Crypto Cloud Computing with Symmetric and Asymmetric Cryptography for Information Security and Storage

Veerapaneni Esther Jyothi, M. Prasanna Lakshmi, R.Rama Krishna

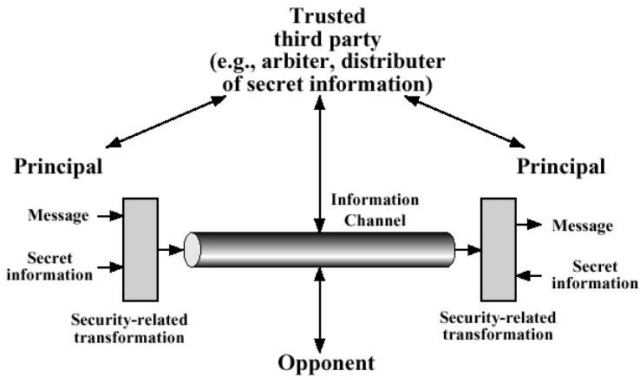
Abstract*: The resources and the services that the cloud provides are attractive for the users and are distinct from one cloud provider to another. The concerning aspect is how much securely our data stored in cloud is and how the data is protected against attacks. Various encryption algorithms or techniques of cryptography are used to protect data against attacks and also provides authenticity and confidentiality of data I an online and offline environment. Therefore in this paper various cryptographic aspects are covered, predominantly compares different algorithms with suggested solutions and results including cloud data protection. Authentication of data, confidentiality of data and data integrity aspects are the primary factors that have to be addressed in today's social networking and in the distributed environments. Cryptography and crypto cloud computing plays major role in secure transfer and storage of information.

***Keywords*: Algorithms, Authentication, Crypto cloud computing, Cryptography.**

I. INTRODUCTION

Securing information and secure transfer of information is been a significant area of research. Many researchers and academicians have been working on the cryptographic attacks and the successful ways of applying encryption and decryption processes. This paper discusses the model of network security, symmetric and asymmetric encryption algorithms in use along with their comparisons, the essentiality of securing information stored in the cloud. Plaintext is the original message generated by the sender. The process of converting plaintext into scrambled message is encryption and the scrambled message is cipher text. The process of converting cipher text into plaintext is decryption. Symmetric and asymmetric algorithms are used for encryption and decryption and they differ in number of keys, key sizes and the algorithms used. The model for network security shown below depicts the scenario of a typical transfer of information in a network.

Fig.1. Model for Network Security



The figure below classifies the cryptographic algorithms based on the key usage and further classifies the type of algorithms as symmetric and asymmetric.

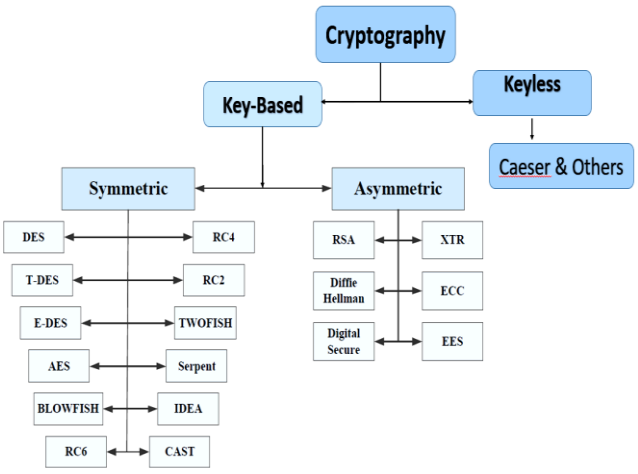


Fig.2. Classification of Cryptography

Section II explains Symmetric cryptography along with advantages and disadvantages. Section III portrays asymmetric cryptography along with its advantages and disadvantages. Section IV summarizes the importance of security of data stored in the cloud. Section V shows the results and comparative analysis. Section VI concludes the research work with the recommendations for the problems discussed in this paper.

Revised Manuscript Received on January 15, 2020
***** Correspondence Author
Veerapaneni Esther Jyothi*, Department of Computer Applications, V.R.Siddhartha Engineering College, Vijayawada, India,
M.Prasanna Lakshmi,, Department of Computer Applications, V.R.Siddhartha Engineering College, Vijayawada, India.
R.Rama Krishna, Department of Computer Applications, V.R.Siddhartha Engineering College, Vijayawada, India.

II. SYMMETRIC CRYPTOGRAPHY

Symmetric encryption converts the plain text into cipher text in which the shared key which is used for encryption and description place an important role. Symmetric encryption algorithms are widely used and are executed faster on computers than asymmetric algorithms [5]. The algorithms used for symmetric encryption are two types – Stream cipher and block cipher. Stream ciphering methods encrypt data as a stream of bits one at a time where as block ciphering methods encrypt data as a block of bits one at a time [6].

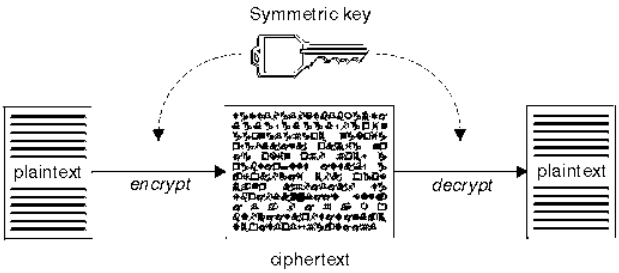


Fig.3. Symmetric Cryptography Process

The algorithms used for symmetric encryption are DES, T-DES, E-DES, AES, BLOWFISH, RC6, RC4, RC2, TWOFISH, SERPENT, IDEA, and CAST. Even though the authentication and confidentiality is better provides in symmetric encryption the key management or the key distribution is the concerning factor. The most popular of these DES and AES are explained in brief.

DES (Data Encryption Standard) is a symmetric block cipher algorithm developed by IBM which implements Feistel Cipher. DES has 16 rounds of encryption process with block size of 64-bit and a key length of 56 bits. The DES process is depicted in the following figure.

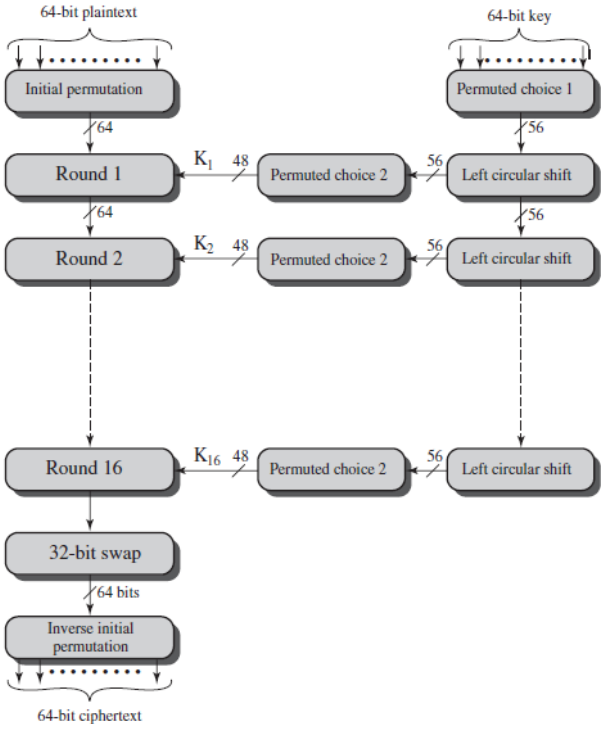


Fig.4. General structure of DES algorithm

AES symmetric encryption algorithm is a better alternative because of its improved speed and security than DES algorithm. AES encryption process is diepicted in the following figure.

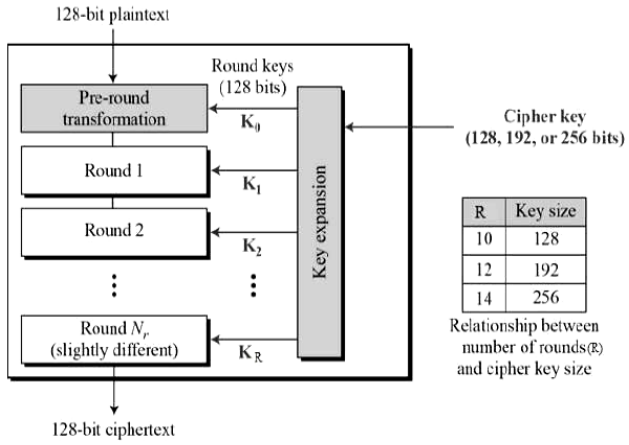


Fig.5. AES algorithm encryption Process

The advantages of symmetric algorithms are: authentication which proves the receiver's identity, confidentiality of data which provides secrecy and the symmetric cryptosystem which uses countersign [2]. The disadvantages of symmetric algorithms are: the attacks while the shared key is distributed, unable to provide digital signature which proves sender's identity and moreover the methods or the ways of key distribution [1].

III. ASYMMETRIC CRYPTOGRAPHY

Unlike symmetric encryption asymmetric cryptography uses a pair of keys for encrypting the data. The private key and the public key constitute a pair where both the sender and the receiver generate their own pair of keys. The sharing of public key is the predominant factor in asymmetric cryptography which we call it as key management.

Authentication is provided in asymmetric cryptography by

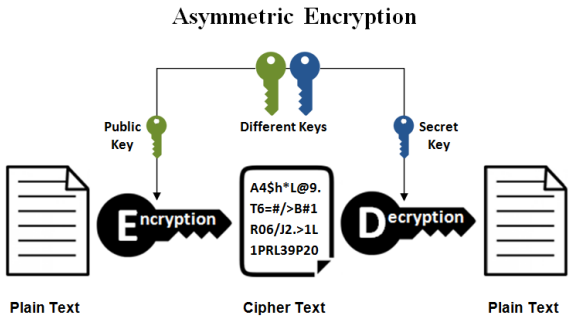


Fig.6. Asymmetric Cryptography Process

encrypting data by the sender's private key and decryption is done by the receiver with sender's public key. The algorithms used in asymmetric cryptography are: RSA, DIFFIE-HELLMAN, DIGITAL SECURE, ECC and EES. The most popular of these RSA and DIFFIE-HELLMAN are explained in brief.

RSA algorithm is for encryption of data, key exchange and digital signature. The primary advantage of RSA is superior security compared with other algorithms [7]. The description of this algorithm is depicted below.

Key Generation	
Select p, q	p and q both prime
Calculate n	$n = p \times q$
Select integer d	$gcd(\phi(n), d) = 1;\ 1 < d < \phi(n)$
Calculate e	$e = d^{-1} \bmod \phi(n)$
Public Key	KU = $\{e, n\}$
Private Key	KR = $\{d, n\}$
Encryption	
Plaintext: $M < n$	
Ciphertext: $C = M^e \pmod n$	
Decryption	
Ciphertext: C	
Plaintext: $M = C^d \pmod n$	

Fig.7.The Process of RSA algorithm

Diffie-Hellman algorithm is used to exchange a shared secret without actually sharing it between the two parties as depicted in figure 8.

Global Public Elements	
q	prime number
α	$\alpha < q$ and α a primitive root of q
User A Key Generation	
Select private X_A	$X_A < q$
Calculate public Y_A	$Y_A = \alpha^{X_A} \bmod q$
User B Key Generation	
Select private X_B	$X_B < q$
Calculate public Y_B	$Y_B = \alpha^{X_B} \bmod q$
Calculation of Secret Key by User A	
$K = (Y_B)^{X_A} \bmod q$	
Calculation of Secret Key by User B	
$K = (Y_A)^{X_B} \bmod q$	

Fig.8.The Diffie-Hellman key exchange process

The major advantages of asymmetric cryptography are: it provides digital signature, no major issues with public key distribution. The disadvantages of asymmetric cryptography are: slow execution compared to symmetric process and the issues in key management.

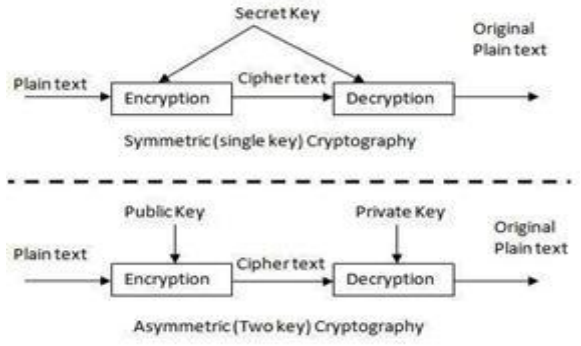


Fig.9.The Symmetric and asymmetric cryptography process

IV. SECURITY OF DATA STORED IN CLOUD

The data in the cloud is to be securely stored. Cryptography in the cloud allows the security of the data. As a customer, he/she will be no control on the security mechanisms that are applied on data stored in the cloud [3]. Various cryptographic algorithms and mechanisms are used to protect the information and stored in an encrypted form.

Quantum Direct Key System is a set of classy asymmetric key mechanism that can be applied on the data stored in cloud. In this process the global public key elements and the private key are matched with the ID and moreover an entity can construct other entity's public key without the help of any trusted third party. This type of crypto cloud mechanisms avoid the traffic congestion compared to other encryption processes.

Table- I: Comparison of cryptography algorithms

Algorithm	Key size	In steps of
Symmetric Encryption		
DES	40-56 bits	8 bits
3DES	64-112 bits	8 bits
Asymmetric Encryption		
Diffie-Hellman	512-2048 bits	64 bits
RSA	512-2048 bits	64bits
Digital Signatures		
RSA	512-2048 bits	64 bits
DSA	512-2048 bits	64 bits

Proper key management assures the security of information which is as important as encrypting the information stored in cloud. Both key management and encryption are the essential factors for authentication and confidentiality of data stored in cloud [4]. Possible key management factors are securing key stores, authorized access to key stores and key backup with recovery features.

V. RESULT AND COMPARATIVE ANALYSIS

The proper and appropriate implementation of the cryptographic algorithms leads to authenticity, confidentiality and data integrity. Using DES symmetric encryption algorithm as a first level of encryption and further applying RSA asymmetric encryption process leads to a strong cipher text. While decrypting first RSA is applied on the cipher text and then the DES decryption process done on the intermediate plaintext leads to an authenticated and confidential plaintext [8]. The following table shows the comparison of symmetric and asymmetric encryption algorithms with the battery consumption and time consumption along with the attacks possible on them. Also shown below the graphical representation of the battery and time consumptions of various symmetric and asymmetric encryption algorithms.

Table- II: Comparison of cryptography algorithms based on their performance

Algorithm	Battery Consumption	Time Consumption	Attack
Symmetric cryptographic algorithms			
DES	Medium	Slow	Brute force
3DES	High	Very Slow	Brute force, Known Plaintext
AES	High	Fast	Side channel
Blowfish	Lowest	Very fast	Dictionary
RC6	Medium	Fast	Brute force
RC4	High	Fast	Brute force
RC2	High	Fast	Brute force
CAST	High	Fast	Timing, Chosen plaintext
Serpant	Medium	Fast	XSL attack
Asymmetric cryptographic algorithms			
RSA	Low	Slowest	Cycle attack
Diffie-Hellman	High	Medium	Man-in-the-middle attack
ECC	Medium	Fast	Side channel

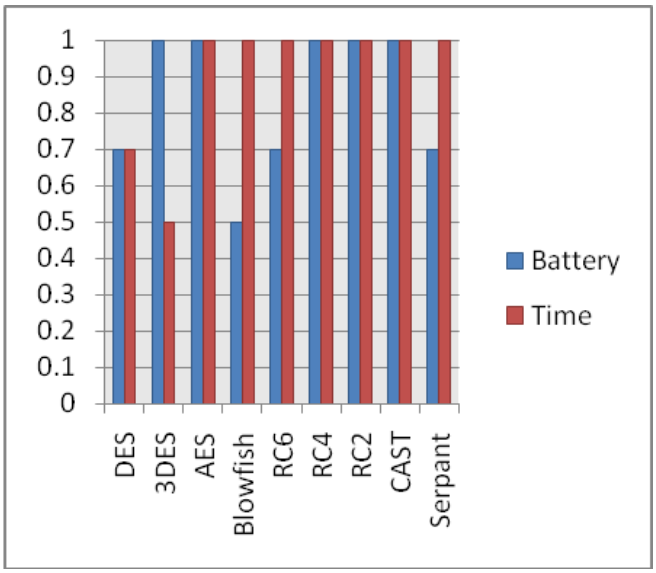


Fig.10.The graph that depicts the performance of Symmetric algorithms

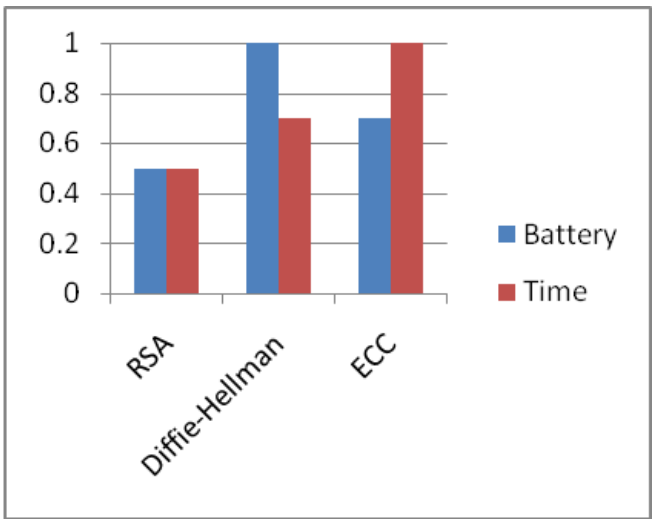


Fig.11.The graph that depicts the performance of Asymmetric algorithms

VI. CONCLUSION

Various cryptographic aspects are covered, predominantly different symmetric and asymmetric cryptography algorithms, their comparisons with suggested solutions and results including cloud data protection. Using DES symmetric encryption algorithm as a first level of encryption and further applying RSA asymmetric encryption process leads to a strong cipher text. As cryptography and crypto cloud computing plays major role in secure transfer and storage of information both key management and encryption are the essential factors for authentication and confidentiality of data stored in cloud. Quantum Direct Key System is a set of classy asymmetric key mechanism that can be applied on the data stored in cloud.

REFERENCES

1. Zhijie Liu Xiaoyao Xie, Member , IEEE ,School of Mathematics and Computer Science and Zhen Wang, Key Laboratory of Information Computing Science of Guizhou Province , Guizhou Normal University Guiyang , China, The Research of Network Security Technologies.
2. Bowen, Janine Anthony (2011). Cloud Computing: Issues in Data Privacy/Security and Commercial Considerations. Computer and Internet Lawyer Trade Journal, 28 (8), 8.
3. Veerapaneni Esther Jyothi, K. Nageswara Rao (2014) Effective implementation of agile practices – In Collaboration with Cloud Computing, International Journal of Current Engineering and Technology, Vol.4, No.3 (June 2014).
4. Anitha Y, "Security Issues in cloud computing", "International Journal of Thesis Projects and Dissertations "(IJTPD) Vol. 1, Issue 1, PP :(1-6), Month: October 2013.
5. D. S. Abdul. Elminaam, H. M. Abdul Kader and M. M. Hadhoud, "Performance Evaluation of Symmetric Encryption Algorithms", Communications of the IBIMA Volume 8, 2009.
6. C A. S. a. A. R. A. Devi, "Performance analysis of Symmetric Key Algorithms: DES, AES"," International Journal of Engineering and Computer Science, vol. 4, no. 6, pp. 12646-12651, 2015.
7. X. Z. &. X. Tang, "Research and Implementation of RSA Algorithm for Encryption and Decryption In Strategic Technology (IFOST)," in 6th International Forum on IEEE, 2011.
8. AmareAnagawAyele, VudaSreenivasarao, "A Modified RSA Encryption Technique Based on Multiple public keys", International Journal of Innovative Research in Computer and Communication Engineering, vol. 1, no. 4, June 2013.

AUTHORS PROFILE

Dr. Veerapaneni Esther Jyothi is a Microsoft Certified Professional and Solution Developer, currently working as an Assistant Professor in the department of Computer Applications, Velagapudi Ramakrishna Siddhartha Engineering College, Vijayawada, Andhra Pradesh, India. She has 11 years of teaching experience. She has published papers in various reputed international journals and conferences and her area of interest include Cloud Computing, Software Engineering, .NET Technologies.

Mrs.M.Prasanna Lakshmi is currently working as an Assistant Professor, Department of Computer Applications, VRSEC (Autonomous), Vijayawada, Andhra Pradesh. She has 11 years of teaching experience. Her research interests include Data security in cloud, image classification and data analytics.

Mr.RamaKrishna Regulagadda is currently working as an Assistant Professor, Department of Computer Applications, VRSEC (Autonomous), Vijayawada, Andhra Pradesh. He has 12 years of teaching experience. His areas of interest include Software Engineering, Artificial Intelligence, Java and Cloud Computing. He has several publications in Computer Science in reputed national and international journals. He had received M.C.A from Acharya Nagarjuna University, Guntur.