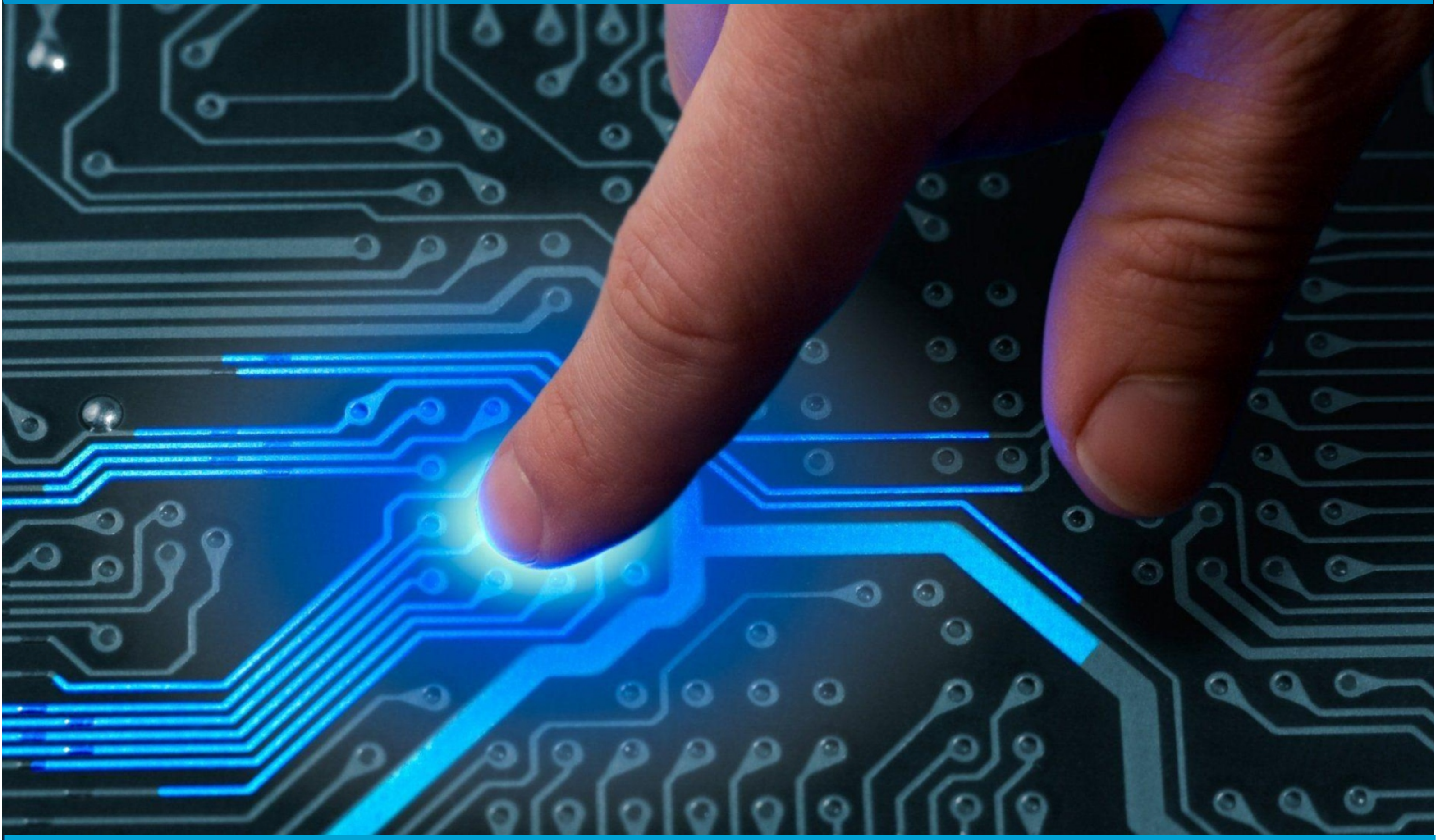
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 8, Issue 9, September 2020

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

Attribute-Based Encryption for Preserving Privacy

Jyoti Yogesh Deshmukh

J.J.T. University and JSPM's Bhivarabai Sawant institute of Technology and Research, Wagholi, Pune, India.

ABSTRACT: Cloud storage system endows users to remotely store their data and utilize the on-demand superiority cloud applications without the burden of local hardware and software management. While cloud computing induces these advantages more appealing than ever, it also brings revolutionary and challenging security threats to the outsourced data. To ensure the data security and integrity in cloud storage, until now, a large number of techniques have been proposed to handle this problem, but all of them have possess their own inherent limitations. In this project, give the formal model of Ciphertext-policy Attribute Based Encryption (CP-ABE) algorithm with a hierarchical structure to improve scalability and flexibility. This effectively eliminates the need to rely on the data storage server for preventing unauthorized data access and integrity. The performance measurements indicate that the proposed scheme is efficient to securely manage the data stored in the data storage servers and significantly reduces the computation time.

KEYWORDS: Attribute encryption, Cloud Computing, Privacy Preserving ,CipherText.

I. INTRODUCTION

In traditional access control schemes, user's sensitive data access can be controlled by a central authority. This system can be working efficiently with some limited advantages. First, as the scheme is having central authority, it becomes difficult task to manage numerous identities of different authorities in a distributed system for validation purpose. Second, all controls and validations are to the central authority, so by default all users and resources need to trust central authority. In this case if authority is malicious then the system will be in big trouble. In attribute based access control users will be validated with set of descriptive attributes, which are more than single identity. These attributes can have an access structure for secure sharing of data. Therefore, attribute-based access control schemes are efficient to share data securely with many users without taking care of their identities. To overcome the disadvantage of central authority, decentralized and distributed access control schemes are proposed. After these schemes, a decentralized attribute based access control with privacy preserving is addressed to provide the great secure sharing of sensitive data with multiple users. Attribute-based encryption (ABE) introduced by Sahai and Waters, is a more proficient encryption scheme and it can articulate an intricate access structure. In an ABE scheme, both the user's secret keys and the ciphertext are labeled with sets of attributes. The encrypter can encrypt a message under a set of attributes. Prior to decrypting the ciphertext, the receiver must obtain the secret keys from the central authority. The receiver can decrypt the ciphertext and obtain the data if and only if there is a match between its secret keys and the attributes listed in the cipher text. In attributes there is compulsory field of date to specify its access period, so that it will be valid within that period only. After specified period file will not be available to owner as well as to users. Essentially, there are two kinds of ABE schemes: Key Policy ABE (KPABE). In these schemes, the secret keys are associated with an access structure, while the cipher text is labeled with a set of attributes Cipher text Policy ABE (CPABE). In these schemes, the cipher text is associated with an access structure, while the secret keys are labeled with a set of attributes. Attrapadung and Imai proposed a dual policy ABE scheme which combines a KPABE scheme with CPABE scheme. In this scheme, two access structures are created. One is for the objective attributes labeled with the cipher text, and the other is for the subjective attributes held by the users. Furthermore, there is only one access structure in both KPABE and CPABE schemes. Centralized Key policy attribute based encryption is supporting attribute based encryption. Where all messages are created with their attributes and some policies designed by same attributes and stores encrypted messages. These messages will be encrypted with a key and at the time decryption, same key will be used. Overall operation in CKPABE can be summarized as with the help of following steps:

1. Data owner will create a message with attributes and policy. These details will be submitted to centralized authority for key generation.
2. Once key is generated it is issued to data owner
3. Using this key message will be encrypted by data owner.
4. User will send its global identifiers to data owner.
5. If those details are validated by any of data owner then file will be downloaded to user.
6. Valid user will request for key generation to centralized authority.

7. Centralized authority will issue key to user for decryption downloaded file to user. Decentralized Key policy attribute based encryption is supporting attribute based encryption. Where all messages are created with their attributes and some policies designed by same attributes and stores encrypted messages to data store. These messages will be encrypted with a key and at the time of decryption, same key will be used. DKPABE will be explained with the help of Figure 2, and stepwise explanation.

   1. Data owner will create a message and with some attributes and with combination of it one policy will be designed. These details will be submitted to Decentralized Authority to generate key.
   2. Decentralized authority will issue the generated key to data owner.
   3. With the help of key decentralized authority will encrypt the message.
   4. These encrypted messages will be stored in data store in organized format.
   5. User will send its details to data sore for validation and verification.
   6. Data sore will go through validate user details.
   7. After validation data store will allow user to download the file.
   8. Valid user will request decentralized authority for keys by which message was encrypted.
   9. Finally decentralized authority will issue the same key to user for decryption of message.

II. REVIEW OF LITERATURE

1. **M. Chase and S.S. Chow (2009)**,Attribute based encryption (ABE) determines decryption ability based on a user's attributes. In a multi-authority ABE scheme, multiple attribute-authorities monitor different sets of attributes and issue corresponding decryption keys to users and encryptors can require that a user obtain keys for appropriate attributes from each authority before decrypting a message. Chase gave a multi-authority ABE scheme using the concepts of a trusted central authority (CA) and global identifiers (GID). However, the CA in that construction has the power to decrypt every cipher text, which seems somehow contradictory to the original goal of distributing control over many potentially untrusted authorities. Moreover, in that construction, the use of a consistent GID allowed the authorities to combine their information to build a full profile with all of a user's attributes, which unnecessarily compromises the privacy of the user. In this paper, we propose a solution which removes the trusted central authority, and protects the users' privacy by preventing the authorities from pooling their information on particular users, thus making ABE more usable in practice. [24]

2. **J. Camenisch, M. Kohlweiss (2009)**,Searchable encryption schemes provide an important mechanism to cryptographically protect data while keeping it available to be searched and accessed. In a common approach for their construction, the encrypting entity chooses one or several keywords that describe the content of each encrypted record of data. To perform a search, a user obtains a trapdoor for a keyword of her interest and uses this trapdoor to find all the data described by this keyword. We present a searchable encryption scheme that allows users to privately search by keywords on encrypted data in a public key setting and decrypt the search results. To this end, we define and implement two primitives: public key encryption with oblivious keyword search (PEOKS) and committed blind anonymous identity-based encryption (IBE). PEOKS is an extension of public key encryption with keyword search (PEKS) in which users can obtain trapdoors from the secret key holder without revealing the keywords. Furthermore, we define committed blind trapdoor extraction, which facilitates the definition of authorization policies to describe which trapdoor a particular user can request. We construct a PEOKS scheme by using our other primitive, which we believe to be the first blind and anonymous IBE scheme. We apply our PEOKS scheme to build a public key encrypted database that permits authorized private searches, i.e., neither the keywords nor the search results are revealed. [2]

3. **Lewko and B. Waters** , we propose a Multi-Authority Attribute-Based Encryption (ABE) system. In our system, any party can become an authority and there is no requirement for any global coordination other than the creation of an initial set of common reference parameters. A party can simply act as an ABE authority by creating a public key and issuing private keys to different users that reflect their attributes. A user can encrypt data in terms of any boolean formula over attributes issued from any chosen set of authorities. Finally, our system does not require any central authority. In constructing our system, our largest technical hurdle is to make it collusion resistant. Prior Attribute-Based Encryption systems achieved collusion resistance when the ABE system authority “tied” together different components (representing different attributes) of a user’s private key by randomizing the key. However, in our system each component will come from a potentially different authority, where we assume no coordination between such authorities. We create new techniques to tie key components together and prevent collusion attacks between users with different global identifiers. We

prove our system secure using the recent dual system encryption methodology where the security proof works by first converting the challenge ciphertext and private keys to a semi-functional form and then arguing security. We follow a recent variant of the dual system proof technique due to Lewko and Waters and build our system using bilinear groups of Composite order. We prove security under similar static assumptions to the LW paper in the random oracle model. [3]

4. **Rial and B. Preneel**, author propose two constructions of oblivious transfer with access control (OTAC), i.e., oblivious transfer schemes in which a receiver can obtain a message only if her attributes, which are certified by a credential issuer, satisfy the access control policy of that message. The receiver remains anonymous towards the sender and the receiver's attributes are not disclosed to the sender. Our constructions are based on any cipher text policy attribute based encryption (CPABE) scheme that fulfills the committing and key separation properties, which we define. We also provide a committing CPABE with key separation scheme that supports any policy described by a monotone access structure, which, in comparison to previous work, allows our OTAC construction to support efficiently a wider variety of access control policies. In our constructions, a receiver obtains from the sender a CPABE secret key for her attributes by using a blind key extraction with access control protocol. We provide a blind key extraction with access control protocol for any committing CPABE with key separation scheme. Previous work only provided adhoc constructions of blind key extraction protocols. Our generic protocol works in a hybrid model that employs novel ideal functionalities for oblivious transfer and for anonymous attribute authentication. We propose constructions that realize those novel ideal functionalities and analyze the overall efficiency of our OTAC constructions. [4]

5. **AkoMuhamad Abdullah, "**In this paper it is described how AES has the best ability to protect sensitive data from attackers and is not allowed them to break the encrypt data AES algorithm uses a particular structure to encrypt data to provide the best security. To do that it relies on a number of rounds and inside each round comprise of four sub-process. Each round consists of the following four steps to encrypt 128-bit block" [5]
6. **Sukumar Sharmila**, "Searchable encryption is increasing interest for protecting the data privacy in secure searchable cloud storage. The security of a well-known cryptographic primitive, namely, public key encryption with keyword search (PEKS) which is very useful in many applications of cloud storage. the semantic-security against chosen keyword attack which guarantees that no adversary is able to distinguish a keyword from another one given the corresponding PEKS ciphertext. Performance is evaluated by making the comparison between existing schemes and our scheme in terms of computation, size and security. All the existing system require the pairing computation during the generation of PEKS cipher text and testing." [6]

7. **Ch.Ramesh, "**The evaluation was performed considering the renewal and revocation of keys and the presence of attacks of false accusation. The distribution occurs in the network boot. In it, the external team each node PKG with cryptographic material necessary for the functioning of the network. It generates the parameters of cryptographic functions, assembles and distributes the shared secret, generates keys for all nodes and update parameters of keys. Among all parameters generated, is the hash function H, used for the construction of the keys for the next phases of the network. The PKG also distribute the administrative tasks of the network to some ofthe nodes, in order to enable updates and withdrawals of keys" [7]

8. **Qiong Huang, "**Ideally, the keyword space is assumed to be at least super-polynomials large. However, in real applications it is usually not that large. Keywords are often chosen from a low-entropy keywords space. Therefore, it may be feasible for the adversary to guess what keywords a document contains by launching the keyword guessing attack. Data sender not only encrypts the keyword but also authenticates it, so that the server cannot encrypt a keyword itself and thus cannot launch the inside keyword guessing attack successfully." [8]

9. **Dan Boneh, "**Our second PEKS construction is based on general trapdoor permutations, assuming that the total number of keywords that the user wishes to search for is bounded by some polynomial function in the security parameter. For our purposes, giving the adversary an encryption of a random message is sufficient. Source indistinguishability can be attained from any trapdoor permutation family, where for a given security parameter all permutations in the family are defined over the same domain. Such a family can be constructed from any family of trapdoor permutations as described If we have an upper-bound on the total number ofkeyword trapdoors that the user will release to the email gateway**"** [9]

10. **Husna Tariq, "**This paper deals with the secure searching, storage and retrieval of user data in the cloud system. Various services of cloud, security issues and security requirements of cloud data are discussed. We present a new approach of dual encryption system based on authentication of the server to provide stronger security to the existing fuzzy keyword searching schemes. We have integrated symmetric and asymmetric encryption algorithms to enhance data security. This work mainly focuses on authentication of the server so as to improve the security system and protect sensitive user's data from unauthorized disclosure." [10]

11. **Chi Harold Liu**, "In this paper, the author proposes a block-chain enable well-organized data collection and secure sharing scheme combining Ethereum block-chain and deep reinforcement-learning (DRL) to create a reliable and safe environment. In this schemed is used to attain the highest amount of collected data, &the block-chain technology is used to guarantee safety & reliability of data sharing." [11]

12. **Shangping Wang**, "In this paper, we propose a product traceability system based on blockchain technology, in which all product transferring histories are perpetually recorded in a distributed ledger by using smart contracts and a chain is formed that can trace back to the source of the products. Our system has obvious decentralized characteristics, which significantly reduces the possibility of privately tampering with data within enterprises. our system is characterized by data accessibility, tamper proofing, and resistance to man-in-the-middle attacks." [12]

13. **M. Nakasumi**, "This paper proposed a new information sharing scheme based on blockchain technology. Users can manage their data and understand the data being collected about them and how to use it without trusting any third party. However, the scheme did not take into account the possibility of the enterprise itself tampering with data." [13]

14. **KuiRen,** "In this paper the designing security into the cloud benefits users and CSPs, it inevitably increases overhead for both. For users in particular, such overheads could offset the cloud's economically appealing benefits and might conflict with their reasons for using the cloud in the first place. Any solution to this question will help users make better-informed decisions before moving to the cloud. We've described several critical security challenges for the commercial public cloud, but our list is by no means comprehensive. Secure role-based access control on encrypted data in cloud storage on public cloud." [14]

III. SYSTEM OVERVIEW

Cloud Server:

• The Cloud Server, who is assumed to have adequate storage capacity, does nothing but store them.

N Attribute Authorities:

• Authorities are assumed to have powerful computation abilities, and they are supervised by government offices.

• The whole attribute set is divided into N disjoint sets and controlled by each authority, therefore each authority is aware of only part of attributes.

Data Owner:

• A Data Owner is the entity who wishes to outsource encrypted data file to the Cloud Servers. A user can be a Data owner and a Data consumer simultaneously

Data Consumers:

• Newly joined Data Consumers request private keys from all of the authorities, and they do not know which attributes are controlled by which authorities. When the Data Consumers request their private keys from the authorities, authorities will jointly create corresponding private key and send it to them.

• All Data Consumers are able to download any of the encrypted data files, but only those whose private keys satisfy the Encryption Policy can execute the operation.

IV. SYSTEM ARCHITECTURE

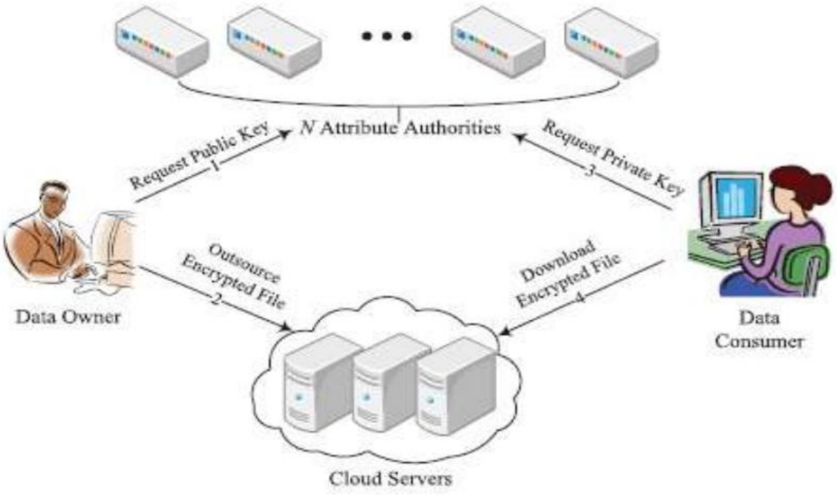


Fig. 01 System architecture

V. ALGORITHMS

1) Fully Anonymity AchievedAlgorithm:

1. The key point of the identity information leakage we had in our previous scheme as well as every existing attribute based encryption schemes is that key generator (or attribute authorities in our scheme) issues private key based on the reported attribute, and the generator has to know the user’s attribute (identities) to do so.
2. We need to introduce a new technique to let key generators issue the correct attribute key without knowing what attributes the users have.
3. The solution is to give all the private keys of all the attributes to the key requester and let him pick whatever he wants.
4. In this way, the key generator does not know which private keys the key requester picked, but we have to fully trust the key requester.
5. To solve this, we leverage the following to Oblivious Transfer (OT)
6. 1-out-of-n oblivious transfer
7. In cryptography, an oblivious transfer protocol (OT) is a type of protocol in which a sender transfers one of many pieces of information to a receiver, but sender remains oblivious(unware) as what piece of information has been transferred to receiver.
8. In an 1-out-of-n OT, the sender Bob has n messages M1, . . . , Mn , and the receiver Alice wants to pick one Mi from those M1, . . . , Mn . Alice successfully achieves Mi, and Bob does not know which Mi is picked by Alice.
9. By introducing the 1-out-of-k Oblivious Transfer in our KeyGenerate algorithm, the key-requester achieves the correct private key that he wants but the attribute authority does not have any useful information about what attribute is achieved by the requester.
10. The key requester achieves the full anonymity(user identity privacy) in our scheme and no matter how many attribute authorities collude (come to secret understanding) his identity information is kept secret

2) AES ALGORITHM:

1. This algorithm is use for security purpose i.e., to enter the data into encrypted format into a database.
2. Input:
3. Generate an Initialization Vector (IV)
4. Generating or Loading a Secret Key.
5. Creating the Cipher.
6. Encrypting a String.
7. Decrypting Back to a String.

```
Output: Inserting the data into the database into an encrypted format
KeyExpansion(byte key[16], word w[44])
{
    word temp
    for(i = 0; i < 4; i + +)
        w[i] = (key[4*i], key[4*i + 1], key[4*i + 2], key[4*i + 3]);
    for(i = 4; i < 44; i + +)
    {
        temp = w[i – 1];
        if ( i mod 4 = 0)
            temp = SubWord(RotWord(temp)) ⊕Rcon[i/4];
        w[i] = w[i-4] ⊕ temp
    }
}
```

- The key is copied into the first 4 words of the expanded key
- Each subsequent word w[i] depends upon w[i-1] and w[i-4]
- For words whose positions are NOT a multiple of 4 w[i] = w[i-4] ⊕ w[i-1]
- Otherwise w[i] = w[i-4] ⊕SubWord(RotWord(temp)) ⊕Rcon[i/4]

VI. CONCLUSION

An attribute-based privilege control scheme and a privacy preserving attribute-based privilege control scheme to address the user privacy problem in a cloud storage server. Using multiple authorities in the cloud computing system, our proposed schemes achieve not only fine-grained privilege control but also identity anonymity while conducting privilege control based on users' identity information.More importantly, our system can tolerate up to N − 2 authority compromise, which is highly preferable especially in Internet-based cloud computing environment.One of the future works is to introduce the efficient user revocation mechanism on top of anonymous Attribute Based Encryption. Supporting user revocation is an important issue in the real application.

REFERENCES

1. M. Chase and S.S. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," Proc. ACM Conf. Computer and Comm. Security (CCS '09), E. Al-Shaer, S. Jha, and A.D. Keromytis, eds., pp. 121-130, Nov. 2009.
2. J. Camenisch, M. Kohlweiss, A. Rial, and C. Sheedy, "Blind and Anonymous Identity-Based Encryption and Authorised Private Searches on Public Key Encrypted Data," Proc. 12th Int'l Conf. Practice nad Theory in Public Key Cryptography (PKC '09), S. Jarecki and G. Tsudik, eds., pp. 196-214, Mar. 2009.
3. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption," EUROCRYPT '10: Proc. Advances in Cryptology, H. Gilbert, ed., pp. 62-91, May/June 2010.
4. Lewko and B. Waters, "Decentralizing Attribute – Based Encryption," EUROCRYPT '11: Proc. 30th Ann. Int'l Conf. Theory and Applications of Cryptographic Techniques: Advances in Cryptology, K.G. Paterson, ed., pp. 568-588, May 2011.
5. Lysyanskaya, R.L. Rivest, A. Sahai, and S. Wolf, "Pseudonym Systems," Proc. Sixth Ann. Int'l Workshop Selected Areas in Cryptography (SAC '99), H.M. Heys and C. M. Adams, eds., pp. 184-199, Aug. 1999.
6. Rial and B. Preneel, "Blind Attribute-Based Encryption and Oblivious Transfer with Fine-Grained Access Control," Proc. 2010th Benelux Workshop Information and System Security (WISSec'10), pp. 1-20, 2010.
7. AkoMuhamad Abdullah ,"Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data" ,Publication Date: June 16, 2017
8. Sukumar Sharmila M, SwathiG,Ranjani C, Nandhini ,"Dual-server public-key encryption with keyword search for secure cloud storage", International Journal of Intellectual Advancements and Research in Engineering Computations Vol. –06(02) 2018
9. Ch.Ramesh , Dr.K.VenuGopalRao , Dr.D.Vasumathi "Evaluation of Key Management Scheme Based on Identity", 2016 IEEE 6th International Conference on Advanced Computing
10. Qiong Huang, Hongbo Li," An Efficient Public-Key Searchable Encryption Scheme Secure against Inside Keyword Guessing Attacks", Information Sciences January 1, 2018

11. Husna Tariq, Dr. ParulAgarwal*,“ Secure Keyword Search Using Dual Encryption in Cloud: An Approach”, International Journal of Computational Intelligence Research ISSN 0973-1873 Volume 13, Number 5
12. Chi Harold Liu, Senior Member, IEEE, Qiuxia Lin, Shilin Wen. “Blockchain-enabled Data Collection and Sharing for Industrial IoT with Deep Reinforcement Learning”, IEEE Transaction on Industrial Volume: 15, Issue: 6 , June 2019.
13. Shangping Wang, Dongyi Li, Yaling Zhang, Juanjuan Chen, “Smart Contract-Based Product Traceability System in the Supply Chain Scenario”, IEEE Access, 2019.
14. M. Nakasumi, “Information Sharing for Supply Chain Management Based on Block Chain Technology,” in 2017 IEEE 19th Conference on Business Informatics (CBI), Thessaloniki, Greece, Jul. 2017.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

Scan to save the contact details

www.ijircce.com