WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Cloud Computing Security by Using Hybrid Cryptography Algorithm

Prof. Satish Kumar Soni[1], Saurabh Mishra[2]

[1]professor & Head of Computer Science Department, JNCT Rewa M.P. 486001 India
[2]scholar, Computer Science Department, JNCT Rewa M.P. 486001 India

ABSTRACT

Cloud Computing is a well-known and adaptable technology in today's world. Through the services, it provides clients with ease, speed, competence, and other benefits in their work environment. The cloud provides a massive data centre to manage vast amounts of data. Organizations gain from cloud computing because it allows them to manage enormous amounts of data. The most important concern in cloud computing is security, because number of customers are sharing same cloud. The goal of this research was to provide a new security approach for data protection in the cloud by utilising a hybrid cryptosystem. The present study is needed to secure data in the cloud from unwanted access or hackers during data transfer by encrypting user data. Data access control, identity management, auditing, and integration are all security concerns with cloud computing. This method also includes the Secure Hash Algorithm – 2 for data integrity. The present study concluded that the proposed method provides high security on data transmission over the internet and proper network access on demand to a shared tank of constructive computing resources, mainly net, server, and storage application.

Keywords—Blowfish;cloud-computing;cryptosystem;RSA;SHA-2.

INTRODUCTION

Cloud computing is a sophisticated technology that helps to manage data and applications on demand. Cloud computing is dependable and constant, so businesses don't have to invest in or manage their own computer infrastructure. It offers customers to resources like as software, applications, and services. Cloud computing is cost saving technology for any type or size of business and organization, just like electricity bill they have to pay for cloud computing resources based on their consumption. Cloud computing is well-known for providing on-demand network access to a pool of productive computer resources, namely the internet, servers, and storage applications. With minimal management or service provider, this may be easily provided and discharged. Most businesspeople, application developers, officers, and students now use cloud on a regular basis since it is simple and convenient.Cloud is profitable because of its characteristics like On-Demand administration, Resource pooling, Broad net access, Rapid flexibility and the most important one is Measured service in which user has to pay for services according to their service usage (just like electricity bill).

Though the cloud has numerous benefits, it also has some drawbacks, one of which being security concerns. Data access control, identity management, risk management, auditing and logging, integrity control, infrastructure, and dependency hazards are all security concerns with cloud computing. If your company is adopting cloud computing, you should send your critical data to the service provider.The possibility of sensitive information going to wrong hand is increasing due to cloud services being easily accessible and available for all. The organizations cannot take risks with their sensitive information. Hence, there is a need to resolve the security issue of cloud computing.Secure facts transmissions prevent contact lists and private electronic mail from being read by using someone other than the intended recipient, maintain firmware enhancements out of devices they do not belong in, and confirm that the sender of a chunk of information is who he says he's. The sensibility of records protection is even mandated with the aid of regulation in positive programs: inside theU.S. Electronic devices can't exchange private medical statistics with out encrypting it first, and digital engine controllers have to no longer allow tampering with the records tables used to govern engine emissions and overall performance.To solve the data security and privacy issue in cloud computing number of methodologies is introduced. There are many risks management is defined. Different ideas or solutions are applied in cloud computing. One of the solutions for data security and integrity problem is encryption.

I.Jain and Agrawal [1], have proposed a hybrid cryptography algorithm using a mix of two symmetric cryptographic approach, viz Data Encryption Standard (DES) and International Data Encryption Algorithm (IDEA) to bolster the encryption set of rules. Authors are specially involved approximately the safety of sensitive statistics switch over extraordinary networks for instance Military statistics and Banking transactions and so on.

II. Sheikh and kaul [2], added a hybrid model using a combination of encryption algorithms well referred to as Advanced Encryption Standard (AES) and Blowfish for Data Confidentiality, Message Digest-5 (MD-5) for Data integrity, Elliptic Curve Diffie Hellmann Algorithm (ECDHA) for Key trade, and Elliptic Curve Digital Signature Algorithm (ECDSA) for Digital signature. They also evaluated the Performance of Encryption algorithms based totally on throughput, and time of encryption/decryption.

III. Ali [3], defined a hybrid encryption set of rules the use of Advanced Encryption Standard (AES) and Blowfish encryption algorithm for particular utility like in bank, military, big web sites those take care of large records base, and in network organizations and many others. Author also examined

special encryption algorithms like Advanced Encryption Standard (AES), Data Encryption Standard (DES), Blowfish Encryption algorithm and Rivest Shamir Adleman (RSA) Encryption set of rules with the assist of Statistical Tests.

IV. El_etriby et al. [4], have centered on the security of records storage inside the desktop and cloud. They have supplied a assessment of the eight encryption algorithms consisting of: Advanced Encryption Standard (AES), Data Encryption Standard (DES), Triple DES (3DES), Rivest Cipher 4 (RC4) Encryption, Rivest Cipher (RC6) Encryption, Two-Fish Encryption, Blow-Fish Encryption, and MARS Encryption at laptop pc and at Amazon Elastic Compute Cloud (Amazon EC2) cloud computing surroundings. The algorithms are assessed by arbitrariness testing with the aid of utilizing NIST actual check as a part of cloud surroundings. Pseudo Random Number Generator (PRNG) is applied to finish up the maximum suitable approach.

V. Najar and Dar [5], have proposed efficient, hard and at ease hybrid encryption algorithm design with the assist of Symmetric key set of rules like Advanced Encryption Standard (AES) and Asymmetric key algorithm like Rivest Shamir Adleman (RSA) set of rules that's accountable for control of key, and Secure Hash Algorithm-1 (SHA-1) used for virtual signature.

VI. Shereek et al. [6], provide a technique via using the Rivest Shamir Adleman (RSA) algorithm and Fermat's theorem to construct a secure environment for cloud computing. Authors are also defined that choice of large length number of key in RSA provide the robust cryptosystem however it will increase the time of key generation and have an effect on the overall performance of RSA set of rules. Fermat's little theorem enables to increase the velocity of RSA set of rules and progressed its overall performance.

VII. Rao and Padmanabham [7], described a brand-new protection scheme for integrity, authentication and confidentiality of documents that are saved at the cloud. Message Digest -five (MD5) algorithm is used for reaching data integrity, Blowfish algorithm is used for statistics confidentiality, and Rivest Shamir Adleman (RSA) set of rules for authentication.

VIII. Sengupta [8], proposed a hybrid Rivest Shamir Adleman (RSA) set of rules to offer excessive records protection in the cloud. Author additionally finish that single RSA set of rules isn't always sufficient to cozy information on the cloud therefore Feistel Encryption Algorithm is used after RSA encryption algorithm to lessen the probabilities of guy-in-the-middle assault.

IX. Thakur and kumar [9], demonstrated that blowfish encryption set of rules is better than different Symmetric key cryptography algorithms including DES and AES. They analyzed the overall performance of DES, AES and Blowfish Encryption set of rules on the idea of different parameters including block length, key size and velocity.

X. Suresh and Prasad [10], described approximately the Cloud Computing protection troubles, attacks and a few security algorithms inclusive of Advanced Encryption Standard (AES), Rivest Shamir Adleman (RSA), and Message Digest -5 (MD- five).

XI. Seth et al. [11], is set presenting safety for the records this is to be transferred over internet in order that any intruder need to no longer exchange the statistics earlier than the intended receiver gets it. This paper proposed a new methodology wherein Token-identity is generated robotically for man or woman carrier of cloud. Authors are supplied more dependable, worthwhile and safe surroundings for cloud computing the use of automobile generated Token-identification with Digital signature. The use of above referred to approach can reduce the security threats in order that the confidentiality of facts is completed.

This paper proposed a new hybrid cryptography method to solve the records security and privacy troubles of cloud computing. The intention is to achieve safe transmission of exclusive statistics by applying hybrid encryption set of rules that's a aggregate of Blowfish symmetric and RSA uneven cryptographic algorithm, and additionally virtual signature on transmitting statistics.

2.METHODOLOGY

This new hybrid cryptography technique includes the combination of each symmetric and asymmetric algorithm for extra exceptional result. Each cryptography technique follows the encryption and decryption system. In encryption method the unique facts are converted into cipher information, which is not apprehend through any human or person. To get the unique facts from cipher data decryption manner is used. In this observe -time encryption and decryption procedure is executed because using symmetric and asymmetric set of rules.

Encryption

Encryption process converts the authentic facts into cipher information with the help of Blowfish algorithm. Blowfish algorithm is a symmetric key cryptography approach, which makes use of secret key to encrypt the original facts and send this key with encrypted data to the receiver. The risk involved in symmetric cryptography is the moving of secret key over the net. To overcome the chance of symmetric cryptography, RSA algorithm is used that is an uneven key cryptography approach.

Blowfish set of rules is chargeable for encryption of information, which is selected via the person. Blowfish is a symmetric cryptographic set of rules which uses unmarried key to encrypt and decrypt the authentic facts. This single key's referred to as secret key. Secret key is transmitted with encrypted facts over the net and consequently want to encrypt the name of the game key. This secret key's encrypted using RSA algorithm, which is an asymmetric cryptographic algorithm. RSA algorithm uses one-of-a-kindkeys for encryption and decryption.

Signature era phase offers the message authentication with the assist of Digital signature the use of SHA-2. For secure transmission and authorization, digital signature is used. Digital signature assures that the data is authorized by authenticated person; it is not modified by any third person during data transmission. Private key is used for digital signature on message digest. Message digest is produced by applying Secure Hash Algorithm-2 (SHA-2) on encrypted user data.

SHA-2 is a message digest function with a block size of 512- bit generates 256-bit message digest.

TABLE I Comparison between MD5 and SHA

Sr.No.	**ComparisonParameters**	**MD-5**	**SHA**
1	Security	LessSecure	HighSecure
2	Message DigestLength	128bits	160bits
3	Attackrequiredto find out originalmessage	2^{128} bitoperation	2^{160} bitoperation
4	Attacks to try andfindtwomessages producing thesameMD	2^{64}bitoperation	2^{80}bit operation
5	Speed	Faster, only 64iteration	Slower, required80iteration

TABLE II Comparison of SHA Functions

Sr. No.	**Algorithmand Variant**	**SHA0**	**SHA1**	**SHA2**	
1	Outputsize	160bits		256/224bits	512/384bits
2	Internalstatesize	160bits		256bits	512bits
3	Blocksize	512bits		512bits	1024bits
4	Maxmessage size	2^{64}-1bits		2^{64}-1bits	2^{128}-1bits
5	Wordsize	32bits		32bits	64bits
6	Rounds	80		64	80
7	Operations	AND,OR,XOR,shr,ROT, ADD(2^{32})		AND, OR, XOR, shr, ROT, ADD(2^{32})	AND,OR, XOR,shr, ROT, ADD(2^{64})
8	Securitybits	<34 (Collisionfound)	<63 (Collisionfound)	112 128	192 256 112 128

Table 1 and table 2, shows why SHA 2 is better than other hash algorithms such as MD 5 and SHA-1.

.

Decryption

In decryption process cipher data is converted into original data. In this cryptography method first phase is hybrid decryption phase and second phase is signature verification phase. Hybrid decryption phase is a reverse process of hybrid encryption phase. This phase is responsible for decryption of encrypted message with the help of RSA and Blowfish. First step, RSA decryption algorithm decrypts the encrypted key, which helps to get original data. Second step, with the help of decrypted key blowfish decryption algorithm decrypt the encrypted data.In signature verification phase, message digest is generated using SHA 2 to verify the signature.

3.PROPOSED ALGORITHM

EncryptionProcess

Basic function of this project is to encrypt the user data to protect data from unauthorized access or hackers in cloud at the time of data transmission also. After encryption data will convert into cipher text.

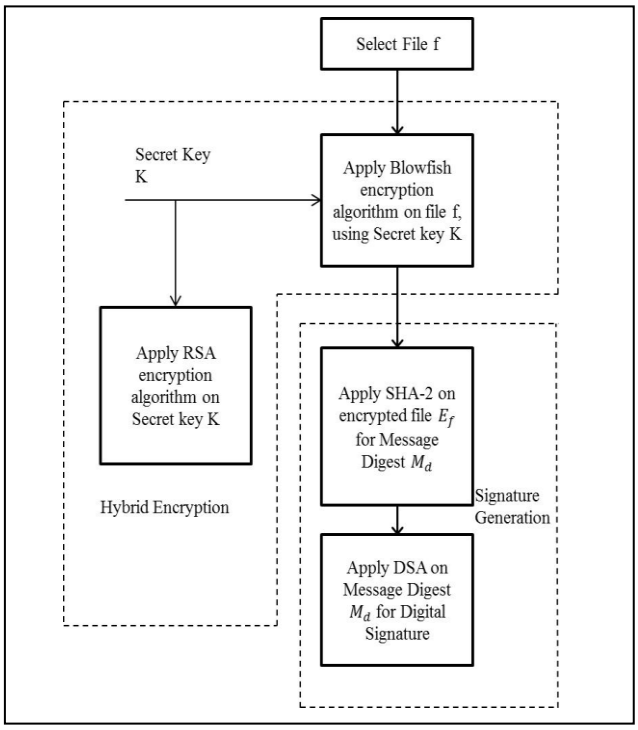


Figure1:Encryption Process

(i) Select a secret key K between the ranges of 448 bits to1024 bits of variable length.

(ii) Encrypt the selected file f, by applying Blowfish algorithm with the help of secret key. Blowfish algorithm is a symmetric key cryptographic algorithm, which uses single key to convert the original data into cipher data and vice versa. This key is known as secret key or private key. It has a 64 bit block size and the length of key is from 32 bits to 448 bits.

$$E_f = EB_K(f)$$

(iii) Encrypt the secret key K, using RSA algorithm. RSA algorithm is an Asymmetric key cryptographic algorithm, which uses pair of key for encryption and decryption.

$$E_K = ER(K)$$

(iv) Apply SHA 2 on encrypted file E_f to generate message digest or hash code. SHA stands for Secure Hash Algorithm, which is used to generate the message digest.

$$M_d = S(E_f)$$

(v) Apply digital signature algorithm on message digest to generate digital signature.

$D_S = D(M_d)$

DecryptionProcess

Decryption process converts the cipher text into original data, so that user can read or access this data. Only authorized user can decrypt the cipher text or in other word only authorized user can access the data.

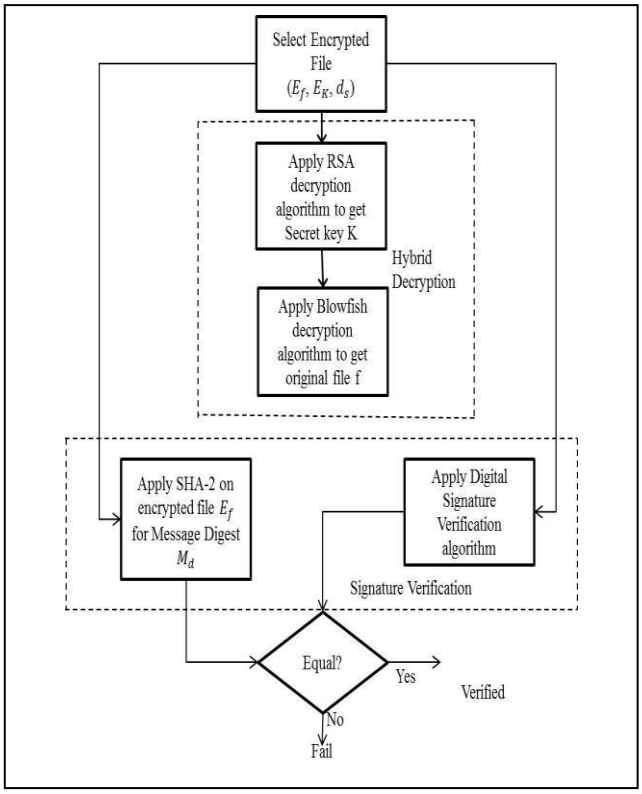


Figure 2: Decryption Process

(i) To get the secret key K, decrypt the encrypted secret key EK by applying RSA decryption algorithm.

$K = DR(E_K)$

(ii) Using above secret key, obtain the original file f, byapplying blowfish decryption algorithm on encrypted file E_f.

$f = DB_K(E_f)$

(iii) Apply verification algorithm of digital signature on digital signature on d_s to get the expected message digest or hash code.

$M_d = V(D_s)$

(iv) Compare this message digest or hash code with the SHA 2 generated message digest or hash code.

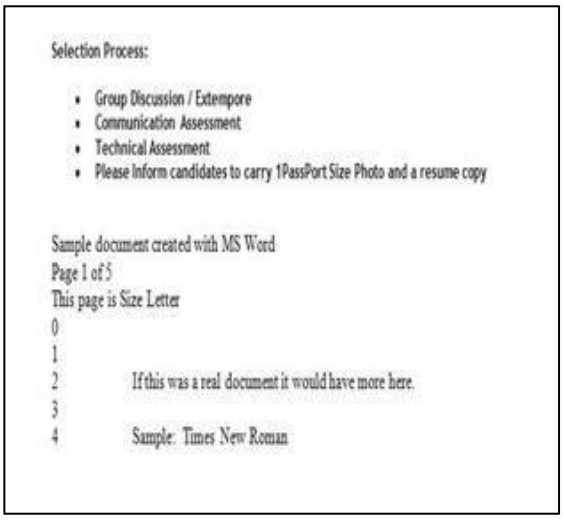
$M_d = S(E_f)$

Result and Discussion

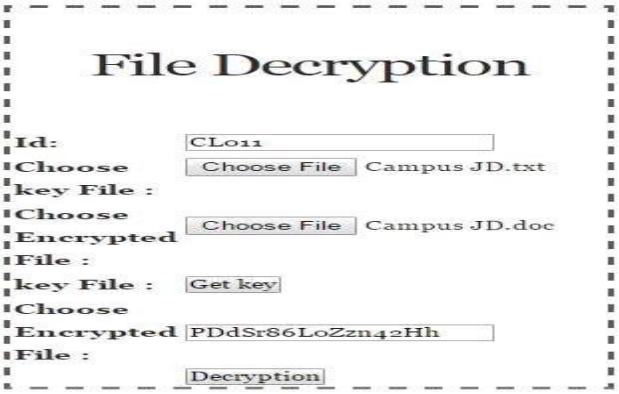
The proposed method protected the consumer records, from unauthorized access at the time of transmission and also in Amazon Simple Storage

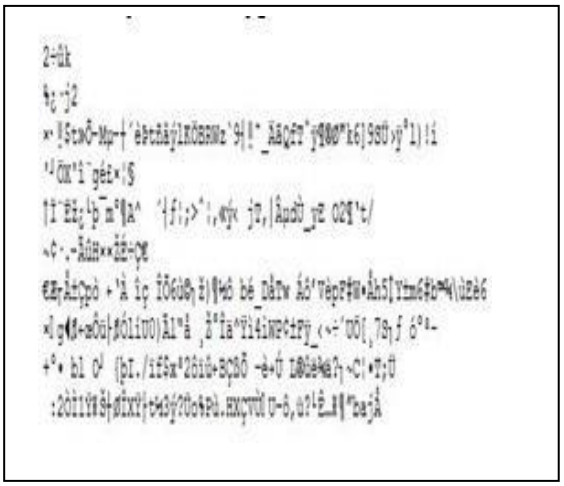
Service Bucket. Proposed system accelerated the problem level for unauthorized person or hacker to decrypt the encrypted information, via encrypted key, through RSA.

InputFile:jnc.doc



After Hybrid Encryption





4. CONCLUSION

A new hybrid cryptography algorithm is proposed using Blowfish, RSA, and SHA-2 algorithms. The combination of symmetric and asymmetric algorithm provides efficiency to proposed system. The proposed method provides high security on data transmission over the internet using SHA-2 algorithm.

.

REFERENCES

[1] Mahavir Jain, and Arpit 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 (IOSR- JCE), Volume 16, Issue 3, pp. 80-85, May-June 2014.

[3] Ali E.TakiEl_Deen, "Design and Implementation of Hybrid Encryption Algorithm", International Journal of Scientific & Engineering Research, Volume 4, Issue 12, pp. 669-673, December- 2013.

[4] Sherif El-etriby, Hatem S. Abdul-kader, and Eman M. Mohamed, "Modern Encryption Techniques for Cloud Computing", ICCIT, pp. 800-805, 2012.

[5] Jan Mohammad Najar, and Shahid Bashir Dar, "A New Design of a Hybrid Encryption Algorithm", International Journal of Engineering and Computer Science, Volume 3, Issue 11, pp. 9169-9171, November 2014.

[6] Balkees Mohamed Shereek, Zaiton Muda, and Sharifah Yasin "Improvecloud computing security using RSA encryption withFermat'slittletheorem", IOSR Journal of Computer Engineering (IOSR-JCE), Volume4,Issue2,pp.1-8, February-2014.

[7] HanumanthaRao.GalliandDr.P.Padmanabham,**"**DataSecurityinCloud using HybridEncryption and Decryption**",** International Journalof Advanced Research in Computer Science and Software Engineering,Volume3,Issue10,pp.494-497,October-2013.

[8] Dr. Nandita Sengupta, "Designing of Hybrid RSA Encryption Algorithmfor CloudSecurity",International Journal of Innovative Research inComputer and Communication Engineering, Vol. 3, Issue 5, pp. 4146-4152,May-2015.

[9] JawaharThakurandNageshKumar,"DES, AES and Blowfish:SymmetricKeyCryptographyAlgorithmsSimulationBasedPerformance Analysis", International Journal of Emerging TechnologyandAdvancedEngineering,Vol.1.Issue2,pp.06-12,December-2011.

[10] K. S. Suresh and Prof K. V. Prasad, "Security IssuesandSecurityAlgorithmsinCloud Computing", International Journal of AdvancedResearch in Computer Science and Software Engineering, Vol. 2, Issue10,pp.110-114,October-2012.

[11] R. K. Seth, RimmyChuchra and Simran, "TBDS – A New Data SecurityAlgorithminCloudComputing",InternationalJournalofComputerScience and Information Technology, Vol. 5, Issue 3, pp. 2703-2706,2014.

[12] Piyush Gupta and Sandeep Kumar, "A Comparative Analysis of SHAand MD 5 Algorithm", International Journal of Computer Science andInformation Technologies,Vol. 5, Issue3,pp.4492-4495,2014.