EAI Endorsed Transactions
on Cloud Systems
Research Article EAI.EU

Extensible and fine-grained characteristics-positioned information storage in cloud computing

M. IYAPPARAJA[1,*], C. NAVANEETHAN[2], S. MEENATCHI[3]

[1]SITE School, VIT, Vellore, TamilNadu-632014 (iyapparaja.m@vit.ac.in)
[2]SITE School, VIT, Vellore, TamilNadu-632014 (navaneethan.c@vit.ac.in)
[3] SITE School, VIT, Vellore, TamilNadu-632014 (meenatchi.s@vit.ac.in)

Abstract

With the improvement of distributed computing, outsourcing information to cloud server pulls in loads of considerations. To ensure the security and accomplish adaptable fine-grained record access control, (ABE) was proposed and utilized as a part of distributed storage framework. Be that as it may, client repudiation is the essential issue in ABE plans. In this article, we give a cipher text-arrangement trait-based encryption (CP-ABE) plan with effective client repudiation for distributed storage framework. The issue of client repudiation can be explained productively by presenting the idea of client gathering. At the point when any client leaves, the gathering supervisor will redesign clientôs PK with the exception of the individuals, who have been declined. Also, CP-ABE plan has substantial calculation cost, as it becomes straightly with the intricacy for the entrance structure. To diminish the calculation cost, we outsource high calculation burden to cloud administration suppliers without spilling document substance and mystery keys. Notably, our plan can withstand conspiracy assault performed by denied clients collaborating with existing clients.

Keywords: Distributed computing, cipher-text attribute-based encryption, Data owner, cloud server

Received on 18 February 2018, accepted on 22 March 2018, published on 26 March 2018

doi: 10.4108/eai.20-12-2017.153493

1. Introduction

Distributed computing is a general indication used to depict another classification of a system based registering that happens over the web, Essentially a stage on from adequacy Computing. Pay for utilizing and as required, versatile, scale all over in limit and functionalities. It has met the growing demand for handling resources and limits assets for a couple wanders due to its purposes of economy, flexibility, and accessibility. Starting late, a couple appropriated capacity organizations, e.g. Microsoft Azure and Google App Engine were constructed and can supply customers with versatile and element store. With the extending of tricky data outsourced to Cloud, circulated capacity organizations are going up against numerous challenges including data security and data get to overlook. To grasp those issues, characteristic based encryption (ABE) arranges has been associated with conveyed store services. Sahai and Waters. Initially proposed ABE plot named fu zzy personality based encryption which is gotten from id substance based encryption (IBE). As another proposed cryptographic primitive, ABE scheme has the upside of IBE plan and also gives the typical for "one-to-numerous" encryption. Straightforwardly, ABE chiefly principally incorporates two orders called ciphertext-system ABE (CP-ABE) and key p olicy plan ABE (KP-ABE).In CP-ABE, cipher-texts are interconnected with getting to procedures and customer's private keys are interconnected to quality sets. A customer can de-cipher the ciphertext if his attributes satisfy the get to arrangement installed in the ciphertext. It is inverse in KP-ABE. CP-ABE is more appropriate for the outsourcing data building than KP-ABE in light of the way that the impact of the procedure is demonstrated by the data proprietors. In this article, we demonstrate a beneficial CP-ABE with customer dissent limit. The equipment and programming administrations are accessible to overall population, endeavors, partnerships and organizations markets. With the change of passed on figuring, outsourcing information to cloud server pulls in stores of thoughts. To ensure the security and complete adaptable fine-grained record get the chance to control, quality based encryption (ABE) was proposed and utilized as a bit of passed on stockpiling structure. In any case, client denial is the fundamental issue in ABE organizes. In this project, we give a ciphertext-strategy quality based encryption (CP-ABE) agrrange with effective client repudiation for appropriated stored framework. The issue of client denial can be elucidated productively by presenting the likelihood of client get-together. Precisely when any client leaves, the social event executive will overhaul clients' private keys with the exception of the general population who have been

Denied. Furthermore, CP-ABE mastermind has impressive forget about cost, as it swings to be candid with the eccentrics for the path structure. To decrease the number cost, we outsource high figuring weight to cloud association suppliers without spilling report substance and center keys. Outstandingly, our course of action can withstand interest assault performed by denied clients collaborating with existing clients. We show the security of our game plan under the unmistakable calculation Diffie-Hellman (DCDH) supposition. The late result of our test displays estimation cost for adjacent contraptions is adequately low and can be dependable. Our scheme is suitable for asset compelled contraptions.

Figure1.Cloud structure

2. Literature survey

One drawback of encrypting data is that it giving another party your private key. A new cryptosystem for fine-grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KP-ABE).cipher-text are marked with a cluster of attributes and private keys are identify with accessed structures that control which cipher-texts a user can decrypt.[1] An attribute-based DRM scheme in cloud computing by combining the techniques of cipher-text policy attribute-based encryption (CP-ABE) and proxy re-encryption (PRE).we achieve efficient attribute and user revocation by allowing the attribute authority to delegate the key server to refuse to issue the assistant key for the revoked users.The proposed scheme is secure, efficient, and privacy-preserving.[2] we design an access control framework in cloud storage systems and propose a fine-grained access control scheme based on Cipher text-Policy Attribute-based Encryption (CP-ABE) approach. the data owner is in charge of defining and enforcing the access policy and efficient attribute revocation method for CP-ABE systems, which can greatly reduce the

attribute revocation cost. Resulted inefficient and provably secure in the random oracle model[3]. The issue of at the same time accomplishing fine-grained, versatility, and information privacy of getting to control in reality still stays uncertain. We accomplish this objective by abusing and interestingly consolidating strategies of trait-based encryption (ABE), intermediary re-encryption, and languid re-encryption. Broad investigation demonstrates that our proposed plan is exceedingly proficient and provably secure under existing security models[4]. In Fuzzy IBE we see a way of life as an arrangement of graphic qualities. A Fuzzy IBE plot takes into consideration a private key for a be seen as an Identity-Based Encryption of a message under a few qualities that form a (fluffy) character. Our IBE plans are both bug-tolerant and secure against plot assaults. Furthermore, our essential development does not utilize irregular prophets. We demonstrate the security of our plans under the Selective-ID security mo del.[5] Trait-based encryption (ABE) is a promising cryptographic primitive, which has been broadly connected to outline fine-grained get to control framework recently. In any case, ABE is being condemned for its high standard overhead as the computational cost develops with the multifaceted nature of the get to them. This weakness turns out to be more genuine for cell phones since they have compelled processing assets[6]. In a character based encryption plot, every client is recognized by an extraordinary personality string. A trait-based encryption conspire (ABE), interestingly, is a plan in which every client is recognized by an arrangement of characteristics, and some capacity of those credits is utilized to decide unscrambling capacity for each ciphertext. Sa hai and W aters presented the only specialist characteristic encryption plan and left open the topic of whether a plan could be developed in which numerous experts were permitted to circulate traits[7]. In this paper, we propose another multi-expert CP-ABE framework which addresses these two issues decidedly. In this new framework, there are various Central Authorities (CAs) and Attribute Authorities (AAs), the CAs issue personality related keys to clients and are not included in any property related operations, AAs issue describes related keys to clients and every AA deals with an alternate space of characteristics. The framework is adaptively secure in the standard model with versatile specialist debasement and can bolster expansive trait universe[8]. It removes the requirement for an open key framework. It Proposed a fu-zzy IBE model with productive denial, whose many-sided quality of key updates is fundamentally lessened contrasted with the past results. Perfect for adaptability issue. Issue emerges proficient denial in PKI setting[9]. we propose a privacy-preserving decentralized CP-ABE (PPDCP-ABE) scheme where the central authority is not required, namely each authority can work independently without the cooperation to initialize the system.[10].

3. Related work

Despite ABE has shown its merits, user revocation and attribute revocation are the essential concernment.The revocation issue is much hard to do unusually in CP-ABE schemes, due to any attribute shared by users. This implies that revocation will affect the single user as well as other users .short while ago,[9-11]some work proposed to handle this issue in an effective manner.Boldyreya et al [9]showed an IBE scheme with effective revocation, that is suited to KP-ABE. Tysowski et al [12] gave a simple strategy to perform client disavowal operation by joining CP-ABE with re-encryption. In their plan, every client has a place with a gathering and holds a gathering mystery key issued by the gathering. Nonetheless, their plan does not avoid arrangement assault performed by revoked clients collaborating with existing clients. The reason is that every client's gathering mystery key is same for a similar gathering. The qualities of the denied clients can be utilized by the client in a similar gathering without the predetermined attributes. Also, we bring up that there is a similar security hazard in the plans[2-3].Through applying ABE plans for distributed storage ser-indecencies, we can both guarantee the security of put away information and accomplish fine-grained information get to control. Sadly, ABE plot requires high calculation overhead amid performing encryption and unscrambling operations. This deformity turns out to be more extreme for lightweight gadgets because of their obliged figuring assets. To lessen the registering assets. To diminish the computation cost for asset compelled gadgets, some cryptographic operations with high computational load were outsourced to cloud specialist co-ops[4-13].Combined intermediary re-encryption with lethargic re-encryption system, Yu et al [4]composed a KP-ABE conspire with fine-grained information get to control. This plan requires information gets to control. This plan requires that the root hub in the get to the tree is an AND entryway and one kid is a leaf hub which is related to the spurious property. The spurious ascribe is required to be incorporated into each information archive's trait set and will never be refreshed. In their plan, cloud specialist co-op stores all the private key segments for client's private key aside from the one comparing to the fake property. Green et al [14]gave a productive CP-ABE plot with outsourcing decoding. In their plan, user's private key is blinded through utilizing an irregular num-ber. Both the private key and the arbitrary number are kept mystery by the user.The client shares his blinded private key to an intermediary to perform an [4-14] outsourced decoding operation.

In this paper, we utilize the comparative procedures as to extend our plan with outsourcing capacity. no single expert can decode any ciphertext. Keeping in mind the end goal to secure protection of the client, Han et [10] al. presented a decentralized KP-ABE plot with security saving. Essentially, Qian et al.[15] given a decentralized CP-ABE with completely concealed get to structure. Besides,[7] they proposed a protection saving individual wellbeing record utilizing multi-expert ABE with denial. Recently, some traceable CP-ABE [16] plans were genius postured with a specific end goal to discover a productive answer for recognizing malignant clients who intentionally share their decoding keys.

4. Materials and Methods

There were many solutions propose to solve user privacy problem, we have also proposed a strong way to protect user data leakage in untrusted cloud background In today's time mobile user has increased massively and has started using Flickr to de-anonymize Twitter, using Facebook to de-anonymize WiFi mobility traces. And these services are provided by the small organization, so these organizations may use the third party cloud server to process large user query point. So there is always chance that user data will be miss used the malicious cloud service provider.we give a cipher text-arrangement trait-based encryption (CP-ABE) plan with effective client repudiation for distributed storage framework. The issue of client repudiation can be explained productively by presenting the idea of client gathering. At the point when any client leaves, the gathering supervisor will redesign client's PK with the exception of the individuals, who have been declined.
Also, CP-ABE plan has substantial calculation cost, as it becomes straightly with the intricacy for the entrance structure. To diminish the calculation cost, we outsource high calculation burden to cloud administration suppliers without spilling document substance and mystery keys. Notably, our plan can withstand conspiracy assault performed by denied clients collaborating with existing clients.

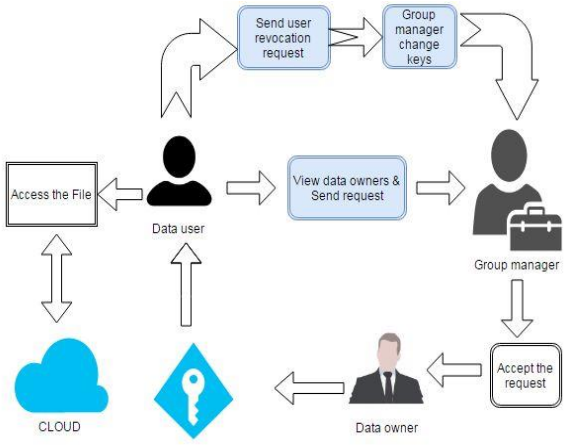


Figure 2. CP-ABE

4.1 System Architecture

The System Architecture consists of four entities Data owner, Cloud storage, group manager and data user. Data owner protection process will take place at the beginning where a user get a private key of downloading file (i.e., owner private key for that file) from cloud storage. In this module, Data owner transfers our document. At the time documents are put away to cloud. Transferring every last record contains mystery key. Trust expert keeps up all information proprietor transferred documents mystery key. This is the third module of our venture. In this module, Data client sees all information proprietor and all information proprietor transferred records. Then the client sends a demand to the proprietor. Right now ask for first go to gathering administrator then information owner.
In this module, data user send the request to data owner at the time request first go to the group manager. Group manager if accept request means this request go to data owner otherwise group manager cancel the request. Then data owner get the data user request if data owner accepts the request means data user get data owner secret key else data owner cancel the request means data user can't access the data owner files. This is the fifth module of our project. In this module data owner and group, the manager accepts the data user request means data user get data owner secret keys. Then data user uses data owners secret keys access the data owner files. This is the six module of our project. In this module, data user sends revocation request to the group manager. Group manager if accepting data user revocation request means at the moment data user left from this application and Group manager change all data owner secret keys.

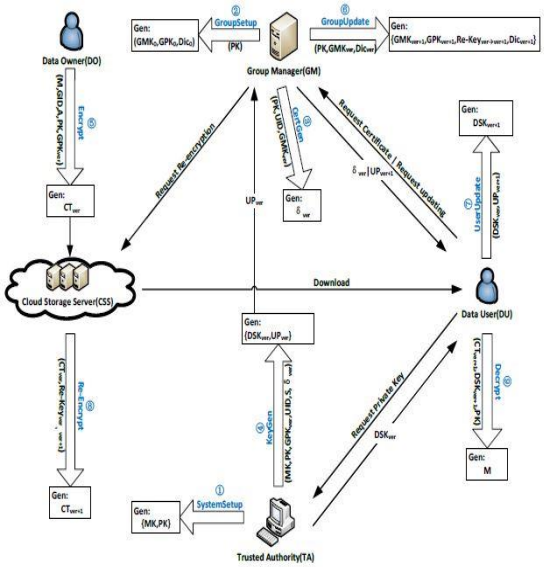


Fig. 3. CP-ABE with efficient user revocation.

5. *System Design*

USER INTERFACE DESIGN:
This is the first module of our project. It is created for security purpose. i.e., Login Page, we have to enter login user id and password. Only a valid user can access the page. It will check username and password is match or not . If any invalid username and password is entered, we can't enter into login window to user window it will display an error message (this is verified by the server) .so that any unauthorized person cannot access this page. By this way we are providing a good security for our project.

DATA OWNER UPLOAD FILE:
This is the second module of our project. In this module Data owner upload our file. At the time files are stored to cloud. Uploading each and every file contains secret key .Trust authority maintains all data owner uploaded files secret key.

DATA USER SEND REQUEST:
This is the third module of our project. In this module Data user view all data owner and all data owner uploaded files .Then user send request to owner. At the moment request first go to group manager then data owner.

RESPOND TO GM & OWNER:
This is the fourth module of our project. In this module data user send request to data owner at the time request first go to group manager. Group manager if accept request means this request go to data owner otherwise group manager cancel the request. Then data owner get the data user request if data owner accept the request means data user get data owner secret key else data owner cancel the request means data user can't be access the data owner files.

USER GET PERMISSION:
This is the fifth module of our project. In this module data owner and group manager are accept the data user request means data user get data owner secret keys . Then data user use data owners secret keys access the data owner files

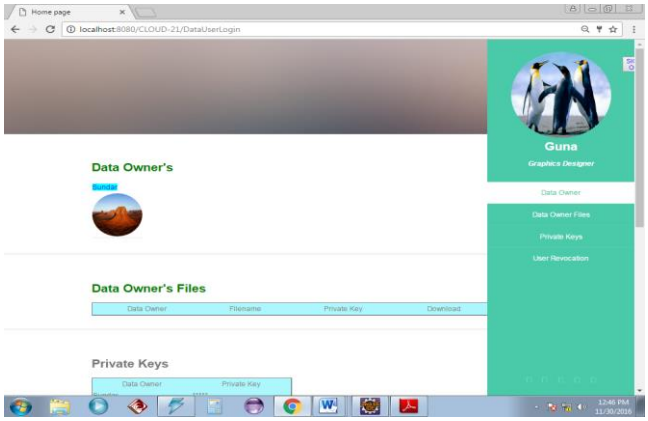
USER REVOCATION REQUEST:
This is the six module of our project. In this module data user send revocation request to group manager. Group manager if accept data user revocation request means at the moment data user left from this application and Group manager change all data owner secret keys.

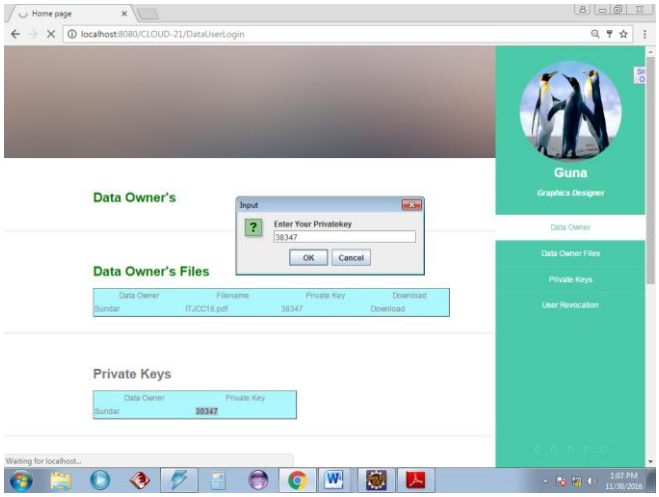
6. Cloud computing

6.1 Microsoft Azure:

Fig.4

Microsoft Azure, in the past known as Windows Azure, is Microsoft's open distributed computing stage. It gives a scope of cloud administrations, including those for register, examination, stockpiling, and systems administration. Clients can pick and look over these administrations to create and scale new applications, or run existing applications, in the general population cloud.there are 11 primary administrations gave by Microsoft Azure i.e., Compute,Web and mobile,Data storage,Analytics,Networking,Media and content conveyance organize (CDN),Hybrid integration,Identity and get to administration (IAM),Internet of Things (IoT) ,Development,Management and security.To guarantee accessibility, Microsoft has Azure server farms situated the world over.





7. Conclusion

In this article, we provided a formal definition and security model for CP-ABE with user revocation. We also construct a concrete CP-ABE scheme which is CPA secure based on DCDH assumption. To resist collusion attack, we embed a certificate into the user's private key. So that malicious users and the revoked users do not have the ability to generate a valid private key through combining their private keys. Additionally, we outsource operations with high computation cost to E-CSP and D-CSP to reduce the user's computation burdens. Through applying the technique of outsource, computation cost for local devices is much lower and relatively fixed . The results of our experiment show that our scheme is efficient for resource constrained devices.

References:

[1] V. Goyal. Pandey, A. Sahai, andB. Wates, " Property Based Encryption for Fine-Grained Access Control of Encrypted Data", Proc.13th ACM Conference on Computer and Communications Security(CCS '06), Vol.4, issue.2, pp. 89-98, 2006, doi:10.1145/1180405.1180418.

[2] K Yang, X Jia, K Ren,2012 "An Efficient Attribute based Encryption Scheme with Revocation for Outsourced Data Sharing Control" Proc.2011International Conference on Instru-mentation, Measurement, Computer, Communication and Control, pp. 516-520,2011.

[3]Shucheng Yu, Cong Wan†, Kui Rn†, and Wenjing Lu,"Achieving Secure, Scal-able, and Fine-Grained Data Access Control in Cloud Compu-ting,"Proc. of IEEE INFOCOM'10,Issue.2, pp. 1-9,2010.

[4] Jin i1, Xiafeng Chen2, Jingwei Li3, Chufu Jia3, Jianfeng Ma4, Wenjing Lou5 "Fine-Grained Access Control System Based on Outsourced Attribute-Based Encryp-tion,"Proc.18th European Symposium on Research in Computer Security(ESORICS '13),LNCS8134,Berlin: Springer-Verlag, pp. 592-609, 2013.

[5] M.Chase, "Multi-authority Attribute Based Encryption" Proc.4th Theory of Cryptography Conference(TCC '07), LNCS4392,Berlin:Springer-Verlag, Vol.2, Issue.1, pp. 515-534, 2007.

[6] Z. Liu, Z. Cao, Q. Huang, D. S. Wongand T. H. Yuen, “Fully Secure Multi-Authority Ciphertext-Policy Attribute-Based Encryption with-out Random Oracles,”Proc.16th European Symposium on Research in Computer Security(ESORICS ’11), LNCS6879, Berlin:Springer-Verlag, pp. 278-297, 2011.

[7] A. Sahai and B. Waters,“Fuzzy Identity-Based Encryption,”EUROCRYPT’05, LNCS, Vol. 3494, Issue. 8, pp. 457-473,2005.

[8] J.G. Han, W. Susilo, Y. Mu andJ. Yan, “Privacy-Preserving Decentral-ized Key-Policy Attribute-Based Encryption,”IEEETransactions on Parallel and Distributed Systems, Vol.23, No.11, pp. 2150-2162, 2012.

[9] Iyapparaja M, Bhanupriya Sharma, Augmenting SCA project management and automation Framework, IOP Conf. Series: Materials Science and Engineering 263 (2017) 042018 doi:10.1088/1757-899X/263/4/042018,pp-1-8

[10] Iyapparaja M et.al. 2012 Coupling and Cohesion Metrics in Java for Adaptive Reusability Risk Reduction IET Chennai 3rd International Conference on Sustainable Energy and Intelligent Systems (SEISCON 2012),52-57.

[11] Iyapparaja M, Tiwari. M, Security policy speculation of user uploaded images on content sharing sites , IOP Conf. Series: Materials Science and Engineering 263 (2017) 042018 doi:10.1088/1757-899X/263/4/042019,pp-1-8

[12] J.W. Li, C.F. Jia, J. Liand X.F. Chen, “Outsourcing Encryption of At-tribute-Based Encryption with Mapreduce,”Proc.14th International conference on Information and Communications Security(ICICS ’12),LNCS7618,Berlin:Springer-Verlag, Vol.2, pp. 191-201, 2012.doi:10.1007/978-3-642-34129-8_17.

[13] M. Green, S. Hohenbergerand B. Waters, “Outsourcing the decryp-tion of ABE ciphertexts,”Proc.20th USENIX Conference on Security(SEC ’11), Vol.10, Issue.8, pp. 34, 2011.

[14] H.L. Qian, J.G. Liand Y.C. Zhang, “Privacy-Preserving Decentralized Ciphertext-Policy Attribute-Based Encryption with Fully Hidden Ac-cess Structure,”Proc.15th International Conferenceon Information and Communications Security (ICICS ’13), CS8233,Berlin:Springer-verlag, Vol. 23, Issue. 4, pp.363-372,2013.

[15] J.T.Ning, Z.F.Cao, X.L.Dong, L.F.Weiand X.D.Lin, “Large Universe Ciphertext-Policy Attribute-Based Encryption with White-Box Trace-ability,”Proc.19th European Symposium on Research in Computer Security(ESORICS ’14), LNCS8713,Berlin:Springer-Verlag, Vol.5, pp. 55-72, 2014.