 ISBN: 978-81-927230-0-9

Hybrid Data Encryption Technique for Data Security in Cloud Computing

Basel Saleh Al-Attab

Research Scholar, Yemen nationality

H.No.26, Garafa , Alodain Street, Ibb City, Yemen. P.O.Box 70270

atbbael@gmail.com

Dr. H. S. Fadewar

Assistant Professor

School of Computational Sciences, S. R. T. M. University, Nanded, India

fadewar_hsf@yahoo.com

***Abstract*—With the enormous growth in cloud computing services, data and network security are important issues in cloud computing environment. Since the cloud computing and all of its data are accessible to anyone over the insecure networks, there have been many security issues and challenges faced the cloud computing. Many of the studies try to solve these issues, but still, some of these issues remain unsolved. One of the efficient techniques to ensure data security is cryptography. This paper attempts to propose a new hybrid data encryption scheme to enhance the security and solve the data security problems such as key and security weakness, time complexity, and slow performance.**

***Keywords*— Cloud Security, Security Algorithm, CSP, Cryptography.**

I. INTRODUCTION

Cloud computing is an emerging computing technology that uses central remote servers and internet to maintain applications and data. Its benefits include on-demand self-service, unlimited resource pooling, broad network access, fast deployment, lower costs, rapid provisioning, rapid, ubiquitous network access, greater resiliency, dynamic scalability, service-measured pricing, and alleviation of management risks [1].

With the development of cloud computing, and its benefits, cloud computing motivates users (individual, or enterprise) to outsource their data to remote servers hosted by a Cloud Server Provider (CSP). As the cloud computing resources and services are open for public use and communication is performed over the Internet, data security risks and challenges are raised under untrusted cloud environments. Confidentiality, integrity and availability (CIA) are the greatest concerns with regards to security in cloud computing [2], so maintaining CIA for data security is a function of the correct application and configuration of network, system, and application security mechanisms at various levels in the cloud computing infrastructure.

The security concerns with respect to cloud computing are network traffic, end user data security, host machine security, and file systems, which cryptography can resolve to some range and thus helps organizations in their opposed acceptance of cloud computing [3]. In the cloud computing, there are various security issues such as ensuring secure data transfer, ensuring secure interface, separation of data, secure stored data, and user access control [4]. Therefore, the current study aims to propose a new data security scheme in cloud computing environment by using hybrid data security with

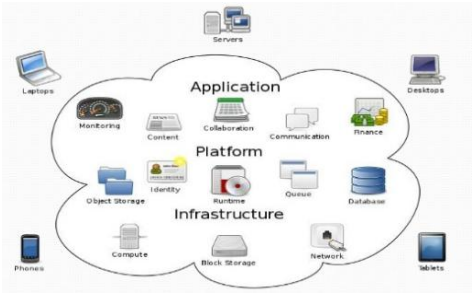

Fig. 1 Cloud Computing Environment

respect to cloud computing requirements and solve the data security issues such as mathematical complexity, key and security weakness, time complexity, complex processing on data and slow performance . This paper is organized as follows: in addition to Introduction, the security requirement in the cloud computing is presented in section II. The third section presents the data security algorithms, the literature study and existing work is presented in the fourth section. The proposed scheme and its working are explained in section V. Finally, the conclusion is presented in section VI.

II. DATA SECURITY REQUIREMENTS

Cloud computing provides the way to share differentiate services and resources which belong to different organizations of sites. Since cloud computing share these resources via network in the open environment thus it make security

problems. There are a number of security threats associated with cloud data services, not only covering traditional security threats, e.g., illegal invasion, network eavesdropping, and denial of service(DOS) attacks, but also including specific cloud computing threats, e.g., virtualization vulnerabilities, side channel attacks, and abuse of cloud services. To choke these threats the following security requirements are to be achieved in a cloud data service [5].

A. *Data Confidentiality*: Data confidentiality is the property by which data contents are not available or accessible to unauthorized users. Outsourced data is stored in a cloud and it became out of the owners' direct control. Only authorized users can access the sensitive data, while others, including cloud server providers (CSPs), should not obtain any information about these data. Meanwhile, data owners expect to fully utilize cloud data services (e.g., data search, data computation, and data sharing) without leakage of the data contents to CSPs or other adversaries.

B. *Data Integrity*: Data integrity seeks to maintain and to ensure the completeness and accuracy of data. A data owner always expects that his or her data in a cloud can be stored trustworthily and correctly, which means that the data should not be intervened with, or maliciously deleted. The data owner should be able to detect the corruption or loss if any undesirable operations corrupt or delete the data. Further, when a portion of the outsourced data is lost or corrupted, the rest of the data should be retrievable.

C. *Data Access Controllability*: Access controllability means that a data owner can perform the selective restriction of access to his or her data outsourced to the cloud. Some users can be authorized by the owner to access the data, while others cannot access it without permission. The access authorization must be controlled only by the owner in cloud computing environments. Further, it is desirable to enforce fine-grained access control to the outsourced data, with regard to different data pieces different users should be granted different access privileges.

III. DATA SECURITY ALGORITHMS

Security algorithms can be classified on based the convert of plaintext, using keys or processing the plain-text. The plaintext can be converted into ciphertext by the substitution techniques, which the letters of plaintext are replaced by other letters or by number or symbols such as Caesar cipher, Hill cipher, Playfair cipher, etc..., or by the transposition technique, which is a kind of mapping achieved by performing some sort of permutation on the plaintext such as rail fence technique [6]. The plain-text is processed even as a block ciphers or stream ciphers. In the block cipher, a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length, where as the stream cipher encrypts a digital data stream one byte or one bit at a time.

On the base of using keys, there are three types: symmetric algorithm, asymmetric algorithm, or Hash algorithm.

A. *Symmetric algorithm*: it is called also secret key algorithm, it is an algorithm which uses the same key for encrypting the plaintext and decrypting the ciphertext [2], this key is known to the sender and receiver of data. The requirement that both parties (sender, and receiver) have access to the secret key is one of the main drawbacks of symmetric key algorithms. The main symmetric algorithms are:

1) *Data Encryption Standard (DES)*: it is a block encryption algorithm that encrypts data with a 56-bit randomly generated the symmetric key. DES is not a secure encryption algorithm and it was cracked many times.
2) *Advanced Encryption Standard (AES)*: This algorithm was developed by Joan Daemen and Vincent Rijmen of Belgium. it is a newer and stronger encryption standard, which uses the Rijndael algorithm. AES will eventually displace DESX and 3DES. It is capable of using 128-bit, 192-bit, and 256-bit keys.
3) *Blowfish*: Blowfish is a symmetric block cipher, designed by Bruce Schneier. Blowfish has a 64-bit block size and a convertible key length from 32 up to 448 bits. Twofish later created by Schneier, which performs a similar function on 128-bit blocks.
4) *Triple DES(3DES)*: 3DES was developed from DES. 3DES is a block encryption algorithm, it uses a 64-bit key consisting of 56 effective key bits and 8 parity bits. DES encryption is applied three times to the plaintext in 3DES. The plaintext is encrypted with key A, decrypted with key B, and encrypted again with key C.

B. *Asymmetric algorithm*: it is called also a public key algorithm, it is an algorithm which use a pair of related keys, public key for encrypting the data and private key for decrypting the data[7]. The main asymmetric algorithms are:

1) *Rivest Shamir Adleman (RSA)*: it is a public key algorithm released to Ron Rivest, Adi Shamir, and Len Adleman (RSA). RSA can be used for signing data and encrypting. The encryption and signing processes are performed through a series of modular multiplications.
2) *Elliptic Curve Cryptography (ECC)*: ECC provides similar functionality to RSA. It is being implemented in smaller devices like cell phones. ECC requires less computing power compared with RSA. Encryption systems for ECC are based on the idea of using points on a curve to define the public/private key pair.
3) *Diffie-Hellman Key Agreement*: It was developed by Dr. Whitfield Diffie and Dr. Martin Hellman. Diffie-Hellman is not for encryption or decryption, but it enable two parties (users, or devices) who are interested in

communication to generate a shared secret key for exchanging information confidentially.

4) *Digital Signature Algorithm (DSA)*: Digital Signature Algorithm can be used only for signing data and it cannot be used for encryption. Signing process in DSA is performed through a series of calculations based on a selected prime number. Although intended to have a maximum the key size of 1,024 bits, longer key sizes are supported. The process of creating the digital

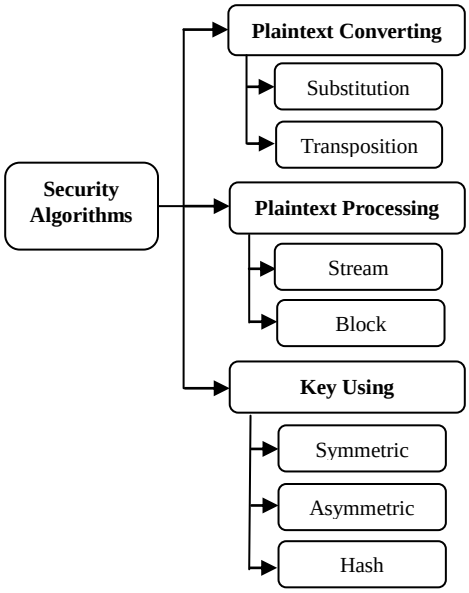

Fig. 2 Data Security Algorithms

signature is faster than validating it when DSA is used, but when RSA is used, the process of validating the digital signature is faster than creating it.

5) *ELGAMAL*: It is an algorithm used for transmitting digital signatures and key exchanges. ElGamal algorithm is based on the characteristics of calculations, and logarithmic numbers. DSA algorithm is based on ElGamal algorithm.

C. *Hash algorithm*: A hash algorithm is a function that converts a data string into a numeric string of fixed length. Hashing is always a one-way operation, and the output string is generally much smaller than the original data. Hash algorithms are designed to be collision-resistant, which mean there is a very low probability that the same string would be created for different data. Values returned by a hash function are called message digest or simply hash values. There are several hash functions used in cryptography, which include the message-digest hash functions MD2, MD4, and MD5, used for hashing digital signatures into a shorter value called a message-digest, and the Secure Hash Algorithm (SHA), a standard algorithm, that makes a larger (60-bit) message digest and it is similar to MD4.

IV. LITERATURE STUDY

Rewagad et.al[8] proposed a combination referred as three way mechanism (authentication, data security and verification). To protect confidentiality of data stored in cloud, they used the digital signature and Diffie-Hellman key exchange blended with (AES) algorithm. For providing security service(confidentiality) in cloud computing services, Gharshi et.al[9] proposed that the ECC algorithm can be used for data encryption instead of RSA, because of its advantages in terms of lower CPU time, less memory usage, and smaller key sizes. Akintoye et. al[10] proposed a scheme for securing transfer of data using Signcryption Based on HyperElliptic curves. In order to achieve minimal computational cost and communication overhead, both encryption functions, and digital signature are combined logically in one step.

K. Sood[11] proposed a framework which is divided into two phases, the first phase deals with the process of transmitting and storing data securely into cloud computing, and the second phase deals with the retrieval of data from cloud computing and showing the generation of requests for data access, double authentication, verification of digital signature and integrity. The proposed method achieves the availability, reliability and integrity of data traversing through owner to cloud and cloud to the user. For secure data transmission from one cloud to other cloud Gampala et. al[12] proposed a secure and authenticated data with elliptic curve cryptography and digital signature.

Gupta et. al[13] proposed a model to ensure file security on the cloud computing by using a hybrid encryption blowfish and the modified version of RSA. Shaikh et. al [14] Proposed a classification technique for data security which can be provided based on the level and the required protection, security provisions at the storage can be applied based on data set classified as per the dimensions. Tebaa et.al[15] Proposed a model to encrypt data before sending it to the cloud provider by using the Homomorphic encryption, and allow servers to perform various operations requested by the client without decrypt the data.

V. PROPOSED METHOD

In this section, a Hybrid Data Encryption algorithm is proposed to serve the security of cloud computing with high performance and low processing. It is a hybridization between the asymmetric key, secret sharing, and key exchange.

Asymmetric key algorithms depend on using two related keys, public key and private key. Public key is used to encrypt data, and private key to decrypt the data. Secret sharing is used to encrypt the secret message in visual form by splitting it into n shares, then it will be transmitted securely via internet or any other communication channels. The secret message can be

decrypted when a sufficient number of shares stacking together using OR of XOR operation. For key exchange, the Diffie-Hellman key agreement algorithm is used. It is a method that allows two parties (devices, users) to communicate over a network by establishing a shared secret key without exchanging any secret data. The security of this algorithm is based on solving discrete logarithm problem.

VI. CONCLUSION

With growing awareness regards to cloud computing security, there is growing awareness and usage of security algorithms into data systems and processes. In this paper we propose a hybrid data security algorithm to serve the security of data in the cloud computing by using the asymmetric key, secret sharing, and key exchange techniques. For future work, the proposed line of research includes designing the whole algorithm with respect to the cloud computing requirements and getting high performance and less processing in data.

REFERENCES

[1] S. Subashini , V. Kavitha," A survey on security issues in service delivery models of cloud computing" Journal of Network and Computer Applications, Elsevier 2011.
[2] Zhifeng Xiao ,Yang Xiao,"Security and privacy in cloud computing", IEEE Communications Surveys & Tutorials,VOL. 15, NO. 2, Second Quarter 2013.
[3] Nelson Gonzalez, Charles Miers, Fernando Redigolo, Marcos Simplicio, Tereza Carvalho, Mats Naslund, Makan Pourzandi "An quantitative analysis of current security concerns and solutions for cloud computing", Springer 2012.
[4] Akashdeep Bhardwaj, GVB Subrahmanyam, Vinay Avasthi, Hanumat Sastry," Security Algorithms for Cloud Computing", International Conference on Computational Modeling and Security (CMS), ScienceDirect 2016
[5] JUN TANG, YONG CUI and QI LI, KUI REN, JIANGCHUAN LIU, RAJKUMAR BUYYA,," Ensuring Security and Privacy Preservation for Cloud Data Services" ACM Computing Surveys, Vol. 49, No. 1, June 2016.
[6] William Stallings, "Cryptograph and Network security principles and practice", sixth edition.
[7] Behrouz Forouzan, "Cryptography and Network Security", McGraw-Hill Special Indian Edition 2007.
[8] Prashant Rewagad, Yogita Pawar," Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing", International Conference on Communication Systems and Network Technologies, IEEE 2013.
[9] Ravi Gharshi, Suresha," Enhancing Security in Cloud Storage using ECC Algorithm", International Journal of Science and Research (IJSR), Volume 2 Issue 7, July 2013.
[10] Samson B. Akintoye, Kayode A. Akintoye," Data Security Scheme For Cloud Computing Using Signcryption Based On Hyperelliptic Curves", Journal of Research and Development Vol. 2, No. 7, 2015.
[11] Sandeep K. Sood," A combined approach to ensure data security in cloud computing", Journal of Network and Computer Applications, ScienceDirect 2012.
[12] Veerraju Gampala, Srilakshmi Inuganti, Satish Muppidi," Data Security in Cloud Computing with Elliptic Curve Cryptography", International Journal of Soft Computing and Engineering (IJSCE) Volume-2, Issue-3, July 2012.
[13] Reema Gupta, Tanisha, Priyanka," Enhanced Security for Cloud Storage using Hybrid Encryption", International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 7, July 2013.
[14] Rizwana Shaikha, Dr. M. Sasikumar," Data Classification for achieving Security in cloud computing", ScienceDirect 2015.
[15] Maha TEBAA, Saïd EL HAJJI, Abdellatif EL GHAZI ," Homomorphic Encryption Applied to the Cloud Computing Security", Proceedings of the World Congress on Engineering 2012 Vol I
WCE 2012, July 4 - 6, 2012, London, U.K.