Advances in Computational Sciences and Technology
ISSN 0973-6107 Volume 15, Number 1 (2022) pp. 1-10

http://www.ripublication.com

Attribute Based Cryptography: Overview & Applications

Smita Kulkarni-Pai

Information Technology Department, Terna Engineering College, Navi Mumbai

Abstract

Massive and outsourced structure of cloud data puts lots of limitations on traditional cryptography. Communication bandwidth, memory consumption and computational power are major concerns in cloud computing environment. Moreover confidentiality and flexible data sharing are main challenges related to multitenant cloud data. Attribute based cryptography, which is a part of applied cryptography, is emerging as a promising solution to all above problems related to cloud data. In this paper we are providing an overview of attribute based cryptography and its applications in various sectors.

Keywords: Cloud Data, Attribute based encryption

INTRODUCTION

Cloud data is mainly characterized as massive, outsourced, shared and distributed. These cloud specific characteristics puts lots of risks to cloud data such as, snooping, spoofing, unauthorized discovery, malicious or accidental deletion of data, unexpected downtime of data service and denial-of-service. Cloud computing environment follows shared responsibility model for security, where client i.e Data Owner (D_O) and cloud service provider (*CSP*) both share common or equal responsibility of their resources. Usually D_O prefer encrypting data in their own premise before outsourcing it to untrusted or semi-trusted *CSP*. In traditional cryptography, it requires large amount of power to encrypt this massive data. It also requires deployment of key management framework such as PKI. Traditional cryptographic algorithms are deterministic, not reusable and don't allow operations on encrypted data. That means, whenever D_O want to process or share its data with Data User (D_U), it requires to download entire encrypted data, decrypt it, search for required data and then process or share it, and again encrypt and outsource it to CSP. Which includes lots of memory consumption, and wastage of communication bandwidth and computational power. Advanced or

applied cryptography is capable for providing solutions to all above mentioned problems and thus is preferred over traditional cryptography in cloud data security. Applied cryptography is classified into three types, viz ID (Identity) Based cryptography, Attribute Based Cryptography and Homomorphic cryptography. ID-based cryptography is an asymmetric key cryptography, where client's or user's identity is treated as its public key and a pairing function is used to create a private key. It is advantageous as it eliminates the requirement of key management and distribution framework but it has major drawback that it requires data to be encrypted for every single user with its unique identity. And it is difficult for thousands and millions of users in cloud computing environment. As a solution to this problem, ID-based cryptography is extended to Attribute based cryptography where user's identity is defined over set of attributes, and private keys and cipher text are associated with this set of attributes or a policy defined over a set of attributes. Cipher text is assigned with a set of descriptive attributes known as keywords and these keywords are used to search over an encrypted data. Moreover, this encrypted data can also be decrypted in different pieces based upon policy attributes, and thus providing fine-grained access control. In third form of applied cryptography, Homomorphic cryptography, homomorphism function allows to perform group operations on encrypted data and thus preserves privacy. These functions are defined over algebraic groups or rings and allow either addition or multiplication operation or both. Homomorphic cryptography is a privacy preserving applied cryptography. Amongst these three, Attribute based cryptography is emerging as a promising solution to majority of problems related to data in cloud computing environment. [1]

Rest of this paper is organized to introduce Attributed Based Encryption (ABE), Searchable Encryption in ABE, and various schemes proposed by researchers in order to provide ABE applications.

ATTRIBUTE BASED ENCRYPTION

Overview, Types and Pairing Function

Attribute Based Encryption (ABE) is a class of asymmetric encryption techniques which extends identity of the user in ID based encryption with a set of attributes that identifies a group of users uniquely and allows users to encipher and rewrite data with collision resistance. This set of attributes is further used to define set of policies for cipher text and its decryption keys to allow fine grained access control over this cipher text. Unlike traditional cryptography, which provides one-to-one encryption, ABE provides one-to-may and many-many encryption. A user D_U is allowed to decrypt the cipher only if it possesses d out of k attributes (i.e. from attribute universe $\boldsymbol{U}$ having k attributes) and matches with the policy in access structure $\boldsymbol{A}$. Two types of access structures are supported by ABE to define policies, viz. Access Trees and Access Matrix.

- ABE is broadly classified into two types:
  1. KP-ABE (Key-Policy based ABE):- Here, decryption keys are defined over access policies and cipher text is associated with set of attributes.

2. CP-ABE (Cipher-text Policy based ABE):- Here, cipher-text is defined over access policies and decryption keys are associated with set of attributes.

- In traditional asymmetric cryptography two large prime numbers are used to create keys of encipher and decipherment of message. These large prime numbers may increase the complexity in terms of time and computational power requirements. Applied cryptography solves this problem by using Elliptic Curve Cryptography (ECC). It is also called as Pairing Based Cryptography (PBC) that is based on pairing function which maps pairs of points on elliptic curve into a finite field. Here two cryptographic groups G_1 and G_2 are mapped with third group G_T by using pairing function $e: G_1 X G_2 \rightarrow G_T$ for constructing or analyzing cryptosystem. Three types of pairing functions are supported by ABE:
  1. Type I: $G_1=G_2$,
  2. Type II: $G_1 \neq G_2$, but there is efficiently computable homomorphism ϕ: $G_1 \rightarrow G_2$
  3. Type III: $G_1 \neq G_2$, and there is no efficiently computable homomorphism between G_1 and G_2

- Generally most of recent ABE based searchable encryption schemes use Type-III pairing to support security level of 128 bit and above, in contrast to original ABE with Type I pairing that supports security level of 80 bits which is not sufficient to provide security in multi-tenant cloud environment. [2][3]
- Figure 1 depicts example of attribute based fine grained access control mechanism used in healthcare cloud data. Hare, Pathologists is a data owner who encrypts patient's reports and outsources it to healthcare cloud. Patient and corresponding doctor can only have access to these encrypted reports.

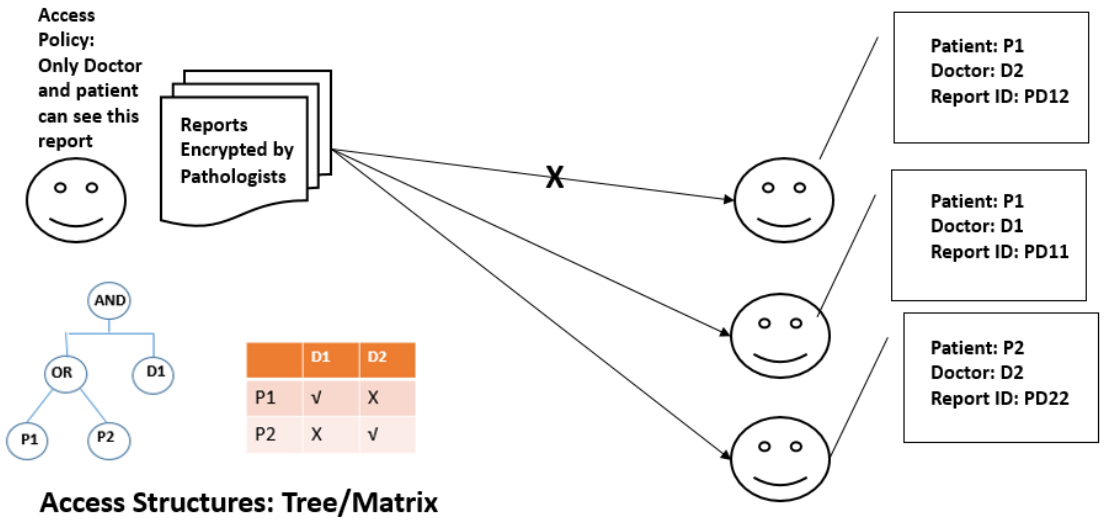

Figure 1: Access Control using Attribute Based Encryption

Searchable Encryption Algorithm

Searchable Encryption in ABE is a method of searching keywords over encrypted data at CSP by identifying and retrieving a set of attributes from a encrypted message that satisfies the query coming from a Data User *(D_U).* This is an encrypted query over encrypted data, so that neither data content, nor the searching criteria and patterns are visible to CSP. Thus privacy preserving. Search can be based on single keyword search and multi keyword search. The generalized method of searchable encryption is defined as follows-

1. ***Step 1: Encryption and outsourcing*:** Let D be a set of documents and W be a set of keywords extracted from documents D by data owner D_O. Let k_1, k_2, k_3 be cryptographic keys created by D_O with security length λ. D_O encrypts D with symmetric cipher E using key k1 (E_{k1} (D)). D_O creates an encrypted index of keywords W using key k_2 (I_{k2}(W)). D_O outsource k1 (E_{k1}(D)) and (I_{k2}(W) to cloud. D_O gives authority to some D_U to search over (E_{k1}(D)) using k_3.
2. **Step2: Trapdoor Creating:** For searching a query word w_q in W using k_3, D_U creates a trapdoor $T_{k3}(w_q)$. DU sends a request to *CSP* to retrieve documents D´ consisting of keyword w_q using the trapdoor $T_{k3}(w_q)$.
3. ***Step 3: Encrypted Search:*** *CSP* searches for keyword w_q in index I_{k2}(W) using this trapdoor $T_{k3}(w_q)$. Encrypted documents D´ found by *CSP* are handed over to D_U, without revealing its contents or search patterns.
4. ***Step 4: Decryption:*** D_O authorizes D_U for accessing D' in plaintext and shares a symmetric key k_1 to decrypt it. Key k_1 is shared using secret sharing algorithm.

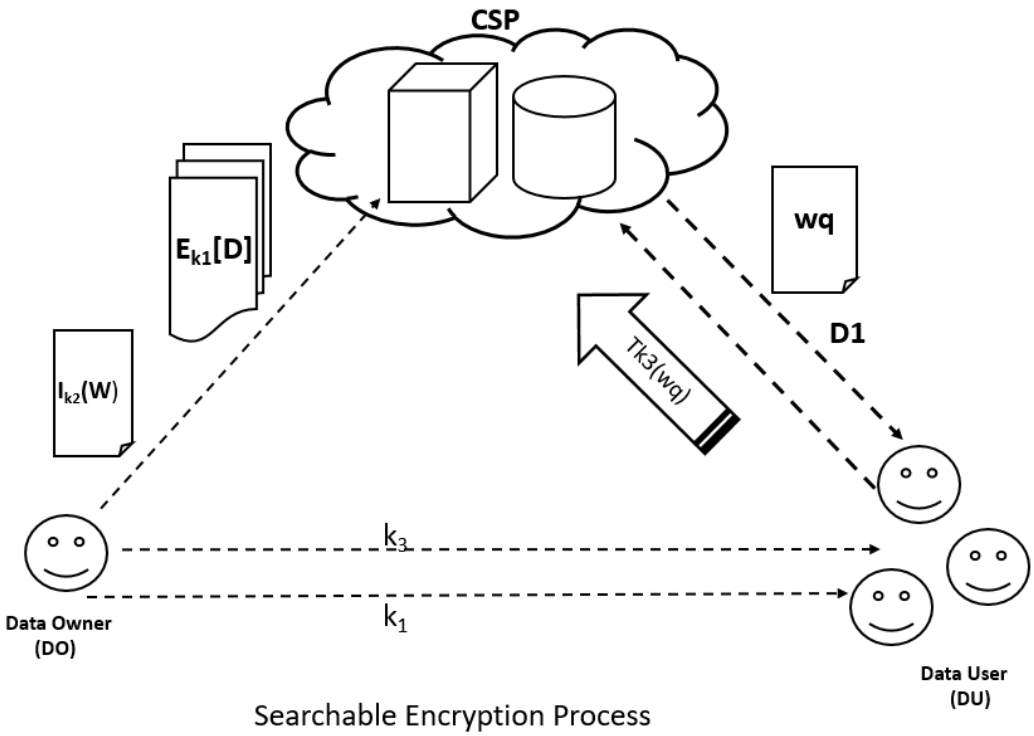

Figure 2: Searchable Encryption Process

Table I: Applications of ABE

Applications of ABE			
Framework	***Author***	***Application Area***	***ABE specification***
FABECS[3]	Miguel Morales-Sandoval	General cloud data	CP-ABSE, DET-ABE
CP-DABKS[4]	Lifeng Guo	eHealth cloud in IoT	Multiuser decryptable CP-ABE
CP-WABE[5]	Hang Li	Internet of Health Things (IoHT)	Weighted Attribute CP-ABE
H-ABC[6]	Kamalakanta Sethi	General cloud data	Hierarchical CP-ABE with user revocation
Tracable Outsourced ABE[7]	Ruoqing Zhang	Mobile Cloud Computing	Traceable CP-ABE with searching and retrieving operations outsourced
ABE-POD [8]	Chaosheng Feng	Edge intelligent Internet of Vehicles (IoV)	Parallel outsourced decryption CP-ABE
TRS-ABE[9]	Huijie Lian	General cloud data	SD method and SUE method CP-ABE
PCP-ABE[10]	Nouha Oualha	IoT application data in cloud	Pre-computation CP-ABE
Multi–authority CP-ABE[11]	Min Xiao	Wireless Body Area Network	Multi-authority CP-ABE with DNF
MABKS[12]	Yinbin Miao	Internet of Medical Things (IoMT)	Multi-authority ABE with keyword search using Robust and Auditable Access Control (RAAC)
O^3-R-CP-ABE[14]	K. Xue	Internet of Medical Things (IoMT)	outsourced online/offline revocable CP-ABE with chameleon hash function based revocation mechanism
RABE-DI[15]	Rui Guo	General cloud data	Revocable CP-ABE with data integration using negligible function
RS-CPABE[16]	Mariem Bouchaala	General cloud data	Sliced revocable CP-ABE with IDA Splitting algorithm
Blockchain based-CPABE[17]	Yuwen Pu	Edge Servers	Recoverable and revocable CPABE using blockchain based attribute revocation chain
Modified – SPIRC[18]	Divyashikha Sethia,	IoT based car aggregation	ABE with Scalable user and attribute revocation and delegation and without the need of re-encryption and re-distribution of keys

Encryption cipher E and secrete sharing algorithm for sharing k1 are not specified in SE, but some of the algorithms used for SE are SSE, SIPC, PKC and ABSE. Amongst all, Symmetric Searchable Encryption (SSE) ~~is~~ and Attribute Based Searchable Encryption (ABSE) are popularly used in most of ABE schemes.[2][3]
Main requirements in cloud data are confidentiality of shared data, authorized access to shared confidential data and search over encrypted data. Potential strengths of ABE and its variants are capable of fulfilling all the three requirements. Digital Envelop Technique (DET) based ABE is best suited for confidentiality and access control whereas SSE and ABSE variants are popularly used for search over encrypted data.[2][3]

ABE APPLICATIONS

ABE and its variants are widely used in sharing, retrieving and storing massive data in cloud computing and its extension edge computing.
Miguel et al. [3] proposes a FABECS framework based on CP-ABSE and DET-ABE using Type-III pairing for storing, sharing and retrieval of documents in cloud environment. They claim to achieve minimum of security level 128 bits and LISA benchmark for data retrieval task. BN-curve practical realizations are used to demonstrate viability of benchmarks. Lifeng et al. [4] has proposed a decryptable attribute-based keyword search scheme on eHealth Cloud in Internet of Things Platforms. The scheme is called secure channel free CP-DABKS as it eliminates the need for secure channel required for transmitting trapdoors between server and receiver. The scheme is designed to support multi-user keyword search by adopting LSSS (Linear Secret Sharing Scheme) access policy. Unlike other ABE schemes, this framework outsources some operations to CSP such as keyword retrieval and partial ciphertext decryption. Hang Li et al. [5] has proposed a Ciphertext-Policy Weighted Attribute-Based Encryption (CP-WABE) for the Internet of Health Things. The attributes are assigned some weightage and access control is realized by comparing these weighted attributes such as greater than, less than and within the interval. The scheme is designed particularly for fine grained access to sensitive information such as patient's EMRs. Kamalakanta et al. has proposed a hierarchical attribute based framework for by introducing hierarchical dependency between users to achieve multilayer verification for fine grained access control and scalability in cloud storage. The scheme also supports user revocation. Ruoqing et al. [7] has proposed a traceable outsourcing CP-ABE scheme with attribute revocation. The scheme adopts outsourcing of computation and uses subset cover algorithm for traceability and revocation. Outsourcing of computation makes it suitable for limited processing capacity mobile devices and traceability helps to identify who leaks the partial decryption keys. Chaosheng et al. [8] has introduced a generic parallel outsourced decryption method for ABE(ABE-POD) for data sharing security in time and compute constrained edge intelligent IoV. The scheme uses LSSS access structure with access tree and parallel decryption method, unlike most ABE which supports serial decryption. The scheme claims to improve the speed of outsourcing decryption and thus improving the speed of overall decryption process which makes it suitable for

secure data sharing in edge intelligent IoV. Huijie et al. proposed a traceable revocable storage ABE (TRS-ABE) which not only supports revocation of attributes but also frequent updating of cipher text. All existing RS-ABE schemes use complete subtree (CS) method for key revocation resulting in long update keys. TRS-ABE uses subset difference (SD) method instead of CS method to reduce update key size and self-updatable encryption (SUE) method for self-update functionality. Nouha et al.[10] extends basic CP-ABE scheme using effective pre-computation techniques for computing and storing a set of pairs derived from expensive cryptographic operations, thus reducing the cost of computations significantly and making it suitable for IoT applications. Min Xiao [11] introduced a multi-authority CP-ABE for wireless body area network for addressing the resource related issues of sensor nodes and diversity in data retrieval. The scheme is featured with multi-authority CP-ABE, introduction to disjunctive normal form (DNF) to replace traditional And/OR structure in key generation, and use of hybrid encryption to make scheme efficient for WBAN. Multi authority structure reduces the workload in traditional single authority by efficiently managing attributes and supporting decentralization. Based on CP-ABE scheme, Yinbin et al. [12] has introduced a new scheme multi-authority CP-ABKS (CP-Attribute based keyword search) called MABKS. The system avoids performance bottleneck caused in single authority ABE schemes and minimize the computation and storage overload on resource constrained devices. The system extends the support to malicious attribute authority tracing attribute update. This is achieved by using the The Robust and Auditable Access Control (RAAC) scheme proposed by K. Xue [13]. IoMT are complex systems than IoT, where in addition to collect analyze and transmit data process, it comprises network of medical equipment's and applications of healthcare system that offers real time, remote measurement and analysis of healthcare data. And this IoMT is suffering from great challenges such as unauthorized access, privacy leakage, and delayed detection of life threatening situations and so on. To address these issues, Rui Guo et al. [14] presents outsourced online/offline revocable ciphertext policy attribute-based encryption (O^3-R-CP-ABE)scheme with the aid of cloud servers and blockchains in the IoMT ecosystem. The scheme is featured with ciphertext verification, user revocation, outsourced decryption, fast encryption and fine grained access control. They claims to be pioneers of revocation mechanism by means of the chameleon hash function, where revocation is achieved by constructing exposure free, collision resistant private keys for data user. Encryption algorithm has online/offline phases which enable smart terminals in IoMT environment with fast and light encryption process. The ciphertext is outsourced to cloud servers with the help of blockchain and allows partial decryption on it to prevent data users from heavy computational overheads providing verifiability of outsourced ciphertext in IoMT. Chunpeng Ge et al. [15] introduces revocable attribute-based encryption with data integrity protection (RABE-DI) to address the confidentiality and integrity issues raised due to attribute revocation cipher text updating mechanisms. RABE-DI scheme uses negligible function to achieve data integrity of original ciphertext and revoked ciphertext. Integrity is said to be achieved if advantage of adversary A is negligible function, which is defined as: If for $\forall c > 0$, there exists an x_c such that $f(x) < 1/x_c$ for $\forall x > x_c$, the f (x) is a negligible function. Mariem et al.[16] proposed a sliced

revocable CP-ABE using IDA (Information Dispersal Algorithm)splitting algorithm, to split a file into n slices. These slices are stored in multiple storage nodes. Whenever revocation occurs only one slice is re-encrypted using CP-ABE. And rest of original data is encrypted using AES symmetric algorithm. In in next round of access, user can decrypt original file if and only if he can successfully decrypt this slice. The heavy computational operations are delegated to cloud servers to improve the performance. The scheme is named as RS-CPABE. Yuwen et al. [17] propose a recoverable and revocable privacy preserving data sharing scheme for edge servers. Scheme introduces blockchain based attribute revocation chain to achieve attribute revocation in CP-ABE. The scheme claims to provide distinguished features such as- secret sharing scheme based data recovery, and re-encryption technology, malfunctioning and compromised edge server detection, blockchain based attribute revocation chain to support immediate revocation method and EDoS (Economic Denial-of-Sustainability) resistant access control based on consensus mechanism and relationship defined over access control tree and attribute set in CP-ABE. Divyashikha et al [18], proposes a modified scalable proxy based immediate revocation of user and attributes with delegation. In this scheme, attributes of a user registered at server are associated with random constant parameters on which are independent of the ciphertext. This association is on temporary basis and once server modifies associated parameters for any attribute of a user, a user is not allowed to decrypt the ciphertext. The scheme is characterized with many features such as- scalable user and attribute revocation, efficient attribute delegation, no re-encryption and re-distribution of keys.

CONCLUSION

In this paper, we have presented an overview about attribute based cryptography, its types and various schemes based on attribute based encryption techniques that are used to provide fine grained access control and security in cloud data of various sectors. With this overview, we can conclude that CP-ABE is popularly used over KP-ABE in many applications. Moreover, most of the recent CP-ABE schemes are designed with attribute and user revocation facility. Some are providing solution to re-encryption of cipher text and re-distribution of keys problem with delegation mechanism and some are solving Integrity issues raised due to attribute revocation using blockchain technology.

REFERENCES

[1] Smita Kulkarni “Overview of Data Security & Cryptography in Cloud Computing Environment”, Advances in Computational Sciences and Technology (ACST) ISSN 0973-6107 Vol.11, No. 1, (2018) © Research India Publications http://www.ripublication.com

[2] Nikhil Chaudhari1, Mohit Saini, Ashwin Kumar, Priya G, “A Review on Attribute Based Encryption”, 2016 8th International Conference on

Computational Intelligence and Communication Networks, DOI 10.1109/CICN.2016.81 , 978-1-5090-1144-5/16 $31.00 © 2016 IEEE

[3] Miguel Morales-Sandoval1, Melissa Hinojosa Cabello1 , Heidy Marisol Marin-Castro , And Jose Luis Gonzalez Compean1 "Attribute-Based Encryption Approach for Storage, Sharing and Retrieval of Encrypted Data in the Cloud." IEEEAccess VOLUME 8, 2020, Digital Object Identifier 10.1109/ACCESS.2020.3023893

[4] LIFENG GUO 1 , ZHIHAO LI 1 , WEI-CHUEN YAU 2 , (Member, IEEE), AND SYH-YUAN TAN 3, "A Decryptable Attribute-Based Keyword Search Scheme on eHealth Cloud in Internet of Things Platforms", IEEEAccess, Vol 8 2020, Digital Object Identifier 10.1109/ACCESS.2020.2971088

[5] Hang Li, Keping Yu, Bin Liu, Chaosheng Feng, Zhiguang Qin, Gautam Srivastava, "An Efficient Ciphertext-Policy Weighted Attribute-Based Encryption for the Internet of Health Things", IEEE Journal of Biomedical and Health Informatics, : DOI 10.1109/JBHI.2021.3075995.

[6] Kamalakanta Sethi, Ankit Pradhan∗ , Punith. R∗ , and Padmalochan Bera, "A Scalable Attribute Based Encryption for Secure Data Storage and Access in Cloud",

[7] Ruoqing Zhang , Lucas Hui , SM Yiu , Xiaoqi Yu , Zechao Liu, Zoe L.Jiang "A Traceable Outsourcing CP-ABE Scheme with Attribute Revocation", 2017 IEEE Trustcom/BigDataSE/ICESS, DOI 10.1109/Trustcom/BigDataSE/ICESS.2017.259

[8] Chaosheng Feng , Keping Yu , Member,Moayad Aloqaily,IEEE, Mamoun Alazab, Zhihan Lv , and Shahid Mumtaz, Senior Member, IEEE "Attribute-Based Encryption With Parallel Outsourced Decryption for Edge Intelligent IoV", IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 69, NO. 11, NOVEMBER 2020

[9] Huijie Lian Qingxian Wang, Guangbo Wang, "Fully Secure Traceable and Revocable-Storage Attribute-Based Encryption with Short Update Keys via Subset Difference Method", 2018 Third International Conference on Security of Smart Cities, Industrial Control System and Communications (SSIC), 978-l-5386-8187-9/18/$31.00 ©2018 IEEE

[10] Nouha Oualha, Kim Thuat Nguyen, "Lightweight Attribute-based Encryption for the Internet of Things", 978-1-5090-2279-3/16/$31.00 ©2016 IEEE

[11] Min Xiao, Xiaoyong Hu, "Multi-Authority Attribute-Based Encryption Access Control Scheme in Wireless Body Area Network" 2018 3rd International Conference on Information Systems Engineering, DOI 10.1109/ICISE.2018.00015

[12] Yinbin Miao, Robert H. Deng , Ximeng Liu , Kim-Kwang Raymond Choo,Hongjun Wu, and Hongwei Li , "Multi-Authority Attribute-Based Keyword Search over Encrypted Cloud Data", Ieee Transactions On Dependable And Secure Computing, Vol. 18, No. 4, July/August 2021, Digital Object Identifier no. 10.1109/TDSC.2019.2935044

[13] K. Xue, Y. Xue, J. Hong, W. Li, H. Yue, D. S. Wei, and P. Hong, "RAAC: Robust and auditable access control with multiple attribute authorities for public

cloud storage," IEEE Trans. Inf. Forensics Secur., vol. 12, no. 4, pp. 953–967, Apr. 2017

[14] Rui Guo , Geng Yang, Huixian Shi , Yinghui Zhang , and Dong Zhen, "O^3 -R-CP-ABE: An Efficient and Revocable Attribute-Based Encryption Scheme in the Cloud-Assisted IoMT System", IEEE Internet Of Things Journal, Vol. 8, No. 11, June 1, 2021,Digital Object Identifier 10.1109/JIOT.2021.3055541.

[15] Chunpeng Ge, Willy Susilo, Joonsang Baek, Zhe Liu, Jinyue Xia, and Liming Fang, "Revocable Attribute-Based Encryption with Data Integrity in Clouds", DOI 10.1109/TDSC.2021.3065999.

[16] Mariem Bouchaala, Cherif Ghazel, Leila Azouz Saidane ,"Revocable Sliced CipherText Policy Attribute Based Encryption Scheme in Cloud Computing"

[17] Yuwen Pu, Chunqiang Hu, Shaojiang Deng, and Arwa Alrawais,"R2PEDS: A Recoverable and Revocable Privacy-Preserving Edge Data Sharing Scheme" Ieee Internet Of Things Journal, Vol. 7, NO. 9, Digital Object Identifier 10.1109/JIOT.2020.2997389.

[18] Divyashikha Sethia, Daya Gupta, Harsh Dabas, Preeti Nagar "Selective IoT Access with Scalable CP-ABE Revocation and Delegation", 2017 International Conference on Computational Science and Computational Intelligence, DOI 10.1109/CSCI.2017.121

[19] Jiaxin Xing , 'Towards Implementing RSA-based CP- ABE Algorithm on Android System," A thesis presented in partial fulfilment of the requirements for the degree of Master of Information Sciences, at Massey University, Auckland, New Zealand, 2019.

[20] www.Wikipedia.com