessing sensitive data. An important line of defence in a Cyber security architecture, encryption makes using intercepted data as difficult as possible.

A. Symmetric Encryption

Symmetric encryption is an old and well known encryption procedure that uses a single key to encrypt (encode) and decrypt (decode) data. The secret key can be a word, a number, or a string of letters, and it's applied on a message. Sender and receiver know the key and they can code and decode any message that would use that specific key.

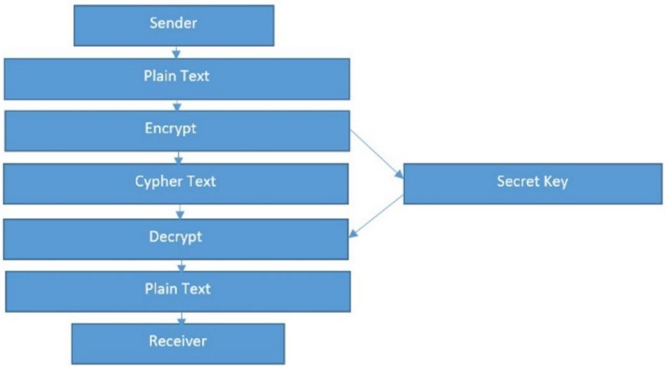


Fig.1: Fundamental cryptographic process

A simple example of an encryption algorithm would be changing all N to a 3, or all Z to a 1. The routine may perform several passes and changes, known as permutations, on the plaintext. Once it's encrypted, you will need a key to unlock it. There are lots of different symmetric key algorithms available. Each has its own strengths and weaknesses. Some of the more common examples are RC4, 3DES, DES, and RC5. Only symmetric encryption has the speed and computational efficiency to handle encryption of large volume of data.

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue X, Oct 2019- Available at www.ijraset.com

II. LITERATURE SURVEY

The approach shown here is a double layer security technique which uses both Cryptography and Steganography for the secret data communication. The sending message is encrypted first using standard S-DES encryption algorithm and then that message is embedded within an image. Unlike other method, this method does not send cryptographic key separately. It creates key from the pixels of edge portion and embeds sending data in the non-edged portion of the image [1].The use of the double layer encryption technique is going to give certification to the user for high security of data and information. Double Layer Encryption is a good approach for securing the data in the cloud. Here the system is upgraded to enhance the security of data in cloud [2].The method proposes here uses mixture of cryptography and image steganography. The cryptographic method used for encrypting the confidential message is based on content encryption algorithm and the techniques which are used for steganography are LSB and raster scan techniques [3].The paper shows multiple terminologies used for the technique and problem associated with the security. The paper has taxonomy for the published techniques, which focus on techniques of Cryptography and Steganography as well as Combined Cryptography and Steganography Techniques [4].The work in this paper shows two level of security on data. Public key cryptography is the first level approach and in final level the encrypted message is stored in a series of shuffled and identical image [5].Multi-layer encryption is the new approach of this paper which is oriented on the algorithm of Advanced Encryption Standard (AES) and Rivest, Shamir ,Adleman (RSA) which helps to provide security and privacy on cloud.[6]

III. DATA SECURITY IN CLOUD COMPUTING

In this paper, we will discuss different security techniques for data storage security and privacy protection in the cloud computing environment. This paper concern the techniques used in the cloud computing through data security aspects including data integrity, confidentiality, and availability, also the data privacy issues and technologies in the cloud are studied because data privacy is associate with data security. Studies on data privacy and security could help to enhance the user's trust by securing data in the cloud computing environment

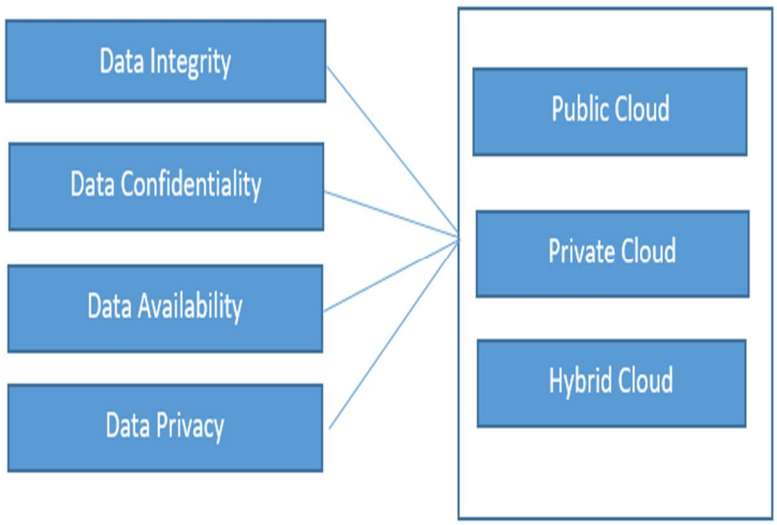


Fig2: Data privacy and security in cloud

A. Data Integrity

Data integrity is one of the most crucial elements in any information system. Generally, data integrity means secure data from unauthorized fabrication, deletion, to ensure that valuable data and services are not abused, misappropriated, or stolen.

Data integrity is simply achieved in a standalone system with a single database. Data integrity in the standalone system is maintained via database constraints and transactions, which is usually finished by a database management system (DBMS). Transactions should follow ACID properties to ensure data integrity. Most of the databases support ACID transactions and maintain the data integrity.

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue X, Oct 2019- Available at www.ijraset.com

B. Data Confidentiality

Data confidentiality is significant for users to store their confidential data in the cloud. Authentication and access control strategies are used to ensure data confidentiality. Increasing the cloud reliability and trustworthiness can be addressed the data confidentiality, authentication, and access control issues in cloud computing.

C. Data Availability

When accidents such as hard disk damage, IDC fire, and network failures occurred the extent that user's data can be used or recovered and how the users verify their data by techniques rather than depending on the credit guarantee by the cloud service provider alone.

D. Data Privacy

In the cloud, the privacy means when users visit the sensitive data, the cloud services can prevent potential adversary from inferring the user's behaviour by the user's visit model (not direct data leakage). Researchers have focused on Oblivious RAM (ORAM) technology. Oblivious-RAM technology visits most of the copies of data to hide the real visiting aims of users. ORAM has been widely used in software protection and has been used in protecting the privacy in the cloud as a promising technology

IV. PROPOSED METHOD

Basic motivation behind this paper is to suggest new encryption technology as combination of AES and rabbit algorithm. Earlier multiple combination is used of RSA, AES and HMAC. Unlike this combination we will use combination of rabbit algorithm and AES algorithm.

A. Rabbit Algorithm

Rabbit algorithm is also called as stream cipher algorithm that has been designed for high Performance in software implementations. Both key setup and encryption are very fast, making the algorithm particularly suite for all applications where large amounts of data have to be encrypted. Technically Rabbit consists of a pseudo-random bit-stream generator that takes a 128-bit key and a 64-bit initialization vector (IV) as input and generates a stream of 128-bit blocks. Encryption in performed by combining this output with the message, using the exclusive-OR operation. Decryption is performed in exactly the same way as encryption.

B. AES Algorithm

When it comes to cyber security, AES is one of those acronyms that you see popping up everywhere. That's because it easy to implement and has become the word-wide acceptance of encryption and it is used to keep a significant amount of our communications safe.

The features of AES are as follows −

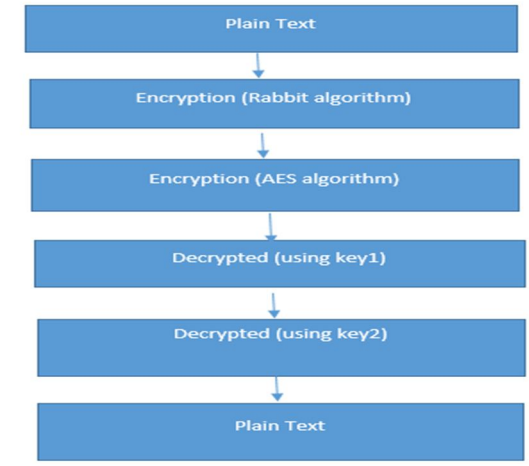
1) Symmetric key symmetric block cipher
2) 128-bit data, 128/192/256-bit keys
3) Stronger and faster

C. Operation of AES

AES is an iterative cipher which is better than feistel cipher. It is based on substitution–permutation network'. It contain a series of linked operations, some of which involve substitutions and others involve permutations. AES performs all its computations on bytes. That's why AES handle the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix.

Unlike DS, the number of rounds in AES is variable and depends on the length of the key. For 128-bit keys AES uses 10 rounds and 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Original AES key calculated a different 128-bit round key which is used in each rounds. When Sender will send the data in the form of plain text it generate a (private key) using rabbit algorithm and will convert into cipher text. This will be the first layer of encryption

©IJRASET: All Rights are Reserved



In second layer of encryption data will be convert cipher text using (public key) AES algorithm. Using these above two algorithm data will be more secure during transmission.

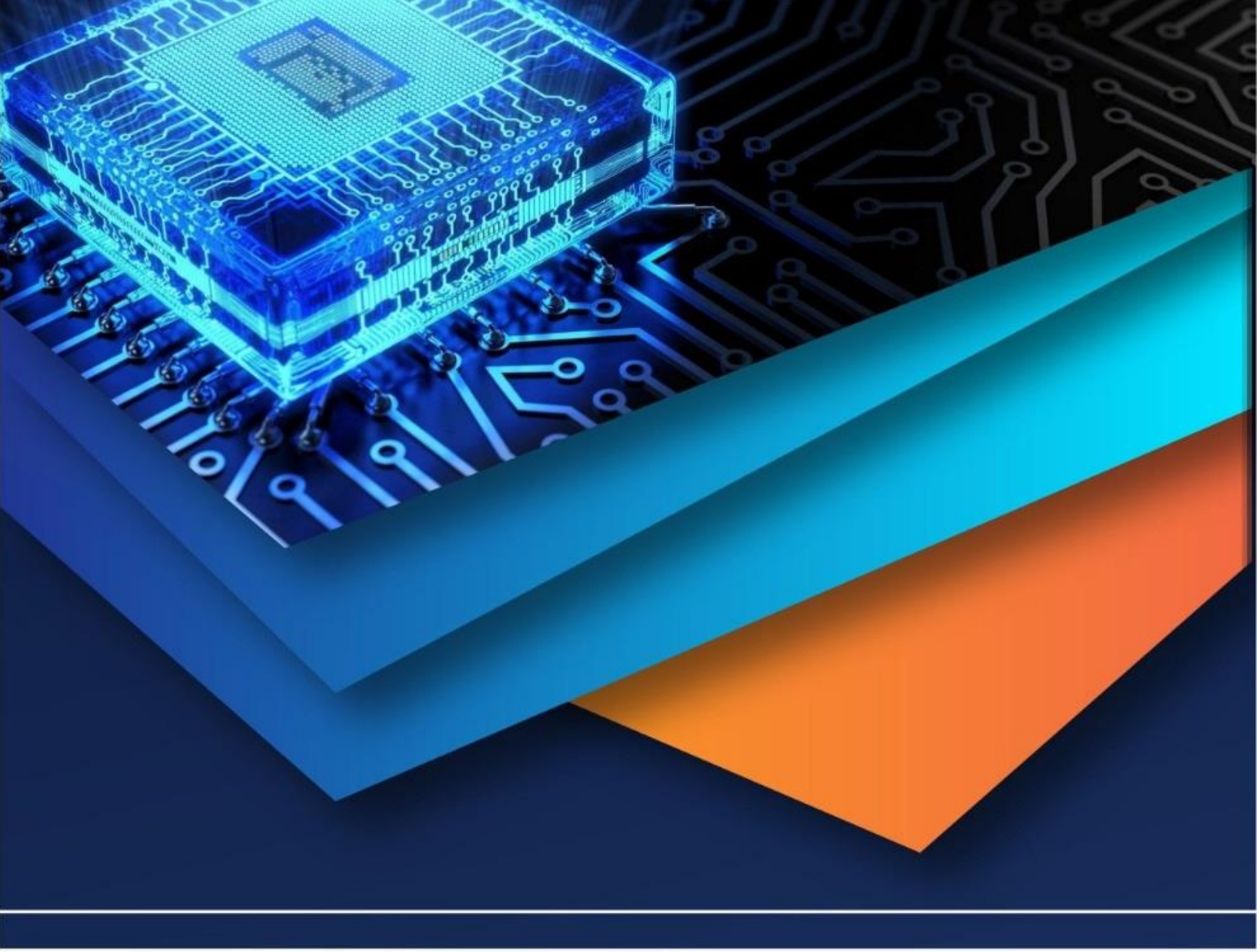
V. CONCLUSION

Increased use of cloud computing for storing data is certainly rise the trend of enhance the ways of storing data in the cloud. Data available in the cloud can be at risk if not protected in a justified manner. This paper discussed the risks and security threats to data in the cloud and given an overview of dual layer data encryption technique. One of the major concerns of this paper was data security and provide its threats solutions to its threats in cloud computing in this paper discuss the dual layer encryption technique which are efficient for encrypting the data in the cloud. The study provided an overview of Rabbit algorithm and AES algorithm which are used for encrypting the data in the cloud.

REFERENCES

[1] Biswajita Datta , Akash Roy , Romit Dutta , Samir Kumar Bandyopadhyay "Secure Communication through Double Layer Security with Efficient Key Transmission" 2018 International Conference on Information Technology (ICIT) (IEEE)
[2] Dr.D.Usha, M.Subbbulakshmi "Double Layer Encryption Algorithm Key Cryptography for Secure Data Sharing in Cloud" International Journal of Scientific & Engineering Research Volume 9, Issue 5, May-2018
[3] Shivani Chauhan , Jyotsna , Janmejai Kumar , Amit Doegar " Multiple layer Text security using Variable block size Cryptography and Image Steganography " 3 rd IEEE International Conference on "Computational Intelligence and Communication Technology" (IEEE-CICT 2017)
[4] Gahan A V , Geetha D Devanagavi[2] "A Empirical Study of Security Issues In Encryption Techniques" International Journal of Applied Engineering Research ISSN 0973-4562 Volume 14, Number 5 (2019)
[5] Ashok Kumar1, Santhosha1, A.Jagan1 " Two layer Security for data storage in cloud " 2015 1st International conference on futuristic trend in computational analysis and knowledge management (ABLAZE 2015)
[6] Naveen N, K.Thippeswamy " Security and Privacy Challenges Using Multi-Layer Encryption Approaches In Cloud Computing Environments" International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-8 June, 2019
[7] Afnan Ullah Khan , Manuel Oriol , Mariam Kiran, Ming Jiang, Karim Djemame " Security Risks and their Management in Cloud Computing " 2012 IEEE 4th International Conference on Cloud Computing Technology and Science
[8] F.Sabahi, "Virtualization-level security in cloud computing," 3rd Int. 2011 IEEE Conf. Commun. Softw. Networks, pp. 250–254, 2011
[9] D. Descher, M., Masser, P., Feilhauer. and Huemer, and A. Klein "Retaining data control to the client in infrastructure clouds," Int. Conf. Availability, Reliab. Secur. (pp. 9-16). IEEE., pp. pp. 9–16, 2009.
[10] Cloud Security Alliance, "The Notorious Nine. Cloud Computing Top Threats in 2013," Security, no. February, pp. 1–14, 2013.
[11] C. Modi, D. Patel, B. Borisaniya, M. Rajarajan, and A. Patel "A survey on security issues and solutions at different layers of Cloud computing,"J.Supercomputer., vol. 63, no. 2, pp. 561–592, 2013.
[12] L. Rodero-Merino, L. M. Vaquero, E. Caron, F. Desprez, and A. Muresan, "Building safe PaaS clouds: A survey on security in multitenant software platforms," Comput. Secur., vol. 31, no. 1, pp. 96–108, 2012.
[13] E. Mohamed, "Enhance data secure model for cloud computing," Informatics Syst. (INFOS), 2012 8th Int. Conf., pp. 12–17, 2012
[14] J. Srinivas, K. Reddy, and A. Qyser, "Cloud Computing Basics," Build. Infrastruct. Cloud Secure., vol. 1, no. September 2011, pp. 3–22, 2014.
[15] P. S. Wooley, "Identifying Cloud Computing Security Risks," Contin. Educ., vol. 1277, no. February, 2011.
[16] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," J. Netw. Comput. Appl., vol. 34, no. 1, pp. 1–11, Jan. 2011.

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)