Proxy Re-encryption Schemes for Secure Cloud Data and Applications: A Survey

VAKATI RAJA KUMAR
Pursuing M.Tech (CSE) from SKR College of Engineering & Technology, Manubolu, SPSR Nellore.AP.

V.CHIRANJEEVI
M. Tech, Assistant Professor in Deportment of CSE, SKR College of Engineering & Technology, Manubolu, SPSR Nellore.AP.

Abstract: **This paper shows an overview on Proxy re-encryption procedures concerning secure cloud information and its application. To keep delicate client information secret against untrusted servers, crypto-realistic strategies are utilized to give security and access control in mists. As the information is shared over the system, it is should have been encoded. There are numerous encryption conspires that give security and access control over the network.Proxy re-encryption empowers the semi-confided in intermediary server to re-scramble the figure content encoded under Alice's open key to another ciphertext en-crypted under Bob's open key. The re-encryption is finished without the server having the capacity to decode the ciphertext.Cloud administrations and applications ought to take after the standard safety efforts in-cluding information secrecy, integrity,privacy, power and access control.In this paper the intermediary re-encryption(PRE) plans, Con-ditional PRE,Identity based PRE and Broadcast PRE,Type based PRE, Key private PRE,Attribute based PRE,Threshold PRE and its part in anchoring the cloud information are clarified.**

1.INTRODUCTION

Distributed computing is rising as an unavoidable choice for web based applications and administrations. Distributed computing is an appropriated registering design where the figuring assets, for example, equipment, programming, preparing power are conveyed as an administration over a system framework. The distributed computing model enables the clients to get to data and different assets from anyplace that a system association is available[1].

In distributed computing all information are put away on circulated servers at re-bit area. The remote areas are server farms. The customer can buy or lease, for example, taking care of time, organize data transfer capacity, plate stockpiling and memory[2]. Information proprietors can remotely store their information in the cloud and no longer groups the information locally. Cloud computing moves the application programming and database to the expansive server farm, where the information administration and administrations may not completely dependable [4].

A distributed storage framework is a dispersed stockpiling framework [3] that con-sists of numerous free stockpiling servers. The capacity of appropriated stockpiling frameworks is to store information privately and reli-capable over extensive stretches of time [6]. The primary explanation behind the raise of the innovation distributed computing is a direct result of the comfort that they give to various recently created applications and for endeavors . The data that are put away in the cloud is been gotten to countless and is frequently subjected to changes. A vital part of distributed storage servers is that, it offers ascend to various security dangers.

Cloud administrations and applications may require all standard security capacities including information classification, respectability, protection, strong ness and access control. Thus anchoring the could and its information is a testing errand. There are a few cryptographic strategies to se-fix the information put away in distributed storage frameworks. Intermediary re-encryption is a generally new information encryption procedure conceived essentially for appropriated information and document security.The focus of intermediary re-encryption is permitting the re-encryption of one figure content to another figure content without depending or confiding in the outsider that plays out the exchange. In circumstances where one client wishes for another client to de-tomb a message utilizing its own or another mystery key rather than the main client's mystery key, one method includes the help of an intermediary.

Intermediary re-encryption[8] is a methods for classified and adaptable procedure for a client to store and offer information. A client can en-tomb the record with an open key and after that store the ciphertext in a confided in server.When a recipient arrives, the sender can assign a re-encryption key related with the specific beneficiary to the confided in server as a proxy.Then the intermediary re-scramble the underlying ciphertext to the coveted receiver.The motivation behind intermediary re-encryption plans is to keep the disclosure of the keys associated with re-encryption and the plaintext that should be re-encoded to the intermediary.

The Proxy re-encryption plans are fundamentally a form of ex-isting encryption plans comprising of determination of content, gener-ation of keys, sharing or transmitting of keys between the standard ties, changeover from plaintext to figure message toward one side and changeover from figure content to plaintext on the opposite end, the dif-ference emerges with the presentation of two more properties Direc-tionality and Transitivity.

Directionality

On the off chance that the re-encryption plot is reversible that is, a similar re-encryption key is utilized to make an interpretation of messages from Alice to Bob, and also from Bob to Alice the plan is delegated a bi-directional plan. In these plans if a client advances a message to another, it consequently offers rights to the recipient to speak with the sender. Such re-encryption keys are thus created with the keys in hands of both sender and recipient and with their shared trust and assent.

A unidirectional plan is one-route in this specific circumstance, giving a larger amount of security and making it a doable alternative in non confided in setups where message passing on is basic yet not to a degree where recipient ought to be offered rights to react to it. So if a mes-sage is re-scrambled from Alice to Bob with a key, it can't be utilized for re-encryption from Bob to Alice. Besides uni-directional plans are more helpful since they can be changed over to bidirec-tional plot whenever essentially by running it in the two bearings, i.e. from Alice to Bob and from Bob to Alice[9].

Transitivity:

Transitivity in intermediary re-encryption plans is characterized as the num-ber of re-encryptions permitted by a calculation. A transitive PRE plan would enable a figure content to be re-scrambled from Alice to Bob, and after that again from Bob to Tom et cetera. While a non-transitive plan would enable a figure content to be re-encoded for a solitary time (or a pre-characterized predetermined number). This infers motel non-transitive plans the intermediary does not have the expert to dole out appointment rights to others next to the combine of imparting clients.

In this paper encryption procedure intermediary re-encryption (PRE) plan and its diverse classifications, for example, Type based PRE,Key-private PRE, Identity based PRE, Attribute based PRE and Thresh-old PRE are talked about in the accompanying area alongside its part in cloud applications.

2.PROXY RE-ENCRYPTION SCHEMES

The proxy re-encryption schemes are proposed by Mambo and Okamoto [5] and Blaze et al. [8]. Proxy re-encryption is a cryp-tographic primitive which translates ciphertexts from one encryp-tion key to another encryption key. It can be used to forward en-crypted messages without having to expose the cleartexts to the potential users. The re-encryption protocol should be key indepen-dent to avoid compromising the private keys of the sender and the recipient. The primary advantage of this PRE [10] scheme is that they are unidirectional (i.e., Alice can delegate to Bob without Bob having to delegate to her) and do not require delegators to reveal their entire secret key to anyone.

Based on these properties many PRE techniques was proposed in the traditional public key infrastructure accompanied with much more sophisticated certificate management.Proxy Re-encryption can be broadly classified into two categories.They are (a)Uni-Directional Schemes and (b) Bi-Directional Schemes.

The Uni-Directional Schemes are further classified as (a)Identity-based PRE, (b)Attribute Based PRE, (c)Ciphertext-Policy Attribute based PRE,(d)Conditional PRE, (e)Time based PRE. The Bi-Directional Schemes are further classified as (a)Type based PRE and (b)Thershold based PRE

2.1 Type Based Proxy Re-encryption Scheme

proposed the Type based proxy re-encryption scheme. This en-cryption scheme guarantees data confidentiality and fine gain ac-cess control. Type based PRE enables the delegator to implement fine grained policies with one key pair without any additional trust on the proxy.

The messages are categorized into different types according to the decryption rights of the intended receivers. The main benefit of this scheme is the single pair of keys which provides re-encryption ca-pability to the proxy for his cipher-texts against his receivers. But the proposed scheme works only for the cipher-texts generated by the sender.The Type Based PRE poses some properties such as:

—The delegator only needs one key pair so that key management problem can be simplified.

—The delegator can choose a particular proxy for a specific dele-gate, which might be based on the sensitiveness of the delega-tion. Compromise of one proxy key will only affect one subset of messages.

2.2 Threshold Based Proxy Re-encryption Scheme

A fundamental approach of threshold PRE scheme [7] is for secure computation. This scheme performs huge number of computations on encrypted data without decrypting it. Threshold PRE technique has multiplicative homomorphic property.A multiplicative homo-morphic encryption scheme supports the encoding operation over encrypted messages and forwarding operations over encrypted and encoded messages.

2.3 Identity-based Proxy Re-encryption Scheme

In Identity-based PRE(IB-PRE) schemes proposed by Ateniese in [1], in which senders encrypt messages using the recipients identity (a string) as the public key.An Identity-Based Proxy Re-encryption (IB-PRE) scheme is an extended Identity Based En-cryption scheme.The identity-based proxy re-encryption (IB-PRE) schemes allow a proxy to translate an encryption under Alice's identity into one computed under Bob's identity. The proxy uses proxy keys, or re-encryption keys, to perform the translation with-out being able to learn the plaintext. Moreover, no information on the secret keys of Alice and Bob can be deduced from the proxy keys.

Both PRE and IB-PRE is confined to single receiver. In case of multiple receivers then the particular system is forced to use PRE or IB-PRE multiple times.Hence to get out of this issue, the idea of broadcast PRE(BPRE) was introduced [10].BPRE which runs the system in same as the PRE and IB-PRE but in a much more satisfying manner.

2.4 Key Private Proxy Re-encryption Scheme

Key private proxy re-encryption scheme are proposed by Ateniese et al. [11]. In a KP-PRE it is quite hectic task for the proxy and a set of colluding users to get the recipient of a message from the ciphertext and the set of public keys. Achieving key private PRE can only happen when the encryption scheme used is key-private. The key privacy encryption provides privacy of the key under which the particular encryption was performed.

The KP-PRE scheme gave raise to the idea of key privacy for proxy re-encryption schemes, where even the proxy who performs the particular translations cannot be able to distinguish the identities of the participants. In addition to hide the contents of files from the proxy, it is also useful to suppress as much meta-data as possible. For example, we might want the proxy file server to re-encrypt sen-sitive files for certain recipients without the proxy the recipient's identity.

2.5 Attribute Based PRE

In attribute based proxy re-encryption scheme [16], a semi trusted proxy with some additional information can transform a cipher-text under a set of attributes into a new ciphertext under another set of attributes on the same message. This encryption scheme, al-lows fine-grained access control on encrypted data. Attribute based encryption is a generalized form of IBE.Two types of attribute based encryption (ABE) namely ciphertext policy attribute based encryption (CP-ABE) and key policy attribute based encryption (KP-ABE).

Ciphertext Policy Attribute-Based PRE provides a fine grained ac-cess control over data by limiting the decryption rights based on some attributes of the receiver but it has an average efficiency and flexibility compared to the other schemes.CP-ABE is more apt for an enterprise environment, and it is an ideal unique scheme for im-plementing a self-contained data protection mechanism.

In KP-ABE [16] scheme, each ciphertext is named by the encryptor with a set of descriptive attributes. Each private key is held with an access scheme that mentions which type of ciphertexts the key can be used to decrypt. An important area of KP-PRE scheme deals with is in the field of secure forensic analysis.

2.6 Conditional PRE

Proxy re-encryption can be used in applications where delegation is required, for an example in case of delegated email processing. But, it is not enough to handle scenarios where a fine-grained delegation is demanded. For example, john is only allowed Lisa's encrypted emails containing a predetermine keyword. In order to overcome the limitation of existing PRE, in [15] the system introduces the no-tion of conditional proxy re-encryption (or C-PRE), whereby only ciphertext satisfying one condition set by Alice can be transformed by the proxy and then decrypted by john. The author formulates its security model and also proposes an efficient C-PRE scheme, whose chosen-ciphertext security is proven under the 3-quotient bilinear Diffe-Hellman assumption. The author further extends the structure, which allows multiple conditions with a somewhat high overhead.

2.7 Time based PRE

Time based PRE is a more recent updated scheme of PRE schemes which provides a scalable user revocation and reduces the work-load of data owners. The major disadvantage of this scheme is that it requires the effective time period to be same for all attributes as-sociated with the user.In this case, the data owner can be offline in the process of user revocations. The main idea is to combine the concept of time together with Attribute based encryption (ABE) and Proxy re-encryption (PRE). In time PRE scheme, the data is held with an attribute based access structure and an access time. Each user is identified by a set of attributes and a set of eligi-ble time periods which denote the period of validity of user's ac-cess right. The scheme allows every user's access right to be effec-tual in a pre-determined time period, and enables the cloud service provider(CSP) to re-encrypt ciphertexts eventually, based on their own time.

3.LITERATURE SURVEY

Cloud service providers finds out the access control mechanisms for data on the cloud. Access control is a method that restricts, denies, or allows access to system. In the cloud, data security is crucial to protect against inside attack, denial of service attack, and collision attack. Traditionally, different successful access control policies are used to protect data stored locally and data stored remotely.One of such approach is Proxy Re-encryption(PRE) tech-nique.

In [5] a methodology for delegating decryption rights was first in-troduced as an efficiency improvement over traditional decrypt-and-then-encrypt approaches. The proxy re-encryption key, cloud server can transform the ciphertext encrypted under the public key of Alice into an encryption under the public key of Bob. By uti-lizing the PRE primitive, the transformed ciphertext can only be decrypted by Bob whereas the cloud server is unable to learn the plaintext or private keys of Alice or Bob. Finally, Bob can down-load and decrypt the requested data with his own private key. In this way, the costly burden of secure data sharing can be offloaded to the semi-trusted cloud server with abundant resources.

In 1998, Blaze, Bleumer, and Strauss [8] proposed the notion of ”atomic proxy cryptography”, in which a semi-trusted proxy com-putes a function that converts ciphertexts for Alice into ciphertexts for Bob without seeing the underlying plaintext.The authors noted, however, that this scheme contained an inherent restriction: it is bidirectional.Thus, this scheme is only useful when the trust rela-tionship between Alice and Bob is mutual.Delegation in the BBS scheme is transitive, which means that the proxy alone can create delegation rights between two entities that have never agreed on this.Another drawback to this scheme is that if the proxy and Bob collude, they can recover her secret key.

Jakobsson [17] developed a quorum-based protocol where the proxy is divided into sub-components, each controlling a share of the re-encryption key; here, the keys of the delegator are safe as long as the proxies are honest. A similar approach was considered by Zhou, Mars, Schneider and Redz [18].

Ivan and Dodis [19] realized unidirectional proxy encryption for El Gamal, RSA, and an IBE scheme by sharing the user’s secret key between two users. They also solved the issue regarding the proxy alone assigning new delegation rights.One exception is the Ivan-Dodis IBE scheme [19] where the global secret that decrypts all ciphertexts is shared between the proxy and the delegatee. Thus, the delegatee need only to take care of a single secret, but an obvious drawback is that when the proxy and any delegatee in the system collude, they can decrypt everyone else’s messages.

Apart from the generic construction of Dodis and Ivan there are two identity-based proxy re encryption schemes: one is proposed by Green and Ateniese [9] and the other is proposed by Matsuo

In both schemes, the delegator and the delegatee are assumed to be registered at the same domain (or, the same key generation center).The IBE has a number of practical applications such as se-cure email forwarding, attribute-based delegations and access con-trol in networked file storage. This type of re-encryption schemes is utilised to realize the secrecy of data.

Sahai and Waters in [20] introduced the first attribute-based en-cryption (ABE) where both the ciphertext and the secret key are la-belled with a set of attributes. A user can decrypt a ciphertext only if there is a match between the attributes listed in the ciphertext and the attributes with in hand of the decryptor. ABE schemes can be classified into two types: key-policy ABE (KPABE) and ciphertext-policy ABE (CP-ABE).

In ABE technique, the data is stored on the storage server in an en-crypted form while different users are still allowed to decrypt dif-ferent pieces of data as per security policy. This successfully elimi-nates the need to rely on the storage server for preventing unautho-rized data access.

Jean Weng in [10] introduced Conditional proxy re-encryption (C-PRE),the proxy is unable to translate those ciphertext whose cor-responding condition keys are not available.However, proxy will obtain no information about the original message. The security re-quirements for C-PRE systems should ensure that, (i) even if the proxy, who does not have both the partial re-encryption key and the condition key, conspire with the delegate, it is still impossible for them to compromise the delegator’s security. (ii) The proxy, who has both the partial reencryption key and the condition key, com-promises neither the delegator not the delegatee’s security.

To employ PRE in the context of TRE(Timed Release Encryp-tion), Emura et al.[22] proposed the first Timed-Release Proxy Re-Encryption (TR-PRE).In TR-PRE, the proxy is allowed to re-encrypt a ciphertext with a release time under a public key to the one with the same release time under another public key by using a re-encryption key given by the delegator.

Conditional Proxy Broadcast Re-Encryption (CPBRE), which was proposed by Chu et al. [15], can further reduce the cost incurred by TR-PRE. Specifically, CPBRE allows a delegator to delegate the decryption rights of a broadcast encryption to a set of delegatees, and to specify a condition to control the re-encryption power of the proxy.

The main intention of cloud storage system is to secure the data itself in such a way that even in the event of a successful attack. The content of the data stored in the cloud storage system remains confidential and secureed. To provide confidentiality for messages in storage servers, a user can encrypt messages by a cryptographic method to encode and store messages.

4.COMPARISON OF PRE SCHEMES

in this section we compare different proxy re-encryption techniques on the bases of the properties advantages and disadvantages.The comparison is compressed and represented in Table 1.

5.SECURE CLOUD DATA AND APPLICATIONS

What is the cloud? In general, the cloud is the concept of remotely hosted IT services, termed cloud apps, provided by a supplier. These suppliers are called cloud providers. Typical cloud apps offered by cloud providers include email, calendar, documents, on-line storage, sales, customer service, and more. Some of today's well known cloud providers include companies such as Amazon, Google, Intuit, Microsoft, and Box. A selection of the top cloud apps in the market today include Cloud Drive, Google Apps for Business, Skype,Quickbase and Box Business.

Using business apps in the cloud has widely recognized advantages: you save money by paying for only the IT computing resources you need, you can use the computing resources quickly without capital investment, and you can increase your reach to employees and users anywhere.Some areas of application of cloud computing are:

Personal Health Record:"An electronic, lifelong resource of health information needed by individuals to make health deci-sions". PHR acts as an important intermediary between physicians and patients. The main goal of PHRS is to enable patients to man age and maintain their personal health records as well as improv-ing healthcare delivery and reducing cost.Security and privacy are the main concern for patients in regard to their health records.By using proper cryptographic encryption techniques the PHR can be secured by the individuals.The right of disclosing the details will be with in the particular individual.This mode of protection of data is necessary as the disclosure of health details at certain situation can cause a negative impact on the person such during a job inter-view,insurance etc.

Data Sharing in Cloud Computing:Despite the abundant re-source provided by the cloud computing, data owners' concerns about the privacy of their outsourced data such that these data can only be accessed by the authorized parties become the main ob-stacles impede cloud computing from spread adoption, especially if the cloud server is only semi-trusted.proxy re-encryption is a promising candidate to enable secure data sharing in the cloud com-puting.

Encrypted Email Forwarding:By utilizing the PRE primitive in a encryption email system, the granted recipient first generates a re-encryption key using his own private key and the delegatee's public key, and delegates this key to a email server. Then relying on the PRE scheme the email server can achieve transformations from the recipient's encrypted emails into the delegatee's encrypted emails without disclosing any information.Finally, the delegatee can check the delegator's encrypted emails conveniently with his own private key. Crucially, the private key for the recipient is protected from being disclosed in this email system.

Digital Rights Management:The digital rights management (DRM) is developed to prevent digital contents from being copied and redistributed illegally by binding a digital content and a unique license together.In order to achieve inter-operability among dif-ferent DRM systems, some primitive of PRE was introduced into DRM.

Vehicular Ad Hoc Networks:By enabling vehicles to communi-cate with other vehicles or roadside units (RSUs) via the equipped on-board units (OBUs) communication devices, vehicular ad hoc networks (VANETs) can be formed to offer a more efficient and comfortable driving experience.VANETs can be formed to offer a more efficient and comfortable driving experience.To address the trust and privacy issues in VANETs,an authentication proto-col with privacy preservation by incorporating appropriate proxy re-encryption schemes.In their authentication protocol, the RSU is able to transform a signature from a OBU into another signature from TA on the traffic message without revealing any private in-formation of the OBU. This conceals the real identity of the OBU from malicious adversary.

6.CONCLUSION

In cloud computing,security is an important step in quality of ser-vice. To keep the sensitive and trustworthy user data confidential against untrusted servers several proxy re-encryption techniques are used.PRE has captured a lot of concern due to the delegation function of decryption.PRE is also an essential technique as many real time applications and many big and small ventures relay on cloud based storage for storing the sensitive data concerning them.

This paper surveys different proxy re-encryption schemes used in cloud storage system. The advantages and disadvantages of the schemes have been studied and summaries for future use. The future work will be concerned withthe development of better PRE schemes which works in distributed environment.

Finding the efficient PRE schemes with full security is also an open problem since most of the existing PRE schemes can only achieve certain selective security.

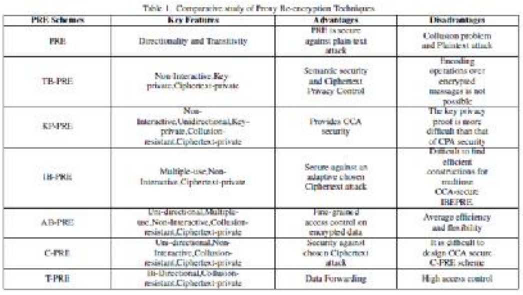

Table 1. Comparative study of Proxy Re-encryption Techniques

PRE Schemes	Key Features	Advantages	Disadvantages
PRE	Directionality and Transitivity	PRE is secure against plain text attack	Collusion problem and Plaintext attack
TB-PRE	Non-Interactive,Key private,Ciphertext-private	Semantic security and Ciphertext Privacy Control	Encoding operations over encrypted messages is not possible
KP-PRE	Non-Interactive,Unidirectional,Key-private,Collusion-resistant,Ciphertext-private	Provides CCA security	The key privacy proof is more difficult than that of CPA security
IB-PRE	Multiple-use,Non-Interactive,Ciphertext-private	Secure against an adaptive chosen Ciphertext attack	Difficult to find efficient constructions for multiuse CCA-secure IBEPRE
AB-PRE	Uni-directional,Multiple-use,Non-Interactive,Collusion-resistant,Ciphertext-private	Fine-grained access control on encrypted data	Average efficiency and flexibility
C-PRE	Uni-directional,Non-Interactive,Collusion-resistant,Ciphertext-private	Security against chosen Ciphertext attack	It is difficult to design CCA secure C-PRE scheme
T-PRE	Bi-Directional,Collusion-resistant,Ciphertext-private	Data Forwarding	High access control

7. REFERENCES

[1]. Giuseppe Ateniese, Kevin Fu, Matthew Green, and Susan Ho-henberger. Improved proxy re-encryption schemes with applications to secure distributed storage, In Proceedings of the 12th Annual Network and Distributed System Security Symposium , pages 29-44. Internet Society, February 2005.

[2]. A. G. Dimakis, P. G. Godfrey, Y. Wu, M. J. Wainwright, and K. Ramchandran, Network coding for distributed storage systems,IEEE, 2010,pp. 4539-4551.

[3]. P. Druschel and A. Rowstron,PAST: A Large- Scale, Persistent Peer-to-Peer Storage Utility, Proc.Eighth Workshop Hot Topics in Operating System, 2001, pp. 75-80.

[4]. C.Wang, QianWang, KuiRen, and Wenjing Lou, Ensuring Data Storage Security in Cloud Computing, Proc. IWQoS 09, July 2009, pp. 1-9.

[5]. M. Mambo and E. Okamoto,Proxy Cryptosystems: Delegation of the Power to Decrypt Ciphertexts, IEICE Trans. Fundamen-tals of Electronics, Comm. and Computer Sciences, 1997, pp. 54-63.

[6]. Q. Tang, Type-Based Proxy Re-Encryption and Its Construc-tion, Proc. Ninth International Conf. Cryptology in India, 2008, pp. 130-144.

[7]. S. Saduqulla and S. Karimulla, Threshold Proxy Re-Encryption in Cloud Storage System, International Journal of Advanced Re-search in Computer Science and Software Engineering,Volume 3, Issue 11, November 2013.

[8]. M. Blaze, G. Bleumer, and M. Strauss, Divertible Protocols and Atomic Proxy Cryptography in Proc. Int. Conf. Theory Appl. Crytographic Techn.: Adv. Cryptol, (1998)127-144.

[9]. M. Green and G. Ateniese, Identity-based proxy re-encryption, in Proc. 5th Int. Conf. Appl. Cryptography Netw. Security, 2007, pp. 288-306.

[10]. C.-K. Chu, J. Weng, S. S. M. Chow, J. Zhou, and R. H. Deng, Conditional proxy broadcast re-encryption,in Proc. 14th Australasian Conf. Inf. Security Privacy, 2009, pp. 327-342.

[11]. G. Ateniese, K. Benson and S. Hohenberger, Key-Private Proxy Re-Encryption, Topics in Cryptology, Springer, 2009.

[12]. Jian Weng, Robert H. Deng, Xuhua Ding, Cheng- Kang Chu, and Junzuo Lai,Conditional proxy reencryption secure against chosen-ciphertext attack,In ASIACCS ,2009,pp. 322-332.

[13]. Rutuja Warhade,Prof. Basha Vankudothu, A Survey on Proxy Re-encryption Schemes for Data Security in Cloud International Journal of Advance Research in Computer Science and Manage-ment Studies,12,(2014)

[14]. A. Boldyreva, M. Fischlin, A. Palacio, and B. Warinschi,A closer look at PKI: Security and efficiency, in Proc. 10th Int. Conf. Practice Theory Public-Key Cryptography, (2007)458-475.

[15]. Jian Weng, Robert H. Deng, Xuhua Ding, Cheng- Kang Chu, and Junzuo Lai, Conditional proxy reencryption secure against chosen-ciphertext attack,In ASIACCS,2009,pp. 322-332.

[16]. Goyal V, Pandey O, Sahai A, and Waters B ,Attribute Based Encryption for Fine-Grained Access Conrol of Encrypted Data,In: ACM conference on Computer and Communications Security, 2006.

AUTHOR's PROFILE

Vakati Raja Kumar, Pursuing M.Tech (CSE) from SKR College of Engineering & Technology, Manubolu, SPSR Nellore.AP.

V.Chiranjeevi M.tech, Assistant Professor in Deportment of CSE, SKR College of Engineering & Technology, Manubolu, SPSR Nellore.AP.