IJIRMET ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 2, Issue 9, September 2017

(EOCA-KGF): Enhanced Outsourcing Cloud Attribute Based Cryptosystem With Key Generating Factor For Cloud Storage

[1] J.Gayathri, [2]Dr.A.Muthukumaravel, [3] P. Shivasakthi
[1] Research Scholar of Computer Department, Bharath University, Chennai.
[2] Head, Department of MCA, Bharath University, Chennai.
[3] Asst. Professor, Dept. of Computer Science, Sri Sankara Arts & Science College, Enathur, Kanchipuram

Abstract: ***In cloud computing, user commonly outsources their data to the cloud service provider. This leads to bigger issues in the cloud settings. Attribute based cipher text is the best method to tackle the problem. However the management cost and encryption size is much higher to access control policy. The outsourced attribute based cipher data with fine grained access control system can mostly decrease the management cost for users who want to access cipher text data stored in cloud by outsourcing the deep reckoning to cloud service provider (CSP). The quantity of encrypted files stored in cloud becomes high range in size which makes obstruct the consequent query processing. To contract with above issues a new scheme is introduced which cryptographic primitive is called attribute-based cipher text scheme with outsourcing key-issuing and outsourcing decryption, which can implement keyword search function. The proposed EOCA-KGF scheme is proved secure against searched decryption attack. Partial decryption is performed by CSP delegated by data user without knowing anything about the decoded form. Moreover, the CSP can carry out cipher keyword search without knowing about the keywords entrenched in trapdoor. This paper extending the trust authority zone for cloud consideration. The secret key is sent to the user mail from authorized party. Data owner verified the user and then by using the key, data is decrypted in confidential manner. Symmetric key and secret keyword in unknown format is sends for user authentication from data owner.***

Keywords- ***attribute-based cipher text policy; cloud computing; outsourced key-issuing; outsourced decryption; keyword search, Decoding, Index, Encoding, access control, trusted computing.***

I. INTRODUCTION

Cloud computing is the key of IT exhortation. Although the meaning of cloud is still "cloudy" sinuously it is data center. Perhaps the simplest operational definition of cloud computing is "being able to access files, data, programs and 3rd party services" from a Web browser via the Internet that are hosted by a 3rd party provider and "pay-per-use" method is followed. The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams.

Past-several years cloud security is the effective topic in an enterprise, researchers, and for providers. Security keeps high concern and mind blowing thinking too, here some key capabilities task is performed to migration between global cloud service providers.

A. Our Work:

In the Proposed system, we organically integrate EOCA-KGF and present a novel cryptographic paradigm called Enhanced outsourcing cloud attribute based cryptosystem with key generating factor for cloud storage. In our system, User sends the confidential data to the cloud system. Before sending, the data will be encrypted using attribute set and indexes will be created for the data such as keywords. If any user wants to view the data, they have to decrypt the attribute set if they have necessary permission in place. Consider the user looking for the word "Cyber", data related to the keyword "Cyber" will be displayed according to the user's permission. User has to choose the one intended to download.

Advantages:

It is efficient since we will download only the decrypted content for the searched keyword. Secure and Time Consuming since it is shared with cloud system. Computed cost will be minimized and Trust worthy. We are using Keyword search which is the best way for search, security and privacy.

Allocating Cloud Service to the user is based on the trust of the user and its relationship. Anonymization is the best method for cloud computing. Its shows only key information and protect confidential data. Privacy is maintained but at the same time we can view the data in secured manner.

In available system, Encrypted data is done by EOCA-KGF and store it as confidential into the server even though it is not authenticated. Unknown user can also share the data and it might leak the decryption method. The respective crypting technique has to be done on both server and client side which result in cost and time.

B. RELATED WORK:

As per our knowledge, there is no current solution is more efficient than our proposed design. Below is the brief description of appropriate techniques.

In the existing technology "KSF-OABE" ensures data in the encrypted format and ensures confidentiality irrespective the destination server is not genuine and ensures privacy with complete file server. In the existing system, there is no Verifiability.

1) Public Key Encryption with Keyword Search

D. Boneh,G.D. Cirescenzo, R. Ostrovsky and G. Persiano

We study the problem of searching on data that is encrypted using a public key system. Consider user A, who sends email to user B encrypted under user A’s public key. An email gateway wants to test whether the email contains the keyword “entity” so that it could route the email accordingly. User A, on the other hand does not wish to give the gateway the ability to decrypt all those messages. We define and

built a mechanism that enables user A to provide a key to the gateway that enables the gateway to test whether the word “entity” is a keyword in the email without reading anything else about the email. We refer to this mechanism as Public Key Encryption with keyword Search. As another example, consider a mail server that stores various messages publicly encrypted for user A by others. Using our mechanism user A can send the mail server a key that will enable the server to identify all messages containing some specific keyword, but nothing else to know. We describe the proposal of public key encryption with keyword search and give several constructions.

2) Public-Key Encryption with Fuzzy Keyword Search: A Provably Secure Scheme under Keyword Guessing Attack

P.Xu, H.Jin, Q.H.Wu, and W.Wang

The public-key encryption with keyword search (PEKS) is to be drawn lot of client interest which keeps public key encrypted documents flexible to secure keyword search. However, PEKS oppose against keyword guessing attack by guessing that the size of the keyword space is beyond the polynomial level. But this option is hopeless in practice. PEKS are insecure under keyword guessing attack. As we observe, to avoid the availability of the exact search trapdoor to adversaries is to defend such attack by make use of the key. Accordingly, we are finding the middle ground exactness of search trapdoor by mapping at least two different keywords into a fuzzy search trapdoor. We suggest here a novel concept of public-key encryption with fuzzy keyword search (PEFKS), by which the un-authorized server only obtains the fuzzy search trapdoor instead of the accurate search trapdoor, and chosen keyword attack (SS-CKA) defines under semantic security and in distinguish ability of keywords under non-adaptively chosen keywords and keyword guessing attack (IK-NCK-KGA). For the keyword space presence and absence of uniform distribution, we respectively present two universal transformations from anonymous identity-based encryption to PEFKS, and prove their SSCKA and IK-NCK-KGA securities. To our sound knowledge, PEFKS is the first scheme to defy against keyword guessing attack on condition that the keyword space is not higher than the polynomial level.

3) Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data

V. Goyal, O. Pandey, A. Sahai, and B. Waters

The data is to be encrypted which is stored in third-party sites via the hosted environment, since all the information is more sensitive. While encrypting the data it shares the coarse-grained level (i.e. providing private key to another party). A new cryptosystem is implemented for fine-grained sharing of encrypted data is said to be Key-Policy Attribute-Based Encryption (KP-ABE). The user is capable to decrypt in the specified cryptosystem, cipher text constructed with set of attribute and private keys are controlled and maintained with access structures. Moreover the sharing of audit-log information and broadcast encryption are demonstrated. It supports the private key delegation which represents the (HIBE) Hierarchical Identity-Based Encryption.

4. Twin Clouds Architecture

Bugiel et al

The two-tier architecture consist the twin cloud for arbitrary computations for an untrusted commodity cloud and outsourcing the data. Based on the twin clouds architecture, originally consider to address the privacy-preserving keyword search problem similarly supporting fine-grained access control through encrypted data in public cloud. However the adversary model is less strong. Especially the private cloud is required to be completely trusted, but here semi-trusted is tasked in our schemes.

5. Symmetric Searchable Encryption

Curtmola et al

Under the prescribed two-layered encryption, the specified keyword encrypted independently. User stores the data in unknown format to the semi-trusted server. Then search with a certain keyword. Additionally, bloom filter is introduced to construct secure indexes to search keyword ,it allow the server to find the file in hosted environment under specified keyword and it only decrypt the partial file. A previous method of SSE was provide the security notions and index approach were introduced an array and look-up table construct for the complete file collection. Each and every entry of the array reposed the encryption file via the file identifier set organized by certain keyword, to locate and decrypt the appropriate element from array the look-up table assist to further concern.

II. SYSTEM DESIGN

The system architecture EOCA-KGF for cloud storage:

The major purpose is to defend the information from CSP and to guard the safety as well as confidentiality of user's concern all the way through creating a trapdoor for encrypted keyword.

It is important to note that the user searching a lot online which is saved in the form of cookies. The cookies log the searched keywords.

Most of the applications use complicated technology to safe guard the data encryption. This type of latest public-key cryptographic primitive permits us to execute access method files which are encrypted by keyword search.

There are two types of ABE methods, namely KP-ABE (key-policy ABE) and CP-ABE (cipher text-policy ABE) are projected. In KP-ABE method, every cipher text is linked to a set of keywords, and every user's confidential key is linked with access guidelines for attributes. A consumer is capable to decrypt the text if is linked to the cipher text satisfy the policy connected with the user's confidential key.

Below are the some terms using in crypto system:

Plain text—an unencrypted format

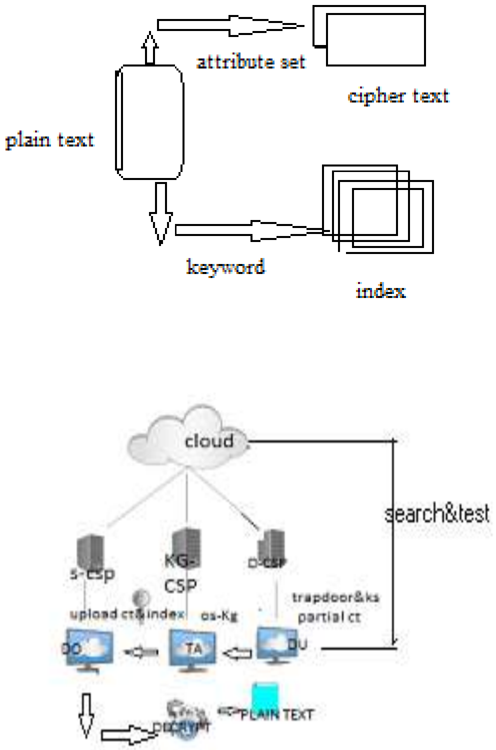
Cipher text—an encrypted format

Cryptology—the art of secure communications Symmetric Encryption—encryption technique that uses one key to encrypt and decrypt

Asymmetric Encryption—encryption method that uses two keys: if you encrypt with one you may decrypt with the other key.

Hash Function—one-way encryption method using an algorithm and no more keys.

Fig 1: System model



Trusted Authority (TA):

TA is the characteristic authority hub, which is answerable for the declaration of system parameters, and the creation of attribute keys & trapdoor.

Cloud Service Provider:

KG-CSP (Key Generation Cloud Service Provider): It is an applicant that provisions computing service outsourcing for Trusted Authority by finishing the generation of costly key allocated by Trusted Authority.

D-CSP (Decryption-Cloud Service Provider): It is an applicant that provisions computing service outsourcing throughout accomplishing partial cipher text decryption and service of keyword search on the partially decrypted cipher texts.

S-CSP (Storage-Cloud Service Provider): It is an applicant that provisions outsourcing information storage space for user wants to share the data in the cloud system.

DO - Data Owner:

This is an applicant who intends to upload and share his information files on the storage of cloud system in a protected way. Encrypted cipher text will be send to the requested users whose access method will be fulfilled by cipher texts. The accountability of Data Owner is to create indexes for keywords and uploads the encrypted data with indexes.

DU - Data User:

This is an applicant who decrypts the data back and stored in Storage-Cloud Service Provider with the assistance of D- Cloud Service Provider. If Data user meets the access structures then is able to access the encrypted data and retrieve the original files. Data user downloads proposed cipher text with the assistance of trapdoor linked with keyword. Data user is answerable for selecting keywords to generate trapdoor, and data decryption.

Trapdoor of the keywords can be recognized by apply a one-way function.

SECURITY MODEL:

The proposed system provides two schemes, the first one is to transforms the unique keyword to delegate the search function, user tracking the set of keyword associated in specified in a trapdoor. The second scheme is deploying the hash chain function frequently to the initial process. Since the user only process and able to traverse the hash chain function both front and rear side, but the server able to traverse only forward process. In this system, the keyword is also coded in encoded format.

ENCRYPTION PROCESS:

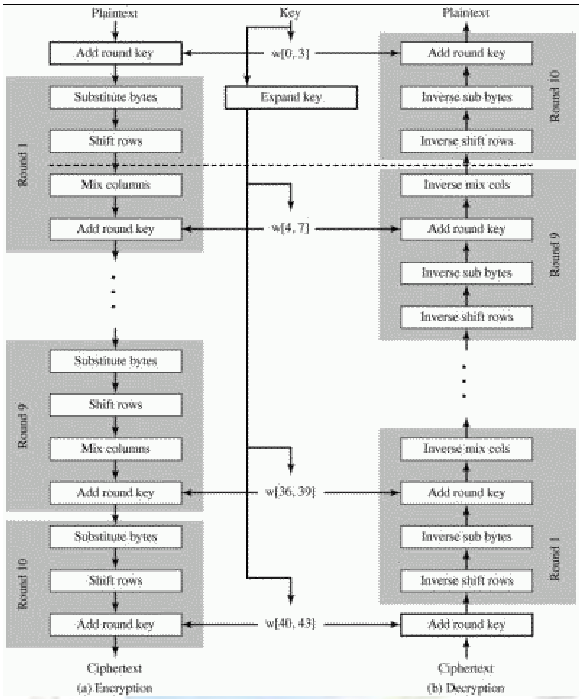
The method of encryption process of a cipher AES (Advanced Encryption Standard) is the reverse order of Decryption process. This method is strength of cryptographic technique. It follows the modular addition and subtraction method for encrypt and decrypt process.

Sub Bytes - Byte Substitution

The 16 input bytes are substituted by noticing a constant table (S-box) given in design. Four rows and four columns is the result of matrix method.

Shift rows

Each of the four rows of the matrix is shifted to the left. Any entries that ‘go down’ are re-inserted on the right side of row



Shift is carried out as follows –

- First row is not shifted.
- Second row is shifted one (byte) position to the left.
- Third row is shifted two positions to the left.
- Fourth row is shifted three positions to the left.
- The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

Mix Columns

By using a special mathematical function each column is now transformed to four byte column wise. This function takes as input the four bytes of one column and outputs four column and to form completely new bytes, also replaces the original column which result is another new matrix consisting of 16 new bytes. It should be noticed that this step is not performed in the last round.

Add round key

The 16 bytes of the matrix are now considered to be as 128 bits and are XOR to the 128 bits of the round key. If this is the final round then the output is the cipher text. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we mention another similar round.

DECRYPTION PROCESS

The method of decryption process of an AES (Advanced Encryption Standard) cipher text is similar to the reverse order of encryption process, each round consists of the four processes conducted to perform reverse order −

- Add round key
- Mix columns
- Shift rows
- Byte substitution

Since sub-processes in each and every round are in invalidate manner the encryption and decryption algorithm needs to be implemented independently, although they are related very closely.

STEMMING ALGORITHM:

A stemming algorithm is a method of linguistic normalization, in which the variant forms of a word are compact to a form an original form,

E.g,

Before stem

User enforcing

Users enforced

Used enforce

After stem

Use engineer

The stemming algorithm is used to detect and remove stop words by own. This algorithm is used to implement by matching similar words and to improve effectiveness of IR (Information Retrieval) this method assist to perform reducing the index size due to the elimination to bring an end words.

SECURE HASH FUNCTION:

The SHA (Secure Hash Algorithm) is one of the cryptographic hash functions. A cryptographic hash is similar to signature for a text or a data file. SHA-256 algorithm generates an almost-unique, fixed size 256-bit (32-byte) has, it cannot be decrypted back since hash is one way function.

III. CONCLUSION:

In this document, we suggest the data owner to manage the search of encrypted data outsourced with respect to an access control policy, while the certified data users sends out the search operations to the cloud system and strength the cloud system to truly execute the data search. CP-ABE method that gives key-issuing outsourcing, decryption technique and search function using keyword. Our method is capable because we download only the partial cipher text decryption with respect to a keyword. In our method, pairing operation is time-consuming which is outsourced to cloud involves only the small operations done by users. Furthermore, the projected system supports the keywords search which can improve the efficiency of communication and ensures the security and privacy. Further aiming is to search the data efficient manner and associate dynamic data and updating technology.

REFERENCES:

[1] S. Pearson, Y. Shen and M. Mowbray, “A Privacy Manager for Cloud Computing,”Proc. First International Conference Cloud Computing (CloudCom’09), M. Gilje-Jaatun, G. Zhao and C. Rong, eds., LNCS 5931, Berlin: Springer-Verlag, pp. 90-106, 2009.

[2] A. Sahai and B. Waters, “Fuzzy Identity-Based Encryption,”EUROCRYPT’05, LNCS, vol. 3494, pp. 457-473,2005.

[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data,”Proc.13th ACM Conference on Computer and Communications Security (CCS ’06), pp. 89-98, 2006, doi:10.1145/1180405.1180418.

[4] J.W. Li, C.F. Jia, J. Liand X.F. Chen, “Outsourcing Encryption of Attribute-Based Encryption with Mapreduce,”Proc.14th International Conference on Information and Communications Security (ICICS’12), LNCS7618, Berlin:Springer-Verlag, pp. 191-201, 2012.doi:10.1007/978-3-642-34129-8_17

[5] A. Lewko, T. Okamoto, A. Sahai, K. Takashimaand B. Waters, “Attribute-Based Encryption and (Hierarchical) Inner Product Encryption,”EUROCRYPT’10, H. Gilbert, ed., LNCS 6110, Berlin: Springer-Verlag, pp. 62-91, 2010.

[6] J.G. Han, W. Susilo, Y. Mu andJ. Yan, “Privacy-Preserving Decentralized Key-Policy Attribute-Based Encryption, ”IEEE Transactions on Parallel and Distributed Systems,vol.23, no.11, pp. 2150-2162, Nov.2012, doi: 10.1109/TPDS.2012.50.

[7] T. Okamoto and K. Takashima, “Fully Secure Functional Encryption with General Relations from the Decisional Linear Assumption,”CRYPTO’10, T. Rabin, ed., LNCS 6223, Berlin: Springer-Verlag, pp. 191-208, 2010.

[8] W.R.Liu, J.W.Liu, Q.H.Wu, B.Qin, and Y.Y.Zhou, “Practical Direct Chosen Ciphertext Secure Key-Policy Attribute-Based Encryption with Public Ciphertext Test,”ESORICS’14, LNCS 8713, Berlin: Springer-Verlag, pp. 91-108, 2014.

[9] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy Attribute-Based Encryption,” Proc. IEEE Symp. Security and Privacy (SP ’07), pp. 321-334, May. 2007, doi:10.1109/SP.2007.11.

[10] L. Cheungand C. Newport, “Provably Secure Ciphertext Policy ABE,”Proc.14th ACM Conference on Computer and Communications Security(CCS ’07),pp. 456-465,2007, doi:10.1145/1180405.1180418.

[11] H.L. Qian, J.G. Liand Y.C. Zhang, “Privacy-Preserving Decentralized Ciphertext-Policy Attribute-Based Encryption with Fully Hidden Access Structure,”Proc.15th International Conference on Information and Communications Security(ICICS ’13),LNCS8233,Berlin:Springer-Verlag,pp. 363-372, 2013.

[12] H.Deng, Q.H.Wu, B. Qin, J.Domingo-Ferrer, L.Zhang, J.W.Liu, and W.C.Shi, “Ciphertext-Policy Hierarchical Attribute-Based Encryption with Short Ciphertexts,” Information Sciences, vol. 275, no. 8, pp. 370-384, Aug. 2014.

[13] J.T.Ning, Z.F.Cao, X.L.Dong, L.F. Wei and X.D.Lin, “Large Universe Ciphertext-Policy Attribute-Based Encryption with White-Box Traceability,” ESORICS’14, LNCS 8713, Berlin: Springer-Verlag, pp. 55-72, 2014.

[14] Z.Liu, Z.F.Cao, and D.S. Wong, “Traceable CP-ABE: How to Trace Decryption Devices Found in the Wild,” IEEE Transactions on Information Forensics and Security,vol.10, no.1, pp. 55-68, Jan.2015.

[15] J.T. Ning, X.L. Dong, Z.F. Cao, L.F. Wei and X.D. Lin, “White-Box Traceable Cphertext-Policy Attribute-Based Encryption Supporting Flexible Attributes,” IEEE Transactions on Information Forensics and Security,vol.10, no.6, pp. 1274-1288, Jun.

[16] J. Li, X.F. Chen, J.W. Li, C.F. Jia, J.F. Maand W.J. Lou, “Fine-Grained Access Control System Based on Outsourced Attribute-Based Encryption,”Proc.18th European Symposium on Research in Computer Security(ESORICS ’13),LNCS8134,Berlin: Springer-Verlag, pp. 592-609, 2013.

[17] J. Li, X. Huang, J. Li and X. Chen, “Securely Outsourcing Attribute-Based Encryption with Checkability, ”IEEE Trans. Parallel and Distributed Systems, vol. 25, no. 8, pp. 2201-2210, Oct 2013/Jul 2014, doi:10.1109/TPDS.2013.271.

[18] S. Hohenberger andA. Lysyanskaya, “How to Securely Outsource Cryptographic Computations,”Proc. Second Theory of Cryptography Conference(TCC’05),J. Kilian, ed., LNCS 3378, Berlin: Springer-Verlag, pp. 264-282, 2005.

[19] M. Yang, F. Liu, J.L. Han and Z.L. Wang, “An Efficient Attribute Based Encryption Scheme with Revocation for Outsourced Data Sharing Control,” Proc. 2011 First International Conference on Instrumentation, Measurement, Computer, Communication and Control (IMCCC ’11), pp. 516-520, Oct. 2011, doi:10.1109/IMCCC.2011.134.

[20] J.Z. Lai, R.H. Dengand C. Guan, “Attribute-Based Encryption with Verifiable Outsourced Decryption, ”IEEE Transactions on Information Forensics and Security, vol. 8, no. 8, pp. 1343-1354,2013, doi: 10.1109/TIFS.2013.2271848.

[21] F. Zhao, T. Nishide and K. Sakurai, “Realizing Fine-Grained and Flexible Access Control to Outsourced Data with Attribute-Based Cryptosystems,”Proc. 7th International Conference. Information Security Practice and Experience(ISPEC’11),F. Bao and J. Weng, eds., LNCS 6672, Berlin: Springer-Verlag, pp. 83-97, 2011.

[22] X. Chen, J. Li, X. Huang and J. Li, “Secure Outsourced Attribute-Based Signatures,” IEEE Trans. Parallel and Distributed Systems, vol. 25, no. 12, pp. 3285-3294, Jan/Nov 2014, doi:10.1109/TPDS.2013.2295809.

[23] G. Ateniese, K. Fu, M. Green and S. Hohenberger, “Improved Proxy Re-encryption Scheme with Application to Secure Distributed Storage,” J. ACM Transactions on Information and System Security (TISSEC), vol. 9, no. 1, pp. 1-30, Feb. 2006, doi:10.1145/1127345.1127346.

[24] B. Libert and D. Vergnaud, “Unidirectional Chosen-Ciphertext Secure Proxy Re-encryption,”Proc. 11th International Workshop on Practice and Theory in Public Key Cryptography(PKC‘08),R. Cramer, ed., LNCS 4939, Berlin: Springer-Verlag, pp. 360-379, 2008.

[25] J.HurandD.K. Noh, “Attribute-based Access Control with Efficient Revocation in Data Outsourcing Systems, ”IEEE Transactions on Parallel and Distributed Systems, vol.22, no.7, pp. 1214-1221, Nov 2010, doi: 10.1109/TPDS.2010.203.

[26] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, “Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption, ”IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 1, pp. 131-143, Jan. 2012, doi:10.1109/TPDS.2012.97.

[27] M. Green, S. Hohenbergerand B. Waters, “Outsourcing the Decryption of ABE Ciphertexts,”Proc.20th USENIX Conference on Security(SEC ’11), pp. 34, 2011.

[28] D. Boneh,G.D. Cirescenzo, R. Ostrovsky and G. Persiano, “Public Key Encryption with Keyword Search, ”EUROCRYPT ’04 , C. Cachin and J.L. Camenisch, eds., LNCS 3027,Berlin: Springer-Verlag, pp. 506-522, 2004.

[29] P.Xu, H.Jin, Q.H.Wu, and W.Wang, “Public-Key Encryption with Fuzzy Keyword Search: A Provably Secure Scheme under Keyword Guessing Attack,”IEEE Transactions on Computers, vol.62, no.11, pp. 2266-2277, Nov.2013.

[30] J.G.Li, Y.R.Shi, and Y.C.Zhang, “Searchable Ciphertext-Policy Attribute-Based Encryption with Revocation in Cloud Storage, ”International Journal of Communication Systems, 2015,doi:10.1002/dac.2942

[31] Q.J.Zheng, S.H.Xu, G.Ateniese, “VABKS: Verifiable Attribute-Based Keyword Search over Outsourced Encrypted Data,”INFOCOM’14,pp. 522-530, 2014,doi:10.1109/INFOCOM.2014.6847976.

[32] H.L. Qian, J.G. Li, Y.C. Zhangand J.G. Han, “PrivacyPreservingPersonalHealthRecordUsingMulti-AuthorityAttribute-BasedEncryption with Revocation, ”International Journal of Information Security, pp. 1-11, 2015,doi:10.1007/s10207-014-0270-9.

[33] A. Shamir, “How to Share a Secret,” Communications of the ACM, vol. 22, no. 11, pp.612-613, Nov 1979.

[34] R. Canetti, H. Krawczyk and J.B. Nielsen, “Relaxing Chosen-Ciphertext Security,”CRYPTO ’03,D. Boneh, ed., LNCS 2729, Berlin: Springer-Verlag, pp. 565-582, 2003.

[35] B. Lynn,“Pairing-Based Cryptography (PBC) Library,”http://crypto.stanford.edu/pbc,2013.