International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Privacy-Preserved Search in mCL-PKE Based Secure Data Sharing over Public Clouds and Credential Trust Management through SMTP Communication

Shintomon Mathew[1], Asha Jose[2]

[1]Final Year M. Tech. (Cyber Security), KMP College of Engineering, Perumbavoor, Kerala, India

[2]Assistant Professor, Department of Computer Science and Engineering, KMP College of Engineering, Perumbavoor, Kerala, India

Abstract: ***With the fast prominence of cloud computing architecture, public key cryptography exhibit certificate revocation problem and in the case of identity based encryption there exist a key escrow problem. Certificateless public key cryptography schemes now available are not properly sufficient because paring operation needs high amount of computational resources or they are vulnerable to partial decryption attacks. Sensitive data must be encrypted before sharing data over public cloud to maintain data confidentiality which make traditional data utilization invalid based on keyword search of plaintext values. In order to resolve these problem, we proposing an improved Mediated certificateless public key encryption (mCL-PKE) scheme that does not use any pairing operations and solve the problem of sharing sensitive information in public clouds, also implement privacy-preserving searching over encrypted data with set of strict privacy axioms. On that public key encryption credential and key that used for encryption and decryption share through secure SMTP communication for maintaining trust management. In our system, the data owner needs to encode the same information encryption key different times, once for every client, utilizing the clients' open keys. To address this deficiency, we present an augmentation of the fundamental mCL-PKE plan. On the retrieval process, the cloud partially decrypts the encrypted data for the users and send the intermediate decryption keys to user by using secure SMTP communication. Our experiments on the real-world cloud data shows that our schemes are efficient for privacy-preserved search and trust management with mCL-PKE based secure storage also its solve the key escrow problem.***

Keywords: Cloud Computing, mCL-PKE, Confidentiality, Trust Management, Access Control, Searchable Encryption, Privacy-Preserving, SMTP Communication**.**

1. Introduction

Cloud computing is new computing terminology or metaphor based on service and Consumption of computing resources. It involves groups of remote servers and interconnected software network that provide a centralised data storage online access to computer services or resources. Cloud processing postures security concerns on the grounds that the administration supplier can get to the data that is on the cloud whenever. It could incidentally or deliberately change or even erase information. Many cloud suppliers can impart data to outsiders if fundamental for purposes of lawfulness even without a warrant. That is allowed in their protection approaches which users need to consent to before they begin utilizing cloud services. Answers for security incorporate arrangement and enactment and additionally end users' decisions for how data is stored. Users can encrypt data that is transformed or put away inside the cloud to prevent unauthorized access.

Its great flexibility and economic investment funds are inspiring both people and enterprises to outsource their neighborhood complex data management system into the cloud. To protect data security and battle unsolicited accesses in the cloud furthermore beyond, sensitive data, for example, e-mails, personal health records, photograph collections, expense documents, monetary exchanges, etc., may have to be encrypted by data owners before outsourcing to the commercial open cloud; this, however, obsoletes the customary data use service based on plaintext keyword search. The trifling arrangement of downloading all the data and decrypting provincially is clearly illogical, due to the huge measure of transfer speed cost in cloud scale systems. Moreover, aside from eliminating the neighborhood storage management, putting away data into the cloud serves no purpose unless they can be easily searched and utilized.

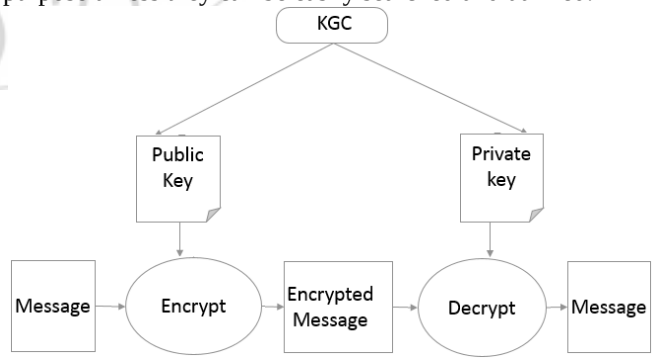

Figure 1: Public-key cryptography

As shown in Figure. 1, Public-key cryptography [18] is a class of cryptographic calculations which obliges two different keys, one of which is mystery (or private) and one of which is public. Albeit distinctive, the two sections of this key pair are numerically connected. People in general key is utilized to encrypt plaintext or to confirm a digital signature;

though the private key is utilized to decrypt cipher text or to make a digital signature.

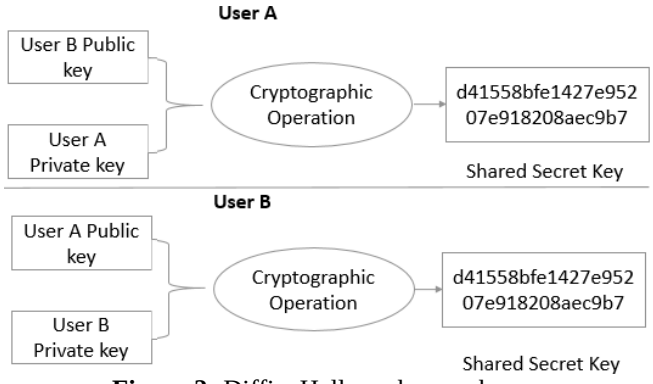

Figure 2: Diffie–Hellman key exchange

As shown in Figure. 1, the Diffie–Hellman key trade scheme [18], every gathering produces a public/private key combine and conveys the public key. In the wake of acquiring a bonafide duplicate of one another's public keys, User A and User B can process an imparted mystery disconnected from the net. The imparted mystery can be utilized, for occurrence, as the key for a symmetric cipher.

Simple Mail Transfer Protocol (SMTP) is an Internet standard for electronic mail (e-mail) transmission. SMTP by default uses TCP port 25. The mail submission Protocol is same, but it uses default port 87. SMTP connections secured by SSL, known as SMTPS, default to port 465.SMTP is also used by electronic mail servers and other mail transfer agents to securely send and receive messages, and also used by user-level client mail applications for sending messages to a mail server for relaying.

In our paper, Past methodologies and propose a novel mediated Certificateless Public Key Encryption (mCL-PKE) [1] scheme that does not use pairing operations. Since most CL-PKC schemes are in light of bilinear pairings, they are computationally costly. Our scheme shorten the computational overhead by utilizing a pairing-free approach. Further, the processing expenses for unscrambling at the clients are diminished as a semi-trusted security go between somewhat decrypts the encrypted data before the clients decrypts. The security go between goes about as an arrangement implementation point also and helps instantaneous revocation of compromised or vindictive users.

In this paper, we address the weaknesses of such we characterize and understand the issues of secure search over encrypted cloud [2] data while saving strict system wise security in the distributed computing ideal model. Among different multi-keyword semantics, we pick the productive similarity measure of "direction matching," i.e., the same number of matches as conceivable, to catch the relevance of information documents to the search query .In particular, we use "inner product similarity", i.e., the quantity of query keywords showing up in a document, to quantitatively assess such similitude measure of that document to the search query.

2. Related Work

Existing mCL-PKE plans are either wasteful in view of the utilization of lavish pairing operations or helpless against partial decryption attacks. With a specific end goal to address the execution what's more security issues, in this paper, we first propose a mCL-PKE plan without utilizing pairing operations.
As the information holder does not keep a duplicate of the information, at whatever point the client flow or ACPs change, the information holder needs to download and decode the information, re-encrypt it with the new keys, and transfer the encrypted information [1]. Recognize additionally that this methodology must be connected to all the information things encrypted with the same key. This is wasteful when the information set to be re-encrypted is vast.

So as to issue the new keys to the clients, the information holder needs to make private correspondence channels with the clients. The successful information recovery require, the huge measure of records request the cloud server to perform result pertinence positioning, as opposed to returning undifferentiated results. Such positioned inquiry framework empowers information clients to discover the most important data rapidly, instead of burdensomely dealing with each match in the substance gathering [2]. Positioned pursuit can likewise carefully take out superfluous system movement by sending back just the most applicable information, which is exceptionally attractive in the "pay-as-you-utilize" cloud standard. For protection insurance, such positioning operation, be that as it may, ought not to release any essential word related data. Then again, to enhance the query output precision and also to upgrade the client seeking background, it is likewise important for such positioning framework to help different decisive words seek.

2.1 Certificateless Public Key Cryptography

At right on time stages Functional encryption permits one to encode a discretionary complex access control approach with the encrypted message. Attribute based encryption (ABE) presented by Sahai and Waters [9] is a more expressive predicate encryption with a public index. Next Introduce Functional encryption permits one to encode a discretionary complex access control approach with the encrypted message.

At that point Al-Riyami [4] and Paterson presented a Certificateless Public Key Cryptography (CL-PKC). Since every client holds a blend of KGC delivered halfway private key and an extra user-chosen secret, the key escrow issue can be determined. Since the coming of CL-PKC, numerous CL-PKE plans have been proposed in view of bilinear pairings. The computational expense needed for pairing is still significantly high contrasted with standard operations such as modular exponentiation in finite fields.

Later Seung-Hyun Seo proposed [1] "An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds" an approach formal security show and give the security confirmation. On that intervened Certificateless open

key encryption mCL-PKE plan does not rely on upon the pairing-based operation. But it experience the ill effects of the Credential Trust Management.

2.2 Secure Searchable Encryption

At earlier stage, Single Keyword Searchable Encryption Customary single decisive word searchable encryption schemes typically build an encoded searchable list such that its content is covered up to the server unless it is given suitable trapdoors produced by means of secret key(s)[12][13][14][15]. Next Comes the Boolean Keyword Searchable Encryption to advance search functionalities, conjunctive keyword search over encoded data have been proposed. These plans bring about substantial overhead created by their major primitives, for example, reckoning cost by bilinear guide, for instance, or correspondence cost by secret sharing, for instance, . As a more general search methodology, predicate encryption plans are as of late proposed to backing both conjunctive and disjunctive search[16][17].

Finaly Ning Cao [2] proposed "Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data " that characterize and understand the issue of keyword ranked search over encrypted cloud data (MRSE) while protecting strict system wise security in the cloud computing paradigm.

2.3 Trust Management with our SMTP Gateway

You can now utilize Protected Trust to encrypt and send mechanized messages with the Protected Trust SMTP hand-off. For instance, you could coordinate your charging framework to email receipts through the Protected Trust SMTP transfer and they will get encrypted before being conveyed to the end beneficiary. Alternately, you could send robotized arrangement updates to your patients in a protected, HIPAA-agreeable way. This can be performed by virtually any stage making incalculable conceivable utilization cases.

Your application associate with the Protected Trust SMTP Relay utilizing TLS encryption and logs as a part of with an Access Credential. When the record is verified, the hand-off sweeps the message body for a <protectedtrust> XML tag. The XML piece is then parsed and if no mistakes are discovered, the email is encrypted and sent through Protected Trust to the beneficiaries utilizing the tagged confirmation technique.

3. Proposed System

Our methodology helps immediate revocation and guarantees the confidentiality of the data stored away in an untrusted public cloud while upholding the access control approaches of the data owner. Further, for various users satisfying the same access control approaches, our enhanced methodology performs just a single encryption of every data set and diminishes the general overhead at the data owner.

To enable Secure data sharing and ranked search with trust management over SMTP correspondence by compelling use of outsourced cloud information under the previously stated model, our framework outline ought to at the same time accomplish security and performance guarantees as follows.

1) We propose another mCL-PKE plan. We exhibit the formal security model and give the security proof. Since our mCL-PKE plan does not rely on upon the pairing-based operation, it decreases the computational overhead. In addition, we present an expansion of mCL-PKE plan to proficiently encrypt data for various client.
2) We propose a novel way to safely impart data in a public cloud. Not at all like traditional methodologies, the KGC just needs to be semi-trusted and can dwell in user in public cloud, in light of the fact that our mCL-PKE plan does not experience the ill effects of the key escrow problem.
3) We have executed our mCL-PKE plan and the augmentation to assess the execution. The trial result demonstrates that our mCL-PKE plan can be practically connected in an open cloud for secure data imparting.
4) Multi-keyword ranked search to outline seek plans which permit multi-keyword query and Give result similitude positioning to successful data retrieval, as opposed to returning undifferentiated results.
5) Privacy-preserving to keep the cloud server from taking in extra data from the data stand the index, and to meet privacy requirements specified the search must me on encrypted index.
6) To meet efficiency, above objectives on usefulness and protection should be attained to with low correspondence and processing overhead.
7) For trust management keys are circulated on a protected SMTP correspondence that have the SSL encryption. Just client that verified to cloud verification can ready to recover key through this management.

3.1 Definitions

In this section, we present the mediated Certificateless Public Key Encryption (mCL-PKE) scheme and its security model. Then, we prove the formal security of mCL-PKE scheme [1].

Definition 1. The mediated certificateless public key encryption (mCL-PKE**) scheme** is a 7-tuple mCL-PKE= (SetUp,SetPrivateKey, SetPublicKey, SEM-KeyExtract, Encrypt,SEM-Decrypt, USER-Decrypt).

Definition 2. The Computational Diffie-Hellman (CDH) problem is defined as follows: Let p and q be primes such that q| (p − 1). Let g be a generator of Z^*_p. Let A be an adversary. A tries to solve the following problem: Given (g, g^a, g^b) for uniformly chosen a, b, c ∈ Z^*_q, compute k = g^{ab}. We define A's advantage in result of CDH problem by **Adv (**A**)** =Pr [A (g, g^a, g^b) = g^{ab}].

3.2 Privacy-Preserving and Secure Cloud Storage

It is essential to perceive that if one specifically applies our fundamental mCL-PKE [6] plan to cloud computing and if numerous clients are approved to get to the same data, the encryption costs at the information owner can get to be high.

As shown in Figure. 3, the cloud is used for trust management which act as secure storage as well as a key generation center (KGC) and secure indexing agent for encrypted data. In proposed system first user generate his own public and private key in order to authenticate with cloud by using secure access control policies and share the credential and public key to key generation center (KGC). On next step the cloud generate key for encrypting owner data, partial decryption and for user to decrypt. Upon successful retrieval of keys from KGC data owner encrypts the sensitive data using the cloud generated user's public keys and uploads the encrypted data to the cloud. Along with this process, create an index for secure search over encrypted cloud data while protecting privacy of owner's data strictly in the cloud and store the values to cloud database.

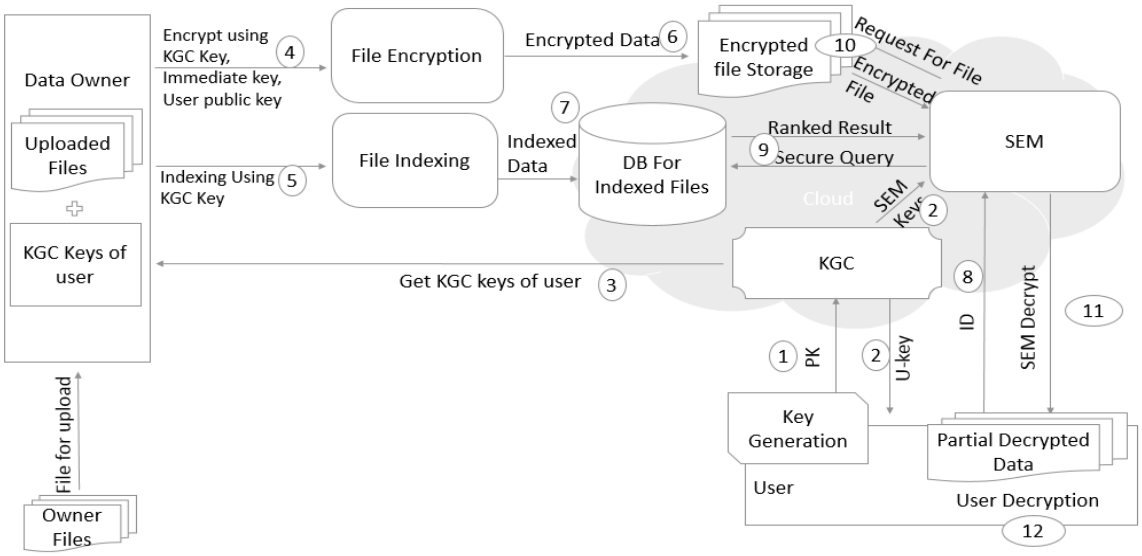

Figure 3: Architecture of overall system and secure search on encrypted cloud data

In this paper, shockingly, we characterize and tackle the issue of multi-keyword ranked search over encrypted cloud data (MRSE) [3] [5] while protecting strict framework shrewd security in the cloud computing standard. Among different multi-keyword semantics, we pick the proficient closeness measure of "direction matching," i.e., whatever number matches as would be prudent, to catch the importance of information reports to the inquiry question. In particular, we utilize "inward item closeness", i.e., the quantity of inquiry pivotal words showing up in an archive, to quantitatively assess such comparability measure of that document to the search query.

3.3 Improved Scheme for Secure Cloud Storage and Search

Our broadened mCL-PKE plan requires the data owner to encode the data encryption key just once and to give some extra data to the cloud so that approved clients can decode the substance utilizing their private keys. As shown in Figure. 4, our proposed framework gives an abnormal state perspective of the expansion. The thought is comparative to Proxy Re-Encryption (PRE) [8] by which the data encryption key is encoded utilizing the data owner's open key and later can be decrypted by diverse private keys after some change by the cloud which goes about as the intermediary. Nonetheless, in our expansion, the cloud essentially goes about as capacity and does not perform any change. Rather, the client has the capacity decrypt utilizing its own particular private key and a middle of the road key issued by the data owner.

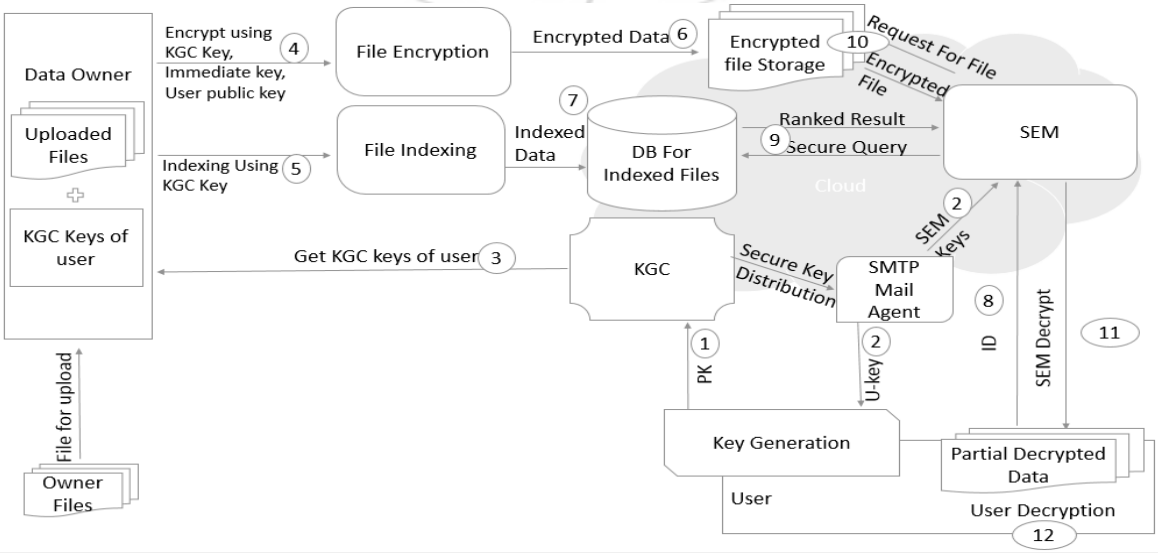

Figure 4: Improved architecture of overall system and secure search on encrypted cloud data with trust management

To retrieve file for user, it perform query from the cloud database and select the file to download. On the retrieval process, the cloud partially decrypts the encrypted data for the users and send the intermediate decryption keys to user by using secure SMTP communication. The user subsequently decrypt partially decrypted data fully using their private keys and the key received from cloud.

Amid the record development, every archive is connected with a parallel vector as a sub-record where every bit speaks to whether comparing decisive word is contained in the archive [7]. The inquiry question is likewise depicted as a double vector where every bit implies whether comparing watchword shows up in this hunt demand, so the likeness could be precisely measured by the internal result of the question vector with the data vector. On the other hand, straightforwardly outsourcing the data vector or the question vector will abuse the file protection then again the hunt security. To meet the test of supporting such multi pivotal word semantic without security ruptures, we propose an essential thought for the MRSE utilizing secure inward item reckoning, which is adjusted from a safe k-closest neighbor (kNN) system [10][11.], and after that give two altogether enhanced MRSE schemes in an orderly way to attain to different stringent protection prerequisites.

4. Experimental Results

Our test results demonstrate the effectiveness of essential mCL-PKE plan and enhanced methodology for the general population cloud. Figure. 5 demonstrates the time needed to perform the encryption operation in the mCL-PKE plan for distinctive message sizes. Since our plan does not utilize blending operations, it performs encryption productively. As can be seen from the chart, the encryption time increments directly as the message size increments. As the bit length of q builds, the expense increments non-straight subsequent to the encryption calculation performs exponentiation operations. A comparable perception applies to the SEM decryption and client decoding.

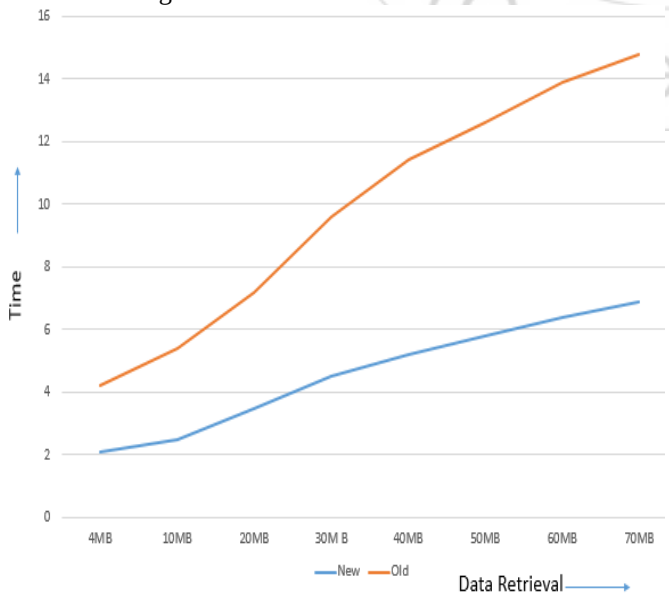

Figure 5: Comparison of decryption

In this section, we show a careful trial assessment of the proposed strategy on a true information. Figure. 6 demonstrates that the exactness in MRSE plan is apparently influenced by the standard deviation of the arbitrary variable". From the thought of adequacy, standard deviation is relied upon to be littler to get high exactness demonstrating the great purity of retrieved documents.

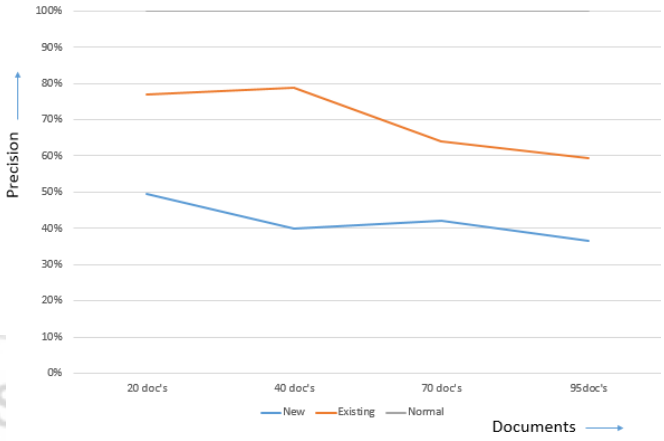

Figure 6: Comparison of Document retrieval

5. Conclusion

In this paper we proposed the first mCL-PKE plan without matching operations and gave its formal security also tackles the key escrow issue and revocation problem. Utilizing the mCL-PKE scheme as a key building square, we proposed an enhanced way to safely impart delicate data public clouds. Our test results demonstrate the proficiency of essential mCL-PKE plan and enhanced methodology for people in public cloud and also provide trust management through SMTP communication. We characterized and explained the issue of multi-keyword ranked search over encrypted cloud data, and created an assortment of protection necessities. For meeting the test of supporting multi-keyword semantic without protection breaks, we proposed a fundamental thought of MRSE utilizing secure internal item calculation. At that point, we gave two moved forward MRSE plans to attain against different stringent security prerequisites in two diverse danger models.

References

[1] Seung-Hyun Seo, Mohamed Nabeel, Xiaoyu Ding and Elisa Bertino "An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds" IEEE Transactions On Knowledge And Data Engineering, Vol. 26, No. 9, September 2014.

[2] Ning Cao, Cong Wang, Ming Li, Kui Ren and Wenjing Lou "Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data" IEEE Transactions On Parallel And Distributed Systems, Vol. 25, No. 1, January 2014.

[3] M. Abdalla et al., "Searchable encryption revisited: Consistency properties, relation to anonymousibe, and extensions," J. Cryptol., vol. 21, no. 3, pp. 350–391, Mar. 2008.

[4] S. Al-Riyami and K. Paterson, "Certificateless public key cryptog raphy," in Proc. ASIACRYPT 2003, C.-S. Laih, Ed. Berlin, Germany: Springer, LNCS 2894, pp. 452–473.
[5] E. Bertino and E. Ferrari. "Secure and selective dissemination of XML documents," ACM TISSEC, vol. 5, no. 3, pp. 290–331, 2002.
[6] G. Miklau and D. Suciu, "Controlling access to published data using cryptography," in Proc. 29th Int. Conf. VLDB, Berlin, Germany, 2003, pp. 898–909.
[7] M. Nabeel, N. Shang, and E. Bertino, "Privacy preserving policy based content sharing in public clouds," IEEE Trans. Knowl. Data Eng., vol. 25, no. 11, pp. 2602–2614, Sept. 2012.
[8] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," J. Cryptology, vol. 13, no. 3, pp. 361–396, 2000.
[9] A. Sahai and B. Waters, "Fuzzy identity-based encryption," LNCS 3494 in Proc. EUROCRYPT, Aarhus, Denmark, 2005, pp. 457–473.
[10] N. Shang, M. Nabeel, F. Paci, and E. Bertino,"A privacypreserving approach to policy-based content dissemination," in Proc. 2010 IEEE 26th ICDE, Long Beach, CA, USA, pp. 944–955.
[11] D. Song, D. Wagner, and A. Perrig, "Practical Techniques for Searches on Encrypted Data," Proc. IEEE Symp. Security and Privacy, 2000.
[12] E.-J. Goh, "Secure Indexes," Cryptology ePrint Archive, http:// eprint.iacr.org/2003/216. 2003.
[13] Y.-C. Chang and M. Mitzenmacher, "Privacy Preserving Keyword Searches on Remote Encrypted Data," Proc. Third Int'l Conf. Applied Cryptography and Network Security, 2005.
[14] R. Curtmola, J.A. Garay, S. Kamara, and R. Ostrovsky, "Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions," Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06), 2006.
[15] D. Boneh and B. Waters, "Conjunctive, Subset, and Range Queries on Encrypted Data," Proc. Fourth Conf. Theory Cryptography (TCC), pp. 535-554, 2007.
[16] R. Brinkman, "Searching in Encrypted Data," PhD thesis, Univ. of Twente, 2007.
[17] Y. Hwang and P. Lee, "Public Key Encryption with Conjunctive Keyword Search and Its Extension to a Multi-User System," Pairing, vol. 4575, pp. 2-22, 2007.
[18] Public-key cryptography. http://en.wikipedia.org/wiki/Public-key_cryptography

Author Profile

Shintomon Mathew received the B.Tech degree in Information Technology from University Of Calicut in 2011 and currently pursuing final year M. Tech degree in Computer Science and Engineering with Specialization in Cyber Security from KMP College of Engineering, Perumbavoor.

Asha Jose received the B.Tech Degree in Computer Science & Engineering from Mahatma Gandhi University, Kerala in 2009 and M.E Degree in Computer Science & Engineering from Annamalai University, Chidambaram in 2011. From 2011 to 2015, she worked in various Engineering Colleges as Asst. Professor. Presently she is engaged as a Ph.D Research Scholar with Department of Computer Science & Engineering at Karpagam University, Coimbatore.