A Review on Securing Cloud Systems using Cryptographic Algorithms

Dr.M.Moorthy
Master of Computer Applications
Muthayammal Engineering College
Rasipuram, India
Director.mca@mec.edu.in

Mr.S.Nobledhas
Master of Computer Applications
Muthayammal Engineering College
Rasipuram, India
Noble.optim@gmail.com

Mr.D.V.Rajkumar
Master of Computer Applications
Muthayammal Engineering College
Rasipuram, India
dvrajkumar@gmail.com

Mr.D.Prabhakaran
Master of Computer Applications
Muthayammal Engineering College
Rasipuram, India
prabhakaranmecmca@gmail.com

Abstract**-In this technological era, cloud systems became a vital one to store data. Nowadays everyone store their important data in cloud architecture. It provides services and resources with the help of internet. On the other hand, security risks of cloud computing represent a major concern that slows down its market growth. There are many frameworks for handling security risks of cloud computing, most of them trust the cloud service provider and do not focus on the new types of security risks that might face the cloud. Hence, they cannot detect attacks that might come from cloud service provider's side or due to vulnerabilities or attacks at the cloud service provider system. Therefore, in this paper, we have done a formal assessment and examination of cloud systems key cryptographic algorithms and given a recommendation of the best combination of algorithms as a result of our different parameters of considerations. These parameters include whether they are a stream or block cipher and their key size or the hash value. We have found out that the most viable cryptographic methods for securing the cloud systems are AES, Diffie-Hellman, RSA and SHA-1 which are from symmetric, asymmetric and hashing cryptographic algorithm. We propose a combination of AES, Diffie-Hellman and SHA-1 algorithm for optimum cloud security.**

Keywords-Cloud Computing; Cloud Security; Cryptography; Symmetric; Asymmetric; Hashing

I. Introduction

Cloud systems concentrate mainly on maximizing the efficiency of the shared resources. Cloud resources are shared by various users and still dynamically allotted as per the requirement.. This technique maximizes the usage of computational capability. One fundamental enabler of cloud computing is virtualization, which can be applied to hardware, middleware and application systems, hence cost effectiveness [1]. While large amount of work focuses on load balancing, system maintenance and energy management of the data center [2]. Since cloud computing is utility available on internet.So various issues like user privacy, data theft and leakage and unauthenticated accesses are raised. However, the current work on strengthening virtualization- aware security operations for the cloud has demonstrated that existing security approaches do not necessarily apply to the cloud because of the discrepancy in security needs and threat [3]. Therefore, this study focuses on the cryptographic algorithms deemed fit for virtualization. Cryptography is the science of securely transmitting and retrieving information using an insecure channel [4].

Cryptography involves mainly two processes [5]. First, the encryption process in which the sender converts data in form of an un recognized string or cipher text for transmission. Secondly, decryption process where encryption is reversed. The receiver transforms sender’s cipher text into a meaningful text known as plaintext. Additionally, hashing algorithms [6] which are part of cryptographic methods have been used in some case to strengthen security over unsecure channels.

The cryptographic algorithms can be categorized into symmetric, asymmetric, and hashing. Symmetric keys are the cryptographic conventional key or private key where both sides of the sender and receiver use the same key. They include AEs, Blowfish, RC4, RC5, RC6, Twofish etc. On the other hand, Asymmetric c key are two cryptographic keys where one is public and the other is private. They include Diffie-Hellman key agreement, RSA, ECC, ElGamal, DSA etc. While hashing algorithm is an algorithm that produces a hash value of a piece of data, such as a message or session key . They are useful in detecting any modification in a data object, such as a message. Typical hash algorithms include M D5, SHA-1, and SHA-2.

II. Related Work

A number of cryptographic algorithms have been applied in the cloud computing for securing data and files in the clouds. Abutaha & Amro [8] in their study proposed a new method for saving data in the cloud system. They use AES and RSA algorithms for securing data and connection based on different keys in encryption and decryption. They used a SHA1 algorithm to secure the hash table of data.

According to M. Gopinathan [9] Elliptic Curve Cryptography (ECC) has been around for a while, but has not garnered widespread usage yet, compared to other cryptosystems such as RSA. However, ECC has considerable advantages when it comes to security performance and is quite compatible with predominant cryptographic methods, like the Diffie-Hellman key exchange. The author recommended further improvement and usage of ECC in cloud computing security.

B.T Reddy et al. [10] in their work presented algorithms to provide security in cloud and protecting the data transmitted through various secure channels by providing security using encryption. They concluded cryptographic algorithms like DES, AES, GOST 28147-89, CAST, RC6, SERPENT, and TWOFISH can be adapted for the optimization of data security in cloud computing. Bhardwaj et al.[11] in their work studied Asymmetric and Symmetric Algorithms Security Algorithms for Cloud Computing. Their emphasis was on symmetric algorithms such as AES.3DES, RC6, Blowfish and M D5. The authors analyzed the algorithms for different encryption and encoding techniques and they found AES to be a good candidate for key encryption and M D5 being faster when encoding.

S. Bhute & S.K. Arjaria [12] work demonstrated an efficient secured user cloud framework with the help of AES and RC6 algorithms. This approach provides the flexibility of inter cloud communication with secure transactions by using AES and RC6 mechanism. Their results show that their approach is better in terms of using the private key, key randomization and provides the support of user to user, user to cloud server and cloud server to user as comparison to the traditional approaches. Patel and Patel [13] proposed to develop the RSA higher efficiency algorithm and TPA for authentication the data over perform transaction on cloud. Further, they applied the digital signature on that TPA through verify the sender and also apply on that HMAC function for hashing the key value on cloud. The experimental results showed that RSA and digital signing algorithm is more efficient than other signature algorithm used on cloud.

S. K. M ajhi [2] proposed a framework for authentication in Virtual Machine migration based on hash based authentication code and Diffie-Hellman key exchange protocol. Their study verified the framework using security analysis. Summing up, the proposed framework is a secured and appropriate method to VM Migration in a two-party migration model. Kumar et al. [7] in their paper did a comparative study of two cryptographic algorithms for addressing cloud security issues. They include Blowfish and Twofish algorithms. Theoretical analysis of the two algorithms were done and it was concluded that Blowfish had more advantages than Twofish. They recommended that an experimental analysis to be conducted to further gain insight of the performance of the algorithms.

III. SECURITY ALGORITHMS

A.Symmetric Key Cryptography

Symmetric Key Cryptography is a class of cryptographic methods that are also referred to as shared key or shared secret encryption. A single key is used both to encrypt and decrypt data i.e. single cryptographic keys are used for encoding of plain text as well as decoding of cipher text as illustrated in Figure 1. Symmetric key encryption can use either stream ciphers or block ciphers. Stream ciphers take the message one bit at a time and encrypt it. Block ciphers take a block of bits of the message and encrypt it. Symmetric Key Cryptography is generally used for long messages [7], [11], [16]. From literature a number of symmetric key cryptographic algorithms exist, some of the algorithms used in cloud security includes: AES, RC4, RC5, RC6, Twofish and Blowfish. These algorithms differ in terms of the key size, block size, computational time etc. Symmetric encryption algorithms can be extremely fast, and their relatively low complexity allows for easy implementation in hardware. Nevertheless, they require that all hosts engaging in the encryption have previously been configured with the secret key through some external mechanisms.

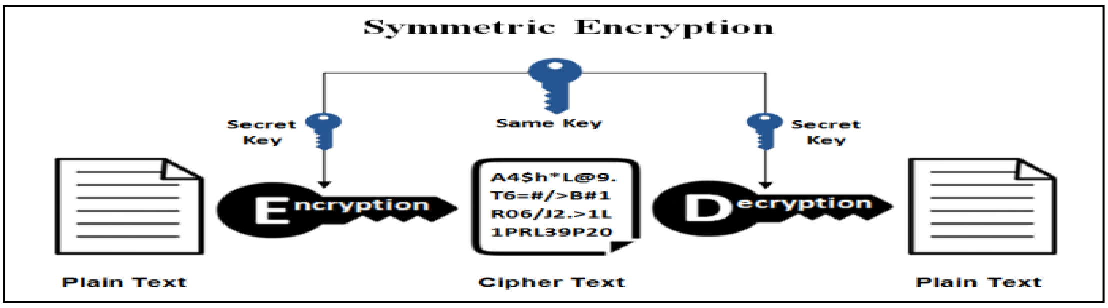

Figure 1: Symmetric Key Cryptography

a. Advanced Encryption Standard (AES)

The AES is a widely adopted symmetric key algorithm originally developed by Joan Daemen and Vincent Rijmen. AES is an iterative block cipher with 128-bit data and variable size bit keys of 128, 192 and 256. Additionally, it is based on a design principle of substitution-permutation network. Moreover, it is fast in both software and hardware. AES performs all its computations on bytes rather than bits. Therefore, it treats the 128 bits of a plaintext block as 16 bytes [4], [11], [12].

b. RC4, RC5 and RC6

RC4, RC5 and RC6 are series of symmetric algorithms developed by RSA security .RC4 is a variable key -size stream cipher which performs its computations based on bytes. Additionally, the algorithm is based on the use of a random permutation. RC4 uses a 24-bit initialization vector (IV) to create key lengths of 40 or 128 bits[3]. **RC5** is a successor of RC4 and its a parameterized algorithm with a variable block size, a variable key size, and a variable number of rounds. Allowable choices for the block size are 32 bits (for experimentation and evaluation purposes only), 64 bits (for use a drop -in replacement for DES), and 128 bits. The number of rounds and keys varies from 0 to 255 and 0 to 2040 bits respectively RC5 comprises three routines which includes key expansion, encryption, and decryption.

RC6 is a successor of RC5 with two added features like the inclusion of integer multiplication and the use of four 4-bit working registers instead of RC5’s two 2-bit registers. Because of more number of registers RC6 is faster than RC5. Additionally, RC6 is a block cipher parameterized algorithm RC6 with varied block size, the key size, and the number of rounds. The upper limit on the key size is 2040 bits[5], [12], [16]. Even though RC5 was improved version of RC4 it has not been widely applied in securing the cloud services compared to its counter parts RC4 and RC6.

B. Asymmetric Key Cryptography

Asymmetric Key Cryptography is a cryptographic algorithm where a key used by one party to perform encryption (encoding) is not the same as the key used by another in decryption (decoding). There is pair of keys, a public encryption key and a private decryption key . It is also referred to as public-key cryptography . The illustration of asymmetric key cryptography is shown in Figure 2. Asymmetric encryption tends to be slower as it imposes a high computational cost compared to symmetric algorithm. However, its major strength is the ability to establish a secure channel over a non-secure medium such as internet. This is achieved through the exchange of public keys that are only used to encrypt data. On the other hand, private key is used only for decrypting.

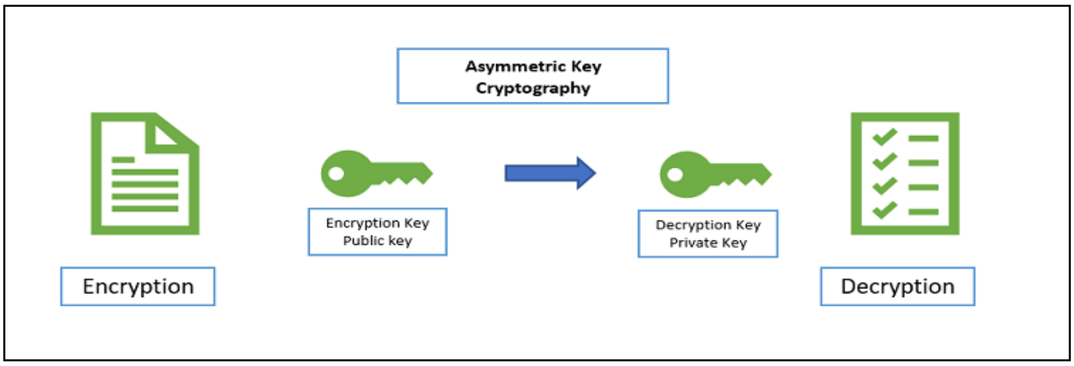
Asymmetric Key Cryptography
Encryption Key Public key
Decryption Key Private Key
Encryption
Decryption

Figure 2: Asymmetric Key Cryptography

A number of Asymmetric key algorithms that have been used for cloud securing the cloud exists from literature, they include: Diffie-Hellman key agreement, RSA, ECC, ElGamal, DSA etc. The following are the major asymmetric encryption algorithms used for encrypting or digitally signing data.

a. Diffie-Hellman key agreement

This is a key agreement algorithm that was developed by Dr. Whitfield Diffie and Dr. M artin Hellman in 1976. It is not an encryption and decryption algorithm parse but it enables two sides that are communicating to come up with a shared secret key for confidential exchange of information. [2][20].

Diffie-Hellman key exchange is a public key cryptography that provides a secure solution for confidentially exchanging information online. It is extensively used with varying techniques by internet security technologies to offer exchange of secret/private keys for confidentiality purpose over communication channel [20].

b. Rivest Shamir Adleman (RSA)

RSA is asymmetric algorithm that was founded by Ron Rivest, Adi Shamir, and Len Adleman in 1978. RSA is used for encrypting and signing data through a series of modular multiplications. RSA algorithms are the most widely used public key algorithms, particularly when being sent over an insecure n etwork like the internet. The RSA key exchange process is used by some security technologies to protect encryption keys [13].

C. Hashing

Hashing is form of cryptographic security technique that condense a message into an irreversible fixed-length value called hash [6]. Hashing is used only to verify data; the original message cannot be retrieved from a hash. In the instances where a hash is used to authenticate a secure communication, its result is typically the original message plus a secret key. The illustration of hashing is depicted in Figure 3. Hashing algorithms are also commonly used without a secret key simply for error checking. The two most common hashing algorithms seen in networking are M D5 and SHA-1.

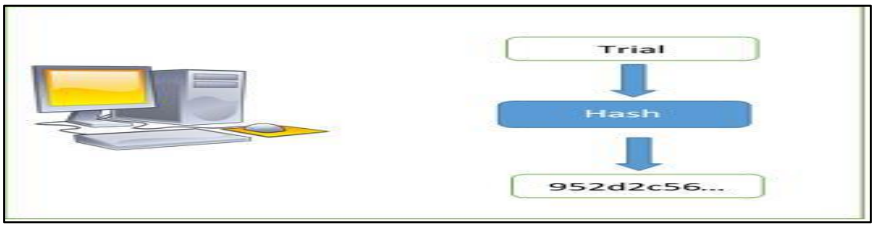

Figure 3: Hashing

a. MD5-(Message-Digest algorithm 5)

According to Patel and Patel [13] M D5 is a widely used cryptographic hash function with a 128-bit hash value, processes a variable-length message into a fixed-length output of 128 bits. The input message is broken up into 512-bit blocks. whenever the message is passed the length of 512 blocks are divisible. In this sender use the public key of the receiver to encrypt the message and receiver use its private key to decrypt the message. They're used in many forms of authentication, such as digital signatures and message authentication codes, as well as for verifying file integrity, because even the slightest change to the data will change its hash value.

For example, many software publishers provide the M D5 hash value of their down-loadable software so that users can verify that the file is authentic and has not been tampered with.

MD5 algorithm yields two advantages. One is that matching messages always produce the same message digest and even if one of the bits of the message is altered, then it generates a different message digest. The other advantage is that M D5 are much shorter than the document from which digests are generated [22]. M D5 security is undoubtedly not appropriate for security -based applications and services like SSL or digital signatures that depend on collision resistance.

b. Secure Hash Algorithm (SHA)

SHA is a cryptographic hashing algorithm used to determine the integrity of a particular piece of data. Variations of this algorithm are often used by SSL certificate authorities to sign certificates. There exist two different versions of the algorithm SHA-1 and SHA-2 which differs in both design and bit-length of the signature. SHA-2 is successor of SHA-1.

SHA-1 is a 160-bit hash. SHA-2 is actually a “family” of hashes and comes in a variety of lengths, the most popular being 256-bit.

TABLE 1: Cryptographic algorithms

Cryptographic Algorithms	**Algorithm**	**Block/Stream Cipher**	**Key Size(bits)**
SYMMETRIC	AES	Block (128 bits)	128/192/256
	RC4	Stream	128
	RC5	Block(32/64/128 bits)	2040
	RC6	Block(32/64/128 bits)	2040
ASYMMETRIC	Diffie – Hellman Key	Block(64 bits)	32-448
	RSA	Block(22/8/6/214/342 bits)	512/1024/2048/3072
HASHING	MD5	Block(512 bits)	128 Hash value
	SHA – 1	Block	160 Hash value
	SHA – 2	Block	224/256/384/512 Hash value

TABLE 2: Cryptography algorithms used in cloud systems

Author/ Existing Study	**Security Requirement**	**Cryptographic Method used**	**Conclusion/ Recommendation**
A. Sachdev & Bhansali	Data confidentiality and security	AES	Implementing AES for security over data provides benefits of less memory consumption and less consumption time as compared to other algorithms
A. Chaudhary et al.	Authentication of the user	Homorphic encryption and Diffie – Hellman algorithm	Diffie Hellman algorithm allows two parties to

			communicate with each other and also exchange their secret keys over an unprotected communication channel without meeting in advance
Abtaha & Amro	Channel and data integrity	AES, RSA and SHA - 1	New model ensures security for whole cloud computing structure.
B.T. Reddy et al	Confidentiality, integrity and authentication among	Blowfish and Key management	The cryptographic algorithms can be adopted for the optimization of data security in cloud computing
M. Gopinathan	Authorization and integrity	ECC and Diffie Hellman key exchange	The authors recommended further improvement and usage of ECC in cloud computing security.
S. Singh et al	Data security and integrity	RSA and SHA-1	Proposed hybrid of RSA and SHA-1 for data security.
P. Salim et al	Data Integrity	RC6	RC6 algorithm gives better performance in terms of speed as compare to AES algorithm but AES algorithm require minimum amount of time for encryption and decryption as compare to RSA. They recommended Blowfish algorithm for the quality of service.

IV. CONCLUSION

In this study, a review of the various cryptographic techniques has been made. Out of the numerous algorithms for securing the cloud systems, hybrid approaches have been widely utilized over single cryptographic algorithm. Therefore, a combination of symmetric, asymmetric and hashing algorithms is proposed. This is because symmetric algorithms are better in terms of computational speed, while asymmetric algorithms are more secured. On the other hand, hashing algorithm can be used for integrity purpose. Thus we recommend experimental study of combination of the popular cryptographic techniques such as AES, Diffie-Hellman and SHA-1. The measure of the algorithms is the applicability in virtual migration security in cloud systems, computational cost and data size.

REFERENCES

[1] S. Njuki, J. Zhang, and E. Too, “Analysis of Virtual M achine M igration Security Architectures in Cloud Computing,” vol. 8, no. 10, pp . 1753–1763, 2017.

[2] S. K. M ajhi, “An Authentication Framework for Securing Virtual M achine M igration,” pp . 1283–1286, 2016.

[3] L. M ishra, “Secure Cloud Computing with RC4 Encryption and Attack Detection M echanism,” vol. 117, no. 14, pp . 40–45, 2015.

[4] R. Dogra, “Improvement of Cloud Security Efficiency by Reducing Data Size and Computational Time Using ECDH , AES , BlowFish & P SO,” vol. 8, no. 2, pp . 136–141, 2017.

[5] P. Salim, A. Abbas, and M . Qasim, “Improving Data Storage Security in Cloud Computing Using RC6 Algorithm,” vol. 19, no. 5, pp . 51–56, 2017.

[6] S. Singh, M . T. Scholar, T. Nafis, and A. Sethi, “Cloud Computing : Security Issues & Solution,” vol. 13, no. 6, pp . 1419–1429, 2017.

[7] G. K. Kumar and M . Gobi, “Comparative Study on Blowfish & Twofish Algorithms for Cloud Security,” vol. 3, no. 9, pp . 1–11, 2017.

[8] M . S. Abutaha and A. A. Amro, “Using AES , RSA , SHA1 for Securing Cloud,” no. April, 2014.

[9] M . Gopinathan, “Elliptic curve crypt ography in cloud computing security,” 2015.

[10] B. T. Reddy, K. B. Chowdappa, and S. R. Reddy, “Cloud Security using Blowfish and Key M anagement Encryption Algorithm,” no. 6, pp . 59–62, 2015.

[11] A. Bhardwaj, G. V. B. Subrahmanyam, V. Avasthi, and H. Sastry, “Security Algorithms for Cloud Computing,” in Procedia Computer Science, 2016, vol. 85, pp . 535–542.

[12] S. Bhute and S. K. Arjaria, “An efficient AES and RC6 based cloud-user data security with attack detection mechanism,” vol. 3, no. 21, 2016.

[13] K. H. Patel and S. S. Patel, “Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing Alpha College of Engineering and Technology Khatraj , Kalol,” vol. 4, no. 1, pp . 543–548, 2016.

[14] D. Thiyagarajan and G. Ramachandrarao, “Ensuring Security for Data Storage in Cloud Computing using HECC- ElGamal Cryptosystem and GSO Optimization,” Int. J. Intell. Eng. Syst., vol. 10, no. 5, pp . 115–124, 2017.

[15] A. P. S and K. Subhashri, “Securing Outsourced Dat a On Cloud Using ElGamal Cryptosystem,” pp . 53–56, 2017.

[16] N. Chandel, “Creation of secure cloud environment using Creation of Secure Cloud Environment using RC6,” no. June, pp . 6–8, 2016.

[17] P. Devi, “Data Security in Cloud Computing Based On Blowfish with Md5 Method,” vol. 3, pp . 149–154, 2017.

[18] G. K. M ythili and D. G. Priya, “Data Security in Cloud using Blowfish Algorithm,” vol. 2, no. 9, pp . 523–525, 2014.

[19] K. L. Hemalatha and C. V Sreevathsa, “Providing Better Security in Cloud Computing Environment using Twofish Encryption,” pp . 12–15, 2016.

[20] A. Chaudhary, R. Thakur, and M . M ann, “Security In Cloud Computing By Using Hom Omorphic Encryption Schem E With Diffie-Hellm An Algorithm ,” pp . 44–47, 2014.

[21] A. O. Adetunmbi and O. S. Adewale, “Ellip tic Curve Cryptography for Securing Cloud Computing Applications,” vol. 66, no. 23, pp . 10–17, 2013.

[22] S. R. Lenka and B. Nayak, “Enhancing Data Security in Cloud Computing Using RSA Encryption and M D5 Algorithm,” vol. 2, no. 3, pp . 60–64, 2014.

[23] M . Shah and A. S. Shah, “Appraisal of the M ost Prominent Attacks due to Vulnerabilities in Cloud Computing,” Int. J. Grid Distrib. Comput., vol. 9, no. 7, pp . 13–22, 2016

[24] Sam Njuki, Jianbiao Zhang, Edna C.Too and Rimiru Richard, “An evaluation of securing cloud systems based on cryptographic key algorithms”, vol. 42, no. 13, pp . 10–17, 2018.

M. Moorthy has received his Ph.D.fromAnnaUniversity,Chennaiin Computer Science and MCA from Manonmaniam Sundaranar University, Tirunelveli. He is Professor and Head of Department in MCA, Muthayammal Engineering College, Namakkal, Tamil Nadu, India. He has published more than 10 journals. His research interest includes Computer Networking, Network Security, Wireless Network, Data Mining, and Artificial Intelligence. He has more than 15 years of research experience and life member of ISTE, CSI, and IAENG.

S.Nobledhas has received his MCA degree from Anna University, Chennai. He is Professor in MCA department, Muthayammal Engineering College, Namakkal, Tamil Nadu, India. He is having around 10 years experience in various research field. His research interest includes Cloud Computing, Computer Networking, Network Security and Artificial Intelligence.

D.V.Rajkumar has received M.Phil (CS) from Periyar University, Salem and M.C.A from K.S.R. College of Technology, Namakkal. He is Assistant Professor in Department of MCA, Muthayammal Engineering College, Namakkal, Tamil Nadu, India. He has above 13 years experience in teaching and specialized in Computer Networking, Network Security, Wireless Network, and Mobile Communication. He is a life time member of Indian Society for Technical Education (ISTE) and Computer Society of India (CSI).

D.Prabhakaran has received MCA from Anna University, Chennai. He is Assistant Professor in Department of MCA in Muthayammal Engineering College, Namakkal, Tamil Nadu, India. He has above 3 years experience in teaching and specialized in Computer Networking, and .NET programming. He is a life time member of Indian Society for Technical Education (ISTE) and IAENG.

Bibliography of authors(4)