EasyChair Preprint

№ 3642

Multilayer Security of Data Using CryptoCloud DNA Technique

Mohammed Basheer Khan, Sneha Soni and Vivek Rawat

June 19, 2020

Multilayer Security of Data Using CryptoCloud DNA Technique

MOHAMMED BASHEER KHAN
Research Scholar, CSE,SIRTE Bhopal
proidbasheerkhan@gmail.com

Sneha Soni
Asst Prof. CSE, SIRTE Bhopal
kuhusoni14@gmail.com

Vivek Rawat
Asst Prof. CSE, SIRTE Bhopal
vivek.rawat7075@gmail.com

***Abstract*—To improve confidentiality in cloud computing it is of great importance there for we need for more ways to keep it from the attackers. In this paper, several levels of multi-coding levels were developed using more than one method to obtain more confidentiality through DNA encryption and adding a higher level of confidentiality by adding Blowfish algorithm or other and then loading it into the cloud storage. A JAVA program has been used for implementing proposed scheme. The Literature Survey show that proposed scheme has a convincing level of security, efficiency, complexity and speed.**

***Keywords*— cloud computing data security, cryptography, DNA, Blowfish, AES.**

I. INTRODUCTION

Cloud computing consists of software, hardware, network, applications and interface that provides a service to its customers. Virtualization is the major concept of the cloud, and can be achieved by pooling and sharing resources. Extensibility, flexibility and multiple leasing are the main features of virtualization. The cloud provides a variety of cloud computing service models to its customers: infrastructure as Service (IAAS), Platform as a Service (PAAS) and Software as a Service (SAAS) [1].

Cloud Computing refers to manipulating, configuring, and accessing the applications online. It offers online data storage, infrastructure and application. We need not to install a piece of software on our local PC and this is how the cloud computing overcomes platform dependency issues. Hence, the Cloud Computing is making our business application mobile and collaborative.

A. DATA SECURITY

Cryptography

The science of secret writing cryptography is necessary when communicating over any untrusted medium, which includes just about any network, particularly the Internet. There are five primary functions of cryptography:

Privacy/confidentiality: Ensuring that no one can read the message except the intended receiver.

Authentication: The process of proving one's identity.

Integrity: Assuring the receiver that the received message has not been altered in any way from the original.

Non-repudiation: A mechanism to prove that the sender really sent this message.

Key exchange: The method by which crypto keys are shared between sender and receiver.

There are several ways of classifying cryptographic algorithms. For purposes of this paper, they will be categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use. The three types of algorithms that will be discussed are (Figure 1):

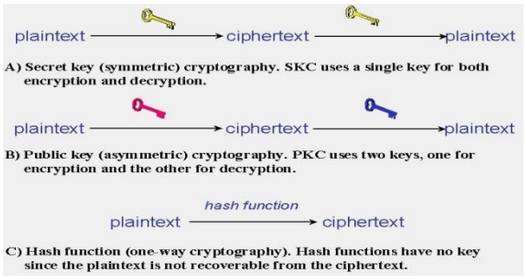

Fig 1 Types of Cryptography

Secret Key Cryptography (SKC): Uses a single key for both encryption and decryption; also called symmetric encryption. Primarily used for privacy and confidentiality.

Public Key Cryptography (PKC): Uses one key for encryption and another for decryption; also called asymmetric encryption. Primarily used for authentication, non-repudiation, and key exchange.

Hash Functions: Uses a mathematical transformation to irreversibly "encrypt" information, providing a digital fingerprint. Primarily used for message integrity.[15]

B. DNA DIGITAL CODING

In information science, the binary digital coding encoded by two state 0 or 1 and a combination of 0 and 1. But DNA digital coding can be encoded by four kind of base as shown in table 1. That is ADENINE (A) and THYMINE (T) or CYTOSINE (C) and GUANINE (G). There are possibly 4!=24 pattern by encoding format like (0123/ATGC) .

Table 1. DNA Digital Coding [3]

Table 1. DNA Digital Coding

Binary value	DNA digital coding
00	A
01	T
10	G
11	C

C. AES

Advanced Encryption Standard(AES Rijndael) is asymmetric encryption technique and it was created by Joan Daemon and Vincent Rijmen [6]. It is a strong and secure encryption algorithm. AES uses the encrypted symmetric key or secret key to encrypt and decrypt a message; therefore it is necessary to utilize the same secret key for both the sender and receiver.[2]

D. Blowfish

Blowfish is a symmetric encryption technique [7]. It takes key size from 32 bits to 448 bits and utilizes a similar key both for encryption and decryption. This is ideal for securing data and it was developed by Bruce Schneier in 1993. It contains 16 rounds and each round comprises of an XOR
Operation and has encryption and key expansion technique [2].

E. RSA Public Key Cryptography

RSA can be used for key exchange as well as digital signatures and the encryption of small blocks of data. Today, RSA is primarily used to encrypt the session key used for secret key encryption (message integrity) or the message's hash value (digital signature)
To create an RSA public/private key pair, here are the basic steps:
1.) Choose two prime numbers, p and q. From these numbers you can calculate the modulus, n = pq.
2.) Select a third number, e, that is relatively prime to (i.e., it does not divide evenly into) the product (p-1)(q-1). The number e is the public exponent.
3.) Calculate an integer d from the quotient (ed-1)/[(p-1)(q-1)]. The number d is the private exponent.

Scheme	Algorithm Type	Contributor	Key Length	Rounds	Block Size
AES	Symmetric	Rijndael	128,192, 256	10 or 12 or 14	128 bits
DES	Symmetric	IBM 75	56-bits	16	64 bits
3DES	Symmetric	IBM 78	168, 112 bits	48	64 bits
BLOWFISH	Symmetric	Bruce Schneier 93	128-448 bits	-	64 bits
RC4	Symmetric	Ronald Rivest 87	40-128-bits	-	-
RSA	Asymmetric	Rivest,Shamir, Adleman 77	1024	1	Minimum 512 bits
DSA	Asymmetric	NIST 91	-	-	-
Diffie-Hellman	Asymmetric	Diffie, Hellman 76	-	-	-
EI-Gamal	Asymmetric	Elgamal 84	-	-	-
Paillier	Asymmetric	Paillier 99	-	-	-
MD5	Hashing	Rivest 91	128	-	512 bit
MD6	Hashing	Prof. Rivest 08	-	-	-
SHA	Hashing	NIST 95	160	-	-
SHA256	Hashing	-	256	-	32 bit

Table 2. Characteristics of cryptography algorithm

II. LITERATURE SURVEY

As per above we can understand what kind of basic technique we have to protect our data and why it is used. It is tested standard cryptographic algorithm excluding DNA technique. Now some more technique we observer in research paper which purposed by researcher we can categorized it in 4 types

1) Pure new cryptography algorithm
2) Hybrid cryptography algorithm
3) Multi layer pure cryptography algorithm
4) Multi layer hybrid cryptography algorithm

Pure new cryptography is combination of new code and mathematic functions, P-box, S-box and XOR logical operation and functions. Like DNA technique is an example. Hybrid cryptography algorithm is combination of standard algorithm made new one algorithm. Multi layer pure cryptography algorithm more than one new algorithm used. Multi layer hybrid cryptography algorithm more than one algorithm standard as well as new cryptography used to make secure environment. Now have some look about recent researches or review papers as given in below table .3

Table 3 Review Papers

Author(s)	Year	Encryption Scheme	Steganography Scheme	Merits	Demerits
S.M Masud Karim,et al [11]	2010	"Encryption using Secret Key"	"Modified LSB substitution Steganography"	Higher PSNR Value and good security	High time complexity. key has to be chosen properly, Low embedding capacity
Shailender gupta et al[12]	2012	"RSA"	"LBS substitution Steganography"	Moderate PSNR, High security. High key Space	High time complexity. limited embedding capacity
R. Nivedhitha, et al	2012	"DES"	"LSB"	Moderate PSNR	High time complexity. limited embedding capacity, low Security and key space

Shingote Parshuram N, et al	2014	“AES”	“LBS substitution”	Higher PSNR value and good Security	High time complexity. limited embedding capacity
Md.Rashedul Islam,et al[13]	2014	“AES”	“LBS substitution using status bit Steganography”	Good PSNR value and good Security	High time complexity. limited embedding capacity
Divya chaudhary,et al [14]	2016	“Visual Cryptography”	“LBS substitution using status bit Steganography”	Higher PSNR and good embedding capacity as Huffman compression is used	High time complexity. limited embedding capacity

III. Conclusion Further Work

we can be produce good performance and effective data security through multi layer hybrid algorithm, multi layer provide strength against high computation power and hybridization makes more complex to hacker, further work is to find standard algorithm and new but reliable and implementable algorithms and make new multi layer hybrid algorithm.

IV. REFERENCES

1. “Comparative analysis onthe performance of selected securit y algorithms in cloud computing”.
Ronald S. Cordova ; Rolou Lyn R. Maata ; Alrence S. Halibas ; Rula Al-Azawi 2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA)Year: 2017 | Conference Paper | Publisher: IEEE

2. “Implementation of DNA cryptography in cloud computing and using socket programming ”.
Prajapati Ashishkumar B. ; Prajapati Barkha 2016 International Conference on Computer Communication and Informatics (ICCCI) Year: 2016 | Conference Paper | Publisher: IEEE

3. “A novel DNA sequence dictionary method for securing data in DNA using spiral approach and framework of DNA cryptography”
Shipra Jain ; Vishal Bhatnagar 2014 International Conference on Advances in Engineering & Technology Research (ICAETR - 2014) Year: 2014 | Conference Paper | Publisher: IEEE

4. “DNA Sequence Based Medical Image Encryption Scheme”
Jan Sher Khan ; Jawad Ahmad ; Saadullah Farooq Abbasi ; Arshad ; Sema Koc Kayhan 2018 10th Computer Science and Electronic Engineering (CEEC) Year: 2018 | Conference Paper | Publisher: IEEE

5. “An efficient implementation of SHA processor including thr ee hash algorithms (SHA-512, SHA-512/224, SHA-512/256) ”
Sang-Hyun Lee ; Kyung-Wook Shin 2018 International Conference on Electronics, Information, and Communication (ICEIC) Year: 2018 | Conference Paper | Publisher: IEEE

6. “Avoiding Data Replication in Cloud Using SHA-2”
R. Raju ; S. Aravind Kumar ; R. Manikandan 2018 International Conference on Computation of Power, Energy, Information and Communication (ICCPEIC) Year: 2018 | Conference Paper | Publisher: IEEE

7. “Failure Management for Reliable Cloud Computing: A Taxonomy, Model, and Future Directions”
Sukhpal Singh Gill ; Rajkumar Buyya ,Computing in Science & Engineering Year: 2020 | Volume: 22, Issue: 3 | Magazine Article | Publisher: IEEE

8. “Failure Management for Reliable Cloud Computing: A Taxonomy, Model, and Future Directions”
Sukhpal Singh Gill ; Rajkumar Buyya
Computing in Science & Engineering
Year: 2020 | Volume: 22, Issue: 3 | Magazine Article | Publisher: IEEE

9. “Modified AES using Dynamic S-Box and DNA Cryptograp hy”
Y. Bhavani ; Sai Srikar Puppala ; B.Jaya Krishna ; Srija Madarapu 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)
Year: 2019 | Conference Paper | Publisher: IEEE

10. “A DNA cryptographic technique based on dynamic DNA en coding and asymmetric cryptosystem”
Md. Rafiul Biswas ; Kazi Md. Rokibul Alam ; Ali Akber ; Yasuhiko Morimoto 2017 4th International Conference on Networking, Systems and Security (NSysS)
Year: 2017 | Conference Paper | Publisher: IEEE

11. “A new approach for LSB based image steganography using secret key”
S. M. Masud Karim ; Md. Saifur Rahman ; Md. Ismail Hossain 14th International Conference on Computer and Information Technology (ICCIT 2011)
Year: 2011 | Conference Paper | Publisher: IEEE

12. “A Robust Multilevel Security Mechanism against Geometric Attacks”
Yamini Jain ; Sangeeta Dhall ; Shailender Gupta 2019 3rd International Conference on Recent Developments in Control, Automation & Power Engineering (RDCAPE)
Year: 2019 | Conference Paper | Publisher: IEEE

13. ”Design and implementation of block cipher in hummingbird algorithm over FPGA”
Shumit Saha ; Md. Rashedul Islam ; Habibur Rahman ; Mehadi Hassan ; A. B. M. Aowlad Hossain
Fifth International Conference on Computing, Communications and Networking Technologies (ICCCNT)
Year: 2014 | Conference Paper | Publisher: IEEE

14. “Analytical study of load scheduling algorithms in cloud computing”
Divya Chaudhary ; Bijendra Kumar
2015 International Conference on Parallel, Distributed and Grid Computing
Year: 2015 | Conference Paper | Publisher: IEEE

15. "An Overview of Cryptography" Gary C. Kessler https://www.garykessler.net/library/crypto.html