International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-7 Issue-4s, November 2018

Secured Cryptosystem using Blowfish and RSA Algorithm for The Data in Public Cloud

G. Sathish Kumar, K. Premalatha, N. Aravindhraj, M. Nivaashini, M. Karthiga

Abstract: ***Data Security makes the finest importance in the area of cloud computing. Cryptosystem will provide the greater security for the data in the cloud. Many encryption techniques are available for secured data storage with its own advantages and disadvantages. There is a problem of Key escrow and certificate revocation in the identity based encryption. Personality based encryption is free from security mediator. The certificate less encryption technique will overcome the key escrow issue and the certificate revocation issue. The task of key production is shared between the cloud and client in the certificateless encryption. In the proposed framework, the data holder encodes the data utilizing his/her secret key. Following that the information holder encode the secret key twice to frame a intermediate key. At that point he/she will send this encoded information and middle of the road keys to the cloud. The cloud will unscramble the middle of the road key in part and send the mostly decoded key and scrambled information to the planned beneficiary. The client will decode again the somewhat decoded information which is sent by the cloud and the client will get the required key for decoding with the goal that the client can decode it totally. The information holder can send similar information to numerous customers with least expense***.

Keywords: ***Blowfish, Cryptography, Cloud, Security, Encryption.***

I. INTRODUCTION

Cloud computing is a structure which has a typical pool of configurable assets that are utilized for enabling universal and on-ask for access that can be immediately provisioned and released with irrelevant organization effort. Cloud computing paradigm is a common term which makes use of utilities, hardware, software and infrastructure to be accessed via a network. This is done with the help of the internet which provides correspondence and transport equipment, programming and systems administrations to customers. These stages conceal the multifaceted nature and subtleties of the basic framework from clients and applications by giving extremely basic graphical interface or API. Moreover, this framework provides on interest benefits, that are dependably on, anyplace, whenever and wherever.

Manuscript published on 30 November 2018.
*****Correspondence Author(s)
Mr. G. Sathish Kumar , Assistant Professor, Department of Computer science and Engineering, Bannari Amman Institute of Technology Sathyamangalam, Erode, Tamilnadu, India.
Dr. K. Premalatha, Professor, Department of Computer Science and Engineering, Bannari Amman Institute of Technology, Sathyamangalam, Erode, Tamilnadu, India.
Mr. N. Aravindhraj, , Assistant Professor, Department of Computer Science and Engineering,Bannari Amman Institute of Technology, Athyamangalam, Erode, Tamilnadu, India.
Ms. M. Nivaashini, Assistant Professor, Department of Computer Science and Engineering, Bannari Amman Institute of Technology Sathyamangalam, Erode, Tamilnadu, India.

Hardware and software services are available to general public, enterprises, corporations and businesses markets on the pay per use and as required mode. However, these increased needs enables a path to drawbacks also. There are many security issues of the data stored on the could. Many people store part of individual data and conceivably anchored information in the cloud. So the security is the major concern in the cloud computing.

There are many encryption schemes available. ID-based encryption, or identity-based encryption (IBE), is a crude of ID-based cryptography. The identity of the client such as client's email can be used as a public key in public key encryption methodology. This implies a sender who approaches people in general parameters of the framework can encode a message utilizing e.g. the content estimation of the collector's name or email address as a key. The receiver acquires its decryption key from a authorized administrator, which should be trusted as it creates secret keys for each client. The disadvantage of ID-based encryption is Key escrow and certificate revocation problem. Certificates revocation and key escrow problems exists in the mediated certificateless method. The bilinear pairing approach is used in mediated certificate less method but our proposed system eliminates this pairing approach because the pairing is difficult and more expensive[1].

So as to give the security to the information in the cloud storage we will scramble the information before putting away into the cloud environment. The cloud environment doesn't know about the keys utilized for encoding the original data[2]. Thus the secrecy of the original information in the cloud is guaranteed. Symmetric key algorithm is the mostly used approach for encryption based access control[3].

An encryption framework in which the sender and receiver of a message share a solitary, normal key that is utilized to encode and decode the message. Balance this with public key cryptology, which uses two keys – a public key to encode messages and a private key to decode them. Symmetric-key algorithms are generally much less computationally intensive than asymmetric key algorithms. In practice, asymmetric key calculations are slower than symmetric key calculations, on the grounds symmetric key calculations we will utilize key match for encryption(public key) and decryption(private key).Even though the asymmetric algorithm is slower it yields a good result in storing and transferring the data in secured manner. One burden of symmetric-key calculations is the prerequisite of a common secret key, with the two gatherings holding a similar duplicate at each end.

So as to guarantee secure interchanges between everybody in a gathering of n individuals a sum of n(n - 1)/2 keys are required, which is the aggregate number of conceivable correspondence channels.

To constrain the effect of a potential revelation by a cryptographic assailant, they ought to be changed frequently and kept secure amid dissemination and in administration. The way toward choosing, dispersing and putting away keys is known as key administration, and is hard to accomplish dependably and safely.

Conventional open key cryptosystem utilizes a confided in Certificate Authority which will issue advanced digital certificates that typifies the general public keys with the clients. So this testament the board makes the framework to be increasingly mind boggling and furthermore excessively costly. To defeat such challenges, identity based public key cryptosystem can be utilized, however it has key escrow issue. Since the key generator can recover the private keys all things considered. Key escrow issue and the certificate revocation problem are the major concerns in the above mentioned encryption techniques. To overcome these shortcomings certificateless encryption has been suggested.

II. BASIC ENCRYPTION TECHNIQUES:

This chapter compares the basic encryption techniques which mainly focus on the symmetric key encryption In Symmetric-key calculations for cryptography, it utilizes the equivalent cryptographic keys for both encryption of plaintext and decoding of cipher content. The fundamental preferred standpoint of symmetric key encryption is that it is generally quick, and secure..

There are numerous calculations accessible identified with Symmetric-key cryptography. Secure calculations in that class are Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Blowfish calculation. Rijndael calculation is one of the Advanced Encryption Standard calculation. AES contrasts from DES in a few terms. DES has a settled square size and key size. DES is an execution of a Feistel Cipher. It uses 16 round Feistel structure. The square size is 64-bit. Be that as it may, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption computation.

The Rijndael calculation have adaptable key size and block size. A prime element of Rijndael is its capacity to work on differing sizes of keys and information squares. It gives additional adaptability in that both the key size and the square size might be 128, 192, or 256 bits. Since Rijndael indicates three key sizes, this implies there are roughly 3.4 x 1038 conceivable 128-bit keys, 6.2 x 1057 conceivable 192-bit keys and 1.1 x 1077 conceivable 256-bit keys individually. To think about, DES keys are just 56 bits in length, which implies there are roughly 7.2 x 1016 conceivable DES keys. Subsequently, they are on the request of multiple times more AES 128-bit keys than DES 56-bit keys.

Blowfish is a symmetric square assume that can be sufficiently used for encryption and safeguarding of data. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for securing data.

Blowfish Algorithm is a symmetric key square figure (Feistel Network), accentuating a clear encryption work on numerous occasions. It gives extraordinary encryption rate. The square size is 64 bits, and the key can be any length up to 448 bits. Regardless of the way that there is an incredible presentation arrange required before any encryption can happen, the real encryption of data is particularly powerful on considerable microchips. The processing Time of the blowfish algorithm will be much higher than the AES[4].Blowfish algorithm yields a better performance than the AES algorithm.

The symmetric key cryptographic technique can be used encrypting and decrypting huge amount of data. Sharing of key is the major is disadvantage of this technique. Once the key has been retrieved or known to the unknown user he/she can decrypt the whole data which is considered as a serious concern.

Elective methodology is public key cryptography which utilizes open public key and a private key. public key cryptography, or uneven cryptography, is any cryptographic framework that utilizes sets of keys: open public keys which might be dispersed generally, and private keys which are known just to the proprietor. This achieves two capacities: validation, which is the point at which open public key is utilized to confirm that a holder of the combined private key has just sent the message, and encryption, whereby just the holder of the matched private key can decode the message encoded with people in open public key. In an open public key encryption framework, any individual can encode a message utilizing people in open public key of the beneficiary, yet such a message can be decoded just with the client's private key. It should be simple for a client to produce an open and private key-match to be utilized for encryption and unscrambling. The quality of an open public key cryptography framework depends on the level of trouble (computational difficulty) for a legitimately produced private key to be resolved from its relating open key. Security at that point depends just on keeping the private key private, and the open public key might be distributed without trading off security.

We can utilize either of the keys such as public or private for encoding. If open public key is used for encoding then the plain text must be encrypted using client’s open public key. At such a case, the open public key of the client should be known to all. After that the client can utilize his private key to decode the data. In another way, one can use sender’s private key to encode the data and distribute his/her public key to the recipient. Be that as it may, both the referenced techniques need a believed outsider called certificate authority(CA). At the point when an unapproved client acquires the private key utilized for encryption then he/she can just unscramble the messages sent to the proprietor of the private key. This is preposterous on account of symmetric key cryptographic method. Significant burden of open public key framework is that the testament the executives is moderate, troublesome and costly.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Open public key encryption plot have authentication repudiation issue too. To kill this disadvantage personality based encryption has been picked. In this strategy any client can produce their open key dependent on a known character which might be an ASCII string. At that point the private key generator is utilized to produce comparing private key. Any approved client can create people in general key of different clients by utilizing the character and master key.

The upside of personality based encryption is that there is no requirement for the utilization of endorsements. Private key generator is utilized to determine the beneficiary open public key scientifically from their character and master key. As the personality based encryption is a brought together methodology, the key creator may think about the private key which is created. This is called as key escrow issue. The testament gets terminated and there is no certificate revocation issue in this strategy yet it has key escrow issue. So as to conquer this key escrow issue in this plan (personality based encryption) another technique called certificateless encryption came into the image. In this approach, the private key age process is separated between the client and the server. The general open public key isn't produced dependent on personality and furthermore the private key isn't known to center. In this way, there is zero chance for key escrow issue to happen.

III. RELATED WORKS

Rui Guo et.al, presented a paper named Certificateless Public Key Encryption Scheme with Hybrid Problems and Its Application to Internet of Things[5]. This paper manages the idea of certificateless open key encryption plan to dodge the key escrow issue. Certificateless cryptography plot goes for joining the benefits of open key cryptography and personality based cryptography to stay away from the certificate management and the key escrow issue.

S.Al-Riyami et.al, manages certificateless open key cryptography [6]. In this paper certificateless open key cryptography (CL-PKE) conspire is utilized to take care of the key escrow issue and certificate revocation issue. It doesn't require authentications and it additionally conquers the issue of implicit key escrow. The downside of the over two plan is that it depends on matching activity.Pairing based protocols are used in a variety of protocols and it is found that many applications uses pairing based protocols as the solution where ID-based cryptographic schemes and the short signature schemes are employed.

To overcome this disadvantages Y. Sun et.al, proposed a paper called Strongly secure certificateless public key encoding without blending. It gives the upside of character based open key cryptography with no key escrow issue. This work has been the primary certificateless encryption procedure without utilizing blending activity. In this paper they have demonstrated the security against adaptive chosen cipher text attack in the arbitrary model.

Sherman S. M., Colin, and Juan Manual Gozalez has given a paper named Security Mediated Certificateless Cryptography. This paper bargains about the idea of security intervened certificateless cryptography. It would have the property of immediate repudiation of keys. And furthermore it conquers the key escrow issue. This model guarantees a security against a completely versatile picked figure assailant, despite the fact that he have a a rogue key generation center. Be that as it may, the plan proposed in this paper depends on bilinear blending. It is more proficient than the character based intervened encryption method.

In identity based and security concerned systems, a third party is needed to generate the key which is termed as key escrow problem. This becomes the major disadvantage of identity based system. To eradicate this problem certificateless cryptosystem is proposed. Every entity will possess a public key but no certificate. Identity strings can be used to assure that only correct entity can have the private key with respective to its public key. Then instant revocation cannot be obtained in this case.

When considering identity based encryption method, it does not depend on security intermediator[7]. It has predefined keys and there are chances of key escrow and certificate revocation issue. Certificateless encryption methodology has removed the key escrow issue but the certificate revocation problem still prevails. In Indentity based security mediated method there is no chance for getting a certificate revocation problem. Therefore security mediated certificateless method can overcome both key escrow and certificate revocation. Also it uses bilinear method which is highly expensive. So there emerges a need for method without using pairing technique[8]. Thus, security mediated certificateless encryption can be used to preserve the data in public cloud which does not employ any pairing technique.

IV. PROPOSED METHOD

The certificate less encoding technique is the blend lying between open public key cryptography and personality based cryptography. Certificateless encoding is proposed by consolidating open public key and personality based cryptography .

In the certificateless encryption conspire customer at first makes its character based cryptography to make certificateless encryption. Client can utilize any open public key encryption calculation to create their very own personality open key and private key match. Alongside the character the general population key is send to the cloud for approval. The cloud will produce two or three open key and private key in the wake of checking the personality for the comparing client. This above phase is called as enrollment. So every client has their own open public key and the private key such as USpu, USpr and the open public key and private key created by cloud such as CLpu,CLpr respectively. Enrollment stage is trailed by the encoding stage. In this stage, if the information proprietor needs to send a few information to client, first the information proprietor will send a demand to cloud for getting the beneficiary cloud produced open public key and recipient's USpu . At the point when the information proprietor got these key, he will initially scramble the information by utilizing recipient's USpu and after that with the collector's CLpu.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

For approval, at long last encode similar information utilizing information proprietor's CLpu. The outcome is sent back to the cloud. Encryption phase is followed by cloud decoding stage.

Cloud initially unscramble the information utilizing information proprietor 's Cloud private key CLpr for verifying. Next it will decrypt using receiver's private key CLpr. After decoding send the information to the comparing client. Cloud decryption phase is followed by the client decoding stage. Finally, receiver decrypts the cipher content and extracts the plain content.

V. IMPROVED SECURE CLOUD STORAGE:

The cloud storage security can be improved by combining symmetric key encoding technique with open public key encoding technique[9]. To improve this further , each client should have a private key that can be produced using Blowfish algorithm and the CLpu, CLpr, USpu, USpr keys are generated using RSA algorithm. The data is encoded at first using Blowfish and then also encode the Blowfish key utilizing RSA. Initially, receiver's open public key Uspu is used to encrypt the key followed by the encryption of the same key utilizing the client's cloud generated key. Such a duly encrypted key is called as the intermediate key. Cipher text and intermediate key are sent to the cloud environment.

The data is decoded at first using receiver's CLpr and the partially decoded intermediate key and cipher text are sent to the client by the cloud. The intermediate keys will be decoded completely and data encoded key are obtained by the client. So it will be easy for the receiver to decrypt the cipher text.

The principle focal points of enhanced framework is that it is moderately quick contrasted with the other methodology, and it can expels the outstanding burden of information proprietors if similar information must be shared among various clients . The information proprietor scrambles similar information once on the off chance that he needs to send the information. The private key is encoded utilizing the general open public keys of the relating beneficiary.

VI. FUNDAMENTAL ALGORITHM:

The below given Algorithm portrays the step by step working of the proposed methodology. It includes cloud server setup, registration phase, encryption phase, and decryption phase.

A. Algorithm:

Data Protection Algorithm
Input: ID and Original Information
Output: Decrypted Information

a. Cloud server Setup:

a) Setup a Cloud Server
b) Start the cloud services

b. Registration Phase:

a) begin
b) read the personality (ID).
c) Utilizing RSA, generate the user public key Uspu and user private key USpr (USpu and USpr).
d) Utilizing Blowfish algorithm , generate private key S to encrypt the data.
e) Send the personality(ID) and public open key USpu to the cloud environment.
f) Cloud verifies the personality (ID) and it generates the public open key CLpu and private CLpr.
g) public open key CLpu is sent to the respective user.
h)end

c. Encryption:

a) begin
b) The personality ID of the receiver will be sent to cloud by the information proprietor.
c) In turn Information proprietor will get CLpu, USpu of recipient.
d) Information proprietor will encode the data.
e) Creation of intermediate key.
f) Pass ciphertext and intermediate key to cloud Environment.
g) end

d. Cloud Decryption:

a) begin
b) Data will be partially decoded
c) pass partially decoded data and ciphertext to intended recipient.
d) end

e. Receiver Side decryption:

a) begin
b) Pass a request to the cloud to receive the data.
c) Completely decode the intermediate key.
d) Decode the ciphertext.
e) end

VII.EXPERIMENTAL RESULTS:

In the proposed work we have compared the result of RSA algorithm, RSA with AES and RSA with Blowfish. We have found that Blowfish algorithm works better than AES in many situations.

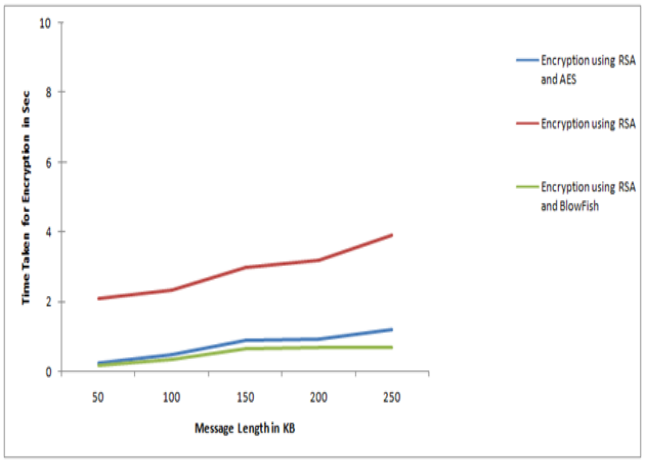

Fig 1: Encryption results with RSA, utilizing RSA with AES, and using RSA with Blowfish

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

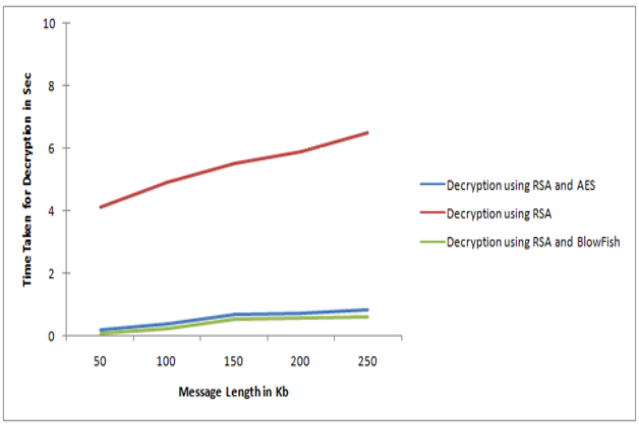

Fig 2: Decryption results with RSA, utilizing RSA with AES, and using RSA with Blowfish

VIII. CONCLUSION

This paper has come up with a technique for securing the cloud storage and sharing. This technique is implemented utilizing Blowfish algorithm and RSA algorithm. Blowfish is utilized for Data encryption and RSA is utilized for key encoding. This technique will solve the key escrow problem and certificate revocation problem. The combination of Blowfish algorithm and RSA algorithm yields the high security to the cloud storage and also comparatively faster than the existing techniques.

REFERENCE

1. Abdalla ., "Searchable encryption revisited: Consistency properties, relation to anonymousibe, and extensions", Journal of . Cryrocraphy., voloume. 21, no. 3, pp. 350391, Marrch 2008.
2. Boneh "Fine-grained control of security capabilities", ACM Trans. Internet Technol., volume.4, no.1, 6082, February. 2004.
3. E. Fujisaki et. Al., "Secure integration of asymmetric and symmetric encryption schemes". In M. J. Wiener, editor, Proceeding . Annual International Cryptology Conference Santa Barbara, 1999, volume 1666, pp.537554. Springer,1999.
4. https://www.cse.wustl. edu /~jain/cse567-06/ftp/encryption_perf/
5. Rui Guo, Qiaoyan Wen, Huixian Shi, Zhengping Jin, and Hua Zhang, Certificateless Public Key Encryption Scheme with Hybrid Problems and Its Application to Internet of Things, in Mathematical Problems in Engineering, Volume 2014, Article ID 980274.
6. S. Al-Riyami and K. Paterson, Certificateless public key cryptography, in Proc. ASIACRYPT 2003, C.-S. Laih, Ed. Berlin, Germany Springer, LNCS 2894, pp. 452473.
7. Green and G. Ateniese. Identity-based proxy re-encryption.Internzational Journal of , Applied Cryptography and Network Security Applied Cryptography and Network Security 2007, volume 42
8. S. S. M. Chow, C. Boyd, and J. M. G. Nieto, Security mediated certificateless cryptography, in Proc. 9th Int. Conf. Theory Practice PKC, New York, NY, USA, 2006, pp.508524.
9. Nubila Jaleel, Chinju, Mediated certificateless cryptosystem for the security of data in public cloud in IJRET: International Journal of Research in Engineering and Technology, eISSN: 2319-1163.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)