International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 5 | Issue 1 | ISSN : 2456-3307
DOI : 10.32628/CSEIT1951110

A Survey on Secure User Data Transaction using Attribute-Based Encryption Scheme over Cloud Data

Navin Sethiya[1], Hrishikesh Patel[1], Akshay Harshe[1], Alekh Gaigole[1], Harshvardhan Donadkar[1], Prof. Priya Karemore[2]

[1]UG Students, Department of Computer Technology, Priyadarshini College of Engineering, Nagpur, Maharashtra, India.

[2]Assistant Professor, Department of Computer Technology, Priyadarshini College of Engineering, Nagpur, Maharashtra, India.

ABSTRACT

Cloud computing is an innovation which utilizes the Internet to store, oversee, and register the information, as opposed to a nearby server or a PC. Clients can access the cloud condition wherever they need on compensation for each utilization way. Transferring of delicate information on un-believed servers in the cloud is a testing assignment. Established encryption procedures are utilized when the re-appropriating of information in the cloud to give access control and secrecy. Access control instruments are not doable in the cloud as a result of the absence of adaptability, versatility, and fine-grained access control. As an option, So, Attribute-Based Encryption (ABE) procedures are acquainted in the cloud with increment the security and adaptability. Attribute-based encryption is an open key cryptographic strategy in which the private key and figure content are based on the attributes. ABE involves IBE, KP-ABE, and CP-ABE. In Identity-Based Encryption (IBE) the mystery key and the attributes are based on the character of the client. In Ciphertext-Policy Attribute-Based Encryption (CP-ABE) a mystery key is gotten from the arrangement of attributes and the access strategy is defined over the universe of attributes inside the framework. In Key Policy – Attribute-Based Encryption (KP – ABE) the figure content is related to the arrangement of attributes and the mystery key is based on the access structure. This paper is a study of all ABE strategies and specialty an evaluation table about ABE keys job in cloud condition.

Keywords : Attribute-Based Encryption, Attributes Revocation, Fine-Grained Access Control, Keywords Search, Mobile Cloud Storage.

I. INTRODUCTION

Cloud computing is a model for empowering pervasive, helpful, on-request organize access to a common pool of configurable computing assets (Eg: Network, Servers, Storage, applications and administrations) that can be quickly provisioned and discharged with negligible administration exertion or specialist organization interaction[1]. It comprises of different basic attributes like On-request access, pervasive access, multitenancy, versatility, estimated utilization, strength. In On-request access, the client can utilize the computing assets in pay per use way. Omnipresent access speaks to the capacity to access a wide scope of gadgets, transport conventions, interfaces and different security innovations in cloud situations. Multitenancy empowers distinctive buyers to share the different cloud storage administrations.

Versatility is the capacity of a cloud to direct scale IT assets as required by the cloud purchaser or cloud supplier. Estimated usage addresses the limitations of a cloud stage to screen the utilization of its IT assets, in a general sense by cloud buyers. Flexibility alludes to excess IT assets inside a similar cloud or over various clouds. Three regular cloud conveyance models are generally utilized and set up: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS). IaaS conveyance demonstrates involved framework driven IT assets that can be accessed and oversaw through cloud benefit based interfaces and instruments. PaaS relies upon the current condition that makes a lot of apparatuses used to help the whole applications. SaaS gives reusable cloud benefit generally accessible to the scope of cloud buyers. Essentially, three sorts of cloud arrangement models are the open cloud, private cloud, and third-party cloud. The open cloud is claimed by an outsider cloud which is accessible by everybody in the cloud condition. Private cloud is possessed by a solitary association where limits are defined. The third party cloud is a mix of open and private cloud models.

Cloud computing is a sort of distributive computing that speaks to the usage models for remotely provisioning versatile and estimated assets [12]. At the point when the business information is moved to the cloud, at that point the security issue will ascend, as information security ends up imparted to the cloud specialist organization. Fundamental wordings utilized in the cloud will be: cloud supplier gives the cloud-based IT assets. Cloud buyer utilizes the cloud-based IT assets. Cloud examiner assesses the security controls, protection effects, and execution. Central security terms important to cloud computing are:

1. Confidentiality: It enables approved gatherings to access the information or assets that is it confines the unapproved access to information in travel and storage.

2. Integrity: It will keep unapproved clients from changing the information which is put away or transmitted in the cloud.

3. Availability: It enables the information to be accessible and usable amid an explicit timeframe.

4. Scalability: Capability to deal with the clients included the system powerfully with no disturbance of administration.

5. Client revocation: If the client leaves the system the plan should disavow his access rights from the system straightforwardly. Something else, the client can't utilize the information put away and the access is repudiated.

6. User revocation: Users can decode the encoded information with their very own attributes since the attributes are identified with polynomial arbitrary encryption work.

7. Access Tree: Based on the attributes, the access tree is produced. The access tree is included hubs. The leaf hubs are spoken to as attributes and the middle of the road hubs are spoken to utilizing doors likes AND, OR, and so on.

II. LITERATURE REVIEW

By expecting the believed cloud service provider gives security additionally to the expansive measure of delicate and significant information put away. ABE calculations can be utilized for securing the confidentiality of the put away information and furthermore ABE gives the access control instrument to information on the cloud. In cloud condition, information confidentiality is imperative to shield against insider assault, crash assault and refusal of administration assault. This area gives the current attribute based encryption components in cloud condition.

ABE was presented by Sahai and Waters [2] in 2005. It is an open key based one to numerous encryption that enables client to scramble and decode the information based on client attributes. The mystery key and figure content are subject to the client attributes. The decoding of ciphertext is conceivable just if the arrangement of attributes of client key matches with the attributes of ciphertext. Decoding should be possible just when the quantity of coordinating keys is equivalent to the referenced limit level. ABE calculation comprise of four stages: Setup, key age, encryption and unscrambling. Crash obstruction is a pivotal highlights of ABE. A rival that holds numerous keys can access the information if the individual key matches.

Drawbacks:
For encryption, the Data proprietor needs to utilize each approved client's open key so it expands the calculation overhead. This strategy is confined in light of the fact that it utilizes access of monotonic attributes to control client's access to the framework.

1. Identity Based Encryption (IBE)

It was proposed by Shamir in 1984[3].In Identity Based Encryption (IBE) the mystery key and the attributes are based on the identity of the client. For instance, email id be the identity of the client. Believed third party will create the private key.

Drawback:
In the event that the believed third party gets traded off, there is no security for the framework. The client protection can't be saved utilizing IBE.

2. Key Policy Attribute Based Encryption (KP-ABE)

It was proposed by Goyal et al. [4]. Each client is assigned with some access tree over the arrangement of attributes. Ciphertexts are based on the arrangement of attributes and the private key is based on the monotonic access structure that controls which ciphertexts a client can decode. This is intended for one to numerous correspondences. Decoding should be possible just when the attribute set fulfills the client's access structure. It bolsters access control conspire.

Disadvantages:
Information proprietor can't choose who can decode the encoded information. It can just pick graphic attributes for the information. It isn't appropriate for broadcasting applications in light of the fact that the information proprietor needs to confide in the key backer.

3. Expressive Key Policy ABE (EKP-ABE)

It is the all-inclusive variant of KP-ABE, the non-monotonic access structures [5] are utilized. Non-monotonic access structure utilizes repudiated doors, for example, NOT in the access structure. It is increasingly adaptable to limit the unapproved use of information.

Disadvantage:
The overhead is expanded on account of negative attributes which isn't pertinent to the encoded information.

4. Ciphertext Policy ABE (CP-ABE)

It is a turn around the form of KP-ABE [6]. In CP-ABE, the ciphertext is related with an access structure and client's private key is based on set of attributes. A client can unscramble the ciphertext just whenever set of attributes related with clients private key fulfills the access policy related with the ciphertext. CP-ABE is more anchored even the believed the third party is imperiled.

Disadvantage:

CP-ABE doesn't fulfilled undertaking needs of the access control component. Decoding keys underpin client attributes that are sorted out intelligently as a solitary set.

5. Hierarchical Attribute Based Encryption (HABE)

The HABE was proposed by Wang et al. [7]. This model comprises of a root ace that relates to the confided in third party, different space ace in which top dimension area aces compares to various venture clients and various clients that relates to all work force in an undertaking. This plan client's hierarchical age of keys. It utilizes randomized polynomial time calculation. It underpins anchored access control, adaptability and completely designation. It can share the ensured information for clients in a cloud in an endeavor situation. It bolsters intermediary reencryption conspire.

Disadvantages:

It is extremely hard to actualize continuously condition. A similar attribute will be utilized by numerous area aces.

6. Multiple Authority ABE (MAABE)

This strategy utilizes numerous experts and the client attributes are dispersed to different specialists. Suppose [8] it comprises of N multiple attribute experts and one focal specialist. The information can be decoded by the client under attribute set an and unscrambling keys for an attribute set Au. It enables any free experts to disseminate private keys and to deal with flawed or lost specialists.

Disadvantages:

Trouble in muti-expert plan is it expects specialist's to keep up disjoint arrangements of attributes.

7. File Hierarchy Attribute Based Encryption (FH-ABE)

This strategy utilizes record progressive system based encryption strategies. The documents are scrambled based on the layered access structure. Both figure content storage and time expenses of encryption are saved [9].

Disadvantage:

The FHABE conspire is turned out to be secure under the standard suspicion.

8. Ciphertext policy Weighted ABE (CPWABE)

This plan assigns [10] load to the attributes based on the inclination defined in the access control structure. Clients will have appointed the load to their attributes. The information proprietor will encode the information based on the attributes. The private key is based on the weighted access structure and the decryption [11] is conceivable just when the ciphertext and the weighted attribute matches with the weighted access structure. It takes care of the key escrow issue by utilizing weighted attributes.

Drawback:

Cost of computation is increased.

III. CONCLUSIONS

This paper abridges different attribute-based encryption systems for information security in cloud condition. Security will be the essential factor to be tended to. The storage cost of the figure writings, time of encryption and unscrambling to be diminished. Based on the qualities like fine-grained access control, adaptability and adaptability in cloud computing we can infer that FH-WABE performs well superior to the next attribute encryption strategies.

IV. REFERENCES

[1]. Muhammad Yasir Shabir, Asif Iqbal, Zahid Mahmood and Ataullah Ghafoor, Analysis of Classical Encryption Techniques in Cloud Computing, IEEE Tsinghua Science & Technology, Vol.21, February 2016.

[2]. A.Sahai and B.Waters, Fuzzy identity based encryption, in Proc. Advances in Cryptology – Eurocrypt, 2005, pp.457-473.

[3]. Adi Shamir. Identity-based cryptosystems and signature schemes, in Proc. of CRYPTO 84 on

Advances in cryptology, pages 47–53. SpringerVerlag New York, Inc., 1985.

[4]. V.Goyal, O.Pandey, A.Sahai and B.Waters, Attribute based encryption for fine grained access control of encrypted data, in proc. ACM conf. computer and communications, 2006.

[5]. J.Bethencourt, A.Sahai, and B.Waters, Ciphertext policy attribute based encryption, in proc. IEEE symposium security and privacy, 2007.

[6]. K.Meena,S.Vinodhini, T.Pallavi & R.Vasugi," Surveillance Based Gcm Home Security System Using Object Motion Detection",International Innovative Research Journal of Engineering and Technology,pp.44-47,2016.

[7]. S.Rifki, Y.Park, and S.Moon, A fully secure ciphertext policy attribute based encryption with a tree-based access structure, Journal of Information Science and Engineering, Vo.31, pp.247-265,2015.

[8]. G.Wang, Q.Liu and J.Wu, Hierarchical attribute based encryption for fine grained access control in cloud storage services, in Proc. ACM conf. computer and communication security, 2010.

[9]. K.Yang, X.Jia, K.Ren and B.Zhang, Dac-Macs: Effective data access control for multiauthority cloud storage systems, in Proc. Of IEEE Infocom, 2013.

[10]. Shulan Wang, Junwei Zhou, Joseph K.Liu, Jianping Yu, Jianyong Chen and Weixin Xie, An efficient file hierarchy attribute based encryption scheme in cloud computing, IEEE Transactions on information forensics and security, Vol. 11, No.6, June 2016.

[11]. Ximeng Liu, Jiafeng Ma, Jinbo Xiong, Qi Li, Jun Ma, Ciphertext – policy weighted attribute based encryption for fine grained access control, International conference on Intelligent networkings and collaborative systems, 2013.

[12]. Shulan Wang, Kaitai Liang, Joseph K.Liu, Jianyong Chen, Jianping Yu, Weixin Xie, Attribute based data sharing scheme revisited in cloud computing, IEEE Transactions on information forensics and security, Vol.11, No.8, August 2016.

[13]. G.K.Sandhia, G.K.Bhaskar, secure data sharing using attribute based encryption in cloud computing, Journal of Chemical & Pharmaceutical Sciences, Vol.9, December 2016.

Cite this article as :

Navin Sethiya, Hrishikesh Patel, Akshay Harshe, Alekh Gaigole, Harshvardhan Donadkar, Prof. Priya Karemore, "A Survey on Secure User Data Transaction using Attribute - Based Encryption Scheme over Cloud Data", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 5 Issue 1, pp. 433-437, January-February 2019.
Journal URL : http://ijsrcseit.com/CSEIT1951110