International Journal of Computer Science
ISSN:2348-6600
Oddity...Probe...Reviste...
Published by SK Research Group of Companies(SKRGC)

http://www.ijcsjournal.com Volume 3, Issue 2, No 2, 2015. ISSN: 2348-6600
Reference ID: IJCS-104 PAGE NO: 591-597.

A Survey of Various Mutual Authentication Techniques in Cloud Computing Security

Miss. Richa Singh Dangi
Scholar
Dept. Of Computer Science & Engg.
Truba Institute of Engg. & I.T
Bhopal (M.P)
richadangi03@gmail.com

Mr. Amit Saxena
Associate Professor
Dept. of Computer Science & Engg.
Truba Institute of Engg. & I.T
Bhopal (M.P)
amitsaxena@trubainstitute.ac.in

Mr. Manish Manoria
Professor
Dept. of Computer Science & Engg.
Truba Institute of Engg. & I.T
Bhopal (M.P)
manishmanoria@trubainstitute.ac.in

Abstract*— Modern technical move ahead have given increase to the recognition and accomplishment of cloud. This novel standard is ahead an increasing awareness, since it gives cost proficient designs that sustain the communication, storage space, and exhaustive computing of data. On the other hand, these shows potential storage space examines bring many difficult design concerns; significantly due to the failure of data organize. These confronts, explicitly data privacy and data reliability, have major control on the safety measures and concerts of the cloud structure. Some threat representations take for granted that the cloud service provider cannot be believed, and consequently security exclusives suggest a high level protection declaration, such as storing encrypted data in cloud servers. Additional assume that cloud providers can be confidences, and that probable threats come mainly from external attackers and additional malicious cloud users.

***Index Terms*— Public key, Cloud Computing, Public Key Encryption, Attacks, Data Sharing.**

I. Introduction

Cloud computing has garnered much interest in recent years in the computing industry, the media, and academia. It is a form of pay-per-use distributed computing consisting of data centres providing commodity resources for massively scalable units of computing and storage for commercial enterprise applications as well as scientific computing; these facilities are delivered as a service to a global population of users over the Internet and wireless data networks.

Cloud computing promises many benefits to the IT profession: the ability to scale resources to get together contrasting consumer require in instantaneous, to bring new computing services faster, and to significantly lower assets and prepared costs for the reason that the computing stores of a cloud are operated by a third-party, clients are reduced from the troubles of hardware possession, protection, and management of the fundamental services. Clients are only accountable for organizing the purposes accomplished in the cloud and paying for the actual consumption of network and computing stores; they need not acquire the resources expenses of hardware with excess capacity to guarantee performance during peak order. In addition, they require not sustain the costs of maintenance, data backup, and security. Data distribution is appropriate gradually more significant for numerous users and sometimes a crucial requirement, especially for businesses and organizations in suspense to increase turnover. Citizens feel affection for to distribute information with one another. To protect a user's identity from being read or modify i.e. Data integrity, we need security. For a message which is signed and encrypted, the message is indication formerly and the signature is confirmed by each receiver. The message is encrypted with each recipient's public key by the correspondent using a symmetric key, and necessity decrypts his encrypted document by the symmetric key. Some aspects like elastic, protection of a digital signature algorithm and pace difficulty of signing and verifying in digital signature must be considered an important concern.

Take a situation in cloud computing as a design. The cloud computing offers a massive computing power and storage space capability which allows customers to distribute responsive data in the public cloud. Maintaining the data confidentiality is a significant well-designed in the cloud environment [2].

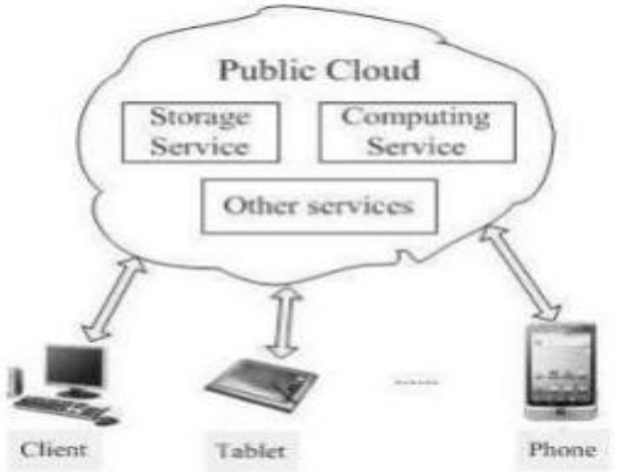

Figure.1 Public Cloud Architecture

The conventional public key cryptosystem (TPKC) employs a certificate to combine a public key with its client's distinctiveness. With the plan of protecting the "certificate free" property of IBC without affliction from the key escrow difficulty, Al-Riyami and Paterson presented "Certificateless Public Key Cryptography" (CLPKC) [1]. In CLPKC, the Key Generation Center (KGC) and a client collaborate to produce a private key; the equivalent public key does not necessitate a certificate to undertaking its legitimacy.

An improvement of using the cloud for storage space is that the provider descriptions for building and sustaining the storage space communications and its connected expenditures including control, cooling and server maintenance. Cloud computing is a scattered method where multiple cloud servers stay alive. Every cloud server has its own master secret key and public key capable by a PKI. Due to the significant influence of certificate association a cloud server may present scrutinizes to consumers transient all the way through IBC in presentation the dependability of PKG. All clients trust the server as a variety of clients may feel like to sustain their confidentiality from the cloud sever, they can use CLPKC by creation use of the cloud sever as a shortened private key creation center. A client in this cloud can exploit authoritative computing stores to accumulate responsive data i.e. by certificateless encryption, or to declare the authenticity of a document i.e. by certificate-less signature shared with others. Other approaches exist [3] that also require a trusted proxy for each decryption, which enlarges the communication expenditure. An interrelated work recommends the amalgamation of Attribute-Based Encryption (ABE) with proxy re-encryption in a cloud computing request permitting excellent-small pieced right of entry organize of possessions while effecting to pass on re-encryption movement to the cloud provider [4].

Past methodologies and propose a novel mediated Certificateless Public Key Encryption (mCL-PKE) [5] scheme that does not use pairing operations. Since most CL-PKC schemes are in illumination of bilinear combinations they are computationally expensive. Their method shortens the computational overhead by utilizing a pairing-free approach. There are many available CL-PKC schemes, it is introduced in this section some examples for them. Here they present are two available CL-PKE methods based on pairings: Basic CL-PKE scheme and Full CL-PKE scheme in [1]. Most constructions of CL-PKE schemes are based on using bilinear pairings although pairing is considered as the largest part luxurious process surrounded by additional mathematical process for example: addition, multiplication, exponentiation, multiplicative opposite and almost immediately. Fundamental CL-PKE method is described by means of seven algorithms and FullCL-PKE scheme is obtained after adding selected ciphertext safety measures to fundamental CL-PKE method. A FullCL-PKE method is also characterized using the identical seven algorithms like BasicCL-PKE, but with some modifications in some algorithms that responsible for achieving the chosen ciphertext security.

II. Theoretical Background

Wherever to rise the demand for new storage and network utilities, along with an increasing need for more cost-effective usage of storage capacities and network bandwidth for data transfer. As such, the use of remote storage systems is in advance an increasing concentration specifically the Cloud storage based services, since they provide profitable architectures. These architectures sustain the transmission, storage space, and exhaustive calculation of outsourced data in a pay per use business model. This widespread interest in cloud storage services mainly emanates from business organizations and government organization try to finding for additional elastic and cost-efficient methods.

That is the advantages of cloud acceptance are extremely substantial in a new era of responsiveness, effectiveness and efficiency in Information Technology service delivery. Dealing with these issues more closely, we perceive that many of the cloud security concerns are essentially have the problem of high costs for key management. With the intention of decrease the operating cost of key management an unusual is to utilize a public key cryptosystem. On the other hand, a conventional public key cryptosystem necessitates a confidence Certificate Authority (CA) to issue digital certificates that connect clients to their public keys. For the reason that the CA has to produce its individual signature on every one customer's public key and deal with each customer's certificate, the taken as a whole certificate organization is extremely cost and difficult. Conventionally, this difficulty can be explained by using certificate revocation catalogs (CRLs); online certificate status protocol (OCSP) [6], numerous solutions may be envisaged to exchange encrypted data with a cloud provider in a protected method such that the cloud provider is not in a directly row assigned with key material but naive schemes often prove difficult to scale.

III. Types of Possible Attacks on Effect Cloud Security

There are numerals of categories of confidentiality and safety measures attacks in the Cloud. The subsequent surrounds a review of the frequent types of attacks that may happen in the Cloud.

- **Flooding Attacks**
  A malicious client can launch demands to the Cloud; he/she can then without difficulty excess the server by generating counterfeit data demands to the Cloud. The effort is to enhance the workload of the Cloud servers by unbearable deliveries of resources without reason.
- **Law Enforcement Requests**
  When the FBI or government demands a Cloud Service Provider access to its data, the Cloud Service Provider is smallest amount probable to disallow them. For this reason, there may an intrinsic threat to user privacy and confidentiality of data.
- **Data Stealing Attacks**
  A term utilized to explain the appropriating of a consumer account and password by any means such as all the way through brute-force attacks or over-the-shoulder methods. The confidentiality and privacy of client's data will be rigorously violated. A widespread method to avoid such attacks is to include an extra value when authenticating. This significance can be circulated to the correct client by SMS and hence mitigate the likelihood of data confidentiality issues.
- **Denial-of-Service Attacks**
  Malicious code is introduced into the browser to open numerous windows and as a consequence refuse genuine customers right of entry to examines.
- **XML Signature Wrapping Attacks**
  Using different kinds of XML signature wrapping attacks individual can entirely take over the organizational accurate of the Cloud consumer and generate, remove, transform images as well as produce occurrences.
- **Cross site scripting attacks**
  Attackers can inject a piece of code into web applications to find a way around right of entry organize methods. Researchers found this possible with Amazon Web Services [7]. They were able to gain complimentary right to use to all client data, confirmation data, and tokens over and above plaintext passwords.

IV. Data Sharing and Accessing in the Cloud

With the progressions in Cloud computing there is at the present an increasing center of attention on executing data sharing competence in the Cloud. With the facility to distribute data by means of the Cloud, the number of advantages augments multifold. Alternatively the structure demands the data owner and the objective client or remote server distribution some general secret [8]. As companies and associations are at this moment outsourcing data and process to the Cloud they advantage additional with the capability to contribute to data between other companies and associations. Member of staffs also advantage as they can contribute to effort and work together with other workers and can also maintain operational at domicile or any other position such as the library. They don't require concerning about trailing employment as it is always in the Cloud. With shared consumers, the capability to distribute files, as well as manuscripts, photos and videos with other consumers make available enormous advantage to them.

When making an allowance for data distribution and group effort uncomplicated encryption methods do not be adequate particularly when allowing for key management. To make possible protected and secret data distribution and association in the cloud there requires to primary be appropriate key administration in the Cloud.

On the other hand, the most important difficulty with data distribution in the Cloud is the confidentiality and protection concerns. As talk about in Section. 2, the Cloud is release to numerous confidentiality and safety attacks, which make many customers suspicious of implementing Cloud expertise for data distribution reasons.

Constraints of Data Sharing in the Cloud

To make possible data distribution in the Cloud, it is very important that only approved customers are proficient to get right of entry to data accumulated in the Cloud. They review the best constraints of data distribution in the Cloud underneath:

- The data owner should be proficient to identify a group of customers that are permitted to analysis his/her data.
- Any component of the collection should gain right of entry to the data anytime exclusive of the data owner's involvement.
- No other customer, on behalf of the data owner and the parts of the group should achieve right of entry to the information including the Cloud Service Provider.
- The data owner should be proficient to withdraw right to use to data for any part of the group.
- The data owner should be proficient to append elements to the group.
- No element of the group should be permitted to withdraw accurate of other parts of the group or join new customers to the group.
- The data owner should be capable to identify who has read/write authorizations on the data owner's files.

To accomplish confidentiality and protection conditions in the Cloud structural design can go an extensive method to create a center of attention large amounts of consumers to implementing and agreement Cloud technology.

- ***Data Confidentiality***: Unauthorized consumers including the Cloud are supposed to not be proficient to right to use data at any particular instance. Data should stay behind secret in transfer passed away and on encouragement medium. Only approved consumers should be proficient to gain right to use to data.
- ***User revocation***: When a client is withdrawing right to use rights to data so that client should not be proficient to gain right to use to the data at any particular time. In an ideal world, client revocation should not have an effect on other approved consumers in the group for good organization reasons.
- ***Scalable and resourceful***: Since the numeral of cloud consumers have a tendency to be enormously huge and at point in times impulsive as consumers link and put down it is very important that the structure sustain competence as well as be scalability.
- ***Agreement between entities***: When making an allowance for data distribution techniques [2] in the Cloud it is very important that still when assured entities join together they should motionless not be proficient to right of entry any of the data without the data owner's authorization. Previous efforts of writing on data distribution did not think this difficulty, on the other hand agreement between entities can not at all be written off as an improbable occurrence.

Require for Key Management in Cloud

Encryption provides data security while key management allows right to use to save from harmed data. It is robustly suggested to encrypt data in transportation over networks passed away and on encouragement medium. Especially, data encryption no longer with us for e.g., for long-term archival storage space can keep away from the possibility of malicious cloud service providers or malicious multi-occupants exploitation. Simultaneously, secure key accumulates as well as key encouragement and recoverability and right to use to key accumulates must be progressively accomplished in view of the fact that inappropriate or access to key storage space could show the way to the cooperation of all encrypted data. Key management is no matter which you do with a key recognize encryption and decryption and wraps the formation/deletion of keys, activation/deactivation of keys, and storage space of keys and so on. Most Cloud service provider's make available essential key encryption methods for defensive data or may disappear it to the consumer to encrypt their own data. Both encryption and key management are very essential to help protected applications and data accumulated in the Cloud. Requirements of efficient key management are talk about below.

- ***Make safe key stores***: The key stores themselves must be confined from malicious clients. If a malicious client increases right to use to the keys they will be capable to right to use any encrypted data the key is communicated. Hence the key stores themselves must be confined in storage space in transportation and on encouragement medium.
- ***Right to use to key stores***: Access to the key stores should be restricted to the customers that have the

accurate to right to use data. Taking apart of responsibilities should be utilized to help organize right to use. The thing that utilizes a given key should not be the unit that stores the key.

- ***Key backup and recoverability***: Keys require make safe backup and recovery explanations. Loss of keys, even though efficient for devastating right to use to data that can be extremely disturbing to a company and Cloud providers require to make sure that keys aren't lost all the way through backup and recovery methods.

Identity and Access Management

Secure management of identity and access control is a serious issue to avoid explanation and examine take controlling. It is robustly suggested to make illegal distribution of account records to influence physically powerful (multi-factor) authentication if probable and to think about entrusted authentication and administration confidence transversely all types of cloud services. Access control is a protection characteristic that manages how clients and methods exchange a few words and cooperate with one another. Access means current of information between subject and object. Subject is a dynamic entity that demands access to an object or the data in an object while object is a reactive entity that holds information. There are generally three types of access control:

- Role Based Access Control (RBAC),
- User Based Access Control (UBAC), and
- Attribute Based Access Control (ABAC).

In UBAC, the access control list (ACL) encloses the record of consumers who are approved to access data. This is not viable in clouds where there are numerous consumers. In RBAC, clients are confidential based on their entity positions. Data can be right to use by consumers who have corresponding responsibilities. The jobs are described by the structure. For example, only faculty members and senior secretary's strength have right to use to data but not the less important secretaries. ABAC is more widened in range in which clients are given characteristics and the data has joined right to use rule. Only consumers with legitimate set of characteristics, assuring the right to use strategy can contact the data.

An area where right to use control is extensively being employed is health care. Clouds are being utilized to accumulate responsive information about uncomplaining to allow right to use to medical experts, hospital employees, researchers, and policy creators. It is significant to manage the right to use of data so that only authorized clients can right to use the data. Using ABE, the evidences are encrypted under some right to use rule and accumulated in the cloud. Clients are specified sets of elements and equivalent keys.

V. Literature Survey

Here in this paper [5] author has proposed a new arbitrated certificateless encryption method without pairing process for strongly distribution sensitive information in open clouds. Here they use Mediated certificateless public key encryption (mCL-PKE) explains the key escrow difficulty in identity based encryption and certificate revocation difficulty in public key cryptography. On the other hand, existing mCL-PKE methods are also in-competent because of utilize of costly pairing process or susceptible beside incomplete decryption attacks. With the intention of concentrate on the presentation and protection concerns, here in this paper they apply their mCL-PKE method to build a realistic explanation to the difficulty of sharing sensitive information in public clouds. The cloud is utilized as a protected storage space and a key generation center. In their method the data owner encrypts the susceptible data using the cloud generated users' public key supported on its right to use manage policies and uploads the encrypted data to the cloud storage space. Due to unbeaten permission, the cloud moderately decrypts the encrypted data for the cloud consumers. The cloud consumers consequently completely decrypt the in some measure decrypted data using their own private keys. The privacy of the content and the keys is protected regarding the cloud, for the reason that the cloud cannot entirely decrypt the information. They also suggest an expansion to the exceeding approach to get better the competence of encryption at the data owner on cloud. Experimental result shows that proposed system has it's enhance security and performance and that schemes are proficient and practical use in real time application.

In this paper author [9] has to propose CL-PRE, a certificateless proxy re-encryption method amplified with certificateless public key cryptography, which influences cloud not only for data storage space but also for secure key sharing for data allocation with public cloud. In this method m CL-PRE, a data owner initially data encrypts with a symmetric data encryption key (DEK) before stored common data in cloud with an encryption key by its data owner, which is additional encrypted and changed by cloud, and then scattered to genuine beneficiary in agreement with access control.

International Journal of Computer Science
ISSN:2348-6600
Oddity...Probe...Reviste...
Published by SK Research Group of Companies(SKRGC)

http://www.ijcsjournal.com Volume 3, Issue 2, No 2, 2015. ISSN: 2348-6600
Reference ID: IJCS-104 PAGE NO: 591-597.

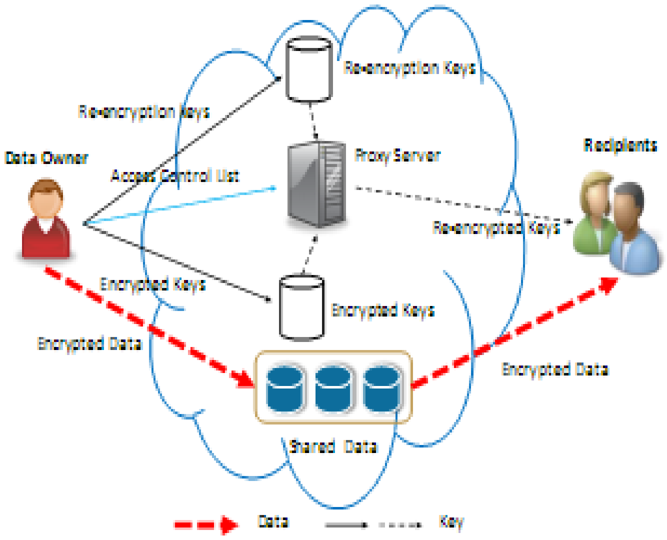

Figure 2: Overview of CL-PRE for data sharing.

The data owner then produces proxy re-encryption keys with its entire possible beneficiary and sends to a cloud inhabitant proxy service, along with the encrypted DEK with its public key of receptions, and reduces the key escrow difficulty in characteristics based cryptography and they require of certificate. While preserving data and key confidentiality from semi-trusted cloud, CL-PRE [9] influences maximal cloud resources to diminish the computing and communication cost for data holder. Using the re-encryption keys, the cloud is then proficient to alter the encrypted DEK to one that can be decrypted using an individual recipient' private key towards running proxy in public cloud atmosphere. In this approach, the cloud efforts only as a proxy for key organization. CL-PRE guarantees that the cloud cannot get the comprehensible DEK during the alteration. To get better the strength of the structure, and randomized CL-PRE to randomize the re-encryption key every time of data distribution to facilitate decrease the trust on the proxy. Experimental result proves that their proposed methods are realistic for cloud-based applications.

In this paper author propose [10] a novel method of using CP-ABE in the circumstance of enterprise applications and also enlarged a revocation instrument that concurrently authorizes superior flexibility, fine-grained right to use control and revocation. The responsibility allocates clients a set of attributes within their secret key and share outs the secret key to the individual customers. Any customer that assures the access control procedure characterized from the data associate can right of entry the data. When a consumer is withdraw access rights the data is re-encrypted in the Cloud submitting the revoked user's key inadequate. The method is demonstrated to be semantically protected against chosen cipher text attacks alongside the CP-ABE representation. On the other hand, the method is not well-designed in the case of customer revocation since the updating of cipher texts after consumer revocation places important calculation transparency even if the weight is removed to the Cloud [10]. The advantages and requirements of the proposed token are also discussed in the paper.

S. No.	Paper	Author	Advantages	Issues
1	Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data Computing. [11]	Ning Cao, Cong Wang, Ming Li, Kui Ren and Wenjing Lou	Here identical amount of matches are also sufficient, to take hold of the significance of information documents to the search query.	To quantitatively evaluate such similarity calculate of that document to the search query
2	CL-PKE: A certificateless proxy re-encryption scheme for secure data sharing with public cloud. [12]	X. W. Lei Xu and X. Zhang.	Number of keys equivalent to as a smallest amount the logarithm of the number of clients	Find a new approach can proficiently deal with symmetric key and user revocations based methods.
3.	Efficient Revocable Certificate-less Encryption Secure in the Standard Model. [13]	L. Shen, F. Zhang, Y. Sun	Removing the use of secret channels for key- update and without resorting to a security.	To revocation in CLPKC with a concrete construction of a revocable certificateless signature (RCLS) scheme

4.	Secure Certificateless Signature Scheme Supporting Batch Verification. [14]	C.-I. Fan, P.-H. Ho, J.-J. Huang and Y.-F. Tseng	CL-PKS scheme with fast batch verification which enables a verifier to verify a set of signatures.	More efficiently verifying them one by one on set of signatures.

VI. Conclusion

Cloud computing gives confidentiality of susceptible and confidential client data is make sure when exchanged between a cloud application and an authorized client and also when it is in storage space on cloud server. The cloud provider is conventionally measured for the most part un-trusted. Scarce assets for mobile device clients are protected, by assigning everyday jobs to the cloud provider, so that high scalability and financial system can be accomplished even in the context of a dynamic consumer inhabitant.

REFERENCES

[1] S.S. Al-Riyami, K.G. Paterson, Certificateless Public Key Cryptography, In Asiacrypt 2003, LNCS 2894, pp 452-473, 2003.

[2] Danan Thilakanathan, Shiping Chen, Surya Nepal and Rafael A, “Secure Data Sharing in the Cloud”, S. Nepal and M. Pathan (eds.), Security, Privacy and Trust in Cloud Systems, 45 DOI: 10.1007/978-3-642-38586-5_2, © Springer-Verlag Berlin Heidelberg 2014.

[3] S. Jahid, P. Mittal, and N. Borisov, \EASiER: encryption-based access control in social networks with efficient revocation," in Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, ser. ASIACCS '11. NewYork, NY, USA: ACM, 2011, pp. 411-415.

[4] S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proceedings of the 29th conference on Information communications, ser. INFOCOM'10. Piscataway, NJ, USA: IEEE Press, 2010, pp. 534-542.

[5] 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.

[6] M. Myers, R. Ankney, A. Alpani, S. Galperin, C. Adams, X.509 Internet Public Key Infrastructure: Online Certificate Status Protocol (OCSP), RFC 2560.

[7] Ruhr “Cloud computing: Gaps in the cloud”. NewsRx Health Sci. (2011).

[8] S. Jarecki, C. S. Jutla, H. Krawczyk, M. Rosu, and M. Steiner. Outsourced symmetric private information retrieval. In CCS’13, Berlin, Germany, 2013, pages 875–888, 2013.

[9] Lei Xu, Xiaoxin Wu, Xinwen Zhang, “CL-PRE: a Certificateless Proxy Re-Encryption Scheme for Secure Data Sharing with Public Cloud” ASIACCS ’12, May 2–4, 2012, Seoul, Korea.

[10] Tu S, Niu S, Li H, Xiao-ming Y, Li M, “Fine-grained access control and revocation for sharing data on clouds,” IEEE 26th international parallel and distributed processing symposium workshops and PhD forum (IPDPSW) 2012, pp 2146–2155.

[11] 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.

[12] X. W. Lei Xu and X. Zhang, “CL-PKE: A certificateless proxy re-encryption scheme for secure data sharing with public cloud,” in ACM Symp. Inform. Comput. Commun. Security, 2012.

[13] L. Shen, F. Zhang, Y. Sun, Efficient Revocable Certificate-less Encryption Secure in the Standard Model, The Computer Journal (2013) doi: 10.1093/comjnl/bxt040. First published online: April 30, 2013.

[14] C.-I. Fan, P.-H. Ho, J.-J. Huan and Y.-F. Tseng, “Secure Certificateless Signature Scheme Supporting Batch Verification.” In AsiaJCIS, 2013, pp. 8–11.