International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 06 | June - 2021 ISSN: 2582-3930

STUDY OF PUBLIC-KEY ENCRYPTION WITH MULTI-CIPHER TEXT EQUALITY TEST IN CLOUD COMPUTING

Dr. V. Prasanna Srinivasan[1], Agalya M[2], Mallela Deepthi[3] , Divya R[4]

[1]Associate Professor, Department of Information Technology, R.M.D Engineering College

[2,3,4] Student, Department of Information Technology, R.M.D Engineering College

---

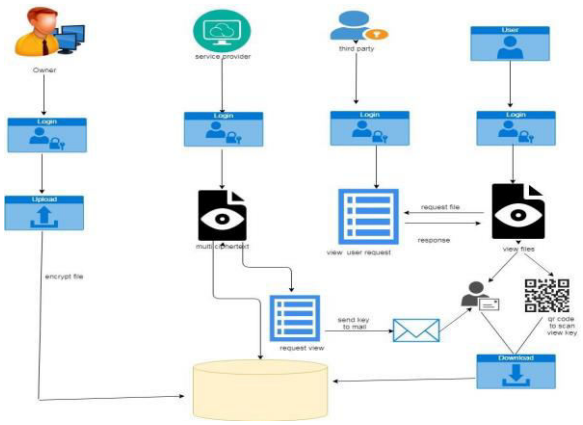
ABSTRACT: Distributed computing empowers clients to eliminate the need of the need of nearby equipment architecture,which eliminates the weight of the clients from high calculation costs. Therefore,it has drawn in much consideration and exploration has been led intensely on it. To ensure clients' privacy,data is typically encryptedprior to being shipped off the cloud worker. As the subsequent framework is unusable, sincethe cloud can presently don't look all through the data,new cryptographic primitivessuch as open key encryption with fairness test (PKEET) have been introduced.In this paper, by giving a novel idea of public-key encryption withmulti-ciphertext equity test (PKE-MET). In PKE-MET, each ciphertext candesignate a number s to such an extent that the cloud worker can just perform balance tests on this ciphertext with other s − 1 ciphertexts, where all their assigned numbers ares.For PKE-MET, other than customary OW-CPA and IND-CPA security, we uniquely characterize Number security. We launch PKE-MET to a substantial plan and give its security proof.Furthermore, to empower the crude to be more down to earth inapplications, we extend it to the idea of PKE with adaptable MET (PKE-FMET).In PKE-FMET, the cloud worker can perform correspondence tests on any number ofciphertexts as long as the greatest number of their assigned numbers is lessthan or equivalent to the quantity of ciphertexts. We build a PKE-FMET schemebased on our PKE-MET development and demonstrate its security under the characterized security models. Moreover, the exhibition examination primarily of productivity andsecurity between our developments and existing uniformity test plans in distributed computing show that our proposed plans are more proficient and secure in the multi-ciphertext situation.

KEYWORDS: Cloud Computing,PKEET,PKE-MET,Equality test.

I.INTRODUCTION

In the current time, enormous data hurries into our workstations and telephones each and every day. This prompts the issue of advanced gadgets to store and register the got huge loads of information. Distributed computing gives an effective method to move the capacity and calculation overheads from clients to the cloud worker. It permits clients to save information on cloud and the cloud worker assists with performing part of calculation on the information. Likewise, to secure information protection against the genuine however inquisitive cloudserver and different vindictive assaults from outside, clients decide to store their encoded information on cloud, which leaves the cloud worker a test to perform calculations on scrambled information The property of PKEET permits exceptionally pragmatic applications, especially cloud-based situations. For instance, PKEET empowers information measurements in the cloud data set since it can perform fairness test over scrambled information even those from various clients. Another application is that individuals can discover companions with similar interests by coordinating with their encoded information with others'. Ensuing endeavors for PKEET have been committed to sorts of approvals to fulfill distinctive security necessities, effectiveness improvements,and augmentations to different natives.

II. DESIGN ARCHITECTURE



III. LITERATURE REVIEW

TITLE: Ciphertext-Policy Attribute-Based Encryption With Delegated Equality Test in Cloud Computing.

AUTHOR : Qiang Wang; Li Peng; Hu Xiong;

YEAR : 2017.

DESCRIPTION: Public key encryption supporting balance tests (alluded to asPKE-ET) gives the ability of testing the identicalness between twomessages encoded under various public keys. Ciphertext-strategy property based encryption (CP-ABE) is a promising crude to accomplish adaptable and secure information partaking in the distributed computing by giving adaptable one-to-numerous encryption. In this paper, we initially instate the idea of CP-ABE with a uniformity test (CP-ABE-ET) by joining the thoughts of PKE-ET and CP-ABE. Utilizing ABE-ET crude, the beneficiary can assign a cloud worker to play out a comparability test between two

messages, which are encoded under various access arrangements. During the designated comparability test, the cloud worker can't acquire any information on the message scrambled under either access strategy. We propose a substantial CP-ABE-ET plot utilizing bilinear blending and Vieta's recipes, and give the security confirmation of the proposed conspire officially in the standard model. In addition, the hypothetical investigation and test reproduction uncover that the proposed conspire is effective and commonsense.

IV.PROPOSED SYSTEM

To take care of this issue, we propose a twofold encryption idea. The proposed structure can both exploit distributed storage and secure the protection of information. Plus, Hash-Solomon code calculation is intended to isolate information into various parts. At that point, we can place a little piece of information in nearby machine and mist worker to ensure the security. In addition, in view of computational knowledge, this calculation can process the appropriation extent put away in cloud, haze, and nearby machine, separately. Through the hypothetical security examination and exploratory assessment, the attainability of our plan has been approved, which is actually an amazing enhancement to existing distributed storage schemes

V.MODULES DESCRIPTION

1.User Interface Design: This is the primary module. The significant job for the client is to move login window touser window. This module has made for the security reason. In this login page we need to enter login client id and secret phrase. It will check username and secret word is match or not (substantial client id and legitimate secret phrase). On the off chance that we enter any invalid username or secret key, we can't go into login window to client window it will shows mistake message. Along these lines, we are keeping from unapproved client going into the login window to client window. It will give a decent security to our undertaking. Along these lines, worker contain client id and secret word worker additionally check the verification of the user.It well improves the security and keeping from unapproved client goes into the organization. In our undertaking we are utilizing JSP for making plan. Here we approve the login client and worker verification.

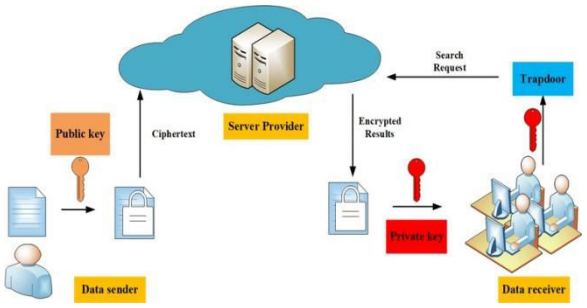
2.File Upload: In this module, after login the owner will transfer the document subtleties and it will be put away in the data set.

3.Re-Encryption Process By Service Provider: In this module, when the document is getting transferred in the back-end there happens the double encryption interaction and it will be put away in the information base.

4.User Request File: In this module, the client will send the file request to the Third party for which documents, the client needs the entrance. Without the consent structure the Third party and specialist organization, the client can't ready to download the document.

5.Response By Third Party And Service Provider: In this module, the Third party and specialist organization will be giving the acknowledgment to the client for which record needs the entrance. After the acknowledgment, the record key will be sent to the client through email.

6.Download The File: In this module, after getting the key from the third party and service provider, the user can download the file using scan qr code show the file key(public key) and give email key(private key) provided by the third party and service provider.



VI.ALGORITHMS

RSA algorithm: It is a public key encryption procedure and is considered as the most secure method of encryption. It was concocted by Rivest, Shamir and Adleman and subsequently name RSA calculation.

Step 1: Generate the RSA modulus

The underlying strategy starts with determination of two indivisible numbers to be specific p and q, and afterward ascertaining their item N, as appeared.

$$N=P*Q$$

Step 2: Derived Number (e)

Consider number e as a derived number which should be greater than 1 and less than (p-1) and (q-1). The primary condition will be that there should be no common factor of (p-1) and (q-1) except 1.

Step 3: Public key

The predefined pair of numbers n and e frames the RSA public key and it is disclosed.

Step 4: Private Key

Private Key d is determined from the numbers p, q and e. The numerical connection between the numbers is as per the following

$$ed = 1 \bmod (p-1)(q-1)$$

Encryption Formula:

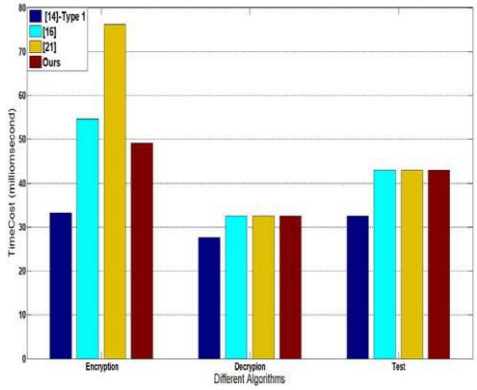
Consider a sender who sends the plain instant message to somebody whose public key is (n,e). To scramble the plain instant message in the given situation, utilize the following syntax –

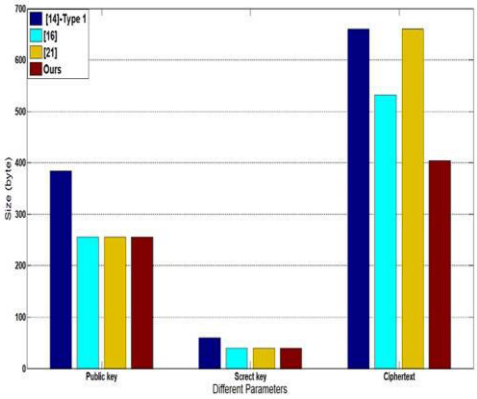
C = Pe mod n

Decryption Formula:

The decoding cycle is straight forward and incorporates examination for computation in a precise methodology. Considering collector C has the private key d, the outcome modulus will be determined as

Plaintext = Cd mod n





VII.CONCLUSION

In this paper, we presented the thought of public-key encryption with multi-ciphertext fairness test (PKE-MET). Along these lines, we started up it to substantial development and gave its security evidences under the characterized security models. Besides, to empower it to fulfill reasonable application, we stretched out PKE-MET to theconception of PKE with adaptable MET (PKE-FMET). At last, in light of our proposed PKE-MET conspire, we introduced a PKE-FMET development accomplishing steady size ciphertext rather than unimportant development where the size is direct.

VIII.REFRENCES:

[1] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with watchword search," in EUROCRYPT 2004, Interlaken, Switzerland, May 2-6, 2004, ser. LNCS, vol.3027. Springer, 2004, pp. 506–522.

[2] C. Upper class, "Completely homomorphic encryption utilizing ideal cross sections," in STOC 2009, Bethesda,MD, USA, May 31 - June 2, 2009. ACM, 2009, pp. 169–178.

[3] G. Yang, C. H. Tan, Q. Huang, and D. S. Wong, "Probabilistic public key encryption with balance test," in CT-RSA 2010, The Cryptographers' Track at the RSA Conference 2010, San Francisco, CA, USA, March 1-5, 2010, ser. LNCS, J. Pieprzyk, Ed., vol. 5985. Springer, 2010, pp.119–131.

[4] Q. Tang, "Towards public key encryption plot supporting fairness test with fine-grained approval," in ACISP 2011, Melbourne, Australia, July 11-13, ser. LNCS, vol. 6812. Springer,2011, pp. 389–406.

[5] Q. Tang, "Public key encryption supporting plaintext balance test and client determined approval," Security and Communication Networks, vol. 5, no. 12, pp. 1351–1362, 2012.

[6] S. Mama, M. Zhang, Q. Huang, and B. Yang, "Public key encryption with designated correspondence test in a multi-client setting," Comput. J., vol. 58, no. 4, pp. 986–1002, 2015.

[7] K. Huang, Y. Chen, and R. Tso, "Semantic secure public key encryption with separated balance test - PKE-FET," in SECRYPT 2015, Colmar, Alsace, France, 20-22 July. SciTePress, 2015, pp.327–334.

[8] Q. Tang, "Public key encryption plans supporting equity test with authorisation of various granularity," International Journal of Applied Cryptography (IJACT), vol. 2, no. 4, pp.67304–321, 2012.

[9] Y. Lu, R. Zhang, and D. Lin, "More grounded security model for publickey encryption with uniformity test," in Pairing 2012, Cologne, Germany, May 16-18, ser. LNCS, vol. 7708. Springer, 2013, pp.65–82.

[10] K. Zhang, J. Chen, H. T. Lee, H. Qian, and H. Wang, "Productive public key encryption with uniformity test in the standard model," Theor. Comput. Sci., vol. 755, pp. 65–80, 2019.