Analytical Approach on Efficient and Robust Secret Sharing Scheme in Big-Data

Miss. P. D. Thakare, Dr.V.M.Thakare, Dr.Mrs.S.N.Kale

Abstract- **Nowadays more and more users are storing their data on big data platforms. Sharing on a big data platform is allowed to help the other users, but security is an essential issue in today's life. This paper focused on five different techniques such as Anonymous Multi -hop identity based conditional proxy re -encryption,sharing scheme based on slepian-wolf coding, SUDRS, Multi-hop identity based conditional proxy re-encryption, Linear secret sharing scheme and attribute bloom filter. But there are some drawbacks in the existing methods of sharing on big data, to overcome the drawbacks the improved sharing scheme "Secure big data sharing scheme using key storage" is proposed in this paper.**

Keywords- **Cipher-text, data-confidentiality, decryption, encryption , privacy, security, sharing.**

I. INTRODUCTION

Secret and secure sharing schemes are essential in today's life to ensure the confidentiality and privacy of data during sharing.This data is not only used by a single user it is used by thousands of user ,so private information of the user should not be leaked during sharing of data. Many sharing schemes such as public key encryption have been proposed but this are not promising approach as it may not preserve privacy of data. This paper, discusses five different secret sharing schemes such as Anonymous Multi-hop identity based conditional proxy re-encryption[1], sharing scheme based on slepian- wolf coding, SUDRS[2], Multi-hop identity based conditional proxy re-encryption[3],Linear secret sharing scheme[4] and attribute bloom filter[5].These sharing schemes provide the better privacy, anonymity ,resistance to various attacks. But these methods also have some problem so to overcome such problems "Secure big data sharing scheme using key storage".

II. BACKGROUND

As per studies on sharing in big data many sharing schemes have been develop to make the sharing secure and efficient. The sharing scheme in recent past years are:The method AMH-IBCPRE which achieves multiple cipher-text receiver update, anonymity, conditional sharing. The scheme is resistive against CCA under the decisional P-bilinear Diffie -Helman assumption. The secret key of the delegator is possible to be secured [1].Slepian -Wolf coding sharing scheme, which enhances the exact-share repair feature whereby the shares remain consistent even if shares are corrupted. This scheme can achieve an optimal share size[2].The SUDRS scheme is a context- aware disclosure and sharing rules for collection of multimedia big-data from dispersed sources in a user friendly, efficient and consistent manner. This method is used for verifying the privacy policy in order to ensure correctness and consistency [3].MH-IBCPRE mechanism can verify users attributes before data sharing, thus satisfying the actual needs of users. The data of users can be shared with users having appointed attributes, and others have no access to the data.[4].Linear secret sharing scheme and attribute bloom filter to hide the whole attributes. Security analysis and performance evaluation show that this scheme can preserve the privacy from any linear secret-sharing schemes access policy without employing much overhead [5].

This paper introduces five sharing scheme i.e. Anonymous Multi-hop identity based conditional proxy re-encryption, sharing scheme based on slepian -wolf coding, SUDRS, Multi-hop identity based conditional proxy re-encryption, Linear secret sharing scheme and attribute bloom filter. The paper is organized as follows: Section 1 Introduction. Section 2 discusses Background. Section 3 discusses previous work. Section 4 discusses existing methodologies. Section 5 analysis and discussion about various sharing scheme. Section 6 proposed method and section 7 outcome and possible result. Section 8 Conclude this review paper and section 9 describes about future scope of the proposed method.

III. PREVIOUS WORK DONE

In research literature, many sharing schemes have been studied to provide security and improve the performance in terms of privacy and confidentiality.

Kaitai Liang et.al [1] has proposed advanced multi hop identity based conditional proxy re-encryption, which is hybrid approach to the merits of proxy re-encryption with anonymous technique in which a cipher-text can be securely and conditionally shared multiple times without leaking both the knowledge of underlying message and the identity information of cipher-text senders/recipients. The method is CCA secure.

Tran Phuong Thao et .al [2] has proposed secret sharing scheme based on slepian –wolf encoding which is can be enhanced by reducing the share size, storage and communication costs. The robustness can be enhanced by supporting exact -share repair feature in which, when a share is corrupted or has errors.

Arjmand Samuel et.al [3] proposed SUDRS which focused on allow user, not a system or security administrator to compose conflict free policies for their online multimedia data. An additional requirement is that such a policy be context-aware.

Kun Wang et.al [4] proposed the multi hop identity based conditional proxy re -encryption (MH-IBCPRE) to meet the requirement that data providers' and receivers' attributes be authenticated before data sharing. It can protect users from mendacious information and wasting time and resource.

Kan Yang, Qi Li et.al [5] has proposed linear secret sharing scheme and attribute bloom filter to hide the whole attributes and preserve the privacy from any linear secret-sharing schemes access policy without employing much overhead.

IV. EXISTING METHEDOLOGIES

Many sharing schemes have been implemented over the last several decades. There are different methodologies that are implemented for different sharing schemes i.e. Anonymous Multi-hop identity based conditional proxy re-encryption, sharing scheme based on slepian -wolf coding, SUDRS, Multi-hop identity based conditional proxy re-encryption, Linear secret sharing scheme and attribute bloom filter.

4.1 Anonymous Multi- hop identity based conditional proxy re-encryption:

AMH-IBCPRE which achieves multiple cipher-text receiver update, anonymity, conditional sharing. The scheme is resistive against CCA under the decisional P-bilinear Diffie-Helman assumption. The secret key of the delegator is possible to be secured .It is a hybrid approach of proxy re-encryption with anonymous technique in which cipher-text can be shared securely without leaking the knowledge of shared message and identity of sender/recipients. It is applicable to many real-world application such as email-forwarding, electronic encrypted data sharing in which security is maintained [1].

4.2 Sharing scheme based on Slepian-wolf coding:

It enhances the exact- share repair feature whereby the shares remain consistent even if shares are corrupted. It can achieve an optimal share size, which utilizes the simple binning idea of the coding. This scheme is robust and efficient, it significantly reduce communication and storage cost. It compresses the data in the network. This scheme is robust as it reduces the share size .It achieves fast computation.[2].

4.3 Secure User Data Repository System:

It is a hybrid approach of traditional access policies takes place with a component that should specify privacy and security requirements. Also it needs to be context-aware and it must share rules for collection of multimedia big-data from dispersed sources in a user friendly and consistent manner .It proposes a method for verifying the privacy policy in order to ensure correctness, consistency and efficiency[3].

4.4 Multi-hop identity based conditional proxy re-encryption:

This method satisfies the essential needs of users as it can verify users attributes before sharing of data.If the appointed attributes are matched with the user's attributes only then the data is going to be shared between two users This mechanism provides privacy in multiple way i.e., multi-dimension privacy such as user identities, user's data and attributes, it ensures the protection of user privacy. This method is secure against the Chosen Cipher-text Attack. It improves the security [4].

4.5 Linear Secret Sharing Scheme and Attribute-bloom Filter:

The linear secret sharing scheme is used to hide the whole attributes ,as other methods failed to hide the whole attributes.The attributes are hide in LSSS by removing the attribute matching function. As attribute matching function is removed, it is necessary to define locality of attribute in the access policy so that attribute bloom filter is designed to find the location of attribute in the access policy whether it is present or not in the access policy. It increases the privacy by decreasing the overhead [5].

V. ANALYSIS ANS DISCUSSION

The AMH-IBCPRE is secure against Attacks such as Chosen Cipher-text Attack. This scheme is secure collision resistant. It provides anonymity of original cipher-text and anonymity of re-encryption key. It provides with Multiple Cipher-text Receiver Update and conditional share property[1]. Sharing Scheme based on Slepian wolf coding it provides exact share repair feature. In this scheme the parameters such as storage cost, computation cost and communication cost has been improved [2].Secure User Data Repository System in this system the intelligent privacy manager is implemented. It improves security and privacy of data sharing.[3].Multi-hop identity based conditional proxy re-encryption this system verify the user's attribute. This scheme is tracing attack secure. It improves the privacy by protecting user's data, identities and attributes. It also enhances the security [4].Linear Secret Sharing Scheme and Attribute bloom Filter This scheme is selective secure against the chosen plaintext attacks under the decisional q -BDHE assumption. It also improves the performance parameters by resisting privacy leakage from access policy [5].

Mobility scheme	**Advantages**	**Disadvantages**
Advanced Multi-hop identity based Conditional proxy reencryption	It provides Anonymity, Multiple receiverupdates and Conditional sharing. The corrupted users to be adaptively chosen by an adversary, while the adversary must output the challenge identity at the outset of security game	complicated in the sense that we categorize the game into two sub games: one is the anonymity for delegator (i.e. given the original ciphertext an adversary cannot output the identity of delegator.
Sharing Scheme based on Slepian wolf coding	This method improves storage cost as well as computation cost. The efficiency can be enhanced by reducing the share size, storage and communication cost. It influences fast computation. It is an efficient and robust secret sharing scheme.	
Secure User Data Repository System	It proposes hybrid approach where traditional access control policies can be integrated by adding a component that should specify privacy requirements regulating under which circumstances the multimedia data of a user can be disclose .It defines context-aware disclosure and sharing rules for collection of multimedia big data from dispersed sources in a user-friendly and consistent manner .It presents a methodology for verifying the privacy policy in order to ensure correctness and consistency	Limitation in verifying individual policies is that a local decision in verification may not present all the optimal solutions available and can overwhelm a user.
Multi-hop identity based conditional proxy reencryption	The proposed mechanism can verify users' attributes before data sharing, thus satisfying the actual needs of users. The data of users can be shared with users having appointed attributes, and others have no access to the data. Proposed preauthentication mechanism can provide multidimension privacy protection including data, user	Encoding operations over encrypted message are complex

	identities, and attributes. It provides rigorous analysis to prove that system is secure against chosen cipher-text attacks, tracing attacks and collusion attacks.	
Secret Sharing Scheme and Attribute bloom Filter	An efficient and fine-grained data access control scheme for big data, where the access policy will not leak any privacy information. It can hide the whole attribute (rather than only its values)in the access policies.	It may lead to great challenges and difficulties for legal data consumers to decrypt data.

VI. PROPOSED METHODOLOGY

Sharing Schemes are essential in these big–data era. To make the sharing secure, this paper explains five different methods. This method enhances security, privacy. But it has also some drawbacks. The method Anonymous Multi-Hop Identity Based Conditional Proxy Re-encryption has described multi-sharing mechanism, but it does not have data storage capacity in the proposed method i.e."Secure & Secret sharing method" ,we have database to store the key and data of user.

In the proposed method there are two users Alice and Bob are given .If Bob wants to access the data from the Alice .Alice and Bob share the data between So that Alice sent the data to proxy server then proxy server encrypt the data and the encrypted the database. The cloud data service again encrypt data and the data is sent to the Bob, another proxy server decrypts the data and key using the Bob's decryption key and then this decrypted data is stored to the database and decrypted key and encrypted key are stored in key storage database of bob and Alice respectively .

Basic steps of algorithm:

Step1: When Alice send the data to the bob he first sent data to the proxy.

Step2: proxy then encrypts the data and sends it to cloud.

Step3: the cloud data service re-encrypts the data and re encrypted data is sent forward to the bob.

Step4: the bob send its key and data to second proxy server and it then decrypt's the data

Step5: the decrypted data is again stored in the data

Step6: two users bob and Alice have their own key storage.

Diagrammatic representation of proposed method is shown as follows:

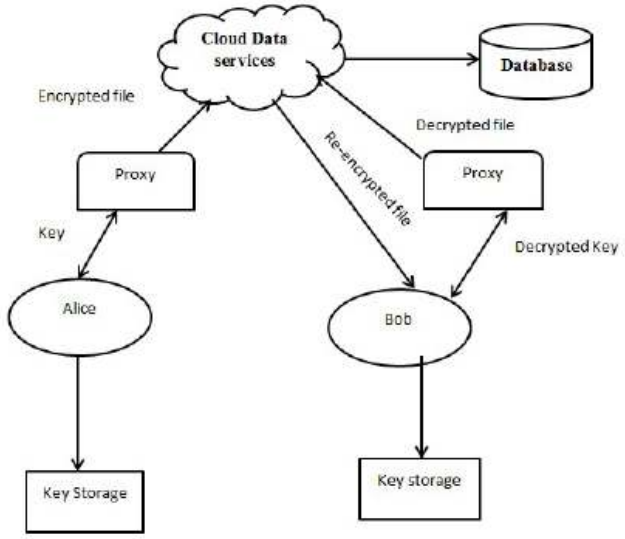

Fig 1: Secure big data sharing scheme using key storage

VI. OUTCOME AND POSSIBLE RESULTS

In this way proposed method performs the encryption and decryption of the data and key. As both the user has their key in their own key storage the scheme is more robust, efficient and secure sharing scheme

VIII. CONCLUSION

This paper focused on the study of various sharing scheme Anonymous Multi-hop identity based conditional proxy re-encryption and attribute bloom filter. But some of the problem are tracked during sharing so to improve this "Secure big data scheme using key storage"

REFERENCES

[1] Kaitai Liang, Joseph K. Liu ,"Privacy-Cipher Control for Big Storage SECURITY 8, August2015.

[2] Tran Phuong Thao Zakirul Alam Shinsaku Omote Share Size in Efficient Big Data", DATA No. X, January 2017.

[3] Arjmand Haseeb, Composition and No.9,SEPTEMBER 2015. [4]Pre-Re Data Context",IEEE BIG No. XX,2017.
[5]Shen, Fellow, IEEE "An Privacy JOURNAL APRIL 2017.