Enhancing the Security of User Data Using the Keyword Encryption and Hybrid Cryptographic Algorithm in Cloud

G.Prabu kanna
Kalasalingam University
Tamil Nadu, India
gpkanna@gmail.com

V.Vasudevan
Kalasalingam university
Tamil Nadu, india
vasudevan_klu@yahoo.co.in

***Abstract*— Cloud computing is a popular model for accessing the computer resources. The data owner outsources their data on cloud server that can be accessed by an authorized user. In Cloud Computing public key encryption with equality test (PKEET) provides an alternative to public key encryption by simplify the public key and credential administration at Public Key Infrastructure (PKI). However it still faces the security risk in outsourced computation on encrypted data. Therefore this paper proposed a novel identity based hybrid encryption (RSA with ECC) to enhance the security of outsourced data. In this approach sender encrypts the sensitive data using hybrid algorithm. Then the proxy re encryption is used to encrypt the keyword and identity in standardize toward enrichment security of data.**

Keywords— Proxy re encryption, Hybrid Encryption, identity based encryption, RSA, ECC.

I. INTRODUCTION

Cloud computing is extremely scalable distributed computing platform in which computing resources are offered as a service[1][2]. Cloud-based services include Infrastructure as Service, Platform as a Service (PaaS) and Software-as-a-Service (SaaS). Amazon's EC2 and S3, IBM's Blue Cloud, Microsoft Windows Azure storage services, etc., are some example of Cloud Computing Services (CSP). Indeed, these providers offer the option to store, regain and share information to their clients with supplementary users based on pay-per-use or subscription-based model. The advantages of cloud computing are dynamic provisioning, low capital expenditures, increased flexibility and economies of scale, unfortunately, in addition to its advantages it commence a variety of new security risks [3].

Providing security to the user data is a major issue in cloud computing. In order to use to the cloud computing effectively, the cloud users need the improved security solutions to store and retrieve the data. Cryptography is an effective way to product the sensitive information, the most popular traditional public key technologies called Identity-based Cryptography[4][5] has recently received considerable attention.

Identity-based Encryption (IBE)[5][6] is a modification to public key encryption. The key management is simple process using IBE that uses the human-intelligible identities such as IP address, unique name and email address, etc. and utilize the credential base Public Key Infrastructure (PKI) as public keys. User be able to in a straight line encrypts text among beneficiary identity without public key and certificate, but PKG provides the private key associated with the corresponding identity, the receiver used this private key to decrypt such ciphertext.

This paper proposed an identity-based hybrid encryption method (RSA with ECC) [7][8]for the outsourced computation on encrypted information in cloud computing. The identity based encryption is combined with hybrid RSA with ECC to encrypt the user data. In standardize to improve the security the proxy re encryption [9] is utilized to encrypt the user identity and keyword. The remaining section of this document is well thought-out as below.

The related concept and algorithm is surveyed in section II. Section III describes the proposed work in detail. The experimental result is described in section IV. Finally section V concludes this paper.

II. RELATED WORKS

RSA is a popular encryption technique used to secure the data. The encryption techniques such as ECC and proxy re-encryption are also a powerful mechanism to secure the data from adversary. This section describes some related work that uses the above mentioned encryption algorithm to provide the security for user data.

Hongbing Wang and ZhenfuCao[10] proposed a fully secure proxy re-encryption scheme. The author designed this scheme to achieve the properties such as non-interactivity, unidirectionality, collusion-safe, non-

978-1-4673-9939-5/16/$31.00 ©2016 IEEE

transitivity and multi-use. This design gives a solution to the second open problem left by Canetti and Hohenberger in [11], the novel PRE is designed based on the bilinear group.

Dan Boneh and Matt Franklin [12] fully functional identity-based encryption scheme (IBE).The security of this method based on a natural analogue assumption of the computational Diffie-Hellman on elliptic curves. Based on the above Assumption this system has a chosen ciphertext security in the random oracle model. The master-key is not at all available in a particular location due to PKG distribution.

Faraz Fatemi Moghaddam et al[13] introduced a hybrid asymmetric-key encryption algorithm based on RSA Small-e and Efficient RSA in order to provide the security in cloud computing environments. The author achieve this by increased the number of exponents to three and the security level of the algorithm is raised by applying a dual encryption process. The security analysis of original RSA and HE-RSA is investigated according to three attacks such as the Brute Force, Mathematical Attacks, and Timing attacks.

Nesrine Kaaniche et al [14] proposed a cryptographic scheme for cloud storage, based on ID-Based Cryptography. This scheme provides secrecy for encrypted data which are stored in public servers. It describes a novel approach to improve the data confidentiality in cloud storage and dynamic sharing is enhanced between the cloud users relies on the use of ID Based Cryptography (IBC), where each client acts as a Public Key Generator (PKG). This is achieved by authenticated client for their backup, data storage and sharing.

III. PROPOSED WORK

In this approach, a novel identity-based hybrid encryption method (RSA with ECC) is proposed. Our main technique is to use an identity based encryption (IBE) [15] to cover the output of public key encryption. This is achieved by hybrid encryption and proxy re encryption techniques. In this approach the sender encrypt their data using the hybrid algorithm with receiver identity (ID_i) which is then added to the encryption of receiver identity and the keyword for generating the resulting ciphertext. Proxy Re Encryption (PRE) is applied to encrypt the identity of receiver and the keyword. Ordinary, secret and top secret are the tags used as keywords. Whenever the user sends a message M with keyword K to receiver, the following data has to send to the server $E(ID_a,M)||$ $PRE(ID_a,K)$.The beneficiary be able to decrypt the ciphertext at any time, through using the decryption key according to its identity which is provided by the PKG. The following section describes the encryption of User data encryption.

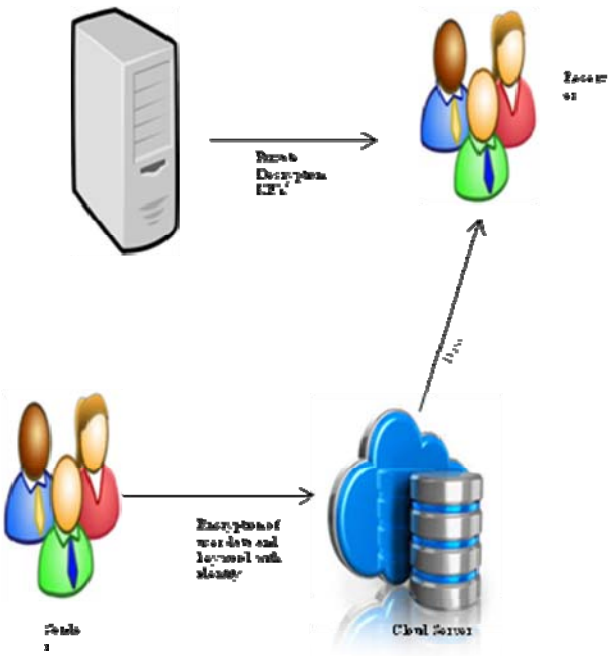

Fig.1. System Model of Proposed Approach

A. *Construction*

In this section the overall construction of proposed work is given

a) Setup:

1. Initialize the random number s and d. where s, d ∈ prime number
2. Represent E (ID_i , m) on Elliptic curve
3. For the security parameter 1^k generate the parameter

b) Extract:

1. For given id and user data generate Euler's totient

Function ϕ(u)

2. Greatest common divisor gcd (d, ϕ(u)) =1
3. Generate public and private key pair (x,y)
4. Randomly select 'd' from [1 – (n-1)]
5. Generate the public key Q = d * P
6. Generates the public and secret key pair (pk_a,sk_a)
7. Generates re-encryption key ($RK_{a \to b}$)

c) Encryption:

1. Generate the ciphertext for M= E(ID_i , m)
2. C ← M^x mod u → E(M)
3. C1 = d*P
4. C2 = M + d*Q
5. Enc(pk_a pkA, M) → C_a
6. [($Rk_{a\to b}$, C_a) → C_b] → E(ID_i, keyword)

d) *Decryption:*

1. Generate the original data M
2. $P \leftarrow C^y \bmod u$
3. $M = C2 - d * C1 \rightarrow [ID_i, m]$
4. $Dec(sk_a, C_a) \rightarrow [ID_i, \text{keyword}]$

The above design denotes the overall encryption and decryption process of user data and their identity. The following section shows the process in each step.

B. Hybrid Encryption RSA with ECC

Rivest-Shamir-Adleman (RSA) [16] is one of the first practical public-key cryptosystems which is used for securing sensitive data over internet. RSA is an asymmetric algorithm that use public and private key for encryption and decryption. It is a one-way function known as integer factorization which is mainly used in key distribution and digital signature processes scheme. The term one-way function means, it computes one way easily, but it is hard compute the inverse of it. In RSA the terms easy and hard should be understood with regard to computational complexity.

The RSA cryptosystem, public key consists of the value u and x, which is called the modulus and public exponent respectively. Similarly the private key consists u and y where u is modulus and y denotes the private exponent. The public key is used for encrypting words that are able to recognize by everybody. Words encrypted with the public key, be able to decrypted using the private key. The key generation procedure for the RSA algorithm is given below.

Input: Initialize two large prime number *s* and *d*.
Output: Two key components are produced
Public key components:
Private Key components:
Step 1: t should be the multiplication of two prime numbers such as

$$u \leftarrow s * d$$

Step 2: Compute $\phi(u) \leftarrow (s-1) * (d-1)$
Step 3: Find a random number e and satisfy the condition below:
$1 < x < \phi(u)$ and $\gcd(x, \phi(u)) = 1$
Step 4: Calculate random number *rn* such as

$$r\,n \leftarrow x^{-1} \bmod (\phi(u))$$

The public key contain a set of integers (u, x) here u is the RSA modulus which is a product of two prime numbers(s,d). These primes are of same bit length generated randomly. x is the encryption exponent should satisfy the condition $1 < x < \phi(u)$ and the greatest common divisor gcd $(d, \phi(u)) = 1$ where $\phi(u) = (s-1)(d-1)$. In the same way the private key y will be generated, it is known as decryption exponent (u, y) and it is a integer. The generated private key should satisfy the condition $1 < y < \phi(u)$ and $xy \equiv 1 \pmod{\phi(u)}$

Input: Plain text message
Output: Cipher text.
Begin
Step 1: Data owner E sends the message to the client F with the public key
Step 2: then client F encrypt the message along with public key to generate cipher text, C

$$C \leftarrow M^x \bmod u$$

Input: Cipher text, C
Output: Decrypted plain text, P
Step 1: Client F transfers the Cipher Text C to data owner E.
Step 2: using private key u, E decrypt the Cipher text into the plain text P.

$$P \leftarrow C^y \bmod u$$

C. Elliptical Curve Cryptography

One of the most popular public-key cryptography approach is Elliptic curve cryptography (ECC). Neal Koblitz [17] and Victor Miller [18] proposed elliptic curves in 1985 to design public key cryptographic systems.

Algebraic form of additive group is described by the group or set of solution along with their point at infinity O.

$$y^2 = x^3 + ax + b$$

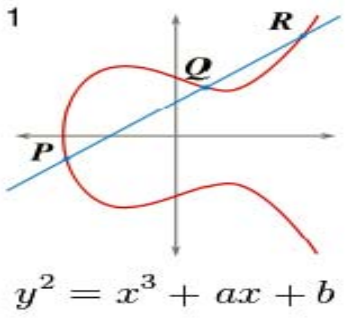

Fig. 1. Simple Elliptical Curve

In this approach the elliptical curve cryptography is utilized to generate the ciphertext of the result which is

provided by RSA. The key generation, encryption and decryption process is described above.

D. Key Generation

Key generation is a major part in ECC where public and private key are generated. By using the receiver's public key the sender encrypt the message and it is decrypted by the receiver with its private key. A random number d has to be selected within the range of 1 to n-1. N is the maximum limit that should be a prime number. The formula for public key generation is

$$Q = d * P$$

Where P is point on the curve, Q denotes the public key and d denotes the private key.

- *Encryption*

Let M be the ciphertext of RSA. This ciphertext has to represent on the curve. The contains $E(ID_i , m)$. That is the encryption of receiver identity and the data. Consider *'m'* has the point *'M'* on the curve *'E'*. Randomly select'd' from [1 – (n-1)].

Two cipher texts will be generated let it be **C1** and **C2**.

$$C1 = d*P$$
$$C2 = M + d*Q$$

- *Decryption*

In decryption process the original message is retrieved. In this work the ciphertext of RSA $E(ID_i , m)$ is obtained. The formula for decryption is

$$\mathbf{M = C2 – d * C1}$$

In this approach encryption is performed in two phase first user data encryption along with receiver identity. In this Encryption part the user data along with receiver identity ciphertext is generated using RSA and ECC encryption algorithm. The following encryption technique is used to encrypt the keyword and user identity which is second phase of this work.

E. Proxy Re Encryption

Proxy Re Encryption (PRE)[19] schemes are cryptosystems which allow third parties to modify the ciphertext that can be encrypted for one user, so that it may be decrypted by another user. In this work the PRE is used to store up the encrypted records in server which is decrypted by the receiver. The PRE based on Canetti and Hohenberger [20] is utilized in this work and its procedure is given below. PRE is a collection of several tuple such as setup, KeyGen, ReKeyGen, Enc, ReEnc, Dec.

- *Procedure of PRE*

Setup: The setup provides the parameter on accepting the input security parameter .

KeyGen(): this function generates the public and secret key pair(pk_a,sk_a), a denotes the user.

ReKeyGen(sk_a,sk_b)**:** Re-encryption key key $(RK_{a \to b})$ is generated using the secret key.

Enc$(pk_a pkA, M)$: With the public key pk_a and message M the encryption process generate the ciphertext(C_a).

ReEnc$(RK_{a \to b}, C_a)$ *:* On input a re-encryption key and a ciphertext, the re-encryption Algorithm generates the second ciphertext C_b.

Dec(sk_a,c_a) *:* the decryption algorithm generates the plaintext M from C_a with the secret key sk_a.

In the proposed approach the user data is secured by applying several encryption techniques such as RSA, ECC and PRE. With these techniques the data can be shared securely. The following section is experimental result where the efficiency of this work is described in detail.

IV. EXPERIMENTAL RESULT

The performance evaluation of the proposed research work is discussed in this section. Net beans IDE and CloudSim tool is used to develop this experiment and the cloud environment respectively. It is a popular tool which provides a general simulation framework that enables simulation, modeling and testing of Cloud computing infrastructures and application services. The performance metrics such as Throughput and execution time evaluated and their report is given in this section.

TABLE.1. Encryption Time Report

Algorithm name	Encryption time
Hybrid encryption method (RSA with ECC)	1.6
Identity Based encryption	2.0

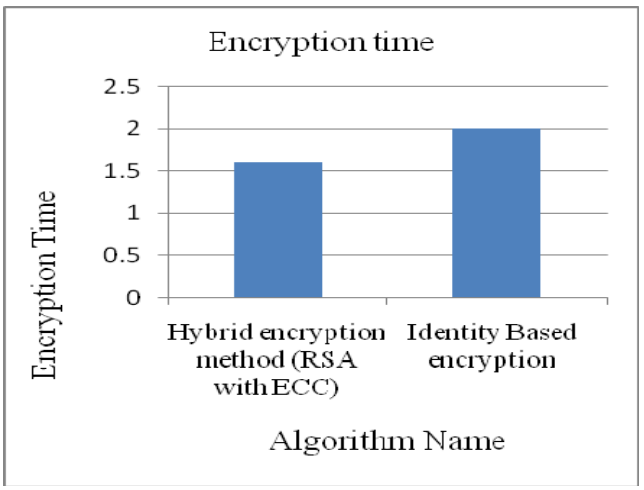

Fig. 2. Encryption Time Report

TABLE. 2.Decryption Time Report

Algorithm name	Decryption Time
Hybrid encryption method (RSA with ECC)	1
Identity Based encryption	1.7

Table 1 and 2 shows the comparative result of Encryption and Decryption time in ms. The proposed work is compared with the identity based encryption technique. The tables clearly explain that both Encryption and Decryption point in time of the proposed work be low down compared existing work.

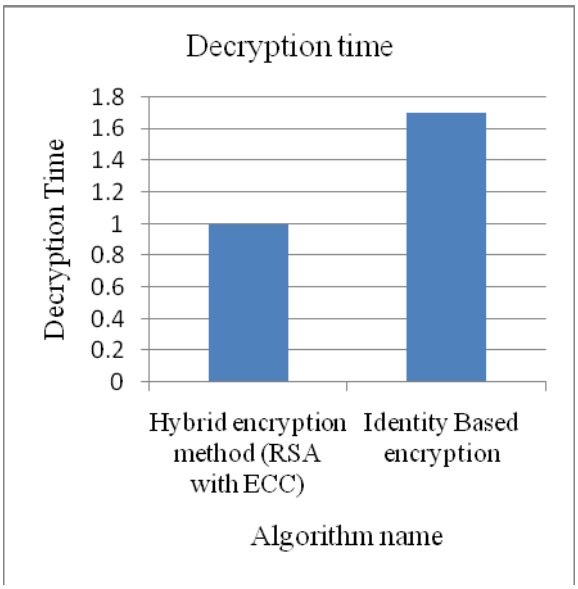

Fig.3. Decryption Time Report

Figure 3 and 4 gives the Encryption and Decryption time Result of the proposed work. Encryption and Decryption point in time of IBE method is 2.0 and 1.7 ms respectively, whereas the proposed work obtains1.6 ms and 1 ms respectively. This shows the proposed research achieved an efficient result.

TABLE. 3.Throughput Report

Algorithm name	**Throughput Time**
Identity Based encryption method	2243.041992
Hybrid encryption method(RSA with ECC) throughput	24456.44803

Table 3 shows the comparative result of throughput. The proposed work is compared with the identity based encryption technique. The tables clearly explain that the proposed work obtain the efficient result.

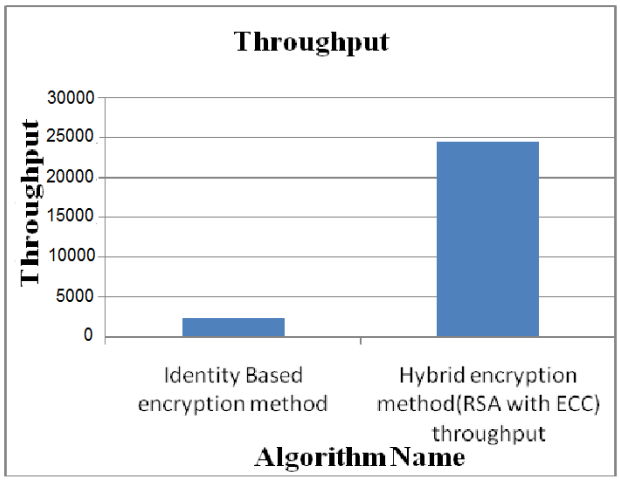

Fig. 4. Throughput Report

Figure 5 and 6gives the throughput report and Execution report of the proposed work. Throughput and execution time of identity based encryption method is 2243.041992 KB and 1094 ms respectively, whereas the proposed work obtain 24456.44803 KB and 94ms respectively. This shows the proposed research achieved an efficient result.

Fig.6. Execution Time Report

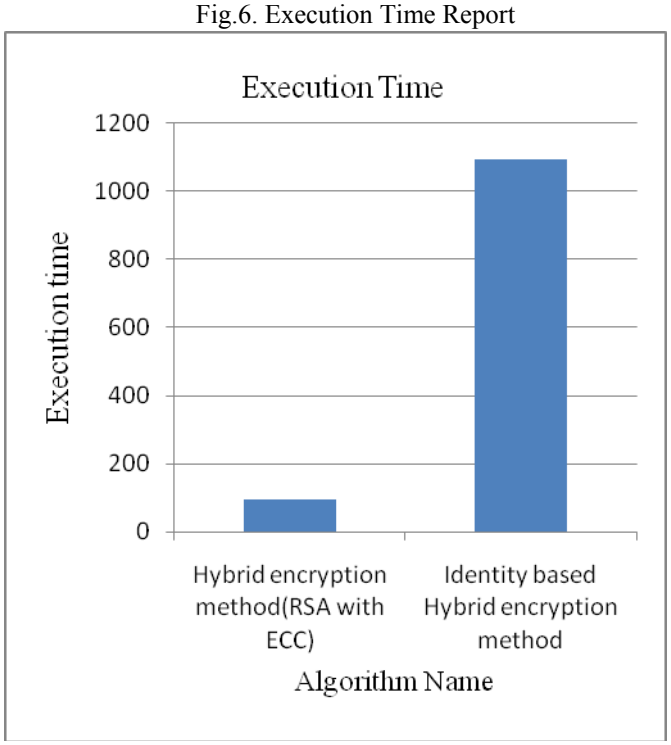

TABLE. 4. Execution Time Report

Algorithm name	Execution Time
Hybrid encryption method(RSA with ECC)	94
Identity based encryption method	1094

Table 4 shows the comparative result of Execution Time. The proposed work is compared with the identity based encryption technique. The tables clearly explain that the proposed work obtain the efficient result.

V. Conclusion

The objective of the proposed work is to improve the security of outsourced data in cloud computing. This is achieved by the efficient hybrid encryption and proxy Re-encryption. The data of the cloud user is encrypted before storing them in cloud storage. In this work the encryption is performed in two phases, In the first the user data is encrypted along with receiver identity. In the second phase the identity (user name, IP address, email id) and the keyword (*Ordinary, secret* and *top secret*) is encrypted using PRE. Finally these two ciphertext is combined and send to the cloud server. The receiver obtains the original message with the private key matching to the identity. This scheme ensures the security of user data and result describes the efficiency of this work.

Reference

[1] H. Erdogmus, "Cloud Computing: Does Nirvana Hide behind the Nebula? " IEEE Software, vol. 26, no.2, pp. 4-6 ,2009.

[2] Y. S. Dai, Y. P. Xiang, G. W. Zhang., "Self-Healing and Hybrid Diagnosis in Cloud Computing, " Lecture Notes of Computer Science (LNCS), vol. 5931, pp. 45-56,2009.

[3] J. Abawajy, "Determining Service Trustworthiness in InterCloud Computing Environments," 10th International Symposium on Pervasive Systems, Algorithms, and Networks (I-SPAN 2009), pp.784- 788, 2009.

[3] B. Waters, "Dual key encryption: Realizing Fully Secure IBE and HIBE Under Simple Assumption," In Proc. of CRYPTO'09, Lecture Notes of Computer Science (LNCS), vol.5677, pp.619-636, 2009.

[4] D. Boneh, "Generalized Identity Based and Broadcast Encryption Schemes ,"In ASIACRYPT'08, Lecture Notes of Computer Science (LNCS), vol.5350, pp. 455-470 ,2008.

[5]. Jin Li; Jingwei Li; Xiaofeng Chen; Chunfu Jia; Wenjing Lou, "Identity-Based Encryption with Outsourced Revocation in Cloud Computing", Computers, IEEE Transactions on Vol: 64, No: 2, PP: 425 – 437, 2015.

[6]. Ms VarshaAgme, Prof.ArchanaC.Lomte, ""Identity-based Encryption data Storage System in Cloud Computing", nternational Journal of Advanced Research in Computer Science and Software Engineering, Vol 3, No 10, 2013.

[7]. Xiaochun Yin; Zengguang Liu; Young Sil Lee; Hoon Jae Lee, "PKI-based cryptography for secure cloud data storage using ECC", Information and Communication Technology Convergence (ICTC), 2014 International Conference, PP: 194 – 199, 2014.

[8]. Eberle H, Gura N, Shantz S C, Gupta V, Rarick L, Sundaram S, "A public-key cryptographic processor for RSA and ECC", Application-Specific Systems, Architectures and Processors,. Proceedings, PP: 98 - 110, 2004.

[9]. Rawat, S.S.; Shrivastava, G.K, "Improved ID-Based Proxy Re-signcryption Scheme", Computational Intelligence and Communication Networks (CICN), PP: 730 – 733,2012.

[10]. Hongbing Wang and Zhenfu Cao, "A Fully Secure Unidirectional and Multi-use Proxy Re-encryption Scheme", 2009.

[11]. R. Canetti and S. Hohenberger. Chosen-ciphertext secure proxy re-encryption. In P. Ning, S. D. C. di Vimercati, and P. F. Syverson, editors, ACM Conference on Computer and Communications Security, pages 185–194. ACM, 2007.

[12]. Dan Boneh and Matt Franklin, "Identity-Based Encryption from the Weil Pairing", SIAM J. of Computing, Vol. 32, No. 3, pp. 586-615, 2003.

[13]. FarazFatemiMoghaddam, Maen T. Alrashdan, and OmidrezaKarimi, "A Hybrid Encryption Algorithm Based on RSA Small-e and Efficient-RSA for Cloud Computing Environments", Journal of Advances in Computer Network, Vol. 1, No. 3, September 2013.

[14]. Kaaniche N, Boudguiga A, Laurent M, "ID Based Cryptography for Cloud Data Storage", Cloud Computing (CLOUD), 2013 IEEE Sixth International Conference , PP: 375 - 382, 2013.

[15]. D.Boneh, M.Franklin, Identity-based encryption from the weil pairing, Advances in Cryptology–CRYPTO2001, SantaBarbara, California,USA, LNCS, 2139, Springer, Berlin, 2001.

[16]. EvgenyMilanov, "The RSA Algorithm", June 2009. pp. 1-11.

[17]. N. Koblitz. Elliptic curve cryptosystems. Mathematics of Computation, 48:203–209, 1987.

[18]. V. Miller. Use of elliptic curves in cryptography. Advances in Cryptology—CRYPTO '85 (LNCS 218) [483], 417–426, 1986

[19]. A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," In :Advances in Cryptology - Proceedings of CRYPTO'84, Lecture Notes of Computer Science (LNCS), vol.196, pp.47-53, 1985

[20]. [].R. Canetti and S. Hohenberger. Chosen-ciphertext secures proxy re-encryption. In Proceedings of the 14th ACM conference on Computer and communications security, pages 185–194. ACM, 2007.