PUBLIC-KEY ENCRYPTION WITH WATCHWORD SEARCH USING CONSENSUS ALGORITHM IN BLOCKCHAIN

Devaraj T[1], Suriya R[2], Sathish Kumar J[3], Vinoth R[4]

[123]Student, [4]Assistant Professor
Department of Information Technology
Gojan School of Business and Technology, Redhills, Chennai-600052

Abstract*: Cloud computing empowers clients to eliminate the need of the need of neighborhood equipment design, which eliminates the weight of the clients from high calculation costs. Along these lines, it has pulled in much consideration and examination has been led intensely on it. To ensure clients' security, information is generally encoded before being shipped off the cloud worker. As the subsequent framework is unusable, since the cloud can at this point don't look all through the information, new cryptographic crude, for example, public-key encryption with correspondence test (PKEET) has been presented. In PKEET, clients can test whether the hidden messages of two code messages encoded under various public keys are equivalent or not without the need to decode those ciphertexts. This is a valuable device, particularly for the cloud data set, since PKEET chiefly centers around the equity test between two ciphertexts. Nonetheless, practically speaking, the cloud worker may have to check the equality among more than two ciphertexts. This prompts unveiling pointless data of clients and repetitive calculation cost will likewise happen when utilizing conventional PKEET plans. Instructions to make this more proficient and down to earth stays an interest search issue. In this paper, to take care of the previously mentioned issues by giving a novel idea of public-key encryption with multi-ciphertext correspondence test (PKE-MET). In PKE-MET, each ciphertext can assign a number s to such an extent that the cloud worker can just perform equity test on this ciphertext with other s − 1 ciphertexts, where all their assigned numbers are s. For PKE-MET, other than customary OW-CPA and IND-CPA security, we extraordinarily characterize Number security. We launch PKE-MET to a solid plan and give its security verification. Moreover, to empower the crude to be more useful in applications, we extend it to the idea of PKE with adaptable MET (PKE-FMET). In PKE-FMET, the cloud worker can perform fairness test on quite a few ciphertexts as long as the most extreme number of their assigned numbers is not exactly or equivalent to the quantity of ciphertexts. We build a PKE-FMET plot dependent on our PKE-MET development and demonstrate its security under the characterized security models. Also, the exhibition examination predominantly of productivity and security between our developments and existing fairness test plans in Cloud computing show that our proposed plans are more effective and secure in the multi-ciphertext situation.

I. INTRODUCTION:

In the current era, massive information rushes into our laptops and phones every single day. This leads to the problem of digital devices to store and compute the received tons of data. Cloud computing provides an efficient way to move the storage and computation overheads from users to the cloud server. It allows users to save data on cloud and the cloud server helps to perform part of computation on the data. In addition, to protect data privacy against the honest but curious cloud server and various malicious attacks from outside, users choose to store their encrypted data on cloud, which leaves the cloud server a challenge to perform computations on encrypted data The property of PKEET allows very practical applications, particularly cloud-based scenarios. For example, PKEET enables data statistics in the cloud database since it can perform equality test over encrypted data even those from different users. Another application is that people can find friends with the same interests by matching their encrypted data with others'. Subsequent efforts for PKEET have been devoted to kinds of authorizations to satisfy different privacy requirements, efficiency improvements, and extensions to other primitives.

II. EXISTING SYSTEM:

In the existing PKEET constructions are absorbed in the equality test on two ciphertexts. Given such a scenario, three users, named Alice, Bob, Caroline, apply to the cloud server for checking whether their received ciphertexts are encrypted with the same message or not. With the traditional PKEET, the cloud server needs to perform two equality tests, In addition, if the underlying messages are not the same, the cloud server is able to obtain redundant information, for example, Alice and Bob received the same messages while Bob and Caroline did not. Furthermore, the computation cost will linearly increase with the number of users. The privacy disclosure and computation overhead prevent this trivial method from being utilized in practice. To fill this gap in the literature, we present a novel concept of public-key encryption with multi-ciphertext equality test (PKE-MET).

III. PROPOSED CONCEPT: -

To better protect users' privacy in cloud computing, we propose the concept of public-key encryption with multi-ciphertext equality test (PKE-MET). In PKE-MET, each ciphertext can designate a number s such that the equality test can only be performed on s ciphertexts including this ciphertext itself. It requires that all the designated numbers of these s ciphertexts are the same s.

We instantiate the PKE-MET to concrete construction and prove its security under the defined security models. It is worth noting that, besides traditional OW-CPA and IND-CPA securities, our construction also satisfies the Number security which is specifically defined for PKE-MET.

To enable PKE-MET to be more applicable in practice, we extend PKE-MET to a flexible version, i.e., PKE with flexible MET (PKE-FMET), where equality test can be performed on t ciphertexts as long as the designated numbers of these t ciphertexts are less than or equal to t.

• We present a PKE-FMET scheme based on the proposed PKE-MET scheme and it achieves constant size ciphertext. By contrast, the ciphertext size in trivial construction is linear. The security proofs under the defined security models are also given.

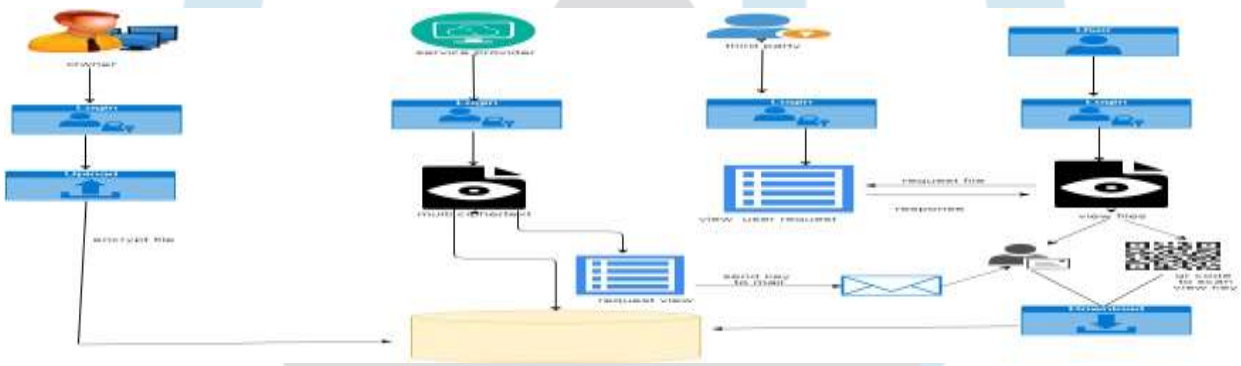
We compare our proposed constructions, namely, PKE-MET and PKE-FMET, with existing equality test schemes in cloud computing mainly on efficiency and security. The comparison shows that our constructions are more suitable for the multi-ciphertext case especially the scenario strict with security.

We conclude that our constructions are more applicable in the multi-ciphertext equality test situation, especially for a larger number of ciphertexts that need to be one-time tested and the scenario that requires high security.

IV. ADVANTAGES:

We introduced the notion of public-key encryption with multi-ciphertext equality test (PKE-MET). Subsequently, we instantiated it to concrete construction and gave its security proofs under the defined security models. Furthermore, to enable it to satisfy practical application, we extended PKE-MET to the conception of PKE with flexible MET (PKE-FMET).The future framework idea of improved PKEET, called certain PKEET (V-PKEET). It underpins confirmation of results from an untrusted cloud worker, at the end of the day, we consider the cloud is pernicious, i.e., that could register a wrong outcome to clients. In our framework, the client checks whether the cloud worker has devotedly played out the approved balance test, which, supposedly, has not been explored already. At last, the proposed plot finishes a wonderful security.

V. SYSTEM ARCHITECTURE:



EXPLANATION:

System architecture is the conceptual model that defines the structure, behavior, and more views of a system. An architecture description is a formal description and representation of a system, organized in a way that supports reasoning about the structures and behaviors of the system. A system architecture can consist of system components and the sub-systems developed, that will work together to implement the overall system. There have been efforts to formalize languages to describe system architecture; collectively these are called architecture description languages.

VI. ALGORITHM EXPLANATION:

The purpose of a PKE is to manage the public keys used by the network for public key encryption, identity management, certificate distribution, certificate revocation, and certificate management. Once enabled, users who enrol for a certificate are identified for later authentication or certificate revocation.

The PKE allows users and systems to verify the legitimacy of certificate-holding entities and securely exchange information between them over the air. The introduction of a PKE enables stronger, certificate-based security, as well as identity services and management tools to maximize network efficiency and security.

PUBLIC KEY: A Public Key is a cryptographic key that can be distributed to the public and does not require secure storage. Messages encrypted by the public key can only be decrypted by the corresponding private key.

PRIVATE KEY: Private Keys are used by the recipient to decrypt a message that is encrypted using a public key. Since the message is encrypted using a given public key, it can only be decrypted by the matching private key. This establishes the ownership of the private and public key, ensuring the message is only read by the approved parties.

WEB APPLICATION AUTHENTICATION: a user connecting to a web application will have their identity confirmed by the web application server. Since the certificate is signed by the trusted CA,they are able to gain access to the application.

VII. MODULE DESCRIPTION:

USER INTERFACE DESIGN

This is the first module of our project. The important role for the user is to move login window to user window. This module has created for the security purpose. In this login page we have to enter login user id and password. It will check username and password is match or not (valid user id and valid password). If we enter any invalid username or password, we can't enter into login window to user window it will shows error message. So, we are preventing from unauthorized user entering into the login window to user window. It will provide a good security for our project. So, server contain user id and password server also check the authentication of the user. It well improves the security and preventing from unauthorized user enters into the network. In our project we are using JSP for creating design. Here we validate the login user and server authentication.

FILE UPLOAD

In this module, after login the owner will upload the file details and it will be stored in the database.

RE-ENCRYPTION PROCESS BY SERVICE PROVIDER

In this module, when the file is getting uploaded in the back-end there happens the double encryption process and it will be stored in the database.

USER REQUEST FILE

In this module, the user will be sending the file request to the Third party for which files, the user needs the access. Without the permission form the Third party and service provider, the user can't able to download the file.

RESPONSE BY THIRD PARTY AND SERVICE PROVIDER

In this module, the Third party and service provider will be giving the acceptance to the user for which file needs the access. After the acceptance, the file key will be send to the user through email.

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.

VIII. CONCLUSION:

In this paper, we introduced the notion of public-key encryption with multi-ciphertext equality test (PKE-MET). Subsequently, we instantiated it to concrete construction and gave its security proofs under the defined security models. Furthermore, to enable it to satisfy practical application, we extended PKE-MET to the conception of PKE with flexible MET (PKE-FMET). Finally, based on our proposed PKE-MET scheme, we presented a PKE-FMET construction achieving constant-size ciphertext in contrast to trivial construction where the size is linear.

REFERENCES:

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

[2] C. Gentry, "Fully homomorphic encryption using ideal lattices," 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 equality 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 scheme supporting equality test with fine-grained authorization," 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 equality test and user-specified authorization," Security and Communication Networks, vol. 5, no. 12, pp. 1351–1362, 2012.

[6] S. Ma, M. Zhang, Q. Huang, and B. Yang, "Public key encryption with delegated equality test in a multi-user 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 filtered equality test - PKE-FET," in SECRYPT 2015, Colmar, Alsace, France, 20-22 July. SciTePress, 2015, pp. 327– 334.

[8] Q. Tang, "Public key encryption schemes supporting equality test with authorization of different granularity," International Journal of Applied Cryptography (IJACT), vol. 2, no. 4, pp. 304–321, 2012.

[9] Y. Lu, R. Zhang, and D. Lin, "Stronger security model for public key encryption with equality 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, "Efficient public key encryption with equality test in the standard model," Theor. Comput. Sci., vol. 755, pp. 65–80, 2019.

[11] Y. Wang, H. Pang, N. H. Tran, and R. H. Deng, "CCA secure encryption supporting authorized equality test on ciphertexts in standard model and its applications," Inf. Sci., vol. 414, pp. 289– 305, 2017.

[12] H. Zhu, L. Wang, S. Qiu, and X. Niu, "New public key encryption with equality test based on non-abelian factorization problems," KSII Transactions on Internet and Information Systems, vol. 12, no. 2, pp. 764–785, 2018.

[13] H. Zhu, L. Wang, H. Ahmad, and X. Niu, "Pairing-free equality test over short ciphertexts," International Journal of Distributed Sensor Networks, vol. 13, no. 6, 2017.

[14] H. T. Lee, S. Ling, J. H. Seo, and H. Wang, "Semi-generic construction of public key encryption and identity-based encryption with equality test," Inf. Sci., vol. 373, pp. 419–440, 2016.

[15] Y. Xu, M. Wang, H. Zhong, J. Cui, L. Liu, and V. N. L. Franqueira, "Verifiable public key encryption scheme with equality test in 5g networks," IEEE Access, vol. 5, pp. 12 702–12 713, 2017.

[16] T. van de Kamp, A. Peter, M. H. Everts, and W. Jonker, "Multi client predicate-only encryption for conjunctive equality tests," in CANS 2017, Hong Kong, China, November 30 - December 2, ser. LNCS, vol. 11261. Springer, 2018, pp. 135–1

[17] R. Vinoth, L. J. Deborah, P. Vijayakumar and N. Kumar, "Secure Multifactor Authenticated Key Agreement Scheme for Industrial IoT," in IEEE Internet of Things Journal, vol. 8, no. 5, pp. 3801-3811, 1 March1, 2021, doi: 10.1109/JIOT.2020.3024703.