Scientific Journal Impact Factor (SJIF): 1.711

International Journal of Modern Trends in Engineering and Research

IJMTER

ISSN (ONLINE) : 2349 - 9745

ISSN (PRINT) : 2393 - 8161

A Fill Controlling Design Based on Reasoning Partitioning Data Access

S.SaiAbhishta Roy [1],B. Sudhakar[2]

Department of CSE, Audisankara College of Engineering and Technology, Gudur

Department of CSE, Audisankara College of Engineering and Technology, Gudur

Abstract - Data Access Control is an effective way to ensure the data security in the cloud.However, one of the biggest hurdles in the widespread adoption of cloud computing issecurity. The multi-tenant nature of the cloud is vulnerable to data leaks, threats, and malicious attacks. Therefore, it is important for enterprises to have strong access control policies in place to maintain the privacy and confidentiality of data in the cloud.Ciphertext-Policy Attribute based Ecryption (CP-ABE) is a promising technique for access control of encrypted data.It give data owners more direct control on access policies.Existing CP-ABE scheme doesnot support attribute revocation.We proposed a revocable Multi-Authority CP-ABE plan that can bolster productive property revocation.Then, we developed a viable information access control plan for multi-power distributed storage systems.We additionally demonstrated that our plan was provable secure in the irregular prophet model.

Index Terms- Access control, Multi-Authority, CP-ABE, Attribute revocation, Cloud storage.

I.INTRODUCTION

CLOUD storage is an important service of cloud computing, which offers services for data owners to host their data in the cloud. This new paradigm of data hosting and data access services introduces a great challenge to data access control .Since the cloud server can't be completely trusted by information proprietors, they can no more depend on servers to do access control .Figure content Policy Attribute-based Encryption (CP-ABE) is viewed as a standout amongst the most suitable advancements for information access control in distributed storage frameworks, on the grounds that it gives the information proprietor more straightforward control on access strategies. In CP-ABE scheme, there is an authority that is responsible for attribute management and key distribution.

The authority can be the registration office in a university, the human resource department in a company, etc. The data owner defines the access policies and encrypts data according to the policies. Each user will be issued a secret key reflecting its attributes. A user can decrypt the data only when its attributes satisfy the access policies. There are two sorts of CP-ABE frameworks: single-power CP-ABE where all characteristics are overseen by a solitary power, and multi-power CP-ABE where properties are from diverse areas and oversaw by distinctive powers. Multi-power CP-ABE is more fitting for information access control of distributed storage frameworks, as clients may hold characteristics issued by numerous powers and information proprietors might likewise share the information utilizing access approach characterized over traits from distinctive powers.For instance, in an E-wellbeing framework, information proprietors may share the information utilizing the entrance arrangement "Doctor AND Researcher", where the quality ""Doctor"" is issued by a therapeutic association and the characteristic ""Researcher"" is issued by the directors of a clinical trial. In any case, it is hard to specifically apply these multi-power CP-ABE plans to multi-power distributed storage frameworks due to the trait denial issue.

II.LITERATURE SURVEY

A. The NIST Definition of Cloud Computing(NIST-National Institute of Standards and Technology).

Distributed computing is a model for empowering universal, helpful, on-interest system access to a mutual pool of configurable registering resources(e.g., systems, servers, stockpiling, applications, and administrations) that can be quickly provisioned and discharged with negligible administration exertion or administration supplier connection.This cloud model is composed of five essential characteristics, three service models, and four deployment models.

B.Ciphertext-Policy Attribute-Based Encryption.

With the rise of the era of "cloud computing", concerns about "Security" continue to increase. Cloud computing environments impose new challenges on access control techniques due to the growing scale and dynamicity of hosts within the cloud infrastructure; we proposed Multi-Authority System (MAS) architecture.

This architecture consists of agents: Cloud Service Provider Agent (CSPA), Control Agent (CA), Third party Auditor (TPA) and Attribute Authority Agent (AAA). The TPA provides a graphical interface to the cloud user that facilitates the access to the services offered by the Cloud Service Provider (CSPA).

C.Bounded Cipher text Policy Attribute Based Encryption.

In a cipher text policy attribute based encryption system, a user's private key is associated with a set of attributes (describing the user) and an encrypted cipher text will specify an access policy over attributes. A user will be able to decrypt if and only if his attributes satisfy the cipher text's policy. In this work, we present the first construction of a cipher text-policy attribute based encryption scheme having a security proof based on a number theoretic assumption and supporting advanced access structures.Past CP-ABE frameworks could either bolster just extremely restricted access Structures or had a proof of security just in the non specific gathering model. Our construction can support access structures which can be represented by a bounded size access tree with threshold gates as its nodes. The bound on the size of the access trees is chosen at the time of the system setup. Our security proof is based on the standard Decisional Bilinear DiffieHellman assumption.

D.Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption.

We present two fully secure functional encryption schemes: a fully secure attribute-based encryption (ABE) scheme and a fully secure(attribute-hiding) predicate encryption (PE) scheme for inner-product predicates.Inboth cases,previousconstrutions were only proven to be selectively secure. Both results use novel strategies to adapt the dual system encryption method-logy introduced by Waters. We construct our ABE scheme in composite order bilinear groups, and prove its security from three static assumptions.

E. Multi-Authority Attribute Based Encryption Techniques.

Attribute based encryption (ABE) is a powerful encryption technique used in cloud computing, IoT, social networks and other technological fields where security and privacy are essential requirements of the system. There are diverse sorts of ABE plans and this article highlights the elements of multi-power quality based encryption (Mama ABE) schemes. A multi-power ABE framework comprises of any number trait powers and any number of clients. An arrangement of worldwide open parameters is characterized in the system. A client can choose a property power and acquire the relating unscrambling keys. The authority executes the corresponding attribute key generation algorithm and the result is returned to the user. The encryption process uses the global public parameters and an attribute set to produce the cipher text.Decryption is performed using the decryption keys for the attribute set.

F. Improving Privacy and Security in Multi-Authority Attribute –Based Encryption.

Attribute based encryption (ABE) [13] determines decryption ability based on a user's attributes. In a multi-authority ABE scheme,numerous quality powers monitor different sets of traits and issue relating decoding keys to clients, and encryptions can oblige that a client get keys for suitable characteristics from every power before unscrambling a message. Chase [5] 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 ofDistributing control over many potentially untrusted authorities. Also, in that development, the utilization of a reliable GID permitted the powers to consolidate their data 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 an answer which evacuates the trusted focal power, and ensures the clients' security by keeping the powers from pooling their information on specific clients, in this manner making ABE more usable practically speaking.

III.CURRENT WORK

Data access control scheme for multi-authority cloud storage systems contains the following phases:-

Phase A: System Initialization
Phase B: Secret Key Generation by AAs.
Phase C: Data Encryption by Owners
Phase D: Data Decryption by Users.
Phase E: Attribute Revocation.

A.System Initialization:

This phase consists of CA setup and AA setup with the following algorithms:

A.a)CASetup(1^{λ})->(GMK,GPP.(GPK_{uid}.GPK^{1}_{uid}).(GSK_{uid}.GSK^{1}_{uid}),Certificate(uid)).

The CA setup algorithm is run by the CA.It takes no input other than the implicit security parameter λ.It generates the global master key GMK of the system and the global public parameters GPP. For each user *uid* ,it generates the user's global public keys($GPK_{uid.}GPK^{1}_{uid}$),the user's global secret keys($GSK_{uid.}GSK^{1}_{uid}$) and certificate *certificate(uid)* of the user.

CA-Certificate Authority.
GMK-Global Master Key.
GPP-Global Public Parameter.
GPK-Global Public Key.
GSK-Global Secret Key.

A.b)AASetup($_{uSKaid}$.PK_{aid},{$VK_{xaid,}PK_{xaid}$}$_{xaid \epsilon uaid}$).

The attribute authority setup algorithm is run by each attribute authority.It takes the attribute universe u_{aid} managed by the AA_{aid}asinput.It outputs a secret and public key pair ($SK_{aid,}PK_{aid}$) of the $AA_{aid}$and a set of version keys and public attribute keys {VK_{xaid}.PK_{xaid}}$_{xaid\epsilon uaid}$ for all the attributes managed by the AA_{aid}.

AA-Attribute Authority.
SK-Secret Key.
PK-Public Key.
VK-Version Key.

B.Secret Key Generation by AAs:-

SKeyGen(GPP,GPK_{uid}.GPK^{1}_{uid}.GSK_{uid} , SK_{aid} ,$S_{uid,aid}$,{VK_{xaid}, PK_{xaid}}$_{xaid\epsilon Suid,aid}$) ->$SK_{uid\,,\,aid}$.

The secret key generation algorithm is run by each AA. It takes as inputs the global public parameters GPP, the global public key(GPK_{uid}, GPK^{1}_{uid}) and one global secret key GSK_{uid} of the user *uid*, the secret key SK_{aid} of the AA_{aid} , a set of attributes $S_{uid,aid}$ that describes the user *uid* from the $AA_{aid}$and its corresponding version keys {VK_{xaid}} and public attribute keys {PK_{xaid}}. It outputs a secret key $SK_{uid.aid}$ for the user *uid* which is used for decryption.

GPP-Global Public Parameter.

GPK-Global Public Key.
VK-Version Key.
GSK-Global Secret Key.
SK-Secret Key.
PK-Public Key.

C.Data Encryption by Owners:-

First,owners encrypt the data with content keys by using symmetric encryption methods.The encryption algorithm is as follows:

Encrypt (GPP ,{PK_{aid}}k,A) ->CT.

The encryption algorithm is run by the data owner to encrypt the content keys.It takes as inputs the global public parameter GPP, a set of public keys $\{PK_{aidk}\}_{aidk \epsilon Ia}$for all the AAs in the encryption set I_A^3,the content key *k* and an access policy A^4.The algorithm encrypts *k* according to the access policy and outputs a ciphertextCT.We will assume that the ciphertext implicitly contains the access policy A.

GPP-Global Public Parameter.
PK-Public Key.
CT-Ciphertext.
A-Access Policy.

D.Data Decryption by Users:-

Initially Users run the decryption algorithm to get the content keys,and then decrypt the data.

Decrypt(CT,GPK_{uid},GSK^1_{uid},$\{SK_{uid.aidk}\}_{aidk \epsilon IA}$) ->K.

The decryption algorithm is run by users to decrypt the ciphertext.It takes as inputs the ciphertext CT which contains an access policy A,a global public key GPK_{uid}, and a global secret key GSK^1_{uid} of the user *uid*, and a set of secret keys $\{\mathbf{SK}_{uid.aidk}\}_{aidk\ \epsilon\ IA}$ from all the involved AAs.If the attributes $\{S_{uid.aidk}\}_{aidk\ \epsilon\ IA}$ of the user *uid* satisfy the access policy A,the algorithm will decrypt the ciphertext and return the content key *k*.

CT-Ciphertext.
GPK-Global Public Key.
GSK-Global Secret Key.
SK-Secret Key.
K-Content Key.

E.Attribute Revocation:-

This phase consists of 3 steps.They are as follows:

E.a) Update Key Generation by AAs.
E.b) Secret Key Generation Update by Non-revoked Users.
E.c) Ciphertext Update by Server.

E.a)UKeyGen (SK_{aid}^1 ,x_{aid}^1 ,$VK_{x\ aid}^1$)->($VK_{x\ aid}^1$, $UK_{s,xaid}^1$,$UK_{c,\ x\ aid}^1$).

The update key generation algorithm is run by the corresponding AA_{aid}^1 that manages the revoked attributes x_{aid}.It takes as inputs the secret key SK_{aid}^1 of AA_{aid}^1,the revoked attribute x_{aid}^1 and its current version key VK_{xaid}.It outputs a new version key VK_{xaid}^1 and the update key$UK_{s,xaid}^1$(for secret key update) and the update key$UK_{c,\ x\ aid}^1$(for ciphertext update).

SK_{aid}^1-Secret Key.
$VK_{x\ aid}$-current Version Key.
X aid-Revoked attribute.
$UK_{s,x\ aid}$-Update Key (For Secret Key). $UK_{c,x\ aid}$-Update Key(For Ciphertext).

E.b)SKUpdate ($SK_{uid\ ,aid}^1$, $UK_{s\ ,xaid}$) ->$SK_{uid\ ,aid}^1$.

The secret key update algorithm is run by each non-revoked user *uid*. It takes as inputs the current secret key of the non-revoked user $SK_{uid,aid}^{1}$and the update key $UK_{s,xaid}$. It outputs a new secret key $SK_{uid.aid}^{1}$ for each non-revoked user *uid*.
uid – Non-revoked user.
$SK_{uid ,aid}^{1}$ – Current Secret Key of the Non-revoked user.
$UK_{s ,xaid}$ –Update Key.

E.c)CTUpdate (CT ,$UK_{c,,x\ aid}^{1}$) -> CT.

The ciphertext update algorithm is run by cloud server. It takes as inputs the ciphertexts which contain the revoked attribute x_{aid}^{1},and the update key $UK_{c,xaid}$.It outputs new ciphertexts CT which contain the latest version of the revoked attribute $x_{aid.}^{1}$
CT-Ciphertext.
UK-Update Key.

IV.SYSTEM MODEL

We considera data access control system in multi-authority cloud storage, as described in Fig.1.Therearefivetypes of entities in the system: a Certificate Authority(CA), Attribute Authorities(AAs), Data owners(owners),the cloud server(server)and data consumers(user).
The CA is a worldwide trusted endorsement power in the framework. It sets up the framework and acknowledges the enrollment of the considerable number of clients and AAs in the framework. Foreachlegaluser inthesystem, theCAassigns aglobaluniqueuser identity to it andalso generatesaglobalpublickeyforthisuser. However ,the CA is not involved in any attribute management and the creation of secret keys that areas sociated. withattributes.Forexample,theCAcanbetheSocialSecurityAdministration,anindependentagencyoft he United States government. Each user will be issued a Social Security Number(SSN) as its global identity. Every AA is an in dependent attribute authority that is responsible for entitling and revoking user's attributes according to their role oridentity in its domain. In our scheme every attribute is associated with single AA, but each AA can manage arbitrary number of attributes. Every AA has full control over the structure and semantics of its attributes.Each AA is responsible for generating a public attribute key for each attribute it manages and a secret key for each user reflecting His /Her attributes.

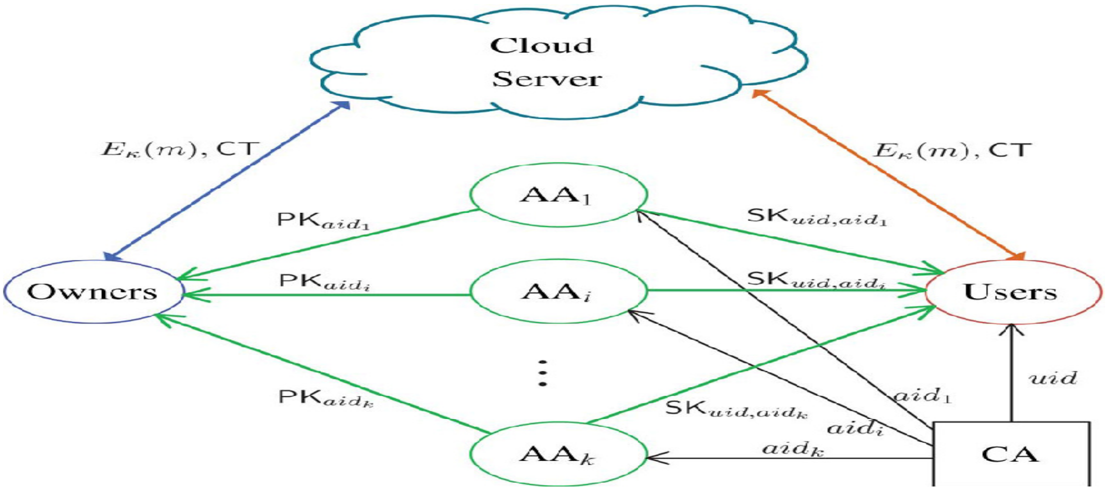

Fig.1: System model of data access control in multi-authority cloud storage.

Eachuserhasaglobalidentityinthesystem. Ausermay be entitled a set ofattributeswhichmaycomefrommultipleattributeauthorities.Theuserwillreceiveasecretkeyassociatedwithitsattributesentitledbythecorrespondingattributeauthorities.

Each owner firstdividesthe data into severalcomponentsaccordingtothelogicgranularitiesandencryptseach data component with different content keys by using symmetricencryption techniques .Then, the owner defines the access policies over attributesfrommultipleattribute authoritiesand encrypts the content keys under the policies.Then,theownersends theencrypteddata tothe cloud server together with the ciphertext.Theydonot rely on the server to do data access control.But the access controlhappens inside cryptography.That is only when the user's attribute satisfy the access policy defined in the ciphertext,the user is able to decrypt the ciphertext.Thususers with different attributes can decryptdifferent numberofcontentkeysand thus obtain differentgranularities ofinformationfrom thesame data.

V.CONCLUSION

In this paper,we have proposed another factual learning Approach to string transformation.Our method is novel and unique in its model,learning algorithm, and string generation algorithm.Two specific applications are addressed with our method, namely spelling error correction of queries and query reformulation in web Search.Test results on two vast information sets and Microsoft Speller Challenge demonstrate that our technique enhances the baselines regarding exactness and proficiency. Our method is particularly useful when the problem occurs on a large scale.

REFERENCES

[1] P. M ell and T. Grace,"The NIST Definition of Cloud Computing,'' NationalInstitute of Standards and Technology, Gaithersburg, MD, USA, Tech. Rep., 2009.

[2] J. Bettencourt, A. Sashay, and B. Waters, ''Ciphertext Policy Attribute Based Encrypt-ion,'' in Proc. IEEE Sump. Security and privacy (S&P'07), 2007, pp. 321-334.

[3] B. Waters, ''Cipher text-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization,'' in Proc.4th Int'l Conf. Practice and Theory in Public Key Cryptography (PKC'11), 2011, pp. 53-70.

[4] V. Goyal,A.Jain,O.Pandey,andA.Sahai, ''Bounded CiphertextPolicy Attribute Based Encryption,'' in Proc. 35th Int'l Colloquium on Automata, Languages, and Programming (ICALP'08), 2008,pp. 579-591.

[5] A.B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters,

[6] M. Chase, ''Multi-Authority Attribute Based Encryption,'' in Proc. 4th Theory of Cryptography Conf. Theory of Cryptography (TCC'07), 2007, pp. 515-534.

[7] M. Chase and S.S.M. Chow, ''Improving Privacy and Security in Multi-Authority Attribute-Based Encryption,'' in Proc. 16thACM Conf. Computer and Comm. Security (CCS'09), 2009,pp. 121-130.

[8]A.B.Lewko and B. Waters, ''Decentralizing Attribute-Based Encryption,'' in Proc. Advances in Cryptology-EUROCRYPT'11,2011, pp. 568-588.

[9] S. Yu, C. Wang, K. Ren, and W. Lou, ''Attribute Based Data Sharing with Attribute Revocation,'' in Proc. 5th ACM Symp. Information, Computer and Comm. Security (ASIACCS'10), 2010,pp. 261-270.

[10] M. Li, S.Yu,Y. Zheng, K. Ren, and W. Lou, ''Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption,'' IEEE Trans. Parallel Distributed Systems, vol. 24, no. 1, pp. 131-143, Jan. 2013.

S.Sai Abhishta Roy
Department of CSE,
Audisankara College of Engineering and Technology, Gudur,
saiabhishtaroy@gmail.com

B. Sudhakar
Department of CSE,
Audisankara College of Engineering and Technology, Gudur,
sudhakar1213@gmail.com