International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 03 | Mar-2018 www.irjet.net p-ISSN: 2395-0072

"PRIVILEDGE LEVEL ATTRIBUTE BASED ENCRYPTION POLICY FOR BIG DATA ACCESS"

Sukanya S. Zanjale[1], Arti S. Kangude[2], Vaishali R. Darekar[3], Komal B. Shete[4], Mayuri Ghorpade[5]

[1,2,3,4] *B.E Student, AES COET, Wadwadi (Maharashtra), India.*
[5]*Professor, Dept. of Computer Engineering, AES COET, Wadwadi (Maharashtra), India.*

Abstract - *The system proposes Associate in Nursing economical and fine-gained huge information access management theme with privacy-preserving policy. Specifically, during this system it hides the complete attribute instead of solely its values within the access policies. to help information coding, it additionally styles a completely unique Attribute Bloom Filter to gauge whether or not Associate in Nursing attribute is within the access policy and find the precise position within the access policy if it's within the access policy. a way to management the access of big quantity of huge information becomes terribly difficult issue, particularly once huge information is keep within the cloud. Cipher Text-Policy Attribute primarily based secret writing (CP-ABE) may be a promising secret writing technique that allows end-users to cipher their information beneath the access policies defined over some attributes of information customers and solely allows data customers whose attributes satisfy the access policies to decode the info.*

Key Words: **Big Data; Access Control; Privacy-preserving Policy; Attribute Bloom Filter.**

1. INTRODUCTION

Due to the versatile and elastic computing resources, cloud computing may be a natural fit storing and process massive knowledge. In attribute-based access management, end-users 1st outline access policies for his or her knowledge and code the info underneath these access policies. solely the users whose attributes will satisfy the access policy area unit eligible to decode the info. though the prevailing attribute-based access management schemes will manage the attribute revocation drawback all of them suffer from one problem: the access policy might leak privacy. for instance, Alice encrypts her knowledge to modify the "Psychology Doctor" to access. So, the access policy might contain the attributes "Psychology" and "Doctor". If anyone sees this knowledge, though he/she might not be able to decode the info, he/she still will guess that Alice might suffer from some psychological issues, that leaks the privacy of Alice. to the current finish, more build a completely unique Attribute Bloom Filter to find the attributes to the anonymous access policy, which might save plenty of storage overhead and computation value particularly for big attribute universe. this technique proposes associate economical and fine-gained massive knowledge access management theme with privacy conserving policy, wherever the complete attributes area unit hidden within the access policy instead of solely the values of the attributes.

2. LITERATURE SURVEY:

[1] Privilege Level Attribute Based Encryption Policy For Big Data Access

The system proposes associate economical and fine-gained massive information access management theme with privacy-preserving policy, wherever the total attributes square measure hidden within the access policy instead of solely the values of the attributes. For encoding purpose, the Advanced encoding commonplace (AES) algorithmic program is employed. to help information decipherment, Attribute Bloom Filter (ABF) is to judge whether or not associate attribute is within the access policy and find the precise position of the attribute if is within the access policy.

[2] Toward Efficient and Privacy-Preserving Computing in Big Data Era

This system investigated the privacy challenges within the massive information era by 1st distinctive massive information privacy needs then existing privacy-preserving techniques square measure comfortable for giant processing. It even has associate economical and privacy-preserving circular function similarity computing protocol in response to the potency and privacy needs of information mining within the massive data era expeditiously calculate the circular function similarity of 2 vectors to every different.

[3] Big Data in Mobile Social Networks: A QoE-Oriented Framework:

This system proposes a unique framework to deliver mobile massive information over Content-Centric Mobile Social Networks(CCMSN). The content-centric spec to deliver mobile massive information in MSNs is bestowed, wherever

every information consists of interest packets and information packets, severally.

[4] Secure and Verifiable Policy Update Outsourcing for Big Data Access Control in the Cloud:

The system specializes in developing associate outsourced policy change technique for ABE systems. This technique will avoid the transmission of encrypted information and minimize the computation work of knowledge house owners, by creating use of the antecedently encrypted information with previous access policies.

[5] Time-domain Attribute-based Access Control for Cloud-based Video Content Sharing: A Cryptographic Approach:

This system planned a cryptologic approach, TAAC, to attain time-domain attribute-based access management for cloud-based video content sharing. Specifically, it's planned a incontrovertibly secure time-domain attribute-based encoding theme by embedding the time into each the cipher texts and also the keys, such solely users WHO hold comfortable attributes in a very specific period will decipher the info.

[6] Enabling Fine-grained Access Control with Efficient Attribute Revocation and Policy Updating in Smart Grid:

It planned fine-grained access management theme (FAC) with economical attribute revocation and policy change in good grid. Specifically, by introducing the thought of Third-party Auditor (TPA), the planned FAC achieves economical attribute revocation. Also, style associate economical policy changes algorithmic program by outsourcing the process task to a cloud server.

[7] Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage:

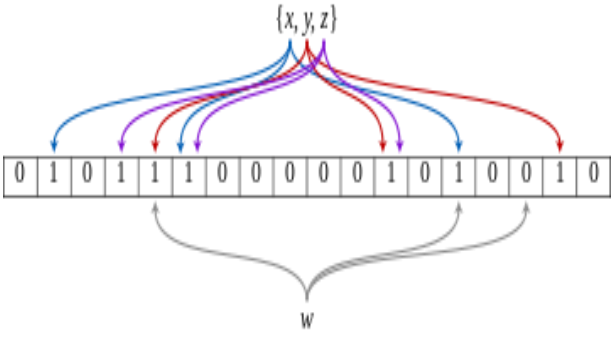
It propose a voidable multi-authority Ciphertext-Policy Attribute-based encoding (CP-ABE) theme, and apply it because the underlying techniques to style the info access management theme. The attribute revocation technique will expeditiously come through each forward security and backward security. In CP-ABE theme, there's associate authority that's answerable for attribute management and key distribution.

3. ADVANCE ENCRYPTION STANDARD:

AES is associate degree repetitive instead of Feistel cipher. it's supported 'substitution–permutation network'. It includes of a series of coupled operations, a number of that involve replacement inputs by specific outputs substitutions et al. involve shuffling bits around permutations. apparently, AES performs all its computations on bytes instead of bits. Hence, AES treats the 128 bits of a plaintext block as sixteen bytes. These sixteen bytes area unit organized in four columns and 4 rows for process as a matrix – not like DES, the amount of rounds in AES is variable and depends on the length of the key. AES uses ten rounds for 128-bit keys, twelve rounds for 192-bit keys and fourteen rounds for 256-bit keys. every of those spherical uses a unique 128-bit round key, that is calculated from the first AES key.

4. ATTRIBUTE BLOOM FILTER:

A Bloom filter may be a organization designed to inform you, chop-chop and memory-efficiently, whether or not parties gift during a set. the value got this potency is that a Bloom filter may be a probabilistic information structure: it tells U.S. that the component either undoubtedly isn't within the set or could also be within the set. the bottom organization of a Bloom filter may be a Bit Vector. Bloom filter is wide utilized in web applications. it's additionally been adopted in dimensional categorization as a result of its space-efficient and time-efficient characteristics in supporting approximate membership queries. Normal Bloom filter takes the whole dimensional information as and generates the indices. Therefore, it cannot support by-attribute queries, during which solely a set of attributes within the queried item are provided. Dimensional dynamic Bloom filter and parallel Bloom filter store every dimensional information during a separate Bloom filter to answer by attribute queries. However, once adopted with high-correlated queries, the performance of the formula degrades plenty. An example of a Bloom filter, representing the set. The colored arrows show the positions within the bit array that every set component is mapped to. The component w isn't within the set, as a result of it hashes to 1 bit-array position containing zero. For this figure, m = eighteen and k = three.



5. ARCHITECTURE DIAGRAM:

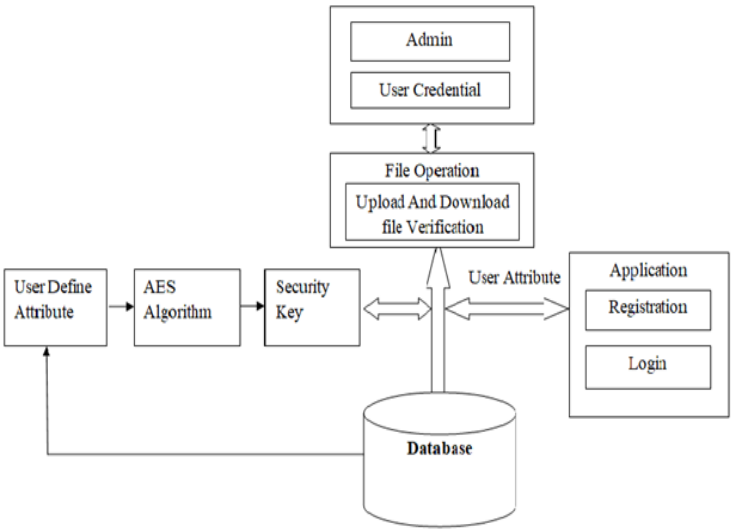


Fig. System Architecture

Every user get registration and if it is already registered then he/she get login into the system. System ask for attribute for example, name, profession, address etc. which user want to set. The selected attribute is stored into database and this user defined attribute is encrypted using the AES (Advanced Encryption Standard) algorithm and it generated both security key and hash value. This is the backend part.

When user get registration it is asking for attribute and the user write the attribute then the user send the request to download any file. How user can check the uploaded files by using the attribute of user. The attribute of user which stored in database are having same values like (dr.-dr., teacher-teacher, etc.) this attribute values are checked by admin. Admin is the one type of module which is authenticate and verify the all user credentials, if they are matched, then the admin shows the uploaded files for same attribute value user. If the one user wants to access the other user files which have different attribute value, in this case admin gives instruction to the other user that another attribute value user want to access your files that time this user`s hash value is different, therefore the first users hash value and another users hash value and secret key are calculated and then the user can download the file of another attribute value user. All authentication is done by checking the user credentials, and only then you get access for files.

Note: If admin is changed then there is no effect on user credentials code it is not changed.

6. PROJECT SYSTEM FLOW:

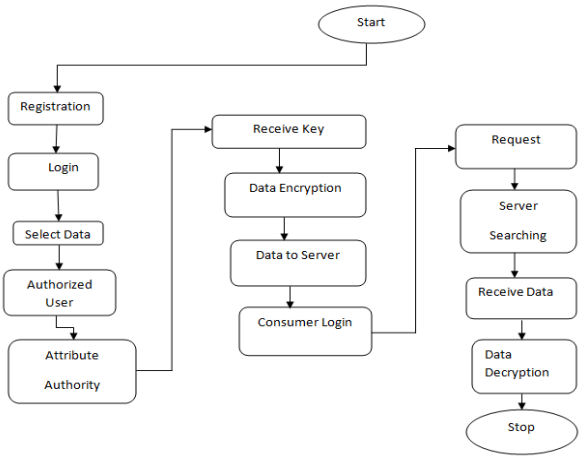


Fig. Project Flow

First user must do the registration then only he/she can get log into the system. The user who is authorized person can choose the file or select any data for uploading on cloud. The attribute authority manages all the attribute in the system and assign attribute chosen from attribute space to end user. Attribute authority can provide the secret key to user. Then user receives the key. By using that key user encrypt his data and send data to server. Data consumer can send request to the server for data when only the attribute can satisfy the access policy in the system. Consumer requested to server when he/she want to download another attribute value users file then server searching that file or data. When file or data are found by server it gives to the data consumer. After receiving the data, consumer can decrypt data using his private key. Here process is done.

7. CONCLUSION:

This system proposed an efficient and fine-grained data access control scheme for big data, where the access policy will not leak any privacy information. This method can hide the whole attribute rather than only its values in the access policies. However, this may lead to great challenges and difficulties for legal data consumers to decrypt data.

REFERENCES:

[1] R.Lu,H.Zhu,X.Liu,J.K.Liu, and J.Shao "Toward efficient and privacy preserving computing in big data era," IEEE Network,vol. 28,no. 4, pp. 46–50, 2014.

[2] Z.Su,Q.Xu,and Q.Qi, "Big data in mobile social networks: a qoe oriented framework," IEEE Network,vol.30,no.1,pp.52–57,2016.

[3] K.Yang,X.Jia,and K.Ren, "Secure and verifiable policy update outsourcing for big data access control in thecloud,IEEETrans.ParallelDistrib.Syst.,vol.26,no.12,pp. 3461–3470, Dec 2015.

[4] K.Yang, Z.Liu, X.Jia, and X.S.Shen, "Time-domain attribute-based access control for cloud-based video content sharing: A cryptographic approach," IEEE Trans. on Multimedia (to appear), February 2016.

[5]H.Li,D.Liu,K.Alharbi,S.Zhang,and X.Lin,"Enabling fine-grained access control with efficient attribute revocation and policy updating in smart grid," KSII Transactions on Internet and Information Systems (TIIS),vol.9,no.4,pp.1404 1423,2015.

[6] K.Yang and X.Jia, "Expressive, efficient, and revocable data access control for multi-authority cloud storage,"IEEETrans.ParallelDistrib.Syst.,vol.25,no.7,pp.1735–1744, July 2014.