International Journal of Digital Information and Wireless Communications (IJDIWC) 9(4): 187-192
The Society of Digital Information and Wireless Communications, 2019 ISSN: 2225-658X (Online); ISSN 2412-6551 (Print)

A Revocable Attribute-based Cloud Security for Data Access using Encryption and Biometric Identification

Maryam Safarian Nejad[1], Dr. Mohammad V. Malakooti[2], Dr. Navid Hashemi Taba[3]

1- Department of Computer Engineering, Islamic Azad University(IAU), UAE Branch, Dubai, UAE
m.safarian@yahoo.com
2- Department of Computer Engineering, Islamic Azad University(IAU), UAE Branch, Dubai, UAE
Malakooti@iau.ae
3- Department of Computer Engineering, Islamic Azad University(IAU), UAE Branch, Dubai, UAE
nhtaba@yahoo.com

Abstract: Cloud computing is an emerging technology in which it has been used to provide an efficient solution for the affordable, trustable, and fastest storage and retrieval of the information. The only problem in cloud computing is security that has been considered by researchers and several methods for providing secure access control are presented. Our method is based on the attribute-based information that provides secure connection to the cloud storage and servers. Our Revocable Attribute- Based Symmetric Encryption (RABSE) is proposed for generating a text-based Policy key that can be used to access the cloud server when the policy key is used to authenticate the user by the server. Once the Policy key is authenticated the server will issue One Time Password (OTP) that can be used for accessing database in the cloud storage. The structure of policy key authentication will be changed occasionally to grant the data access to new users or revoke the privilege of the some users. The information stored in the cloud storage facilities are encrypted and must be decrypted prior to usage. We have used the symmetric key cryptography, the same key for both encryption and decryption processes rather than asymmetric which the public key is used for encryption and private key will be used for decryption processes. Each user will be connected to the server after user has entered the required attributes for server access control. Once the server has issued the access control privilege the user can encrypt the information of its own area. The data are encrypted in different area and each user can only access to its own privilege area. The user can decrypt the first part of the information, low level security area; after server confirmed the user authentication and OPT issued by server to unlock the database. The user will run the Malakooti-Raeisie (M-R) Key Gen algorithm to generate the secret keys required for XOR operation after descrambling process is finished. The user also can decrypt the information on the second and third parts of user area, mid and high level security area, which required fingerprint identification for the second part, and additional face image recognition for the third part.

Keywords— Security, Biometric, Attribute-based, encryption Cloud, OPT, Cipher-text Policy, Access Control, Decryption, Key Gen Algorithm, Revocable, XOR Operation

1. Introduction:

The rapid change in Communication and Information Technology (CIT) and emerge of cloud computing have provided opportunities for high speed transmission in which massive amount of information will be transmitted through local area networks, distributes networks, and internet. The information must be encrypted prior to transmission and network must be protected for more security. There are several types of algorithm for cryptography but all of them fall into two categories of symmetric and asymmetric key cryptography. In symmetric key cryptography the information will be encrypted and decrypted with the same key as opposed to asymmetric cryptography that the public key is used for encryption and private key will be used for decryption process. The best way to keep unauthorized users from accessing the vital information is to encrypt the information prior to the transmission and stablish access control policy for decryption. It means that only privileged users are allowed to access the decrypted information when the text-based Policy key is authenticated by the server algorithm and when OPT is issued by server to unlock the encrypted database. Suppose that FBI is investigating the bribery allegation for one lobbyist in Chicago and one Lawyer in Washington and FBI chief has encrypted sensitive information on main server for security. In addition, he wants to allow only individuals with certain privilege can access the encrypted information [2]. Then the access control policy can be developed based on the user's attribution as following:

Policy Flag=" Public Corruption Office". AND. ("Name: Jack Brown". OR. "Name: Robert Douglas". OR. Management level>6).

It mean that individual who belong to Public Corruption office and have management level>6 or one of employee "Jack brown" or "Robert Douglas" is allowed to access the FBI encrypted information in database for decrypting required data for further investigation.

Attribute-based Encryption (ABE) is a type of text-based Policy key encryption in which the server access control, the database unlock, and encryption of privileged area, at low level security, will be performed through unscrambling of

encrypted information followed by XOR operation of the results with the secret keys, obtained from M-R Key Gen algorithm and applying AND operation with customer ID. The encrypted information at mid-level security and high-level security need additional fingerprint recognition and face recognition, respectively.

In such system, the decryption process will be possible if the set of user key features corresponding to the text attributes of the cipher text are available [1].An important security aspect of attribute-based encryption is collusion resistance because an adversary needs a sequence of text corresponding to elements of the attributes to access the server. In addition, the one- time password issued by server will be sent to the smart phone or email of the users which required for unlocking the database prior to creating the secret key for first level decryption. The ABE is similar to the Attribute-based Access Control (ABAC) in which the access rights are granted to users by using predefined policies which combined the attributes together. The policies can be obtained by combination of the attributes using Boolean logic operators, such as OR, AND, NOT, and XOR. Another word, we can use policies as a means of accessing information which are encrypted and stored in a secured server or group of servers. The logical operators applied on the attribute will generate the Boolean result in which it create a true Boolean value as access right for read/write if the requestor is manager otherwise the access right will be failed.

The rest of this papers is listed as following: The related works regarding to cloud-based access control are mentioned in section 2, Proposed Network Access Method is explained in section 3, Cipher-text Policy ABE is defined in section 4, Proposed Network Authentication and Cryptography is explained in section 5, experimental results are discussed and shown in section 6, and conclusion and future works are summarized in section 7.

2. Cloud-Based Access Control:

The cloud based access control will provide facilities in which our customers, vendors, and employees will be able to have easy and secure access to our resources form their smart phones. The cloud based access control system help us to obtain the easy and affordable services instead of building an expensive networks with many servers and storage facilities. We can focus mainly on business development and keep the access control, security, and management of the resources to the cloud providers. The remote access control are excellent for large business in which required to manage hundreds of entry points at multiple locations. In the traditional control-panel system one person must be on the site location to manage and schedule all of remote access requests while in cloud- based access control system no employee presence is required and cloud system facilities can manage, schedule, an build access concerns remotely via an encrypted mobile connection[8].

Many researchers have used the attribute-base encryption for one to many public key encryptions in which the information will be encrypted by cloud server administrator so that many users can access the server by using the combination of few required attributes. The issues of efficient key updating and user revocation have been a challenging problem in ABE. Boldyreva, et. al. [24] have presented a new user revocation method in which the combination of information form binary-tree data structure and secret key encryption have been used to generate secret keys and periodically broadcast the updated information for user revocation process through a secure channel. Cui, et. al. have proposed [25] a new method of user revocation called Server-Aided Revocable ABE (SR-ABE) in which all workload of the users which have been revoked will be considered as the delegated to the untrusted server. Since in the structure of secure SE-ABE model, the key embedding gadget employed in the construction of SR-ABE, there is no need for having secure channel for key transmission and it is a good efficient system.

Zhang, Yinghui et al. [11] have proposed a method for better confidentiality of outsourced data. An individual's interest in reinforcing access control over search results when performing searches on encrypted data. This security feature is referred to as the ACAS principle. Combined encoding and ABE search methods are presented according to the ACAS property. Secure personal and multi-user access for outsourced data is presented in the proposed model of outstanding search function. This is planned by searching for some keywords, as well as time-consuming catalytic search using high performance computing widely used in cloud computing.

The new method of matching and then decryption is described in the paper [13] where the matching step is also presented before the decryption step. This technique calculates the specific bases contained in the encrypted text for the test, whenever the private key of the attribute matches the access line hidden in the encrypted text without decryption. The specific secret key elements of attributes are produced because the fast decryption is due to the compression during the encryption. They provide the basic anonymous construction of attribute-based encryption, and then receive security-based deployment based on one-time signatures. The Proposed constructions test of the computational cost for the attribute is less than the decryption operation that only requires the number of small, fixed pairs of keys.

The clients can use CP-ABE schemes and share their files without specifying the name of recipient or any attached list. This is good method for sharing information and it is related to the attribute authentication in which the overhead of the system will be high when the number of clients is increased [14]. In past, the researchers have solved this problem by accepting random oracles which reduce the size of public key or secret key. But, Cheng, et. al. [15] have presented a new techniques called attribute union in which certain number of attributes can be integrated in to one. The method is supported by an arithmetic theorem in which each characteristic of the universe set is mapped with a unit code value. Next, they used the product multiplier, showing the set of attributes with all the multiplier product key numbers associated with each attribute in the set. Finally, the access structure can be obtained by the union of features according to the actual situation. They have shown that their technique based on the union of the feature is efficient and safe against the simple attacks.

3. Proposed Network Access Method:

ABE can be used for implementing a secure and legal framework for users, customers, partners, managers, and leaders to access encrypted information by using a policy-based access control in which each user privilege will be gives by a unique policy number. The policy number will be set up by applying the logical operators on some attribute defined for each user along with AND operation of the result with the user Identification Number. For example assume the attribute table is defined as following:

Table 3.1: The User Attribute-based Information

Customer ID	City	State	Country	Birth day	Mother Name
13570246	Seattle	Washington	USA	25-07-1995	Elizabet
12456789	Shiraz	Fars	Iran	11-10-2001	Maria
65347835	Tempe	Arizona	USA	10-06-2002	Mojgan
46535345	Tehran	Tehran	Iran	08-11-1987	Sumaira
37465454	Isfahan	Isfahan	Iran	04-12-2003	Shahnaz
28765452	Richmond	B.C.	Canada	06-10-2006	July
76253443	Tulsa	Oklahoma	USA	11-12-1998	Sara
87353435	Burnaby	B.C.	Canada	08-11-1998	Judi

Policyflag (1)=Att(1,1).AND.{ [Att(1,2).AND. Att(1,3).AND. Att(1,4)].OR. Att(1,5).}. Att(1,6)

The privilege will be given if the City, State, and Country or Birth day along with customer ID and Mother's Name is matched with the information of the customer's attribution table. The policy number for each user depends upon his/her own attributes in the encrypted attributes tables. The policy numbers will be used to access server in which vital information are encrypted and stored in the databases. Once the user has entered the required information, attribute information, the server system algorithm will determine the authentication of the user based on the status of the Policy flag and issue the access right privilege. The privilege for user may be totally different and each user can access certain parts of the encrypted and stored information. Once the user has obtained the access right privilege the server will issue OPT and will be delivered to the smart phone or email of the user to be used for as a secret key for unlocking the database. The OPT only will unlock the database prior to the generation of secret keys. It only can be used to access the encrypted information on the user privilege area. The information in the privilege area is encrypted based on the three levels of security as following:

1-Low Level Security: The first part of information on the privilege area will be decrypted by applying unscrambling algorithm on the encrypted information followed by XOR operation of unscrambled data with secret key which obtained from M-R Key Gen and AND operation of the customer ID.

2-Mid Level Security: The encryption of the second part of information on the privilege area will require biomedical identification techniques based on the fingerprint. Once the fingerprint of the user is authenticated the confirmation by server will be sent and user can access the encrypted information of the second part.

3-High Level Security: The encryption of the third part of information on the privilege area will require additional biomedical identification techniques based on the face image. Once the Face image of the user is authenticated the confirmation by server will be sent and user can access the encrypted information of the third part.

4- Cipher-Text-Policy ABE

Cipher-text-Policy ABE is a cryptographic tool and a promising future of server access control and cryptographic in which the data owner can be identified by the access structure of the user and consequently the sensitive data are encrypted and well protected. The data stored on the Cloud will be encrypted based on the ABE policy text encryption in which only the users who have the right attributes and authorization to access the server can access the encrypted data. The encrypted data will be decrypted based on the user's secret keys which can be derived from logical operation of the generated key and some user attributes. The Cipher-text-Policy ABE system consists of four parts as following:

- Network Authentication
- Key Generation
- Encryption
- Decryption

The details of each subject will be discussed on the next section.

5.0. Proposed Network Authentication and Cryptography

Our proposed algorithm is based of two different phase of security, network authentication and cryptography. The network authentication is related to the authentication of the user's attributes which will be used during the user interaction with the cloud server. The user is responsible to provide correct responses to a series of questions inquired by the cloud server prior to the process of the user's attributes. Once the user's attributes are processed and identity of the user is authenticated then the server will issue an OPT message to be delivered to the user's smart phone or Email which is necessary for the access control confirmation. These two level authentication processes along with network firewall have provided three level of security to access the database. The cryptography, encryption in server side, and decryption in user side, has been proposed based on two-level operations, scrambling of the data, along with XOR operation of the scrambled data with secret key generated by Malakooti-Raisei Key Gen Algorithm. We have suggested a three-level of operations for our previous encryption/decryption process [26] based on Scrambling, Transformation, and XOR operation with secret keys. We have not suggested the transformation process for the cryptography, in this paper, because it is not necessary to apply this additional operation which is time consuming. The privilege user normally will be allowed to decrypt the information at low-level security area. Should the user required to access the mid-level or high level security of database we are suggested additional biometric authentication

based on the fingerprints, or fingerprint along with face image for mid-level, high level security area, respectively.

5.1 Scrambling Algorithms:

Data scrambling is the process of mixing and misplacing the pieces of information for the purpose of hiding the intelligent of some information, such as text, data, image, or multimedia from the unauthorized users. There are several are ways to mix and misplace the piece of information by scrambling algorithm that is formulated based on the mathematics and descrambling will be done by reverse operation. The scrambling of digital information and videos has long history when people used Home Box Office (HBO) and they forced to have some especial box to descramble the channel which they are subscribed. The central office of HBO has used scrambling device and proper algorithm to hide their broadcasted video from illegal users. We have used Malakooti-Saffari Scrambling Algorithm (MSSA) [27] as permutation technique to scramble and mix all data elements so that their intelligent are hidden from unauthorized users. We consider the scramble algorithm one the first level of security for encryption. When the MSSA is used on one image to scramble its pixels, the pixels of the main diagonal image matrix are transferred in to a large size temporary array. Then the pixels of the off diagonals image matrix will be taken from upper and lower diagonal and will be saved into the temporary array, respectively as Figure 5.1. This process will be continued until elements of the upper and lower diagonal are transferred into the temporary array. This process will be done for all three Red, Green, and Blues matrices and the image pixels will be transferred into three different temporary arrays. Once, the contents of image matrix is transferred in to temporary arrays, the elements of the each array will be transferred sequentially to from a matrix of the same size as original one. This process will be done until all pixels of R, G, B matrices are scrambled and mixed. This operation completes the process of applying the first level security on the original image required for encryption.

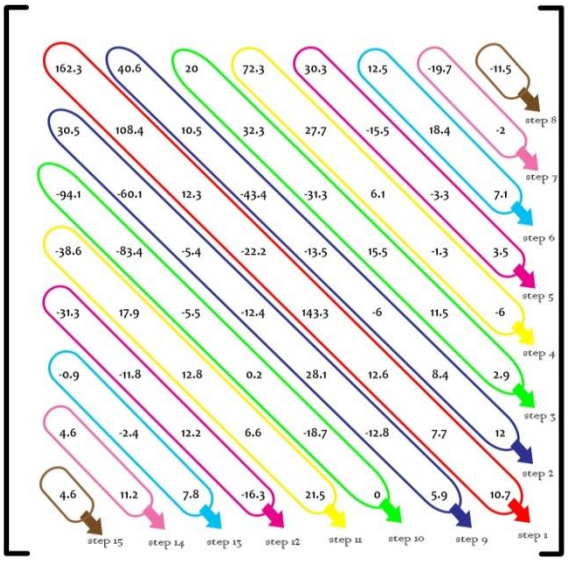


Figure 5.1: The Graphic of MSSA

5.2 Malakooti-Raisei key Gen Algorithm

In cryptography the secret key play a major role in encryption and it can be used to change the content of the data into other format so that it cannot be used by unauthorized users. The secret keys can be used in the process of intelligent hiding by applying the XOR operations on the data elements and secret keys. Several researchers have used the generated keys from the look up table but we have used the Malakooti-Reaisi Key Gen Algorithm to generate the secret keys so that the values of secret keys are the same during the encryption process, server side, or decryption process by client at user side. They have shown[26] that the advantage of M-R key gen algorithm compare with the existing key gen algorithm that have been used to generate random number and required a memory space to retrieve the key information for the decryption process.
The M-R self-key generation algorithm has some interesting properties and has compared with other key gen algorithm. First, the M-R key gen algorithm required only three prime numbers to generate the sequences of the secret key at any size. Second, most of the key gen algorithms can be used to generate the sequence of pseudo random numbers and they are not supported by any structural algorithm. In addition, M-R key gen algorithm can be used for the real time voice encryption as well as the secure chat but old offline key gen procedures can only be used for off line encryption. The Block diagram of M-R key gen algorithm is shown as following:

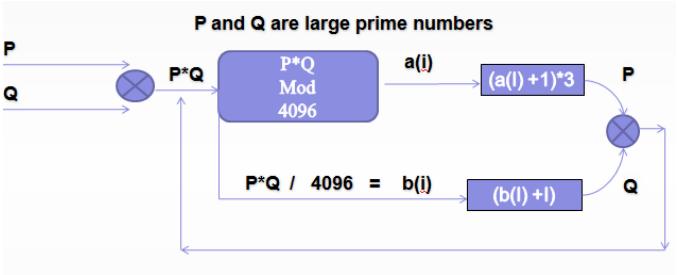


Figure 5.2: The Block Diagram of Malakooti-Raisie Key Gen

5.3 Proposed Encryption/Decryption Algorithm:

The encryption of the information prior to transmission and saving on the cloud storage devices will provide additional security on the vital information. When the information is encrypted, the intruders and hackers cannot steal it during the transmission or the time that unauthorized users have breached the network security and intend to discover the vital information stored inside database or cloud computing storage facilities. They may reached to the heart of database stored on the cloud storage devices but yet cannot discover the intelligent of the stored information. The proposed encryption has two levels of security based on the scrambling and XOR operation of the scrambled data with the secret keys generated by M-R key gen Algorithm. The Encryption process can be done at the server side for encrypting the information prior to saving on the storage facilities.
Encryption Algorithm (Server Side):

1. Read the original RGB Color image form the database.

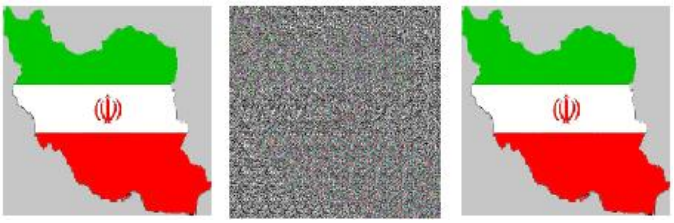
2. Convert the image file into a bitmap.
3. Decompose the bit map into three R, G, B matrices by transferring pixels into ImgR, ImgG, and ImgB matrices (Each matrix is for one color).
4. Use Malakooti-Safari Scrambling algorithm and scramble three matrices ImgR, ImgG, and ImgB and save it as ImgScR, ImgScG, and ImgScB.
5. Divide the scrambled matrices, ImgScR, ImgScG, and ImgScB into smaller blocks of, 16*16 or 32*32.
6. Use the secret keys generated by M-R key gen algorithm and apply the XOR of the each scrambled sub-blocks with the generated secret key to obtain the encrypted sub blocks.
7. If all sub-blocks have not been processed go to step 5, otherwise exit the loop.
8. Combine three encrypted matrices (ImgEncR, ImagEncG, and ImgEncB) to form a single encrypted matrix that represent the encrypted image.

Decryption Algorithm (User Side)

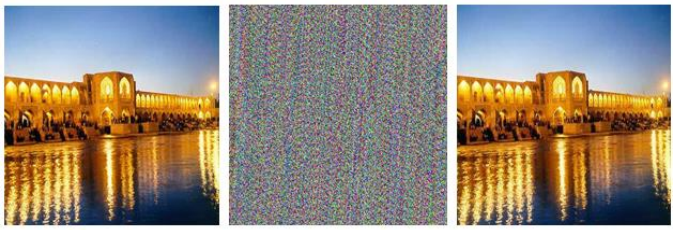
1. Read the encrypted RGB Color image form the database.
2. Convert the image file into a bitmap.
3. Decompose the bit map into three R, G, B matrices by transferring pixels into ImgEncR, ImgEncG, and ImgEncB matrices (Each matrix is for one color).
4. Divide the encrypted matrices, ImgEncR, ImgEncG, and ImgEncB matrices into smaller blocks of, 16*16 or 32*32.
5. Use the secret keys generated by M-R key gen algorithm and apply the XOR of the each encrypted sub-blocks with the generated secret key to obtain the decrypted sub blocks
6. If all sub-blocks have not been processed go to step 5, otherwise exit the loop.
7. Descrambled all matrices ImgDecR, ImgDecG, and ImgDecB.
8. Combine three Decrypted matrices (ImgDecR, ImgDecG, and ImgDecB) to form a single Decrypted matrix that represents the Decrypted image or original image.

6.0 Experimental Results:

The result of our algorithm will be compared with the existing authentication algorithms to compare the speed of operation, robustness, and complexity of our proposed algorithm.



A-Original Image B-Encrypted Image C-Decrypted Image
Fig 6.1: Iran Map Images with size of 512*512



A-Original Image B-Encrypted Image C-Decrypted Image
Fig 6.2: Khaju Bridge Images. Iran with size of 512*512

6. Conclusion

We have introduced a new RABSE Symmetric Encryption (RABSE) to generate a text-based policy key that can be used to access the cloud server when using the policy key for server-side authentication. We have verified the policy key and check for authentication in order to issues a one-time password server (OTP), which can be used to access the database in the cloud storage. The main point is to restructure authentication to verify data access to new users or to revoke some users. Our system will check the authentication process and verify the access control to the data server. We have added on columns to the table of user's attributes to be able to set the status of the privilege flag into ON for users who are authorized and OFF for users that are not authorized to access the database.

We have used Symmetric Key Cryptography, same key for both encryption and decryption, instead of the asymmetric password that uses the public key for encryption and the private key for decryption processes. The proposed encrypted has used two-level of security based on the scrambling and XOR operation with secret key during decryption processes. When the OPT is issued by server authentication the user will be able to unlock the database and it allowed to connect to the database for decryption processes. The user can decrypt the first part of the information, low level security area; after server confirmed the user authentication and OPT issued by server to unlock the database. The user will run the Malakooti-Raeisie (M-R) Key Gen algorithm to generate the secret keys required for XOR operation after descrambling process is finished. The user also can decrypt the information on the second and third parts of user area, mid and high level security area, which required fingerprint identification for the second part, and additional face image recognition for the third part.

We hope that this has the potential to solve important problems, such as allowing the physician to access the patient's while travelling or when he is in a critical health condition, can share her medical history of patients with authorized doctors who lives in a different country.In the future work, we attempt to do the process of user revocation more frequently and efficiently.

References

[1] Kumar, N. Saravana, GV Rajya Lakshmi, and B. Balamurugan. "Enhanced attribute based encryption for cloud computing." Procedia Computer Science 46 (2015): 689-696.

[2] Bethencourt, Sahai, A., and Waters, B.. "Cipher Text-Policy Attribute-Based Encryption", 2007 IEEE Symposium on Security and Privacy (SP '07), May 2007, Berkeley, France. ff10.1109/SP.2007.11.

[3] Tamizharasi, G. S., B. Balamurugan, and H. Abdul Gaffar. "Privacy preserving ciphertext policy attribute based encryption scheme with efficient and constant ciphertextsize." Inventive Computation Technologies (ICICT), International Conference on. Vol. 3. IEEE, 2016.

[4] Jung, Taeho, et al. "Control cloud data access privilege and anonymity with fully anonymous attribute-based encryption." IEEE Transactions on Information Forensics and Security 10.1 (2015): 190-199.

[5] Zhang, Yinghui, et al. "Computationally efficient ciphertext-policy attribute-based encryption with constant-size ciphertexts." International Conference on Provable Security. Springer International Publishing, 2014.

[6] Chen, Cheng, Zhenfeng Zhang, and Dengguo Feng. "Efficient Ciphertext Policy Attribute-Based Encryption with Constant-Size Ciphertext and Constant Computation-Cost." ProvSec 11 (2011): 84-101.

[7] Rafath, N., Ghouri, W., & Raziuddin, S. "Security in Cloud using Ciphertext Policy Attribute-Based Encryption with Checkability". 3(5). International Journal of Innovative Research in Computer and Communication Engineering. (2015).

[8] Shi, Yanfeng, et al. "Directly revocable key-policy attribute-based encryption with verifiable ciphertext delegation." Information Sciences 295 (2015): 221-231.

[9] Liang, Kaitai, et al. "A secure and efficient ciphertext-policy attribute-based proxy re-encryption for cloud data sharing." Future Generation Computer Systems 52 (2015): 95-108.

[10] Jiang, Yinhao, et al. "Ciphertext-policy attribute-based encryption with key-delegation abuse resistance." Australasian Conference on Information Security and Privacy. Springer International Publishing, 2016.

[11] Zhang, Yinghui, et al. "Efficient attribute-based data sharing in mobile clouds." Pervasive and Mobile Computing 28 (2016): 135-149.

[12] Bouabana-Tebibel, Thouraya, and Abdellah Kaci. "Parallel search over encrypted data under attribute based encryption on the Cloud Computing." Computers & security 54 (2015): 77-91.

[13] Chaudhari, Swapnil H., and B. R. Mandre. "Secure Data Retrieval based on Attribute-based Encryption in Cloud." International Journal of Computer Applications 134.13 (2016).

[14] Zhang, Yinghui, et al. "Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing." Information Sciences 379 (2017): 42-61.

[15] Rao, Y. Sreenivasa. "A secure and efficient Ciphertext-Policy Attribute-Based Signcryption for Personal Health Records sharing in cloud computing." Future Generation Computer Systems 67 (2017): 133-151.

[16] Cheng, Yong, Jiangchun Ren, Zhiying Wang, Songzhu Mei, and Jie Zhou. "Attributes union in CP-ABE algorithm for large universe cryptographic access control." In Cloud and Green Computing (CGC), 2012 Second International Conference on, pp. 180-186. IEEE, 2012.

[17] Wang, S., Gao, T., Zhang, Y. ,"Searchable and Revocable Multi-Data Owner Attribute-Based Encryption Scheme with Hidden policy in Cloud storage", Nov. 1,2018, https://doi.org/10.1371/journal.pone.0206126.

[18] Gokuldev, S., and S. Leelavathi. "HASBE: a hierarchical attribute-based solution for flexible and scalable access control by separate encryption/decryption in cloud computing." International Journal of Engineering Science and Innovative Technology (IJESIT) 2, no. 3 (2013).

[19] Cheung, Ling, and Calvin Newport. "Provably secure ciphertext policy ABE." In Proceedings of the 14th ACM conference on Computer and communications security, pp. 456-465. ACM, 2007.

[20] Borgh, Joakim. "Attribute-Based Encryption in Systems with Resource Constrained Devices in an Information Centric Networking Context." (2016).

[21] Bethencourt, John, Amit Sahai, and Brent Waters. "Ciphertext-policy attribute-based encryption." Security and Privacy, 2007. SP'07. IEEE Symposium on. IEEE,

[22] Boldyreva, A., Goyal, V., Kumar, V.," Identity-based encryption with efficient revocation", Proceedings of the 15th ACM Conference on Computer and Communications Security, pp.417-426. CCS,2008, USA.

[23] Derler, D., Hanser,C., Slamanig,D. ," A New Approach To Efficient Revocable Attribute-Based Anonymous Credentials?", IAIK, Graz University of Technology, Austria, IMA Conference on Cryptography and Coding 2015.

[24] Cui, H., Deng, R.H., Qin, B., "Server-Aided Revocable Attribute-Based Encryption", 15 September 2016, Lecture Notes in Computer Science, book series (LNCS, volume 9879).

[25] Shen, J., Tan, H., Moh, S., Chung, I., Liu, Q., Sun, X.: Enhanced secure sensor association and key management in wireless body area networks. J. Commun. Netw. **17**(5), 453–462 (2015). doi: 10.1109/JCN.2015.000083.

[26] Malakooti,M.V., Raeisi , M.N.D,, " A Lossless Digital Encryption System for Multimedia Using Orthogonal Transforms", Bangkok, Thailand, May.

[27] Malakooti,M.V, Saffari,V. Tawfik,S.Z., "A Novel Method for Secure Image Delivery over Mobile Networks Based on Orthogonal Transforms and Scrambling Algorithms", ICDIPC 2013, Dubai,UAE.