IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

Homomorpic Hybrid Encryption for Cloud Computing

Daniya Rao[1], Deepak Painuli[2], Kamal Kant Verma[3]

Student, Computer Science Engineering, Quantum school of Technology, Roorkee, India[1]

Senior Assistant Professor, Computer Science Engineering, Quantum school of Technology, Roorkee, India [2, 3]

Abstract: Cloud Computing is a stretchy, cost-effective, and confirmed delivery platform for providing business or consumer IT services in excess of the Internet. For the best Performance and most excellent security of cloud computing, we proposed homomorphic hybrid encryption technique. With the progress of Cloud Computing, Computer Network and Communication Technology, an immense group of data and information require to be exchanged by public communication networks. High effectiveness and high protection of data transmission become much more vital. In this paper we proposed Homomorphic Encryption technique, ElGamal encryption and Paillier encryption are widely used two algorithms of asymmetric encryption technology. Both are best and top privacy homomorphism, combination of ElGamal and Paillier renewed to hybrid algorithm, which are proficient to secure cloud data since homomorphic encryption allows direct encrypted communication in cloud computing. Here first we are generating key from Pailler cryptosystem then these private and public keys followed by ElGamal for the purpose of encryption/decryption, later Homomorphic encryption is applied for a secure encrypted communication of users in cloud.

Keywords: Include at least 4 keywords or phrases.

I. INTRODUCTION

The encryption algorithm E () is homomorphic if specified E(a) and E(b), one can find E(a ¬ b) without decrypting a; b for some operation ¬. Here we are using ElGamal and Pailliercryptosystem as follows:

1.1. ElGamal Cryptosystem

Since encryption and decryption are converse proceedures, there have to be a mathematical connection between the encryption and decryption keys. Security in public key cryptosystems relies on this relationship being one that cannot simply be exploited to assume the (private) decryption key from knowledge of the (public) encryption key: The primary mathematical problem that would produce the decryption key from the encryption key must be computationally infeasible to decipher. In ElGamal, the underlying mathematical relationship between the encryption and decryption keys relies upon the so-called discrete log problem.

Key generation: The key generator works as follows:

- A generates an efficient description of a cyclic group G of order q with generator g. See below for a discussion on the required properties of this group.
- A chooses an x randomly from {1, …., q-1}.
- A computes h = g^x
- A publishes h, along with the description of G, q, g, as her public key. A retains x as her private key, which must be kept secret
- **Encryption:** The encryption algorithm works as follows: to encrypt a message m to A under her public key (G,q,g,h),
- B chooses a random y from {1, …., q-1}, then calculates $c_1=g^y$.
- B calculates the shared secret $s=h^y$.
- B maps his secret message m onto an element m' of G.
- B calculates c_2=m'.s
- B sends the ciphertext $(c_1,c_2)=(g^y, m'. h^y)=(g^y, m'. (g^x)^y)$ to A.

Note that one can easily find h^y if one knows m'. Therefore, a new y is generated for every message to improve security. For this reason, y is also called a temporary key.

Decryption: The decryption algorithm works as follows: to decrypt a ciphertext (c_1,c_2) with her private key x,

- A calculates the shared secret $s=c_1^x$
- Then computes $m'=c_2s^{-1}$ which he/she then converts back into the plaintext message m, where s^{-1} is the inverse of s in the group G. (E.g. modular multiplicative inverse if G is a subgroup of a multiplicative group of integers modulo n).

The decryption algorithm produces the intended message, since

$c^2s^{-1} = m' h^y (g^{xy})^{-1} = m' g^{xy} g^{-xy} = m'$.

1.2. Paillier Cryptosystem

The individual technique used in public key cryptography is the exploit of asymmetric key algorithms, where the key used to encrypt a message is not the equal as the key used to decrypt it. Each user has a couple of cryptographic keys (public key and private key). The private key is kept secret, even as the public key may be generally distributed.

DOI 10.17148/IJARCCE.2016.55165

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

Messages are encrypted with the recipient's public key and can just be decrypted with the related private key. The keys are allied mathematically, but the private key cannot be possibly derived from the public key.
The Paillier Cryptosystem's method works as follows:

Key Generation

1. Choose two large prime numbers p and q randomly and independently of each other such that gcd(pq,(p-1)(q-1))= 1
This property is assured if both primes are of equivalent length, i.e., $p, q \in 1 \| \{0,1\}s^{-1}$ for security parameter s.
2. Compute RSA modulus n = pq and
Carmichael's function λ = lcm $(p-1, q-1)$ it can be computed using
$\lambda = (p-1)(q-1) / \gcd(p-1, q-1)$
3. Select generator g where $g \in \mathbb{Z}*n^2$, There are two ways of selecting the g.
a. Randomly select g from a set $\mathbb{Z}*n^2$ where
gcd $((g\lambda \bmod n^2-1)/n, n) = 1$
There are $\phi(n) * \phi(n)$ number of valid generators, therefore the probability of choosing them out of $n\phi(n)$ elements of $\mathbb{Z}*n^2$ set is relatively high for big n.
b. Select α and $\beta\beta$ randomly from a set $\mathbb{Z}n*$ then calculate
$g = (\alpha n + 1)\, \beta n \bmod n^2$
In this case the selected generator always meets the condition above.
4. Calculate the following modular multiplicative inverse
$\mu = ((g^{\lambda} \bmod n^2))^{-1} \bmod n$
Where the function L is defined as $(u) = u-1 / n$
The public (encryption) key is (n,g).
The private (decryption) key is (λ,μ).
A simpler variant of the above key generation steps would be to set $g = n + 1$, $\lambda = (n)$ and $\mu = (n)^{-1}$ mod n, where $\varphi(n) = (p-1)(q-1)$.

Encryption

a) Let m be a message to be encrypted where $m \in \mathbb{Z}n$
b) Select random r where $r \in \mathbb{Z}*$ n
c) Compute ciphertext as: $c = g^n \cdot r^n \bmod n^2$

Decryption

a) Ciphertext c $\in \mathbb{Z}*n^2$
b) Compute message: $m = L(c^{\lambda} \bmod n^2) \cdot \mu \bmod n$

II. RELATED WORK

X.LI et al. [1] in his paper has analyzed the security of ElGamal digital signature algorithm under the four attack scheme. He attempted to increase the security of ElGamal algorithm by adding a random number to the original one and thereby creating difficulty in deciphering key. Nentawe Y. et al. [2] in this paper author has presented data encryption and decryption in a network environment that was successfully implemented. S. Subasree, N. K. Sakthivel et al. [3] this protocol provides three cryptographic primitives such as integrity, confidentiality and authentication. These three primitives can be achieved with the help of Elliptic Curve Cryptography, Dual-RSA algorithm and Message Digest MD5. That is it uses Elliptic Curve Cryptography for encryption, Dual-RSA algorithm for authentication and MD-5 for integrity. P. Gutmann et al. [4] this book provides a comprehensive design for a portable, flexible high-security cryptographic architecture, with particular emphasis on incorporating rigorous security models and practices. Suyash Verma et al. [5] this paper authors proposed a new algorithm for evaluations, results calculation using different plaintexts in the same key (DPSK) mode. As the basis of the evaluating process, the plaintext and the corresponding key are both generated by randomly. Ravindra Kumar Chahar et.al [6] a new security protocol for on-line transaction can be designed using combination of both symmetric and asymmetric cryptographic techniques. This protocol provides three cryptographic primitives - integrity, confidentiality and authentication. It uses elliptic curve cryptography for encryption, RSA algorithm for authentication and MD-5 for integrity.

Instead of ECC symmetric cipher (AES-Rijndael) can be used to encrypt, public key cryptography (RSA) to authenticate and MD-5 to check for integrity. Guilin Wang et al. [7] in this paper the author have proposed a new digital contract signing protocol based on RSA digital signature scheme. WANG Shaobin et al. [8] in this paper, authors describes a method of constructing efficient fair-exchange protocols based on improved DSA signatures the problem of fair exchange is of the major threats in the field of secure electronic transactions. In this paper the authors have presented a multi signature scheme based on DSA. Afolabi, A.O et al. [9] this study proffered solution to some identified data insecurity problems in software development by the use of Web-based learning system as a test bed and development of an hybrid crypto-biometric security system. Arjen K. Lenstra et al. [10] we performed a sanity check of public keys collected on the web. Our main goal was to test the validity of the assumption that different random choices are made each time keys are generated. We found that the vast majority of public keys work as intended. ArvindNegi et al. [11] this paper presented a novel mechanism of generating digital signature using RSA algorithm. The security of the system is relatively enhanced using this approach. This technique involves the use of multiple public key exponents which in turn provided multiple public key and private key.

III.PROPOSED WORK

Here we are working on Hybrid Homomorphic Encryption technique. In this paper our essential conception was to encrypt the data before to sending them to the Cloud source. The user wants to grant the private key to the server to decrypt the data prior to perform the calculations required, which might concern the secrecy of data stored in the Cloud.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

In this methodology first we are generating keys from pailler cryptosystem and these private and public keys are followed by ElGamal cryptosystem for the purpose of encryption and decryption, then later we are applying combination of Homomorphic Encryption technique (HEE+HPE) for cloud source. The important purpose of Homomorphic Encryption method is able to perform operations of encrypted data without decrypting them.

1.3. Homomorphic ElGamal Encryption

In the ElGamal Cryptosystem, in a repeated group G of order q with generator g, if the public key is (G, q, g, h), where $h = g^x$, and x is the secret key, then the encryption of a message m is $\mathcal{E}(m) = (g^r, m \cdot h^r)$, for some random $r \in \{0, \ldots, q-1\}$. The homomorphic property is then

$$\begin{aligned}\mathcal{E}(\mathbf{m_1}).\mathcal{E}(\mathbf{m_2}) &= (\mathbf{g^{r_1}}, \mathbf{m_1}.\mathbf{h^{r_1}})(\mathbf{g^{r_2}}, \mathbf{m_2}.\mathbf{h^{r_2}}) \\ &= (\mathbf{g^{r_1+r_2}}, (\mathbf{m_1 m_2})\mathbf{h^{r_1+r_2}}) \\ &= \mathcal{E}(\mathbf{m_1}.\mathbf{m_2})\end{aligned}$$

…… (1)

1.4. Homomorphic Paillier Encryption

In the Paillier Cryptosystem, if the public key is the modulus m and the base g, then the encryption of a message x is $\mathcal{E}(x) = g^x r^m \bmod m^2$, for some random $r \in \{0, \ldots, m-1\}$. The homomorphic property is then

$$\begin{aligned}\mathcal{E}(\mathbf{m_1}).\mathcal{E}(\mathbf{m_2}) &= (\mathbf{q^{x_1} r_1{}^m})(\mathbf{q^{x_2} r_2{}^m}) \\ &= \mathbf{q^{x_1+x_2}(r_1 r_2)^m \bmod m^2} \\ &= \mathcal{E}(\mathbf{x_1 + x_2 \bmod m^2})\end{aligned}$$

…… (2)

From equations 1 & 2 -

$\mathcal{E}(m_1).\mathcal{E}(m_2) = \mathcal{E}(m_1.m_2)$, $\mathcal{E}(x_1).\mathcal{E}(x_2) = \mathcal{E}(x_1 + x_2 \bmod m^2)$

Here we are changing values of x and m, for concatenation of both encryption techniques.

Now, $m_1 = x_1 \& m_2 = x_2$. So, $\mathcal{E}(m_1).\mathcal{E}(m_2) = \mathcal{E}(x_1).\mathcal{E}(x_2)$

$\mathcal{E}(\mathbf{m_1}).\mathcal{E}(\mathbf{m_2}) = \mathcal{E}(\mathbf{x_1}).\mathcal{E}(\mathbf{x_2}) = \mathcal{E}(\mathbf{x_1 + x_2 \bmod m^2})$

…… (3)

Equation 3 showing, The Hybrid Homomorphic Encryption equation for the best Performance and most excellent security of cloud computing, below we are providing a framework of hybrid encryption for ElGamal and Paillier encryption.

In proposed framework figure 1, Encryption/Decryption done by ElGamal cryptosystem and we was discussed it in previous section with pseudonymous flowchart for key generation, message encryption and message decryption.

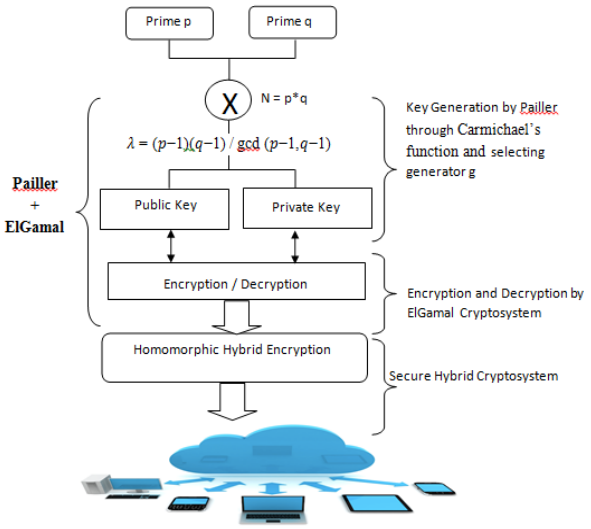

Figure 1: Framework for Hybrid Homomorphic Encryption in Cloud Computing

1.5. Algorithm for proposed methodology

Step 1. Here p and q are two distinct prime numbers chosen randomly.

Step 2. In Pailler cryptosystem n=p*q through RSA algorithm.

Step 3. Key Generation by Pailler using generater g and Carmichael function.

Step 4. Carmichael's function generated, $\lambda = (p-1)(q-1)/\gcd(p-1, q-1)$.

Step 5. Public and Private keys provided by pailler cryptosystem.

Step 6. Both keys captured by ElGamal cryptosystem and followed for encryption/decryption.

Step 7. Now we have an encrypted data, it will be applied for Homomorphic encryption.

Step 8. Steps 5 and 6 show two different cryptosystems, after Homomorphic approach it provide completed secure data for cloud.

IV. CONCLUSION

The Now high effectiveness and high protection of data transmission become much more essential for network or cloud computing. In this paper our center of attention is on hybrid technology for encrypt the cloud data. Here we worked on Homomorphic Encryption technique; (ElGamal encryption and Paillier encryption) are widely used two algorithms of asymmetric encryption technology. Grouping of ElGamal and Paillier renewed to hybrid algorithm, which are proficient to secure cloud data for the reason that Hybrid Homomorphic Encryption allows direct encrypted communication in cloud computing.

REFERENCES

[1] X.Li, X.Shen&H.Chen, "ElGamal Digital Signature Algorithm of Adding a Random Number", JOURNAL OF NETWORKS, VOL. 6, NO. 5, MAY 2011

[2] Nentawe Y. Goshwe, (2013). Data Encryption and Decryption Using RSA Algorithm in a Network Environment. IJCSNS

International Journal of Computer Science and Network Security, VOL.13 No.7.
[3] S. Subasree, N. K. Sakthivel, (2011), Design of a New Security Protocol Using Hybrid Cryptographic Algorithms, ICECT.
[4] P. Gutmann, (2004). Cryptographic Security Architecture: Design andVerification‖. Springer-Verlag.
[5] Suyash Verma, RajnishChoubey, RoopaliSoni, (2012).An Efficient Developed New Symmetric Key Cryptography Algorithm for Information Security. International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 2, Issue 7.
[6] Ravindra Kumar Chahar and et.al, (2007), Design of a new Security Protocol, IEEE International Conference on Computational Intelligence and Multimedia Applications, pp 132 – 134
[7] Guilin Wang, An Abuse-Free Fair Contract-Signing Protocol Based on the based on RSA Signature, Information Forensics and Security, IEEE Transactions on, (Volume:5), Issue: 1, ISSN:1556-6013 , INSPEC : 11149510.
[8] WANG Shaobin, HONG Fan, ZHU Xian, Optimistic Fair-exchange Protocols Based on DSA Signatures, Services Computing, 2004. (SCC 2004). Proceedings. 2004 IEEE International Conference, E-ISBN: 0-7695- 2225-4, INSPEC: 8273373.
[9] Afolabi, A.O and E.R. Adagunodo, (2012). Implementation of an improved data encryption algorithm in a web based learning system. International Journal of research and reviews in Computer Science. Vol. 3, No. 1.
[10] Arjen K. Lenstra, James P. Hughes, Maxime Augier, Joppe W. Bos, Thorsten Kleinjung, and Christophe Wachter, Ron was wrong, Whit is right. EPFL IC LACAL, Station 14, CH-1015 Lausanne, Switzerland, Self, Palo Alto, CA, USA.
[11] Markoff, John (February 14, 2012). Flaw Found in an Online Encryption Method. New York Times.
[12] Willian Stallings, Cryptography and Network Security Principles and Practices, Fourth Edition.
[13] Abraham Silberschatz, Peter Baer Galvin, Greg Gagne, (2012), Operating System Concepts. Wiley India Pvt Ltd, Sixth Edition.

BIOGRAPHIES

Daniya Rao was born in roorkee in 1992 and completed my schooling from roorkee and then I persued my BTECH in computer science from Uttaranchal institute of technology dehradunin session 2010-14. After which I have opted for MTECH in computer science branch from quantum global college **(**uttarakhand technical university)roorkee (2014-16).My area of intrest is computer security and networking.

Er. Deepak Painuli is an Assistant Professor in Dept. of Computer Science at Quantum School of Technology Roorkee. He is B.Tech and M.Tech in Computer Science and has ten year of teaching and research experience in various engineering colleges. He has published twelve research papers in various national and international journals/conferences. His areas of interest are Image Processing and Data Mining.

Kamal Kant Verma is an Assistant Professor in Dept. Of Computer Science at Quantum School of Technology Roorkee. He is B.Tech and M.Tech in Computer Science and has ten year of teaching and research experience in various engineering colleges. He has published twelve research papers in various national and international journals/conferences. His areas of interest are Image Processing and Data Mining.

DOI 10.17148/IJARCCE.2016.55165