International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-8, Issue-3, May 2020
https://doi.org/10.21276/ijircst.2020.8.3.38
www.ijircst.org

Analysis of Frameworks in Cloud Environment

Ashima Narang

ABSTRACT- Cloud is one of the advances, whose utilization is being expanded step by step for various purposes according to client's prerequisite. For the most part this innovation is utilized for capacity reason as a result of this, the clients need not to have any equipment stockpiling gadgets rather than that their information will be put away on the system. These frameworks must be increasingly secure with the goal that they give secrecy, protection and assurance for their consumer loyalty. Different calculations were created to make sure about cloud systems yet these calculations can't meet the prerequisites of the clients. In this paper, there is a comparison, of a hybrid approach and the individual algorithm to get the best results.

KEYWORDS- RSA, ECC, Hybrid, Cloud Computing, Encryption

I. INTRODUCTION

In this relentless life, individuals are currently particularly slanted to the innovation and the world will turn out to be more educated as contrast with previous times and in these times, cloud has become one of the most loved specialized worldview in the field of calculation and offers a different types of assistance as required by clients which incorporates programming assets just as equipment assets from unmistakable server farms utilizing Internet to satisfy the requests of their customers.

The quantities of administrations are given by cloud models that incorporate programming as a help, Software as a service (SaaS), stage as assistance, Platform as a service (PaaS), and foundation as a help, Infrastructure as a service (IaaS) according to the need of the clients. These administration models are secluded with their isolated capacities and the liabilities of these are under risky circumstances. Along these lines, there is a need to secure cloud foundation and it is one of the significant worry as its use will be expanding step by step. There is diverse security instruments were proposed by numerous scientists yet these methods are not capable guarantee that the cloud is presently chance free. For example, the principle focal point of the conventional security calculations was either to give a defensive shield to the information that client needs to store or to cook confirmation for the approval of the clients by utilizing unmistakable instruments which doesn't address the security issues thus, these days a protected framework is required which will exceptionally concentrate on the security boundaries and furthermore need to team up validation and information protection for the massive degree of security, and for this, need to deal with the whole parts of the cloud either from client end or administration end.

Besides, cloud turns into the key element for the vast majority of the business associations which help to the decrease of the extra room for the heap of bountiful information as that can be hold by the cloud. Nowadays, even normal clients are firmly impacted by the highlights of the cloud like devoted storerooms so they are quick to utilize it. Be that as it may, this expanded interest will be the fundamental driver of the weakness of the information. Cloud security worldview incorporates set of approaches and innovations that notice to shield cloud framework and its information from phonies. Different information insurance and security procedures have been proposed by various specialists that engaged to pick up the client's enthusiasm by giving confirmation of the security.

Besides, the issues of the security are getting looked at as cloud despite everything faces the difficulties as far as assurance of information just as misrepresentation and these can likewise be veer off in light of the kind of the information. The fundamental target of this paper is to examine most recent arrangements and discover which one will be increasingly viable to deal with the up and coming difficulties of distributed computing. In the next section of this paper, I shall be discussing about the individual Rivest-Shamir-Adleman (RSA) [1] environment and RSA hybrid with Elliptic curve cryptography (ECC) [2]. I have taken parameter of time as encryption time and decryption time which is believed to be the biggest issue of encryption while uploading the data over the Cloud environment.

II. DESCRIPTION OF ALGORITHMS

Giving secure environment to the client information is a significant problem in distributed computing. So as to practice the distributed computing adequately, the clients using the cloud services need the enhanced security answers for storage and recovery of the information. Cryptography is a viable approach to item the touchy data, importantly.

Manuscript received May 23, 2020

Ashima Narang, Assistant Professor, Department of Computer Science & Engineering, Amity School of Engineering and Technology, Amity University Haryana, Gurugram, India, +91-7087780777, (e-mail: ashimanarang04@gamil.com).

The key administration is straightforward procedure utilizing IBE that utilizes the human-comprehensible personalities, for example, IP addresses, novel names and email addresses, and so on and use the qualification based Public Key Framework (PKI) as open keys. Client have the option to write code in a plain line and encode the text among recipient character and does not use the open key and declaration, yet PKG gives the private key related with the comparing personality, the beneficiary utilized this private key to unscramble such cipher text.

RSA is a famous method used for encryption to secure the information. The encryption strategies, for example, Elyptical Cryptography and intermediary re-encryption is likewise a ground-breaking instrument to secure the information from foe. This segment depicts a few related works that utilizes the previously mentioned encryption calculation to give the security to client information. The RSA open key cryptosystem was created by R. Rivest, A. Shamir and L. Adleman.[4] The RSA cryptosystem depends on the sensational contrast between the simplicity of discovering enormous primes and the trouble of considering the result of two huge prime numbers.

RSA is an open key calculation designed by Rivest, Shamir and Adleman. The key utilized for encryption is not quite same as (however identified with) the decoding key utilized to decode. [5]

- The calculation relies on measured exponentials. Numbers n, m and M are picked with the property that on the off chance that B will be a number not as much as M, at that point (Bn mod M)m mod M = B.
- Hence this results that you can encode B with n and decode by using m. Further, again you can scramble using d and decode utilizing n (however to adjust is generally alluded to as marking and check).
- The numbers (n, M) is known as the open key and can be distributed
- The numbers (n, M) is known as the secret key and must be left well enough alone.
- n, is a number which is known as the open example, and m, is the number that is known to be the private type, and M will be taken as modulus. When discussing the length of the key regarding RSA, what is implied is the length of the modulus.
- A calculation that utilizes various keys which revert to encryption and unscrambling is supposed to be awry.
- Anybody who realizes the open key can use it to make encoded information, yet just the owner of the secret key can unscramble them.
- Conversely the proprietor of the secret key can scramble the information which is able to be decoded by somebody having the open key. Who so ever unscrambles the information has be have certainly have the secret key to encode the data received.
- Assume P wishes to communicate something specific (state's') to Q. To encode the message utilizing the RSA encryption plot, P must acquire Q's open pair of keys (n, s). The message to send should now be scrambled utilizing this pair (n , s). In any case, the message 'T' must be spoken to as a whole number in the stretch [0, s-1]. To encrypt, we have just process the number 'c' where c = T ^ n mod s. We have sent the figure text c to Q.

RSA Algorithm:

1. Pick 2 unmistakable numbers which are prime say a and b.
2. Let m = a*b.
3. Let φ(a*b) = (a − 1)(b − 1) where φ is the totient work.
4. Pick a number e with the ultimate goal that 1 < n < φ(a*b), and n and φ(a*b) shares only 1 as a divisor (n and φ(a*b) so they are said to be coprime).
5. Discover K

K is a mystery key example. The open key comprises of e (frequently called open example) and m (mostly said to be modulus). The mystery key comprises of n and K (secret type). The message m is encrypted utilizing recipe, where c is the scrambled message. The scrambled message is unscrambled utilizing equation.

Encryption and unscrambling recipes tell the best way to encode and decipher a solitary number. Greater (or unique) snippets of data are encoded by changing over them into (possibly huge) whole numbers first. As RSA isn't especially quick, it is normally just to scrambles the key of few quicker calculation. After RSA unscrambles the key, this strengthening calculation utilizes it to unscramble the remainder of the text. [5]

The most usde mainstream open key approach for cryptography is Elliptic curve cryptography (ECC). Neal Koblitz [2] and Victor Miller [3] explained elliptic bend in 1985 to structure open key framework for cryptographic reasons. Mathematical type of added substance bunch is portrayed by the gathering or set of arrangement alongside their point at limitlessness O.

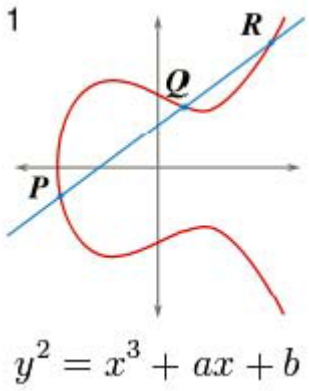

Fig.1: Simple Elliptical Curve

Generation of the key [6] is a significant part in ECC where open and secret keys are created. By utilizing the beneficiary's open key, the scrambling of the sender's the message is done and it is unscrambled by the recipient using its key which is private to him. An arbitrary number taken as s must be chosen inside the scope of 1 and n-1. M is the most extreme cutoff that ought to be a prime number. The generation for open key is done as:

P = K * Q

Where Q is point on the curve, P denotes the open key and K depicts the secret key. [6]

• Encryption

Leave D, alone the plain text of RSA. This plain text needs to speak to on the bend. This contains T(IDi , p). That means the encryption of recipient personality and the information.

Consider 'p' has the point 'D' on the twist 'T'. Heedlessly select 'm' from [1 – (n-1)].2 figure writings will be produced left them alone F1 and F2.

F1 = n*Q

F2 = D + n*P

• Decryption

The actual information is received when the decryption is performed. Here, the plain text of RSA is received i.e. T(IDi , m).

To decrypt, the following formulae is used:

D = F2 – n * F1 [6]

Two phases are performed to get the complete encryption. We also get the user's and the receiver's identity. In this type of Encryption, part the client information alongside collector personality cipher text is created utilizing combination of RSA plus ECC encryption calculation. The accompanying encryption method utilizes to scramble the watchword and client personality which is secondary stage of this work.

III. COMPARISION

When uploaded over cloud, the performance metrics, encryption time and decryption time was calculated for encrypting and decrypting of the data using RSA and RSA and ECC hybrid algorithms. For comparison, the data with the size of 138683 KBs was uploaded on both the environments and the encryption time for the same are compared as below:

Table 1: Encryption time taken by RSA and RSA + ECC

Algorithm	Data Size	Encryption Time (in sec)
RSA	138683 KB	99059.2
RSA+ECC	138683 KB	3346

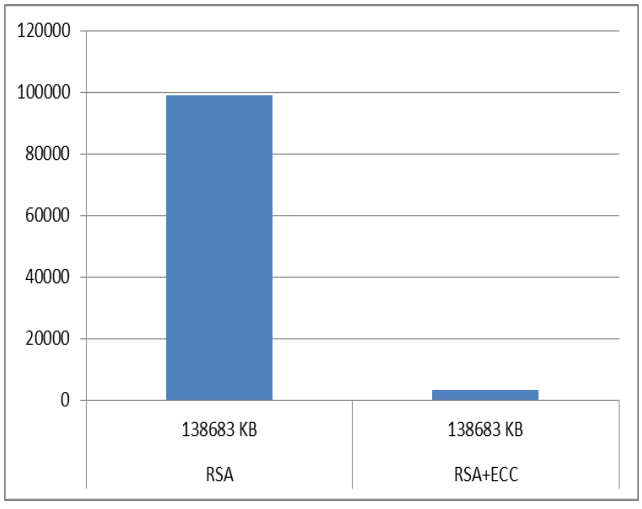

Fig 2. Comparision showing results for Encryption Time for RSA and RSA + ECC

Table 2: Decryption time taken by RSA and RSA + ECC

Algorithm	Data Size	Decryption Time (in sec)
RSA	138683 KB	515108.2
RSA+ECC	138683 KB	17399

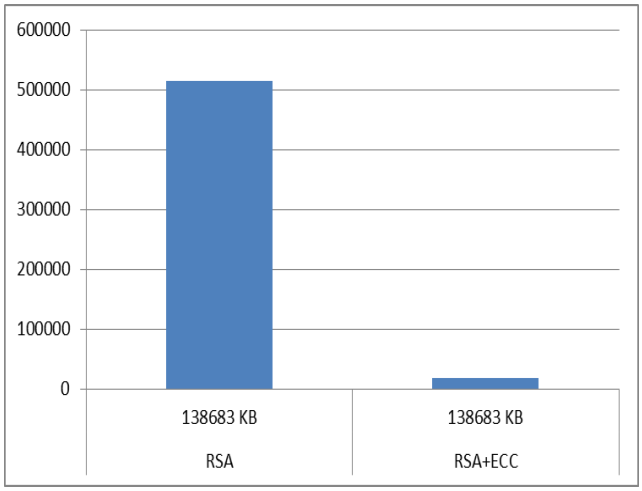

Fig 3: Comparision showing results for Decryption Time for RSA and RSA + ECC

The above results clearly show us that the RSA + ECC takes much lesser time as compared to only RSA algorithm individually. The time taken for Encryption and for decryption to upload the same data over the cloud and then encryting and decrypting them, for both of them, the best results are for the hybrid algorithm, RSA + ECC.

IV. CONCLUSION

In today's high pace world, where there is a lot of data bundled with everybody, people want to use cloud to store their data. When it comes to security, encryption comes up first. But when encryption comes, time taken for encryption and decryption becomes the matter of concern. Hence, the comparison was performed to find out the better encryption algorithm out of RSA + ECC hybrid algorithm and RSA individually. From the experimentation performed in the simulated cloud environment, RSA + ECC, hybrid approach, was found out to be much better in terms of time taken for encryption and decryption. For the future work, I would like to compare its results with other algorithms available and also with additional performance metrics.

REFERENCES

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

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

[3] V. Miller. Use of elliptic curves in cryptography .Advances in Cryptology—CRYPTO ’85 (LNCS 218) [483], 417–426, 1986
[4] 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
[5] M. Preetha, “A STUDY AND PERFORMANCE ANALYSIS OF RSA ALGORITHM”, International Journal of Computer Science and Mobile Computing, Vol. 2, Issue. 6, June 2013, pg.126 – 139.
[6] G.Prabu kanna, “Enhancing the Security of User Data Using the Keyword Encryption and Hybrid Cryptographic Algorithm in Cloud”, International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) – 2016, pp. 3688-3693
[7] A. D. Gupta, “Comparative Analysis of Various Cloud Security Frameworks”, International Conference on cyber security and privacy in communication networks (ICCS-2018), pp. 379-384.
[8] D.Boneh, M.Franklin, Identity-based encryption from the weil pairing, Advances in Cryptology–CRYPTO2001, SantaBarbara, California,USA, LNCS, 2139, Springer, Berlin, 2001.
[9] 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.
[10] Y. Chen and J.-F. Tu, “A Novel Cloud Computing Algorithm of Security and Privacy,” Mathematical Problems in Engineering, vol. 2013, pp. 1–6, 2013.

ABOUT THE AUTHORS

Ashima Narang has completed her B.Tech, M.Tech and is pursuing PhD in the field of computer Science from various prestigious institutes of India. She has published 16 research papers in reputed journals and conferences and has guided students for projects from undergraduate and graduate courses. She is also an active member in the various professional bodies like IAASSE, internet society, SCIEI etc. She is the reviewer to various journals from her expertise field.

