Review of International Geographical Education | RIGEO | 2020

RIGEO

ISSN: 2146 - 0353

Review of International GEOGRAPHICAL EDUCATION

www.rigeo.org

CIPHERTEXT-POLICY ATTRIBUTE PRIMARILY BASED ENCRYPTION FOR DATA STORAGE IN CLOUD

[1] Eslavath Ravi,[2] Sabavath Raju, [3] Mudumba Sreepavani, [4] Malothu Ravi

[1,2,3,4] Assistant Professor, Department of Computer Science Engineering,

Pallavi Engineering College, Hayathnagar_Khalsa, Hyderabad, Telangana 501505

Article Info

Received: 05-09-2023 *Revised: 11 -10-2023* *Accepted: 05-11-2023*

Abstract:

In this paper we proposed to control the access of the large quantity of big facts becomes a very tough problem, especially while massive statistics are saved inside the cloud. Ciphertext-Policy Attribute primarily based Encryption (CP-ABE) is a promising encryption method that allows stop-users to encrypt their statistics underneath the get admission to policies defined over a few attributes of data customers and handiest lets in records consumers whose attributes satisfy the get right of entry to policies to decrypt the statistics. In CP-ABE, the get admission to coverage is connected to the ciphertext in plaintext shape, which may additionally leak some non-public facts approximately quit-customers. To assist records decryption, we also layout a unique Attribute Bloom Filter to assess whether an characteristic is within the access coverage and discover the exact position in the get right of entry to policy if it's far in the get admission to policy. Existing strategies best partially conceal the characteristic values in the get right of entry to rules, whilst the attribute names are still unprotected. In this paper, we advocate an green and first-rate-grained large information access manage scheme with privacy-keeping policy. Specifically, we conceal the whole characteristic (in preference to best its values) in the get entry to regulations.

Keywords: - Attribute Authority, Description, Cloud Servers, End-user, and Encryption.

1. INTRODUCTION

In the generation of big data, a massive quantity of statistics can be generated quickly from diverse assets (e.G., smart phones, sensors, machines, social networks, and so forth.). Towards these huge data, traditional computer systems aren't ready to save and technique these facts. Due to the flexible and elastic computing resources, cloud computing is a natural match for storing andprocessing huge information. With cloud computing, give up-customers store their information into the cloud, and depend on the cloud server to proportion their statistics to other customers (records consumers). In order to simplest share end-users' statistics to legal customers, it's far necessary to layout access control mechanisms in line with the requirements of quit-users. When outsourcing statistics into the cloud, endusers lose the bodily manage in their information. Moreover, cloud carrier ompanies aren't completely-relied on by way of end-customers, which makes the access control extra tough. For instance, if the traditional get entry to control mechanisms (e.G., Access Control Lists) are applied, the cloud server will become the decide to evaluate the get right of entry to policy and make get right of entry to choice. Thus, cease-users may also worry that the cloud server may additionally make wrong access choice intentionally or accidentally, and divulge their information to a few unauthorized users. In order to permit quit- customers to govern the access of their very own facts, some attribute-primarily based access manage schemes are proposed with the aid of leveraging attribute-primarily based encryption. In characteristic-primarily based get entry to manage, cease-customers first define get right of entry to guidelines for their information and encrypt the statistics under those get admission to regulations.

2. RELATED WORK

Existing System:

The current characteristic-based access manipulate schemes can be afflicted by one trouble: the get right of entry to coverage may also leak privacy. This is because the get admission to coverage is associated with theencrypted information in plaintext form. From the plaintext of get right of entry to coverage, the adversaries may also acquire a few privateness records about the cease-user. For instance, Alice encrypts her facts to allow the "Psychology Doctor" to access. So, the get entry to coverage may additionally include the attributes "Psychology" and "Doctor". If all of us sees this facts, even though he/she won't be capable of decrypt the statistics, he/she nevertheless can guess that Alice can also be afflicted by a few mental troubles, which leaks the privateness of Alice.

Proposed System:

To save you the privateness leakage from the access coverage, a trustworthy technique is to hide the attributes inside the access policy. However, while the attributes are hidden, not only the unauthorized users but additionally the authorized customers can't know which attributes are concerned in the get entry to coverage. In this paper, we intention to hide the whole attribute in place of simplest partially hiding the characteristic values. Moreover, we do no longer restrict our method to a few specific get entry to systems. The fundamental concept is to explicit the get entry to policy in LSSS access structure (M;r) where M is a coverage matrix and r matches every row Mi of the matrix M to an attribute,

and cover the attributes by using truely getting rid of the attribute matching function r. Without the characteristic matching function r, it's far important to layout an characteristic localization algorithm to assess whether or not an characteristic is in the get admission to policy and in that case find the proper function in the get admission to policy. To this give up, we similarly construct a novel Attribute Bloom Filter to discover the attributes to the nameless get right of entry to coverage, which could keep a variety of storage overhead and computation fee particularly for large characteristic universe.

Advantages:

1) We propose an efficient and excellent-gained massive facts access manipulate scheme with privateness-preserving policy, in which the whole attributes are hidden within the get right of entry to coverage instead of most effective the values of the attributes.

2) We additionally design a singular Attribute Bloom Filter to assess whether an attribute is within the access coverage and discover the exact position inside the get entry to coverage if it's miles within the get right of entry to policy.

3. IMPLEMENTATION

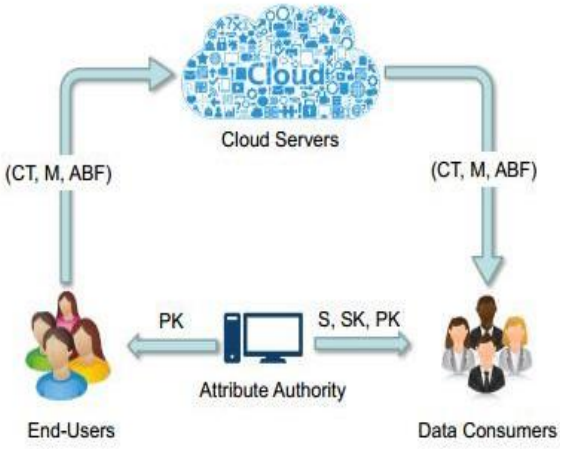


Fig:-1 System Architecture

Cloud Servers

Cloud Servers are employed to shop, percentage and method big statistics in the device. The cloud servers are controlled via cloud provider carriers, who aren't inside the identical consider domain as end-customers. Thus, cloud servers can't be trusted by means of cease-customers to enforce the get entry to policy and make access selections. We additionally count on that the cloud server cannot collude with any End-users or Data Consumers.

Attribute Authority

The attribute authority manages all the attributes in the gadget and assigns attributes selected from the characteristic space to cease-users. It is likewise a key technology center, wherein the general public parameters are generated. It also presents exceptional get right of entry to privileges to stop-users by using issuing secret keys consistent with their attributes. The attribute authority is assumed to be fully depended on in the gadget.

End-user:- End-users are the information owners/producers who outsource their facts into the cloud. They also would really like to manipulate the access in their statistics by way of encrypting the facts with CP-ABE. End-users are assumed to be sincere inside the gadget.

Data Consumers: - Data purchasers request facts from cloud servers. Only when their attributes can fulfill the get entry to policies of the facts, data customers can decrypt the data. However, information customers might also try and collude collectively to access a few facts that aren't accessible in my view

End User Sign up: - all of the stop users ought to provide all the obligatory Fields and get an Account in our software to get entry to our application

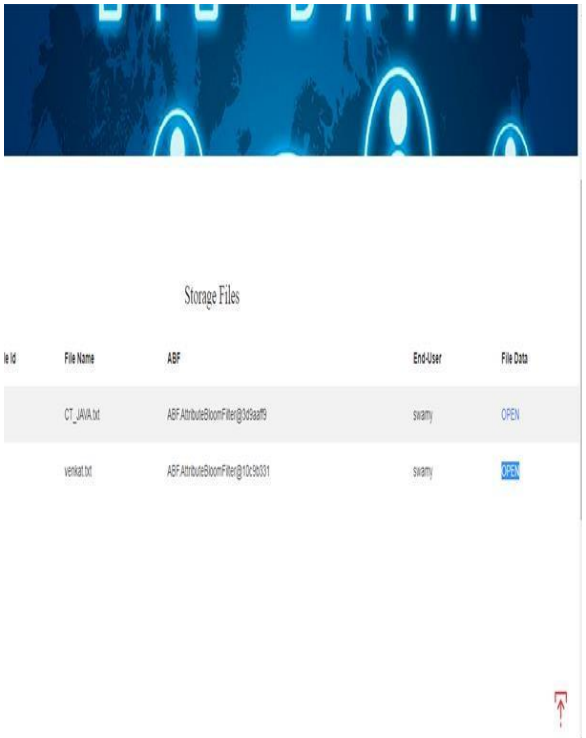
End User Login: - To get entry to the software we are verifying the give up customers login person call and Password **Data Consumer Sign up: -** all of the information client customers must deliver all the obligatory Fields and get an Account in our software to access our software

Data Consumer Login: - To get admission to the application we are verifying the facts customer login consumer call and Password**Attribute Authority Login: -** he is attribute company of the application where he can login into the application with his/her user call and password.

File Encryption: - The stop customers can encrypt the information with the characteristic and upload in cloud server.

File Description: - Data client view all of the stored files and decrypt and down load the document that's fit along with his attributes.

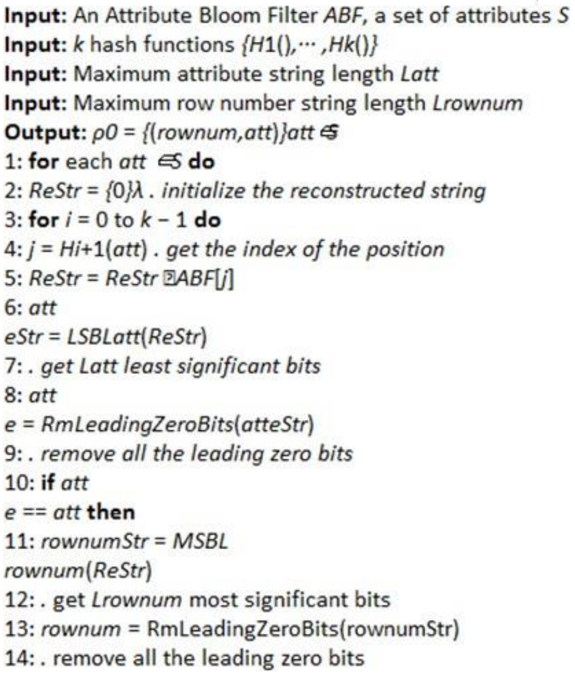
Algorithm



Storage Files

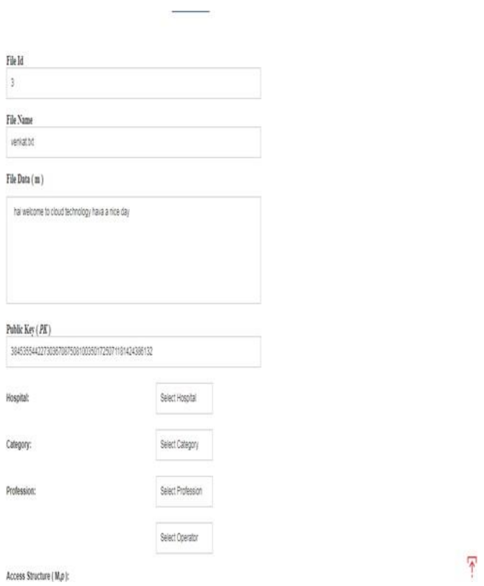
le Id	File Name	ABF	End-User	File Data
	CT_JAVA.txt	ABF.AttributeBloomFilter@3d3aaff9	swamy	OPEN
	venkat.txt	ABF.AttributeBloomFilter@10c9b331	swamy	OPEN

Fig:-4 ABF Query generation Page



```
Input: An Attribute Bloom Filter ABF, a set of attributes S
Input: k hash functions {H1(),··· ,Hk()}
Input: Maximum attribute string length Latt
Input: Maximum row number string length Lrownum
Output: ρ0 = {(rownum,att)}att ∈S
1: for each att ∈S do
2: ReStr = {0}λ . initialize the reconstructed string
3: for i = 0 to k − 1 do
4: j = Hi+1(att) . get the index of the position
5: ReStr = ReStr ⊡ABF[j]
6: att
eStr = LSBLatt(ReStr)
7: . get Latt least significant bits
8: att
e = RmLeadingZeroBits(atteStr)
9: . remove all the leading zero bits
10: if att
e == att then
11: rownumStr = MSBL
rownum(ReStr)
12: . get Lrownum most significant bits
13: rownum = RmLeadingZeroBits(rownumStr)
14: . remove all the leading zero bits
```

4. EXPERIMENTAL RESULTS



File Id: 3

File Name: venkat.txt

File Data (m): hai welcome to cloud technology hava a nice day

Public Key (PK): 384535544227303670875081003501725071181424386132

Hospital: Select Hospital

Category: Select Category

Profession: Select Profession

Select Operator

Access Structure (M,ρ):

Fig:-5 Set Attributes Page

5. CONCLUSIONS

In this paper, we've proposed an efficient and first-class-grained records get right of entry to manage scheme for big information, where the access coverage will no longer leak any privacy data. Different from the existing techniques which simplest partially conceal the characteristic values in the access regulations, our approach can conceal the entire attribute (in place of simplest its values) inside the get entry to guidelines. However, this could cause exquisite demanding situations and problems for criminal records consumers to decrypt statistics. To cope with this problem, we've also designed an attribute localization algorithm to assess whether an attribute is in the access coverage. In order to enhance the performance, a novel Attribute Bloom Filter has been designed to find the appropriate row numbers of attributes inside the get admission to matrix. We have additionally demonstrated that our scheme is selectively relaxed in opposition to selected plaintext attacks. Moreover, we have implemented the ABF by way of using Murmur Hash and the get entry to manipulate scheme to reveal that our scheme can hold the privacy from any LSSS get entry to coverage without employing tons overhead. In our future work, we can cognizance on the way to deal with the offline attribute guessing assault that take a look at the guessing “characteristic strings” by means of continually querying the ABF.

6. REFERENCES

[1] P. Mell and T. Grance, “The NIST definition of cloud computing,” [Recommendations of the National Institute of Standards and TechnologySpecial Publication 800-145], 2011.

[2] 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.

[3] K. Yang and X. Jia, “Expressive, efficient, and revocable data access control for multi-authority cloud storage,” IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 7, pp. 1735–1744, July 2014.

[4] 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.

[5] 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.

[6] B. Waters, “Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization,” in Proc. of PKC’11. Berlin, Heidelberg: Springer-Verlag, 2011, pp. 53–70.

[7] H. Lin, Z. Cao, X. Liang, and J. Shao, “Secure threshold multi authority attribute based encryption without a central

authority," in Proc. of INDOCRYPT'08. Springer, 2008, pp. 426–436.

[8] T. Nishide, K. Yoneyama, and K. Ohta, "Attribute-based encryption with partially hidden encryptor-specified access structures," in Applied cryptography and network security. Springer, 2008, pp. 111–129.

[9] J. Li, K. Ren, B. Zhu, and Z. Wan, "Privacy-aware attribute-based encryption with user accountability," in Information Security. Springer, 2009, pp. 347–362.

[10] D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," in Theory of cryptography. Springer, 2007, pp. 535– 554.