A REVIEW ON HYBRID ENCRYPTION IN CLOUD COMPUTING

Lalit Kumar
Department of Computer Science & Engineering
Kamla Nehru Institute of Technology
Sultanpur, India
lalitkmr170@gmail.com

Dr. Neelendra Badal
Department of Computer Science & Engineering
Kamla Nehru Institute of Technology
Sultanpur, India
n_badal@hotmail.com

Abstract - In today world scenario, user wants to keep our data in storage as well as on cloud, so in cloud user uses cloud storage. To provide security to cloud storage user uses hybrid encryption instead of single encryption algorithm. In this paper user provides some previous information about that types of works and the major focus of user is on the hybrid approach of AES and FHE. This hybrid approach helps the user to keep data into more redundant and secure in comparisons of some other. By using this method, user can protect data confidentiality, privacy and integrity from the hackers. In this methodology section of this paper user also discuss about its working by using flow chart and algorithm to understand this approach properly.

Keywords- Cloud computing, Encryption, Decryption, Cipher Text, Hybrid encryption

I. Introduction

In today world scenario technology gets positive effect on human life. The mainly person follow the scenario where every people want to communicate to each other using various technologies. This extension of technology has also reached at offices, industries & other places. The Employee & manager have not need to work on the old file system. By using this they can sparse the information & take advantage of it quickly. By this they can attend meeting in absentia your physical presence. This enhancement in the technology has also risen up by using the computing tools. In the business world, to meet up with the present scenario of technology user uses latest technology trends. They urge to advancement of their existing system. Advancement in the hardware system is more costly & time taken especially for small industries & companies. For all users need cloud computing to overcome from these difficulties.

Cloud computing is basically defined as a computing process where user store, manage & process the data by remote servers on the internet rather than a local server on your own computer. Cloud computing is basically use a shared pool of information i.e. used by any people. Cloud computing also provides various models to provide security and protect the information from the other people. Cloud helps to store & manage more data by using cloud storage. Cloud computing is also provide an easy way to share information among between each other remotely.

Cryptography is a method also named as "code creation", which makes an interpretation of a set of information into another set of encrypted data which is not accessible and readable by everyone i.e. it contains a private and public by using this user protect the details from other. Only that person can access this information which has key for that particular encrypted data set and then it will decode the data to access and make readable information. User can categorize it into two parts as Symmetric and Asymmetric cryptographic process on the basis of key distribution.

1.) Symmetric Key Cryptography- In this cryptography process common key is applied by the sender and receiver for encryption and decryption. Here key is applied for encrypt data into cipher text and the receiver uses the same key for decode the cipher text into Normal text. Here sender creates a private key and by using this private key sender encrypt all data. After this all data send to the receiver then the receiver receives the encrypt data and decrypt the data by using the same private key.

2.) Asymmetric Key Cryptography- In this cryptography process, here user uses two key i.e. private and public key for encoding and decoding of the information. A Public key is that type of key which is used by everyone to decrypt the information from the encrypted data. Whereas the private key is known by only the authorized people who can perform decryption of cipher text to gets back the

978-1-7281-1253-4/19/$31.00 © 2019 IEEE

same data. So both private and public key plays an important role in asymmetric key cryptography.

With advancements in computer technology, providing security becomes more important task due to the increase of information. So consider this issue to propose a new group hash function based enhanced and maintain integrity and security of entire data security. It manages trust node for different resources to provide security and integrity. Here user basically uses a hash algorithm that is used to convert the plain password into hash function and it is not reversible into plain text. But attackers uses brute force attack to deduct the password and they succeeded after some iteration due to some possible combination. So user used hybrid approach. The Hybrid approach helps to keep data more secure instead of using a single algorithm. By using this hybrid approach user create a hash function which can’t be easily cracked by using various methods because it makes the data more complex. Now days the hybrid encryption is used on cloud for securing data of military system, banking data, hospital etc over the internet [16] [17].

By using this paper user proposed a hybrid encryption procedure to secure the touchy and secret information of cloud server from any malevolent action and unapproved client get to. Utilization of symmetric key cryptography makes this process quick and proficient.

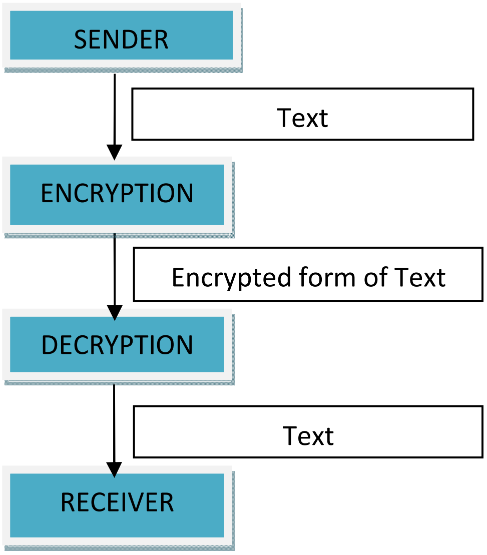

Figure 1:- process of encryption and decryption

(A.)Encryption

Encryption process changes primary data into encoded data with aid of Blowfish estimation. Blowfish computation is a symmetric key cryptography process which uses private key to scramble the data and send this key with encoded data to the other one to decode it (Figure 1). The risk related with symmetric cryptography is moving of private key over the web. To prevent from this risk of symmetric key cryptography [6], R S A computation is applied which is an asymmetric key cryptography system.

The Blowfish encryption process is liable for scramble of the data i.e. picked by customer. Blowfish is a symmetric key cryptographic process which exercises a key to encode and decode the data. That type of a key knows as private key. The private key is passed with encoded data over the web to decrypt the data by using private key. That private key is encoded using RSA figuring, which is an awry cryptographic computation. For encryption and decryption, RSA encryption algorithm uses unmistakable key.

SHA2 encryption algorithm helps to the assistance of Digital signature. For safe and efficient communication and endorsement, digital signature is applied. Propelled check ensures that data is endorsed by confirmed individual; it isn't changed by any third party in the midst of data communication. Secret key is applied for digital signature during the communication for message authentication. The message authentication is done by enforcing Secure Hash Algorithm-2on encoded customer data.

(B.) Hybrid encryption Techniques

There are many encryption algorithm by which user creates some hybrid encryption schemes that are discussed below:-

In early 2012, Gupta & Sharma discussed about the Asymmetric encryption i.e. the best way to protect information in storage or information communication over the internet into existence of a third party. The Researcher discussed about a new hybrid encryption scheme by integrating Diffie Hellman and RSA to get data security for the services of cloud. The idea of this integration is to exploit secret key cryptography includes that are encoding, decoding process speed and public key cryptography includes that is management of key. Diffie Hellman is an aged encryption technique utilized for security in protocols over internet. Along these lines, the investigators utilize this innovation since it can subtly trade information over the general population arrange in absentia public obstructions. This technology additionally bolsters a few protocols, including Secure Shell, Secure Sockets Layer and Internet Protocol Security. Sharma & Gupta [11] focused on the properties on building up a protected transmission medium between two people or clients that have never seen and met to each other which can be

978-1-7281-1253-4/19/$31.00 © 2019 IEEE

compared to client and the service provider of cloud computing. Security of the hybrid encryption stands in RSA's arbitrary prime number choice and it is outstanding that the likelihood of speculating two prime numbers is constrained to 0%. It is also instantaneous for the confirmation i.e. lacking in Diffie Hellman encryption Anyway the hybrid encryption is defenseless against agent assault, in the event that the cloud supplier representatives utilize many harmful applications incidentally. Although a few DRM plans have been being used in cloud computing, the reality remains these plans are as yet inclined to assault from inside the framework, where harmful workers in industry area can re-scramble substance or substance keys to clients in absentia the learning of D R M server.

Qin-Iong, et al. addressed this problem i.e. Hybridization of proxy re-encryption with the homomorphic encryption [12]. Proxy re encryption is utilized in semi confided in conditions for security. The idea driving proposition is to utilize homomorphic encryption, especially the added substance recipe, for substance encryption and utilizing proxy re-encryption spare section over the web, consequently, isolating the substance and the substance enter in various servers and furthermore concealed the character of the clients. Clients will get content from a substance server and allowed from the allowed server endless supply of substance and substance key client check is performed. The test with this arrangement is it can work for D R M services.

Finally, Encryption technology [5] with most abnormal amount of protection can't be successful if reaction time isn't extensive quick. Information encoded and put away in the cloud should be decoded to play out specific capacities to almost certainly work on it. The Symmetric encryptions are fast in scrambling and unscrambling forms particularly A.E.S. with 128 pieces to 256 pieces and D.E.S. with 64 bit.

Rege et al. [13], they exploited procedure pace of private key encryption and proper key administration of public key encryption to develop hybrid scramble algorithm dependent on A.E.S. and RSA in Bluetooth innovation. They propose that this creation can likewise be utilized in cloud computing if the A.E.S. can utilize 256-piece of square figure with 14 encompasses for encryption. Encryption technology is penetrable to brute-force attack so D.E.S. did not use.

It is additionally seen that this creation can be utilized on big amount of records in light of its scramble procedure motion. Creating a private key from pass phrase in encryption procedure, the novel key will be utilized.

1) Advanced Encryption Standard (AES):- This standard was projected by J. Daemen and V. Rijmen [14]. They exploited the procedure speed of secret key encryption and proper key administration of common key encryption to develop hybrid encryption calculations dependent on A.E.S. and R S A in Bluetooth innovation. They propose that this creation can likewise be utilized in cloud computing if A.E.S. can utilize 256-piece of square figure with 14 cycles for encryption. D.E.S. did not utilize in light of the fact that the encryption innovation is helpless against savage power assault. It is additionally seen that this innovation can be utilized on huge documents in light of its scramble procedure speed. Creating a private key from the pass phrase, the new key will be utilized for scramble procedure.

A.) Addition of Round key performs byte-by-byte XOR operations on state matrix.

B.)The Sub Bytes performs replacement function that takes byte in state matrix and replaced with maiden byte.

C.) Moving of Rows performs organize task that turns bytes in the state matrix to left, and Mix Column performs substitution by overriding each byte with an outcome of numerical field additional an expansion of characteristics in byte areas.

2) Fully Homomorphic Encryption Scheme (FHE): - In second phase, encryption process depends on Criag. The capacity to inquiry, file and work on encoded information in absentia decoding it makes this encryption strategy one of a kind. This plan performs two tasks, added substance and multiplicative homomorphic. User will utilize just added substance calculations. At this phase, user has cipher text from the maiden scramble and private key utilized. This Cipher content and secret key will currently be encoded together by utilizing added substance homomorphic encryption [15].

II. Methodology

Hybrid cryptography strategy incorporates the integration of both asymmetric and symmetric algorithm for progressively incredible outcome. Every cryptography strategy pursues the scramble and decryption process. In encryption process, first information is changed into non-understandable format, which isn't understood easily by any person or individual. To obtain first information from figure, information decoding process is utilized. In this investigation two time encryption and decoding process is performed in light of fact that the utilization of asymmetric and symmetric process.

Year of Publication & Author Name	**Algorithm**	**Mechanism**	**Features**	**Limitation /Challenges**	**Applications**
(2012) [8] Hajji, Tebaa M., S.E., GhaziAE,	Here Homomorphic Encryption Method has been employed	Multiplicative & Addition Scheme	Assymmetric Encryption, Not need private key to find out encrypted data	Here Multiplicative is used	Basic application is Cloud Storage
(2012) [9] Saravanan, N.,Mahendiran, A,Subramanian,N. V. andSairam, N.	Here RSA Algorithm is used	-	Data is encypted with private key,Cipher text and plain text is also used	Here need more time	Cloud SQL
(2014) [10] Abhishek, P., Sunny, B.	Here RSA Algorithm is used	-	Encryption convert data in cipher text, Decryption convert the data in plain text	Takes more time to encrypt and decrypt data	-
(2014) [7] F.Zhao, Li .C, Liu .C .F.	Here Homomorphic Encryption Method has been used	Additive property Verification or multiplicative property verification	Ability to store encrypted data with CSP	It has high computational time	Cloud Storage
(2013) [12] Qin-Iong, H., Zhao-Feng, M., Yi-Xian, H., Jing-Yi, F., Xin-Xin, N.	Here proxy re-encryption & Homomorphic Encryption has been used	Here Additive Homomorphic is used	Not sharing of private key, non understandable to proxy,two phase Encryption	It Works only on D R M components like e-books musics so on.	D R M service
(2018) [16] Prachi more, Shubham Chandugade, Shaikh Mohammad Shafi Rafiq, Prof. Priya Pise	Here Attribute based encryption and byte rotation encryption is used	Combination of Attribute Based Encryption and Byte Rotation Algorithm are applied for encryption of data.	Data privacy can be acheived by adding of BRE and ABE algorithm.	user can’t work on any machine	Sharing of banking information into a secure manner on cloud
2018 [17] P. Chinnasamy, P. Deepalakshmi,	Hybrid encryption of user data by using Blowfish and enhanced RSA algorithms	Here basic operation of Blowfish and enhanced RSA algorithm is used	Minimum encryption and decryption time in comparision to other symmetric technique like Blowfish and AES	-	Securing health care data on cloud using hybrid Cryptography

(Table 1:- all paper summaries form related to previous work)

III. Security Issues

Some major issues in the cloud computing are as followed: - (Table 2)

Serial Number	**Issues of security**	**Description of security issues**
1	Data Confidentiality	Due to security reason user are wanted to read information by right people. So for this, unknown accessing and uses of information must be stopped.
2	Data Authenticity	Authenticity is affirmation that a message, exchange, or other trade of data is from the source it professes to be from. Realness includes evidence of personality. user can check realness through confirmation.
3	Data Integrity	The Security necessity in which messages ought not to get altered while exchanging among sender and beneficiary.
4	Data Authenticity	Security necessity guarantees the personality of node with which correspondence happens is certified.
5	Data Authorization	Security necessity to guarantee that data dispersal should just from approved sensors.
6	Non-	It manages re-transmitting of

	repudiation	message through a node. A node ought not to preclude re-transmitting from claiming officially sent a message.
7	Data Freshness	It manages keeping up and scattering up and coming data by sensor nodes.

(Table 2:- security issues related to cloud computing)

IV. Review on related Work

[1] Jain et al. they have proposed a hybrid cryptography algorithm utilizing a blend of two symmetric cryptographic strategy, viz International Data Encryption Algorithm (IDEA) and Data Encryption Standard (DES) to reinforce the encryption calculation. Makers are generally stressed over the security of sensitive data trade over different frameworks for example military data and Banking trades, etc.

[2] Sheik et al. displayed a hybrid encryption demonstrate utilizing a hybridization of A.E.S. and Blowfish for Confidentiality in information, Message Digest-5 for Data dependability, Elliptic Curve Diffie Hellmann Algorithm (ECDHA) for Key exchange, and Elliptic Curve Digital Signature Algorithm (ECDSA) for Digital imprint. They in like manner surveyed the Performance of Encryption computations subject to time of encryption/unscrambling and throughput.

[3] Ali et al. defined a hybrid encryption algorithm using Blowfish and A.E.S. encryption algorithm for specific application like in bank, military, big websites those control big data base, and in network companies etc. Author also examined different encryption algorithms like A.E.S., D.E.S., Blowfish Encryption algorithm and Rivest Shamir Adleman (RSA) Encryption algorithm with the aid of Statistical Tests.

[4] Rao et al. proposed a novel approach in data security for authentication, integrity and confidentiality of data which are stored on the cloud. Message Digest-5 (MD5) algorithm is used to achieve data integrity. Blowfish algorithm is applied for confidentiality in data, and Rivest Shamir Adleman (RSA) algorithm for data authentication.

[16] P. more et al. proposed a secure system for exchanging of information into an efficient manner for banking system by using Byte Rotation Encryption Algorithm and Attribute based Encryption Algorithm in additive manner.

[17] P. Chinnasamy and P. Deepalakshmi proposed hybrid encryption system for designing secure storage for healthcare data on cloud by using Blowfish and RSA. It helps to minimize encryption and decryption time in comparison to the other symmetric techniques.

V. Conclusion

Client require be prepared to deal with security issues in Cloud Computing. Hence, user have given a hybrid encryption conspire that can be utilized to ensure client's information in the cloud. This hybrid encryption permits just the approve clients to get to it. The proposed arrangement depends on Advanced Encryption Standard and completely homomorphic encryption. This has given a protected entry of information over the Internet, the dependable key age process, double encryption processes lastly check of clients. The proposed arrangement has given far reaching subtleties on how encryption technique can secure clients privately, honesty, protection, and malware assault. The proposed model has tried in cloud condition and the outcomes have contrasted and past arrangements and the discoveries have assessed as they are superior to past chosen arrangements. The proposed work has got explicit highlights by decoding in absentia private key and in fast. The future work will be the work making this work perfect with all cloud administrations which move toward becoming as a confinement in this work.

VI. References

[1] M. Jain, and A. Agrawal, "Implementation of Hybrid Cryptography Algorithm", International journal of Core Engineering & Management, Volume 1, Issue 3, pp. 1-8, June 2014.

[2] P Shaikh, and V. Kaul, "Enhanced Security Algorithm using Hybrid Encryption and ECC", IOSR Journal of Computer Engineering (IOSRJCE), Volume 16, Issue 3, pp. 80-85, May-June 2014.

[3] Ali E.Taki El_Deen, "Design and Implementation of Hybrid Encryption Algorithm", International Journal of Scientific & Engineering Research, Volume 4, Issue 12, pp. 669-673, December2013.

[4] H. Rao. Galli and Dr. P. Padmanabham, " Data Security in Cloud using Hybrid Encryption and Decryption", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 10, pp. 494-497, October-2013. Engineering Research, Volume 4, Issue 12, pp. 669-673, December2013.

[5] A. Olumide and A. Alsadoon , "A Hybrid Encryption model for Secure Cloud Computing", School of Computing and Mathematics, Sydney Study Centre Charles Sturt University Sydney, Australia, Thirteenth International Conference on ICT and Knowledge Engineering, 2015.

[6] D. Prathana Timothy and A. K. Santra, “A Hybrid Cryptography Algorithm for Cloud Computing Security”, Vellore Institute of Technology Vellore, India, 2015.

[7] F. Zhao, C. Li, C. F. Liu, "A cloud Computing security solution based on fully Homomorphic Encryption, 2014 16th International Conference on Advanced Communication Technology, pp., 2014.

[8] M. Tebaa, S.E. Hajji, AE. Ghazi, "Homomorphic Encryption method applied to Cloud Computing. Department of Mathematical and Computer Sciences," Laboratory of Mathematics, Computing and Applications Rabat, 2012.

[9] N. Saravanan, A Mahendiran, N. V. Subramanian, and N. Sairam, "An Implementation of RSA Algorithm in Google Cloud using Cloud SQL," Research Journal of Applied Sciences, Engineering and Technology, vol. 4(19),2012.

[10]A. Patial, S. Behal, “RSA Algorithm achievement with Federal information processing Signature for Data protection in Cloud Computing”, International Journal of Computers and Technology, 2012.

[11] G. Shilpi, and J. Sharma "A hybrid encryption algorithm based on RSA and Diffie Hellman," IEEE International Conference on Computational Intelligence and Computing Research, pp.I-4, 2012.

[12] H. Qin-Iong, M. Zhao-feng, Y. Yi-xian, F. Jing-yi, N. Xin-xin, "Secure and privacy-preserving DRM scheme using homomorphic encryptionin cloud computing," The Journal of China Universities of Posts and Telecommunications, vol. 20(6), pp. 88-95,2013.

[13] K. Rege, N. Goenka, P. Bhutada, and S. Mane, "Bluetooth Communication using Hybrid Encryption Algorithm based on AES and RSA," International Journal of Computer Applications (0975 - 8887) Vol. 71 (22), 2013.

[14] D. Joan, V. Rijmen, "Vincent the Design of Rijndael - AES – The Advanced Encryption Standard”, Springer, 2001.

[15] G. Craig, "A fully homomorphic Encryption Scheme," Submitted to the Department of Computer Science, University of Stanford, 2009.

[16] P. more, S. Chandugade, S. M. S. Rafiq, Prof. P. Pise, “Hybrid Encryption Techniques for Secure Sharing sensitive data for banking system over Cloud”, ICACCT, 2018.

[17] P. Chinnasamy, P. Deepalakshmi, “Design of Secure Storage for Health-care Cloud using Hybrid Cryptography”, ICICCT, 2018