A Comparative Study of Encryption Security for Cloud Computing

[1]Y. M. Wazery, [2]E. Anwar
[1]Department of information technology, Faculty of computer and information, Minia university
[2]Department of information systems, Faculty of computer and information, Minia university

Abstract

Cloud computing plays an important role nowadays. The migration from on premises infrastructure to cloud computing systems takes a huge amount of interest and research. Cloud computing is a new popular, out- of- the way environment for storing and retrieving data from different place, one of the most significant areas of research in cloud computing is securing the environment.It became to be difficult to keep information because of absence of solid information encryption system;Security via encryption of messages could solve some of the important problemsabout to cloud computing systems.

Keywords: *cloud computing, encryption, security, AES encryption Algorithm, Rijndael encryption Algorithm, asymmetric keys; client-based service*

I. INTRODUCTION

Cloud computing is a model that allows on-demand network access to sharecomputing resource.it is modeling for managing, storing and processing data online via the internet. Cloud computing refer to the delivery of computer resource over the internet rather of retaining data on your own hard drive, you utilize benefits over the web at another location.Now days there are a considerable measure of organizations that are utilizing cloud computing, such as, Amazon Cloud Drive, G Space, Minus, Web email suppliers like Gmail, Hotmail and Yahoo! Mail store email messages without anyone else servers, A Drive YouTube, Social systems network locales like Face book.

The services model of cloud computing are infrastructure as a service (IAAS), platform as a service (PAAS) and software as a service (SAAS), in (IAAS) model provides just network and hardware, the client installs or develops its own operating system, application and software, (PAAS) model an operating system ,hardware and network are provided and client installs or develops its own application and software, (SAAS) model a pre-made application ,along with any required software ,hardware ,operating system and network are provided.

The characteristics of cloud computing are On-demand service: consumers utilize an online self-benefit gateway to see a service catalog and demand cloud services,Network access: costumersget to cloud services on any client/end-point device from anyplace over a network, Shared resource: enables suppliers to improve resource utilization and to flexibly provision and recover resources and scalability.

The deployment of cloud computing services are made accessible by a private cloud the cloud infrastructure is operated solely for specific organization there are two variants on-premise and externally hosted, public cloud: it is open use and is offered over the internet and are possessed and operated by cloud provider, community cloud is shared by several organization and made an accessible just to those gatherings, hybrid cloud is mix of deferens methods of resource pulling.

Cloud computing is a term that has increased far-reaching using over the last few years. With the exponential increment in data utilize that has went with society's change into the digital 21st century, it is ending up increasingly troublesome for people and associations to keep the majority of their vital information, programs, and systems up and running on in-house PC servers. The answer for this issue is one that has been around for almost as long as the web, however that has just as of late increased across the board application for organizations.

cloud computing works on a similar standard as web-based email customers, enabling customers to get to the greater part of the highlights and files of the system without keeping the main part of that system all alone PCs. Actually, themajority as of now utilize avariety of cloud computing services without acknowledging it'Gmail, Google Drive, TurboTax, and even Facebook and Instagram are all cloud-based applications. For these services, consumers are sending their own data to a cloud-hosted server that stores the data for later access. What's more, as helpful as these applications are for personal utilize, they're much more valuable for organizations that should have the capacity to get to a lot of information over a security, online system connection.

For example, employees can get to users data by means of cloud-based CRM software like Sales force from their cell phone or tablet at home or while travelling, and can rapidly share that data to other approved parties anyplace on the world. In any case, there are those leaders that are staying hesitant about resolving to cloud computing answers for their associations. In this way, we'd get a kick out of the chance to take a couple of minutes andoffer businessadvantages of cloud computing.

A. Cost savings

The most imperative cloud computing benefit is in terms of IT cost investment funds. Organizations, no issue what their type or size, exist to reap money while keeping capital and operational spending to a minimum. With cloud computing, you can keepfundamental capital expenses with zero in-house server storage and application requirements.

B. Reliability

With a managed service platform, cloud computing is considerably more reliable andconsistent than in-house IT infrastructure. Your organization can profitby a huge pool of excess IT resources, and in addition quick failover mechanism – if a server fails,hosted applications and services can easily be transmitted to any of the accessible servers.

C. Manageability

Cloud computing provides upgraded and simplified IT administration and maintenance capabilities through central organization of resource; vendor oversaw infrastructure and SLA back agreement.

D. Flexibility

Your business has just a limited measure of focus to partition between all of its responsibilities. On the off chance that your present IT arrangements are compelling you to confer excessively of your thoughtfulness regarding PC and data storage issue, at that point you wouldn't have the capacity to focus on achieving business objectives and fulfilling clients. Then again, by depending on an outside association to deal with all IT facilitating and infrastructure, you'll have more opportunity to give towards the parts of your business that specifically affect your main concern.

E. Quality control

There are couples of things as detrimental to the achievement of a business as low quality, conflicting detailing. In a cloud-based system, all documents are put away in one place and in a single format. With everybody getting to a similar data, you can keep up consistency in information, maintain a strategic distance from human mistake, and have a clear record of any revisions or updates. Then again, managing data in storehouses can prompt representatives coincidentally sparing distinctive versions of documents, which prompts disarray and weakened information.

Cloud services are well known in light of the fact that they can decrease cost, flexibility, transport new services, continuous, availability, quick deployment and ease of integration. These properties ensure that consumer's data is constantly secure and can't be changed by unapproved consumers and the data is dependably at the most recent forms while being recovered by the consumer.

Despite the fact that there are numerous advantages to adopting Cloud Computing, there are likewise some noteworthy obstructions to selection. A standout amongst the most noteworthy boundaries to adoption is security, followed by issues with respect to consistence, encryption and legal issues. Since Cloud Computing represent to a moderately new computing model, there is a lot of vulnerability about how security at all levels (e.g., network, host, application, and information levels) can be accomplished and how applications security is moved to Cloud Computing. That vulnerability has reliably lead data executives to state that security is their main worry with Cloud Computing. And some association is still not feeling great in the adoption of technology because to concerns of trust and security, data security is one of them.

The importance of data security issues and portion of its solution in cloud environment was talked about and it was additionally feature that encryption is the most generallyutilizedtechnique to make sure the security of data in cloud.

Security is an imperative challenge in cloud.Various security threats and fortifying methodologies used for resolving the encryption issues in cloud resources are analyzed.

Many cryptographic algorithms are accessible to solve data security issue in cloud. Algorithms hide data from unauthorized users, twoactivities performed by these algorithms are encryption and decryption.Encryption is the way toward converting data into mixed form.

Security objectives of data include privacy, accessibility and integrity. The principlepart of encryption is deal with data security from attackers.

Both symmetric key and asymmetric key algorithm can be utilized to encryption data in cloud computing.

II RELATED WORK

In [4]This paper is a method has been proposed rely upon comparison between DES, 3DES and AES were exhibited in to nine variables, Which are key length, cipher type, block size, created, cryptanalysis opposition, security, probability key, possible ACSII printable character keys, time requiredto check all probability key at 50 billion second that achieving effectiveness, give and security, which is at the challenge of researchers, these qualifier's proved the AES is better than DES and 3DES.

Keyword_ Data Encryption, Triple Data Encryption Standard, Advance Encryption Standard.

In [5] this paper is a method has been proposed rely upon Gives a comparison between some symmetric and asymmetric procedures. The components are achieving an effectiveness, adaptability and security, which is a face of specialists. As a result, the better answer for the symmetric key encryption and the asymmetric key encryption is given.The cryptography algorithm and characterization of the kinds of the cryptography algorithmthat presents a performance assessment ofchose symmetric and asymmetric encryption algorithms such as DES, 3DES, AES, Blowfish, RSA. The key length is high in asymmetric encryption algorithm to break the code is complex in RSA. In the part of throughput, Throughput is expanded so control utilization is decreased. Throughput is high in blowfish and blowfish is less power utilization algorithm subsequently speed is quick in the Symmetric key encryption is seen as great. At long last, in the symmetric key encryption strategies the blowfish algorithm is determined as the better solution. In the Asymmetric encryption procedure the RSA algorithm is more secure since it utilizes the factoring of high prime number for key generation. Subsequently, the RSA algorithm is found as the better solution in this technique.

Keywords- Cryptography; Encryption; AES; DES; 3DES; Symmetric key encryption; Asymmetric key encryption.

In [6] this paper is a method has been proposed1
rely upon Searchable Encryption and homomorphic2
Encryption algorithms are most well-known cryptosystems utilized as part of cloud. HE techniques are highly secured but less efficient contrasted with SE techniques, while SE methods are more proficient and less secured contrasted with HE techniques. SE is a best tradeoff amongst efficiency and security. By considering distinctivecriteria's of SE techniques one can devise another efficient hybrid algorithm to enhance the hardness of security as close as conceivable to FHE methods.

In [7]This paper is a method has been proposed rely upon model based on discrete data and key cloud servers and a customer-based data encryption benefit for expanding the reliability in cloud computing environments. The key generation process is done in a different cloud application and public and private keys are put away in key cloud servers. In addition, the encryption and decryption forms are done in client side by a service that named "data encryption service".View of independent information and key cloud servers and a client based data encryption service,for applying this encryption system a relative study was done by analyzing the qualities and weaknesses of six famous asymmetric key encryption algorithms (i.e. Unique RSA, RSA Small-e, RSA Small-d, MREA, E-RSA, and EAMRSA). These algorithms were quicklydepictedand redeveloped in a similar situation for the reproduction procedure to research the performance in client-based data encryption service. Besides, the security investigation was finished byassessing the performance of described algorithms against three popular attacks: Brute Force, Mathematical, and Timing Attack. As per theoutcomes E-RSA in the most proper algorithm for utilizing as a part of client-based data encryption service by accomplishing increasing speed, accuracy, and security in this service in light of similarity issues in a client-side service.

III. SECURITY AND ENCRYPTION ISSUES

In[1] This paper is a method has been proposed rely upon describing data security in cloud utilized public key cryptography with matrices which is structure divided into two parts one of them deal with pre-processing of data and another part deal with the key generation ,key agreement and encryption/decryption processes.

In the first part it includes two processes of data shuffling and traversing of the data.

A Preprocessing Of Data

This divided into two stages

1. shuffling of the data

The first stage includes the shuffling of the data for which the straight congruenttechnique is utilized and after that the data is orchestrated in the form of a matrix of some dimension n x n.

Expect L be the length of the message to be encrypted. We consider here two arrays as take after

1) Index [1…….L] is an array including all the index of the message, and

2) Hash [1……..M] is the array including some interest numbers with the end goal when we apply the linear compatible technique to the array index [1…L] then the output of the index [1…L] array does not contain any duplicateindex.

The linear compatibletechnique can be detailed as follows:

STEP 1) For I = 1 to initialize index [I] = I, and initialize x = 1, STEP 2) For J = 1 to M, repeat Step (3) to Step (5),STEP 3) For K = 1 to L, repeat Step (4) to Step (5)

STEP 4) x = ((J+1)*x + hash [(J+K) mod M]) mod L, STEP 5) Swap (index [K], index[x]), STEP 6) Return index [1…..L]

The first message is shuffled or rearranged based on the array index [1….L] that we have gotten as an output utilizing the technique depicted above. Presently an integer N is chosen to such as extent that N2 ≥ L, i.e. the estimation of N2is more noteworthy than or equal to that of L and the data is orchestrated in an N x N matrix form.

2. Traversing the Data Matrix

Includes reading out of the data from the data matrix of order N x N.

This can be accomplished in any of the accompanyingbehavior which are delineated through suitable self-explanatory diagrams:

1.1.1 Spiral Traversal
1.1.2 Reversed Spiral Traversal
1.1.3 Helical Traversal
1.1.4 Sine Waveform Traversal
1.1.5 Reverse Helical

Since here there are five patterns, so there can be 5! Conceivable sequences. give the sequences be T1, T2… T120.Suppose that the arrangement represented above is T1.

B. Key generation

We first take a matrix G of size n X n such that |G| = 0 and a list L = {a1, a2……an} of integers. So, we can form a circulant matrix Lc = Circe(x1, x2….. xn) where the xi's are nothing but ai's. Now, let σ be a permutation on the set {1, 2, 3 ……. n}.

Now, we try to find a Y such that Ri.Y = Lc σ (i) i.e. Ri.Y = Lc (1, i) where i = 1, 2, 3 …. N.

The above system of equations can be put in the form G.Y = X The above system of equations should be consistent and as we have taken |G| = 0, so the system cannot have a unique solution. We take one such Y and from the elements of Y, we can form a circulant matrix Yc. Now, we formulate a matrix P = Lc.G.Yc Then we take Public Key: {G, Lc, P} Private Key: {Yc, σ}.

C. Key Agreement

1. G is the matrix known to both the communicating parties.Party 1 chooses a private key {Lc,Yc, σ1} by utilizing a list L Find T1 and send to PARTY 2Party 2 will also choose a private key {Mc, Zc, σ2}utilizing list M. discover T2 and send to PARTY 1.PARTY 1 receive T2 and calculates S=T2.Yc, PARTY 2 receive T1 and calculates S=T1.Mc.

D. Encryption And Decryption Algorithm

1 Encryption Algorithm

Let S be the data matrix to be encrypted. We create two circulant matrices X1 and X2.

Calculate

D1 = X1.G.X2 and D2 = {(X1.P.X2) XOR S} where XOR operator between the symmetrical elements of the two operand matrices. The set {D1, D2} is the encrypted form of the data S.

2 . The Decryption Algorithm

In the above stage we got the encrypted data {D1, D2} of the data S. presently we can get the first data S back from this encrypted data by utilizing the secret key of the communicating party as follows:

Lc.D1. YcXOR D2 = Lc.X1.G.X2. YcXOR X1.P.X2 XOR S

= Lc.X1.G.X2. YcXOR X1.Lc.G. Yc.X2 XOR S

= Lc.X1.G.X2. YcXOR Lc.X1.G.X2. YcXOR S

= 0 XOR S = S

Hence we have decoded the data utilizing the private key of the communicating party.

D. Security Of The Algorithm

The possible assaults on the security of this algorithm can be either by specifically solving the system of equations G.Y = X or utilizing the matrix P = Lc.G.Yc. To maintain a strategic distance from the primary probability of, we need to choose the augmented matrix [G: X] with the end goal that the rank of [G: X] = rank of G = r < n, where n is the number of unknowns.

At that point the n-r variables are independent and so we can take any self-assertive values for these variables and the remaining r variables are dependent on these n-r variables.

In this way, on the off chance that we can discover matrices G and X with the end goal that the value of rank r is least and that of n is all the more, at that point it will be ensured that the number of independent variables is high[7,8,9], so that searching the solution becomes an NP-Complete issue. In the second case, the intruder can attempt to know the estimationof Ycutilizing P = Lc.G.Yc. By utilizing the list L given in the public key, he can have possibly n! Estimations of Lcthus the intruder have n! Different systems of equations of the form P = Lc.G.Yc, which again gives rise to NP-Complete issue.

In [2] this paper is a method has been proposed rely upon issue of data security in the midst of transmission of data by utilizingRijndael encryption Algorithm-Rijndael as the standard symmetric key encryption algorithm to be utilized to encrypt sensitive data. Rijndael is an iterated block cipher, the encryption or decryption of a block of data is refined by the iteration (a round) of a particular change (a round function). As input, Rijndaelacknowledges one-dimensional 8-bit byte arrays that make data blocks. The plaintext is input and afterward mapped onto state bytes. The cipher key is additionally a one-dimensional 8-bit byte array. With an iterated block cipher, the distinctive transformations operate in sequence on intermediate cipher results (states)

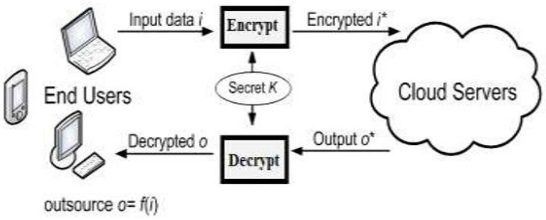

Figure 1. Methodology [2]

The steps of the technique shown in figure 1 are given below:-

1. User sends the authentication request to the Cloud Service Provider (CSP).
2. CSP checks the authorization utilizing EAP-CHAP and sends the acknowledgement back to the user.
3. User first encrypts his data and then outsources it to the server.
4. When the user downloads his data from CSP, it is gotten in the encrypted formula.
5. To utilize the data user can decrypt it utilizing same key utilized for encryption.

This paper achieves confidentiality and security.

IV ENCRYPTION

The code for encryption process. The User data is encrypted by utilizingRijndeal Encryption. Symmetric key is utilized for encryption. The Rijndeal can be executed easily and it is a standout amongst the most secure algorithms in the world. Rijndealexecution has 128,192or 256 bit key lengths. Size of data blocks to be encrypted with Rijndeal is always 128 bits. Initial round of Rijndeal is AddRoundKey, this is trailed by four iterative round including subBytes, shiftRows, and mixColumns and add round key. Rijndeal with 128 bit key length has 10 rounds, 192-bit has 12 rounds and 256 bit has 14 rounds. Each round comprises of the following steps.

1. Initial AddRoundKey
2. SubBytes () Transformation
3. Substitutional Box Created ForSubbytes
4. MixColumns () Transformation
5. AddRoundKey () transformation

In [3] this paper is a method has been proposed rely upon two encryption algorithm one for plaint text and another for encrypted text.

It changed over plain text to whitened text; the whitened text transformationoccurs by changing over the message to hexadecimal format using MD5 and converting to encryption outlineutilizing AES and performing XOR with the Key that will be utilized for the encryption.

The schema is very extremely basic yet wouldn’t fret have been taken to secure the key used for encrypting the data[10,11].

The steps of the proposed algorithm come with the AES (Advance Encryption Standard) Algorithm. The essential difference between the AES and the proposed one is that the quantities of the rounds are restricted to 5 which are basically 10, 12 and 14 for 128,192 and 256 bit blocks. Alongside this the encryption of the AES is given one key as well as with two keys so that if breaching occur in middle of then one can know one of the key the block encrypted with and the alternate keys are saved.

The numbers of steps that are processed on each block are basically:

1. Convert to State Array
2. Transformations (and their inverses)
   1. Add Rounds Keys: every byte of the state is joined with the round key utilizing bitwise xor.
   2. Substitute Byte: a non-linear substitution step where every byte is replaced with another according to a lookup table.
   3. Shift Row: transposition step where each row of the state is moved cyclically a certain number of steps.
   4. Mix Column: a mixing operation which operates on the columns of the state joining the four bytes in every column.

V. KEY EXPANSION

The transformation is performed at[9] each round on each block of the data. The given input is firstly divided into the block of the fixed size values.

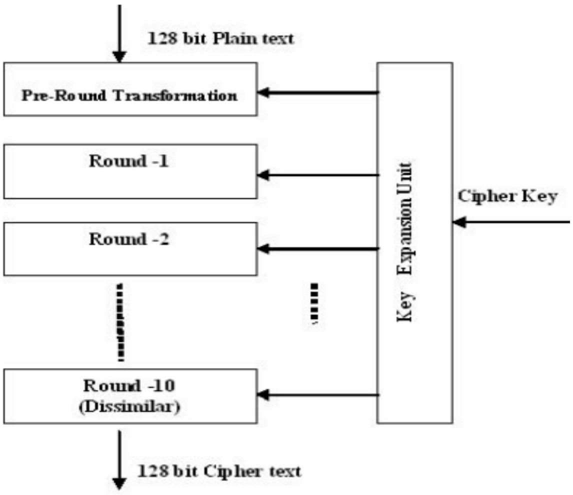

Figure 2 AES algorithm [3]

The last step of the algorithm will occur. The AES encrypted text is given as the input to the RC4.The algorithm process the data in the formula of the stream. RC4 creates a pseudorandom stream of bits similarlyas with any stream cipher. These can be utilized for encryption by joining it with the plaintext utilizing bit-wise select-or; decryption is played out a similar way arranged stream. To create the key stream the cipher makes utilization of a secret inside state which consists of two parts:

1. A permutation of all 256 possible bytes (meant "S”).
2. Two 8-bit index-pointers (meant "i" and "j").

The permutation is initialized with a variable length key normallyin the vicinity 40 and 256 bits.

VI . CONCLUSION AND FUTURE WORK

About Cloud computing and advantages that is enabling manage resource and cost by means of internet. Data security has become the vital problem of cloud computing security; security is a major requirement in cloud computing while we talk about data storage. Security through encryption of messages could tackle a portion of the vital issues in regards to cloud computing frameworks so There are number of existing techniques utilized to implement security in cloud such symmetric and asymmetric algorithms of cloud encryption techniques.

New security strategies should be produced and more established security techniques should have been drastically changed to have the capacity to work with the cloud architecture.There will be all the more better comprehension of the outline difficulties of cloudcomputing, and make ready for additionally researchin this area.

REFERENCES

[1] Enhancing security in cloud computing using public key cryptography with matrices by Birendra Goswami and Dr.S.N.Singh.

[2] Cloud data security using encryption technique by Sanjoli Singla and Jasmeat Singh.

[3] Enhancing security in cloud computing structure by hybrid encryption by Aparjita Sidhu and Rajiv Mahajan.

[4] New Comparative Study Between DES, 3DES and AES within Nine Factors byHamdan.O.Alanazi, B.B.Zaidan, A.A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani .

[5] Comparative Study of Symmetric and Asymmetric Cryptography Techniques by Ritu Tripathi1, Sanjay Agrawal2.

[6] A Comparative Study of Homomorphic and Searchable Encryption Schemes for Cloud Computing by Prasanna B T and C B Akki.

[7] A comparative study of applying real-time encryption in cloud computing environments by Faraz Fatemi Moghaddam, Omidrezakarimi, MaenT.Alrashdan.

[8] Hanafy, I.M., Salama, A.A., Abdelfattah, M. and Wazery, Y., 2012. Security in Mant based on Pki using fuzzy function. IOSR Journal of Computer Engineering, 6(3), pp.54-60.

[9] Hanafy, I.M., Salama, A.A., Abdelfattah, M. and Wazery, Y.M., 2013. AIS Model For Botnet Detection In MANET Using Fuzzy Function. International Journal of Computer Networking, Wireless and Mobile Communications (IJCNWMC), 3(1), pp.95-102.

[10] Houssein, E.H. and Wazery, Y.M., Vortex Search Topology Control Algorithm for Wireless Sensor Networks.

[11] Y.M.Wazery Survey on Wireless Sensor Network Current Security issues, INTERNATIONAL JOURNAL FOR RESEARCH & DEVELOPMENT IN TECHNOLOGY, Volume-6,Issue-5(Dec-16)