Review on Approaches of Optimizeencryption for Cloud Data

Chimpy Salgotra[1], Mohit Marwaha[2], Sanjeev Mahajan[3]
Student, Assistant Professor, Associate Professor
[1]Student,
Pathankot, India

Abstract- Encryption is an essential strategy for ensuring significant electronic data. Encryption is the way toward encoding a message so as to conceal its substance. Current cryptography incorporates a few secure algorithms for encoding and decoding messages. They are all together in light of the utilization of insider facts called keys. A cryptography key is a parameter utilized as a part of an encryption algorithm such that the encryption can't be turned around without the information of the key. Review on It runs DES three times on the information in three stages: scramble, unscramble, and then encode once more. It really doesn't give a triple increment in the quality of the cipher (in light of the fact that the principal encryption key is utilized twice to scramble the information and then a moment key is utilized to encode the aftereffects of that procedure), yet despite everything it gives a compelling key length of 168 bits, which is bounty solid for all employment.

Keywords- cryptography, DES, encryption, cloud

I. INTRODUCTION

Today, cloud computing is considered to be a progressive area that supply dynamically flexible services and on interest over the internet along virtualization of hardware and software.

Cloud computing presents privacy involve because the service provider can outbreak the data that is in the cloud at any time. It could purposely delete the information. In a cloud, provider shared platform by various users there may be a probability that information belonging to distinct clients resides on similar data server. Therefore information escaped by mistake when one customer information is given to another.

There are various kinds of security issues associated with cloud computing but fall into two broad categories:

- Security issues faced by cloud providers' alike organizations providing software, infrastructure as a service via the cloud.
- security issues experienced by their customers (organizations who store data on the cloud)

Cryptography in the cloud allows for securing critical data beyond your corporate IT environment, where that data is no longer under your control. Cryptography expert Ralph Spencer Poore explains that "information in motion and information at rest are best protected by cryptographic security measures. In the cloud, we don't have the luxury of having actual, physical control over the storage of information, so the only way we can ensure that the information is protected is for it to be stored cryptographically, with us maintaining control of the cryptographic key."

Encryption is an essential strategy for ensuring significant electronic data. Encryption is the way toward encoding a message so as to conceal its substance. Current cryptography incorporates a few secure algorithms for encoding and decoding messages. They are all together in light of the utilization of insider facts called keys. A cryptography key is a parameter utilized as a part of an encryption algorithm such that the encryption can't be turned around without the information of the key.

Encryption Techniques used for data security:

- Symmetric encryption
- Asymmetric encryption

Mostly used encryption algorithms are following:-

Data Encryption Standard (DES)

DES is the first standard that the U.S. government started advancing for both government and business utilize. Initially thought to be for all intents and purposes unbreakable in the 1970s, the expansion in power and lessening in the cost of figuring has made its 56-bit key practically outdated for exceptionally delicate data. Be that as it may, it is as yet utilized as a part of numerous business items and is viewed as satisfactory for bringing down security applications. It likewise is utilized as a part of items that have slower processors, for example, savvy cards and mechanical gadgets that can't procedure a bigger key size.

Triple DES

Triple DES, or 3DES as it is now and again composed, is the more up to date, the enhanced variant of DES, and its name suggests what it does. It runs DES three times on the information in three stages: scramble, unscramble, and then encode once more. It really doesn't give a triple increment in the quality of the cipher (in light of the fact that the principal encryption key is utilized twice to scramble the information and then a moment key is utilized to encode the aftereffects of

that procedure), yet despite everything it gives a compelling key length of 168 bits, which is bounty solid for all employment.

RC4, RC5, and RC6

This is an encryption algorithm created by Ronald Rivest, one of the engineers of RSA, the main business utilization of open key cryptography. Enhancements have been set aside a few minutes to make it more grounded and fix minor issues. The present adaptation, RC6, permits up to a 2,040-piece key size and variable square size up to 128 bits.

II. RELATED STUDY

A) AES Based Approach

Aghili et al proposed security algorithm which is based on the blowfish algorithm solves the issue of deduplication in the cloud security. This algorithm worked on the 20mb block size as compared to traditional security algorithm. The failure time of the blowfish algorithm as compared to DES and AES is less. This algorithm provides the effective security to the original data[1]. Liu, Jia, et al. formulated the optimization approaches by using mixed encryption system for data security. In this work mix column and inverse mix column operation is applied on the finite field and consumes the same resources in encryption and decryption. The hybridization of AES and RSA gives optimized results with high speed and effective feasibility [2].

Gadelha, Mikhail YR et al. presented another technique for information encryption utilizing pictures that investigate the arbitrary spatial circulation of pixel dark levels of a picture. For the technique test, text messages were made in Portuguese. Despite the fact that the scrambled message sizes got with the proposed technique are bigger than the comparing sizes acquired with other conventional strategies, for example, AES and RSA, the proposed strategy has the benefit of creating an alternate encoded document each time it is utilized to scramble a similar message [3].

B) RSA Based Approach

Rahman, Mostafizur, et al. exhibited the outline and usage of a RSA crypto quickening agent. The intention is to exhibit a productive equipment execution system of RSA cryptosystem utilizing standard algorithms and HDL based equipment outline philosophy. The paper will cover the RSA encryption algorithm, Interleaved Multiplication, Miller Rabin algorithm for primality test, broadened Euclidean math, non-reestablishing division and Verilog HDL based equipment execution in FPGA gadget of the proposed RSA count design. The consequences of quick executions of RSA engineering utilizing Xilinx's Virtex FPGA gadget are introduced and examined. At long last, conclusion is drawn, which features the upsides of a completely adaptable and parameterized outline [4].

Patidar, Ritu, et al. recommended another algorithm idea to presents the altered type of RSA algorithm so as to accelerate the execution of RSA algorithm amid information trade over the system. This incorporates the structural plan and upgraded type of RSA algorithm using third prime number so as to make a modulus n which is not effortlessly decomposable by gatecrashers. A database framework is utilized to store the key parameters of RSA cryptosystem before it begins the algorithm. The proposed RSA technique is contrasted and the first RSA strategy by some hypothetical angles. Relative outcomes give better security proposed algorithm [5]. Wang, Hongjun, et al. presented the fundamental number speculations of RSA cryptosystem and applies to the key algorithm of RSA cryptosystems, for example, Euclidean and its augmentation hypothesis, square-duplicate algorithm and prime number testing. Finally, gives a depiction of Matlab reenactment of the key algorithm and RSA encryption and unscrambling. The outcome demonstrates that the entire reproduction took 0.140176s, and tackles the issue of key transmission [6].

C) Deffie Hellman Based Approach

NehaTirthani et al interpreted about cloud security problem and then proposed a security model for cloud in which Deffie Hellman Key Exchange and Elliptical Curve Cryptography algorithms are used. The whole model is explained in four steps in which first step develops connection, the second is account formation, third is verification and last step composed of data exchange [7]

D) Other Approaches

Bansal, Viney Pal et al. exhibited a mixture Cryptosystem utilizing RSA and Blowfish algorithm. This half and half cryptosystem are considered for distributed computing where the advanced mark is a must for client verification. In this way, this system gives highlights of both symmetric and uneven cryptography. Likewise, blowfish is unpatented, so this cryptosystem is additionally taken a toll effective. The FPGA gadget Virtex-4 is utilized for execution utilizing Xilinx ISE 14.1 [8].

Dhakar, Ravi Shankar et al. RSA is an outstanding open key cryptography algorithm. It is the primary algorithm referred to be appropriate for marking and in addition encryption and was one of the principal incredible advances in broad daylight key cryptography. The security of the RSA cryptosystem depends on two scientific issues: the issue of considering extensive numbers knows numerical assault and the issue of attempting all conceivable private keys know beast constrain assault. So to enhance the security, this plan shows another cryptography algorithm in light of added substance homomorphic properties called Modified RSA Encryption Algorithm (MREA). MREA is secure when contrasted with RSA as it depends on the figuring issue and also decisional composite residuosity

suspicions which are the recall citrance speculation. The plan is an added substance homomorphic cryptosystem, this implies, given just people in general key and the encryption of m1 and m2, one can register the encryption of m1 + m2. This plan likewise exhibits examination amongst RSA and MREA cryptosystems as far as security and execution [9].

Sabri, SharizalFadlie, et al investigated the improvement of CDM that depends on useful necessity through the safety effort is not considered right now. This paper clarifies the engineering of CDM and how the security will be actualized on the frameworks. RSA algorithm is picked as the encryption strategy which will be connected to the framework. Recreation result demonstrates that this system is possible for the specified execution [10].

Shakeeba et al. proposed an approach, a work plan to eradicate that involve with regards to data privacy using cryptographic algorithms to advance the security in cloud as per distinct approach of cloud customers. Advantages of cloud storage are easy approach to your knowledge anyplace, anyhow, anytime, scalability, cost efficiency, and high reliability of the data. Because of these advantages each and every organization is adopting cloud, means it uses the storage service provided by the cloud provider. So there is a requirement to safeguard that data against unrecognized access, changes or denial of services etc. To protect the Cloud means to secure the calculations and storage [11]

III. INFERENCES FROM LITERATURE REVIEW

Author Name	Publishing Year	Algorithm	Outcomes
Aghili, et al	2019	AES Algorithm	Reduces the Failure time
Liu, Jia, et al	2017	AES Algorithm	Provides optimized and feasible results at high speed
Gadelha et al.	2012	AES Algorithm	The proposed strategy has the benefit of creating an alternate encoded document each time it is utilized to scramble a similar message
Rahman et al.	2013	RSA Algorithm	FPGA gadget are introduced and examined. Features the upsides of a completely adaptable and parameterized outline
Patidar, et al.	2013	RSA Algorithm	The proposed RSA technique is contrasted and the first RSA strategy by some hypothetical angles. Relative outcomes give better security proposed algorithm.
Wang, Hongjun, et al	2013	RSA Algorithm	Tackles the issue of key transmission.
NehaTirthani et al.	2015	Deffie Hellman Algorithm	The whole model is explained in four steps in which first step develops connection, the second is account formation, third is verification and last step composed of data exchange.
Bansal et al.	2012	FPGA	This cryptosystem is additionally taken a toll effective. The FPGA gadget Virtex-4 is utilized for execution utilizing Xilinx ISE 14.1
Dhakar, et al.	2015	Modified RSA Encryption Algorithm	Provides the effective security to the systems due to hybridization of RSA algorithm.
Sabri, SharizalFadlie, et al.	2015	CDM Algorithm	RSA algorithm is picked as the encryption strategy which will be connected to the framework. Recreation result demonstrates that this system is possible for the specified execution.
Shakeeba et al.	2015	Review of cryptographic algorithms	Advantages of cloud storage are easy approach to your knowledge anyplace, anyhow, anytime, scalability, cost efficiency, and high reliability of the data.

IV. CONCLUSION

The security of the RSA cryptosystem depends on two scientific issues: the issue of considering extensive numbers knows numerical assault and the issue of attempting all conceivable private keys know beast constrain assault. So to enhance the security, this plan shows another cryptography algorithm in light of added substance homomorphic properties called Modified RSA Encryption Algorithm (MREA). MREA is secure when contrasted with RSA as it depends on the figuring issue and also decisional composite residuosity suspicions which are the recall citrance speculation.

V. REFERENCES

[1]. Aghili, Hamed. "Improving Security Using Blow Fish Algorithm on Deduplication Cloud Storage." *Fundamental Research in Electrical Engineering*. Springer, Singapore, 2019. 723-731.

[2]. Liu, Jia, et al. "Optimization of AES and RSA Algorithm and Its Mixed Encryption System." *International Conference on Intelligent Information Hiding and Multimedia Signal Processing*. Springer, Cham, 2017.

[3]. Gadelha, Mikhail YR, Cicero Ferreira Fernandes Costa Filho, and MarlyGuimarãesFernandes Costa. "Proposal of a cryptography method using gray scale digital images." *Internet Technology And Secured Transactions, 2012 International Conference for*. IEEE, 2012.

[4]. Rahman, Mostafizur, Iqbalur Rahman Rokon, and Miftahur Rahman. "Efficient hardware implementation of RSA cryptography." *Anti-counterfeiting, Security, and Identification in Communication, 2009. ASID 2009. 3rd International Conference on*. IEEE, 2009.

[5]. Patidar, Ritu, and RupaliBhartiya. "Modified RSA cryptosystem based on offline storage and prime number." *Computational Intelligence and Computing Research (ICCIC), 2013 IEEE International Conference on*. IEEE, 2013.

[6]. Wang, Hongjun, et al. "Key generation research of RSA public cryptosystem and matlab implement." *Sensor Network Security Technology and Privacy Communication System (SNS & PCS), 2013 International Conference on*. IEEE, 2013.

[7]. NehaTirthani, GanesanR,"Data Security in Cloud Architecture Based on diffie Hellman and Elliptical Curve Cryptography," International Association for Cryptologic Research, Nov 2013.

[8]. Bansal, Viney Pal, and Sandeep Singh. "A hybrid data encryption technique using RSA and Blowfish for cloud computing on FPGAs." *Recent Advances in Engineering & Computational Sciences (RAECS), 2015 2nd International Conference on*. IEEE, 2015.

[9]. Dhakar, Ravi Shankar, Amit Kumar Gupta, and Prashant Sharma. "Modified RSA encryption algorithm (MREA)." *Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on*. IEEE, 2012.

[10]. Sabri, SharizalFadlie, et al. "Implementation of security in computer designated mode system." *Digital Information Processing and Communications (ICDIPC), 2015 Fifth International Conference on*. IEEE, 2015.

[11]. Shakeeba S. Khan ,Prof.R.R. Tuteja, Security in Cloud Computing using Cryptographic Algorithms, Vol. 3, Issue 1, January 2015