Homomorphic Hybrid Encryption Technique using IKC and IEC Algorithms

Aakanksha Pundir, Sumit Chaudhary

Abstract: Distributed computing is a pliable, practical, and affirmed conveyance stage for giving business or shopper IT administrations in abundance of the Internet. For the best Performance and most superb security of distributed computing, we proposed Homomorphic half and half encryption strategy. With the advancement of Cloud Computing, Computer Network and Communication Technology, an enormous gathering of information and data require to be traded by open correspondence systems. High adequacy and high security of information transmission turn out to be a great deal more essential. In this paper we proposed Homomorphic Encryption strategy, Identity based Key Cryptosystem (IKC) and Identity based Encryption Cryptosystem (IEC) are broadly utilized two calculations of topsy-turvy encryption innovation. Both are ideal and top protection homomorphism, mix of IEC and IKC recharged to half breed calculation, which are capable to secure cloud information since Homomorphic encryption permits direct scrambled correspondence in distributed computing. Here first we are producing key from IKC then these private and open keys took after by IEC with the end goal of encryption/decoding, later Homomorphic encryption is connected for a protected encoded correspondence of clients in distributed computing.

Keywords - Cloud, cryptosystem, distributed, homomorphic.

I. INTRODUCTION

The encryption calculation E () is Homomorphic if determined E(a) and E(b), one can discover E(a ¬ b) without unscrambling a; b for some operation ¬. Here we are using *IEC* and *IKC* as follows:

A. Identity based Key Cryptosystem

For key era here in this paper we are utilizing Identity based Key cryptosystem (IKC), two or three cryptographic keys (open key and private key) has given to every client. The private key is kept mystery, even as people in general key might be by and large circulated and the private key is kept mystery. The beneficiary's open key is utilized for encoding the message and message can be unscrambled with the related private key. The keys are unified scientifically, yet the private key can't be gotten from the general population key. Recognizable proof of the client is most imperative so in this technique two personalities of the client are encased i.e. client's PAN number and Mail ID**.**

The Key Cryptosystem's key era fills in as takes after:

Key Generation

- Two extensive prime numbers a and b are choosen by A arbitrarily from (Identity of B's) and freely of each other such that gcd(ab,(a-1)(b-1))= 1
- RSA modulus n = a*b and Carmichael's capacity λ = lcm (a− 1, b − 1) it can be figured usingλ = (a−1)(b−1)/gcd (a−1,b−1)
- A Select generator g haphazardly from G,where G is a cyclic gathering of characters of second individual gcd (($g\lambda$ mod n2−1)/n, n) = 1, n is number in cyclic gathering.
- There are $\phi(n) * \phi(n)$ number of substantial generators, in this manner the likelihood of picking them out of $n\phi(n)$ components of G is generally high for huge n.
- Calculate the accompanying measured multiplicative reverse

μ = (($g\lambda$ mod $n2$))−1 mod n published (encryption) key is (n,g).

The secret (decoding) key is (λ,μ).

An easier variation of the above key era steps would be to set $g = n + 1$, $\lambda = (n)$ and $= (n)^{-1}$ mod n, where $\varphi(n)$ = (a − 1)(b − 1).

B. Identity based Encryption Cryptosystem

As encryption and unscrambling are speak strategies, there must be a numerical association between the encryption and decoding keys. Security out in the open key cryptosystems depends on this relationship being one that can't just be abused to expect the (private) unscrambling key from information of (people in general) encryption key: The essential scientific issue that would deliver the decoding key from the encryption key must be computationally infeasible to translate. In Identity basedEncryption Cryptosystem (IEC), the hidden scientific relationship between the encryption and unscrambling keys depends upon the supposed discrete log issue.

Here we are utilizing keys from IKC and overhauling it with IEC**.**

Key generation:

Open key (n,g) and private key (λ,μ) taken by Key calculation and a few adjustments by Encryption for key era are takes after:

- Random numbers and cyclic gathering G taken by IKC.
- A figures z = gk1
- A distributes h, alongside all parts so (G, g,z,n)as her open key. Furthermore, holds (k1, λ,μ) as his private key**.**

Encryption**:**

A ready to encode his message m under his open key (G,g,z, n)

- B picks an irregular k2 from (A's characters), then computes c1=gy.
- B computes the mutual mystery s=zk2.
- B maps his mystery message m onto a component m' of G.

Revised Version Manuscript Received on June 11, 2016.

Aakanksha Pundir, M.Tech Student, Department of Computer Science and Engineering, Uttaranchal Institute of Technology, Prem Nagar P.O Chandanwari, Dehradun (Uttarakhand). India.

Sumit Chaudhary, Assistant Professor, Department of Computer Science and Engineering, Uttaranchal Institute of Technology, Prem Nagar P.O Chandanwari, Dehradun (Uttarakhand). India.

- B computes c2=m'.s
- B sends the ciphertext (c1,c2)=(gk2, m'. zk2)=(gk2, m'. (gk1)k2) to A.

Decryption: Decoding done by ciphertext (c1,c2) with his private key x,

- A calculates the mutual mystery s=c1k1
- Then processes m'=c2s-1 then changes over once again into the plaintext message m, where s-1 is the reverse of s in the gathering G.
- The decoding calculation creates the proposed message, subsequent to $c^2s^{-1} = m' z^{k2} (g^{k1k2})^{-1} = m' g^{k1k2} g^{-k1k2} = m'$.

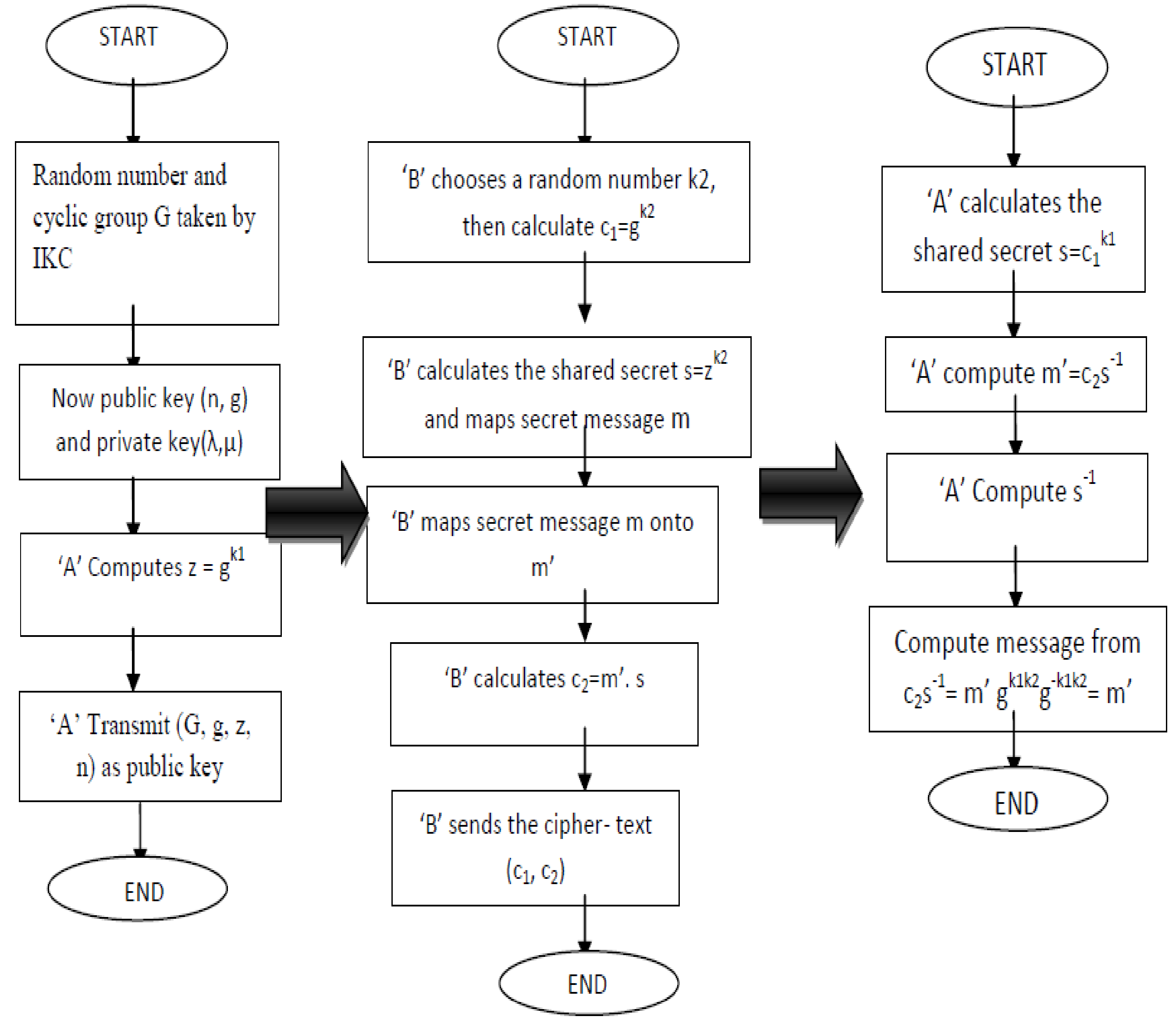

Figure 1: Pseudonymous flow chart for key generation by IKC + IEC and message encryption/decryption by Encryption cryptosystem

II. RELATED WORK

X.LI et al. [1] in his paper has examined the security of Encryption computerized signature calculation under the four assault plan. He endeavored to build the security of Encryption calculation by adding an irregular number to the first one and along these lines making trouble in interpreting key. Nentawe Y. et al. [2] in this paper creator has introduced information encryption and decoding in a system domain that was effectively executed. S. Subasree, N. K. Sakthivel et al. [3] this convention gives three cryptographic primitives, for example, trustworthiness, privacy and validation. These three primitives can be accomplished with the assistance of Elliptic Curve Cryptography, Dual-RSA calculation and Message Digest MD5. That is it utilizes Elliptic Curve Cryptography for encryption, Dual-RSA calculation for verification and MD-5 for honesty. P. Gutmann et al. [4] this book gives a complete configuration to a compact, adaptable high-security cryptographic design, with specific accentuation on joining thorough security models and practices. Suyash Verma et al. [5] this paper creators proposed another calculation for assessments, results computation utilizing diverse plaintexts as a part of the same key (DPSK) mode. As the premise of the assessing procedure, the plaintext and the relating key are both created by haphazardly. Ravindra Kumar Chahar et.al [6] another security convention for on-line exchange can be composed utilizing mix of both symmetric and uneven cryptographic methods.

Published By:
Blue Eyes Intelligence Engineering & Sciences Publication Pvt. Ltd.

This convention gives three cryptographic primitives - honesty, classification and validation. It utilizes elliptic bend cryptography for encryption, RSA calculation for verification and MD-5 for respectability. Rather than ECC symmetric figure (AES-Rijndael) can be utilized to encode, open key cryptography (RSA) to verify and MD-5 to check for respectability.

Guilin Wang et al. [7] in this paper the creator have proposed another computerized contract marking convention in view of RSA advanced mark plan.

WANG Shaobin et al. [8] in this paper, creators portrays a strategy for developing proficient reasonable trade conventions in view of enhanced DSA marks the issue of reasonable trade is of the significant dangers in the field of secure electronic exchanges. In this paper the creators have displayed a multi signature plan taking into account DSA.

Afolabi, A.O et al. [9] this study proffered answer for some recognized information instability issues in programming improvement by the utilization of Web-based learning framework as a proving ground and advancement of a half breed crypto-biometric security framework. Arjen K. Lenstra et al. [10] we performed an once-over to verify everything is ok of open keys gathered on the web. Our principle objective was to test the legitimacy of the presumption that diverse irregular decisions are made every time keys are produced. We found that most by far of open keys act as expected.

Arvind Negi et al. [11] this paper introduced a novel component of creating computerized signature utilizing RSA calculation. The security of the framework is moderately upgraded utilizing this methodology. This system includes the utilization of various open key examples which thusly gave numerous open key and private key.

III. PROPOSED WORK

Here we are chipping away at Hybrid Homomorphic Encryption method. In this paper our fundamental origination was to scramble the information before to sending them to the Cloud source.

The userwants to allow the private key to the server to unscramble the information earlier to perform the figurings required, which may concern the mystery of information put away in the Cloud.

In this strategy first we are creating keys from proposed IKC and these private and open keys are trailed by proposed IEC with the end goal of encryption and unscrambling, open and private keys again redesigned by IEC for more security and later we are applying mix of Homomorphic Encryption procedure (HIKC+HIEC) for cloud source.

The critical reason of Homomorphic Encryption strategy can perform operations of scrambled information without decoding them.

A. Basic Flowchart for proposed methodology

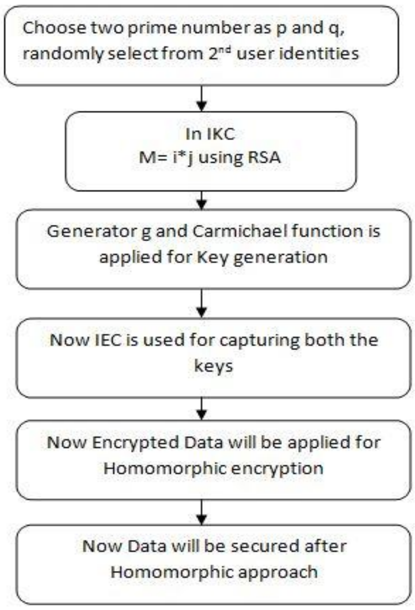

Figure3: Basic Flowchart for proposed methodology

B. Main Algorithm for proposed methodology

Step1. Key Generation

- A Choose two large prime numbers a and b randomly from (Identity of B's) and independently of each other such that gcd(ab,(a-1)(b-1))= 1
- A Compute RSA modulus n = ab and Carmichael's function $\lambda = lcm\ (a-1, b-1)$ it can be computed using$\lambda = (a-1)(b-1) / \gcd(a-1,b-1)$
- A Select generator g randomly from G,where G is a cyclic group of identities of 2nd person gcd $((g\lambda \bmod n^{2}-1)/n, n) = 1$, n is number in cyclic group.
- There are $\phi(n) * \phi(n)$ number of valid generators, therefore the probability of choosing them out of $n\phi(n)$ elements of G is relatively high for big n.

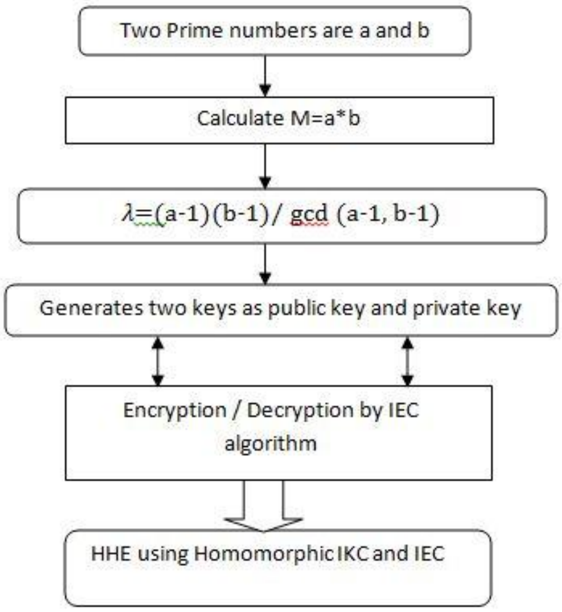

Figure 2: Flowchart for Hybrid Homomorphic Encryption (HHE) in Cloud Computing

- Calculate the following modular multiplicative inverse $\mu = ((g^{\lambda} \bmod n^2))^{-1} \bmod n$
  The public (encryption) key is (n,g).
  The private (decryption) key is (λ,μ).

  Step 2. Key Updating

  Public key (n,g) and private key (λ,μ) taken by Key algorithm and some modifications by Encryption for key generation are follows:
- Randomnumbers and cyclic group G taken by Key.
- A computes $z = g^{k1}$
- A publishes h, along with all components so (G, g, z, n) as her public key. And holds (k_1, λ,μ)
  The public (encryption) key is (G, n, z, g).
  The private (decryption) key is (k_1, λ,μ).

  Step 3.Encryption**:**

A able to encrypt his message m under his public key (G, g, z, n)

- B chooses a random y from (A's identities), then calculates $c_1=g^{k2}$.
- B calculates the shared secret $s=z^{k2}$.
- B maps his secret message m onto an element m' of G.
- B calculates c_2=m'.s
- B sends the ciphertext $(c_1,c_2)=(g^{k2}, m'. z^{k2})=(g^{k2}, m'. (g^{k1})^{k2})$ to A.

Step4. Decryption**:**

Decryption done by ciphertext (c_1,c_2) with his private key x,

- A calculates the shared secret $s=c_1^{k1}$
- Then computes $m'=c_2s^{-1}$ then converts back into the plaintext message m, where s^{-1} is the inverse of s in the group G.
- The decryption algorithm produces the intended message, since
  $c^2s^{-1} = m' h^{k2} (g^{k1k2})^{-1} = m' g^{k1k2} g^{-k1k2} = m'$.

Step 5. Homomorphic Property

- The encryption of a message is,
  $\mathcal{E}(m) = (g^r, m \cdot h^r)$ for some random $r \in \{0, \ldots, q-1\}$.
- The homomorphic property for m_1 and $m_2$inIEC is:

$\boldsymbol{E(m_1).E(m_2) = (g^{r_1}, m_1.\mathrm{h}^{r_1})(g^{r_2}, m_2.\mathrm{h}^{r_2}) = (g^{r_1+r_2}, (m_1m_2)h^{r_1+r_2}) = E(m_1.m_2)}\ldots$ (1)

- Theencryption of a message is
  $\mathcal{E}(x) = g^x r^m \bmod m^2$, for some random $r \in \{0, \ldots, m-1\}$.
- The homomorphic property for IKCis:

$$\boldsymbol{E(m_1).E(m_2) = (q^{x_1}{r_1}^m)(q^{x_2}{r_2}^m) = q^{x_1+x_2}(r_1r_2)^m mod\ m^2 = \mathcal{E}(x_1 + x_2\ mod\ m^2)}..(2)$$

- From equations 1 & 2 -

$E(m_1).E(m_2) = E(m_1.m_2)$, $E(x_1).E(x_2) = E(x_1 + x_2\ mod\ m^2)$

- 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, $E(m_1).E(m_2) = E(x_1).E(x_2)$

$\boldsymbol{E(m_1).E(m_2) = E(x_1).E(x_2) = E(x_1 + x_2\ mod\ m^2)}$ …………………………….. (3)

Equation 3 showing, The *Hybrid Homomorphic Encryption* equation for the best Performance and most excellent security of cloud computing. In proposed framework figure 2, Encryption/ Decryption done by IEC and we was discussed it in previous section with pseudonymous flowchart for key generation, message encryption and message decryption.

C. Mathematical Proof as Implementation

Key Generation

- A chooses two prime numbers from B's identity, suppose B having an identity which vary from (0 to 30). And same A's identities vary from (0 to 20).
  So, a = 3, b = 11.
  a-1 = 2, b-1 = 10
  gcd (ab, (a-1)(b-1)) =1. So, gcd (33, 20) =1.
- A computes RSA, n = a*b, n = 3 *11 = 33.
  Now Carmichael's function, $\lambda = lcm\ (a - 1, b - 1)$
  So, $\lambda = lcm\ (2, 20) = 10$.
  $\lambda = (a-1)(b-1) / \gcd(a-1,b-1)$
  $\lambda = (3-1)(11-1) / \gcd(3-1,11-1) = 2*20 / \gcd(2, 20) = 10$.
- A Select g, randomly from G (G is a cyclic group of identities).
  gcd $((g\lambda \bmod n^2-1)/n, n) = 1$
  if g = 2, so $g\lambda \bmod n^2 = 2*10 \bmod (33^2-1) = 20 \bmod 1088 = 20$.
  gcd $((g\lambda \bmod n^2-1)/n, n)$ = gcd (20/33 , 33) = gcd (0.606, 33) =1.11
  (Around 1, here we overlook fractional values)
  So, gcd (0.606, 33) = 1
- Calculate modular multiplicative inverse, $\mu = ((g^{\lambda} \bmod n^2))^{-1} \bmod n$
  $\mu = ((g^{\lambda} \bmod n^2))^{-1} \bmod n$
  $((g^{\lambda} \bmod n^2))^{-1} = (2^{10} \bmod 33^2)^{-1} = (1024 \bmod 1089)^{-1} = 67$.
  $\mu = ((g^{\lambda} \bmod n^2))^{-1} \bmod n = 67 \bmod 33 = 1$.
  The public (encryption) key is (n,g) = (33,2).
  The private (decryption) key is (λ,μ) = (10,1).

Step 1. Key Updating

- A computes $z = g^{k1}$
  If k_1 = 4, Random number from B's id.
  $z = 2^4 = 16$.
  G is a cyclic group of B's identities so here we contain its value equal to last value of id.
  G = 30.
  The public (encryption) key is (G, n, z, g) = (30, 33, 16, 2).
  The private (decryption) key is (k_1, λ, μ) = (4, 10, 1).

Step 2. Encryption

- B chooses a random number k_2 from (A's identities), then calculates $c_1=g^{k2}$
  If k_2 = 3. So, $c_1=g^{k2} = 2^3 =8$.
- B calculates the shared secret $s=z^{k2} = 16^3 = 4096$.
  S = 4096.
- B maps his secret message m onto an element m' of G, if m' =2.
- Then c_2=m'.s = 2*4096 = 8192.

Published By:
Blue Eyes Intelligence Engineering & Sciences Publication Pvt. Ltd.

$c_2 = 8192$.

- B sends the ciphertext (c_1,c_2) to A
  $(c_1, c_2) = (g^{k2}, m'. z^{k2}) = (g^{k2}, m'. (g^{k1})^{k2})$
  $(c_1, c_2) = (2^3, 2{*}16^3) = (2^3, 2{*} (2^4)^3)$
  $(c_1, c_2) = (8, 8192) = (8, 8192)$

Step 3. Decryption

- Decryption done by ciphertext (c_1,c_2)
- A calculates the shared secret $s=c_1^{k1} = 8^4 = 4096$.
  S = 4096.
- Computes $m'=c_2s^{-1}$
  $2 = c_2\,(4096)^{-1}$
  $c_2 = 8192$.
- Now we prove value of m' equal to c_2s^{-1}
  $c_2s^{-1} = m'\, z^{k2}\, (g^{k1k2})^{-1} = m'\, g^{k1k2}\, g^{-k1k2} = m'$
  $c_2s^{-1} = 2\,(16^3\,(2^{4*3})^{-1}) = 2\,(2^{4*3})(2^{-4*3}) = m'$
  $c_2s^{-1} = 2\,(4096\,(4096)^{-1}) = 2\,(2^{12})(2^{-12}) = m'$
  $c_2s^{-1} = 2\,(1) = 2\,(1) = m'$
  $c_2s^{-1} = m' = 2$.

For Homomorphic encryption we take multiple messages like (m_1, m_2) and calculate its value same as our proposed algorithm. The value of Homomorphic property for m_1 and m_2 in IKC is equal to value of Homomorphic property for m_1 and m_2 in IEC.

So,

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

IV. CONCLUSION

Presently high adequacy and high insurance of information transmission turn out to be a great deal more fundamental for system or distributed computing. In this paper our focal point of consideration is on half breed innovation for encode the cloud information. In this strategy key era done by some particular characters (PAN number and Mail ID) of other client's utilizing IKC calculation which encoded and decoded by IEC. Here we chipped away at Hybrid Homomorphic Encryption strategy (Identity based Encryption Cryptosystem and Identity based Key Cryptosystem) are generally utilized two calculations of lopsided encryption innovation. Gathering of IEC and IKC restored to half and half calculation, for key era and security here we proposed three calculations which are capable to secure cloud information for the reason that Hybrid Homomorphic Encryption permits direct scrambled correspondence in distributed computing.

REFERENCES

1. X.Li, X.Shen&H.Chen, "Encryption 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 NetworkEnvironment. IJCSNS International Journal of Computer Science and Network Security, VOL.13No.7.
3. S. Subasree, N. K. Sakthivel, (2011), Design of a New Security Protocol Using Hybrid CryptographicAlgorithms, 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 InternationalConference 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 algorithmin 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. ArvindNegi, Punit Sharma, PrasantChaudhary and Himanshu Gupta. New Method for Obtaining Digital Signature Certificate using Proposed RSA Algorithm. *International Journal of Computer Applications* 121(23):24-29, July 2015.
12. Markoff, John (February 14, 2012). Flaw Found in an Online Encryption Method. New York Times.
13. Willian Stallings, Cryptography and Network Security Principles and Practices, Fourth Edition.
14. Abraham Silberschatz, Peter Baer Galvin, Greg Gagne, (2012), Operating System Concepts. Wiley India Pvt Ltd, Sixth Edition.

AUTHORS PROFILE

Aakanksha Pundir, was born in dehradun in 1992 and completed my schooling from dehradun and then I persued my BTECH in computer science from quantum global college (uttarakhand technical university)roorkee (2009-13) After which I have opted for MTECH in computer science branch from Uttaranchal institute of technology dehradun in session 2014-16.My area of intrest is computer security and networking.

Sumit Chaudhary, is working as Assistant Professor in CSE department at Uttaranchal University, Dehradun, Uttarakhand, INDIA. He is pursuing Ph.D from Uttaranchal University. He is B.Tech and M.Tech in Computer Science and has seven year of teaching and research experience in various engineering colleges. He has attended several seminars, workshops and conferences at various levels. His many papers are published in various national, international journals and conferences. His area of research includes Network Security, Cloud Computing.