An Approach for Enhancing Privacy and Protection in Decentralized Multi-Authority Characteristic-based on Encryption in Cloud Computing

G. Swaraj Reddy, Rajesh Tiwari, Mrutyunjaya S Yalawar

***Abstract:** The Decentralizing multi-authority Attribute- Based secret writing has applied for finding issues arising from sharing various confidential company information in resources like cloud computing. The dispersivemulti-authority trait- Grounded secret jotting systems that wont accept the central authority, conspiracy resistance may be achieved employing a transnational symbol. thus, identity must be managed encyclopedically, which ends in pivotal issues of sequestration and security. A theme is developed which do not use the central authority to manage druggies and keys and solely easy trust relations ought to get shaped by participating the general public key between every Authority. stoner individualities square measure distinctive by combining a stoner's identity with the Attribute Authority wherever the stoner is set up. Once a crucial request must be created to an authority outside the sphere, the request must be performed by the authority within the current sphere rather of by the druggies, so, stoner individualities stay nonpublic to the Attribute Authority outside the sphere, which can enhance sequestration and security and also the crucial supplying. The theme relies on order direct brigades. an suggestion of security is bestowed that uses the binary System secret jotting methodology. Once the trait authorities in each sphere are members of a hierarchicalmulti-authority ABE, the goal for future work must be to develop a system that combines the plan presented in this study with the hierarchicalmulti-authority ABE.*

***Keywords:** Attribute Based Encryption, Privacy, Multi-Authority.*

I. INTRODUCTION

Now a day's cloud computing permits users store their sensitive information in an un trusted remotely accessible cloud service suppliers to realize scalable services on-demand. In light of this, it is suggested that the most important security demands for knowledge, information storage, and management incorporate information security and privacy and call for the use of strong coding techniques and fine-grained access control for data security in cloud computing. In the context of cloud computing, attribute-based encryption (ABE) is a cost-effective encoding solution with granular access control. Use secret writing techniques with fine-grained access control (ABE) to encrypt outsourced data in cloud computing. ABE is a cost-effective secret writing system with fine-grained access control. Hence the Single-authority ABE cannot meet the demands of decentralized distribution, and decentralizing multi-authority for basic Identity-based cryptography (IBE) and ABE, all private keys are managed by an authorized centre. However, in follow may give a performance bottle-neck requiring analysis because of large numbers of requests Hence the Hierarchical IBE (HIBE) [1-7] and graded ABE (HABE) [8]area unit currently being employed.

Manuscript received on 19 August 2022 | Revised Manuscript received on 29 August 2022 | Manuscript Accepted on 15 September 2022 | Manuscript published on 30 September 2022.

* Correspondence Author

G. Swaraj Reddy, Department of Computer Science and Engineering, CMR Engineering College, Hyderabad (Telangana), India.

Dr. Rajesh Tiwari, Department of Computer Science and Engineering, CMR Engineering College, Hyderabad (Telangana), India.

Mrutyunjaya S Yalawar*, Department of Computer Science and Engineering, CMR Engineering College, Hyderabad (Telangana), India. Email: mrutyunjaya.cmrec20@cmrec.ac.in

II. LITERATURE REVIEW

In this paper [1] we are using the encryption based data that which data that can be encrypted by the Ciphertext-Policy Attribute-Based Hierarchical collection of a documents by using the scheme called the CP-ABHE i.e by this method we can illustrate the security and efficiency.

[2] In this page we have taken the reference of the hierarchical IBE schemes and signature schemes that can resistance on the arbitratry number of level in cipher text security in random oracle model.

Even we can use the cipher text without the random oracle model [3] by using the identity based encryption. [4] This paper we use the wildcard identity-based encryption which says that the sender can decide to make the ciphertext decryptable by a whole range of users.[5] In this paper where we can use the anonymous hierarchical encryption without the random oracle that which can have fully anonymous cipher text and hierarchical key delegation. In paper [6] With rapid development of cloud computing, more and more enterprises will outsource their sensitive data for sharing in a cloud.

Decentralizing multi-authority Attribute-Based Encryption has been used in paper [7] to address issues with sharing confidential information.

According to Paper [8], attribute-based encryption (ABE) uses a user's attributes to identify a user's capacity to decode data. Decentralized attribute-based encryption (ABE), a subset of multi-authority based ABE, is described in Paper [9]. In writing [10]. A dealer may distribute shares to parties via a secret-sharing mechanism.

III. METHODOLOGY

The decentralising multi-authority ABE's core technique is conspiracy resistant; the users' keys must be separated in multiple authorities. The secret value is sliced into private keys suitable for the stoner in the Chase07 scheme, and decryption is accomplished by reconstructing the secret values of each sphere and encyclopedically. This secret slicing methodology is appropriate for simple access programmes with relatively stable trait authorities. For the Lewko-Waters system, a secret value is divided among the access policy's many characteristics; the access policy need not be taken into account during essential distribution; and the secret share is located in the cipher-access book's policy. Thus, Lewko-approach Waters's is made flexible and adaptable to changing data requirements. The Lewko-Waters scheme's secret slicing technique is employed in this essay's scheme as a guide to create a flexible access policy. The Lewko-Waters approach relies on the stoner identity operation provided by a relevant operation centre even though it doesn't employ a central authority to ensure that drug users' identities are completely unique. A stoner outside the sphere demands a key from the AA directly, which is suitable to influence in problems with security and trustability for the stoner, which to some extent results in sequestration and security issues. Furthermore, a significant improvement in working capacity will be made. The authorities can obtain comprehensive information on drug users based on their GIDs because drug users are required to submit their own GIDs to each authority. However, once the information from the stoner's GID is recovered, it may compromise the stoner's privacy. Stoner identities in our topic are utterly separate, and supporting a stoner identity doesn't necessarily require the assistance of related organisations. For privacy and security reasons, identity use and operation take place inside certain fields, and stoner identities won't be encyclopedically disclosed. Key requests made outside of a website are handled by a trait authority rather than by stoners. Due to this, there will be significantly fewer critical operations from outside the sphere, and the likelihood of cheating drug users will also decline. Only the public and secret keys of the AA are required, simplifying the method and reducing operational complexity. Public key of trait does not need that each trait have a pair of random numbers. 1: Assume that P=P1, P2,..., Pn is a group of parties. Only if the conditions outlined below are satisfied is the secret sharing system over P referred to as a Linear Secret-Sharing Scheme (LSSS). The shares are a vector over Zp for each set of P. There is an access structure A and a share-generating matrix A for it. A is a matrix with l rows and n columns. For all i=1,...,l, is a mapping from 1,...,l to P such that the ith line of matrix A is mapped to one participant, Pi. s is the secret sharing value, and v2,v3,...vn are the n1 values drawn at random from Zp that create a vector =(s,v2,v3,...vn) with n dimensions; hence, A=(c1,c2,c3,...cn). If Ai is the representative vector for the ith line across matrix A, then the secret sharing value of participant I can be identified as ci=Aiv. Assume that S is an authorised set, is an LSSS for accessing structure A, and SA for linear secret reconstruction. Describe I=i|(i)S. The equation, iIici=s can be obtained if the vector 1,0...,0 is in the range of rows of A indexed by I and a constant iZpiI exists. There aren't any such constants for unauthorised sets.

A. Composite Order Bilinear Groups

Definition 2:

Assume that N=p1p2p3 (p1, p2, p3 are distinct prime numbers), that G and GT are cyclic groups of order N, and that g stands for a generator of G. The composite order bilinear map e: G: G:GT has the following characteristics:

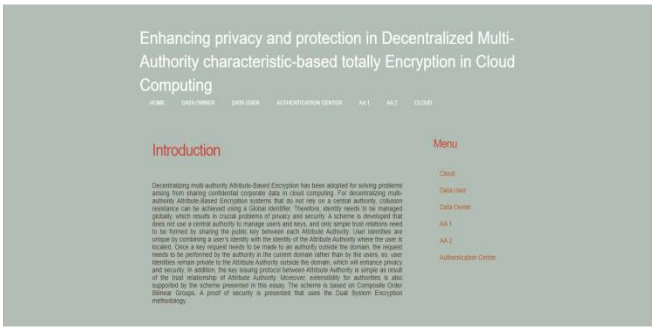
1. Bilinear: ∀a,b∈ZN,e(ga,gb)=e(g,g)ab .
2. Non-degenerate: ∃g∈G such that e(g,g) has order N in GT .
3. Computable: ∀ X, Y∈ZN, the bilinear map e(X,Y) is computable in polynomial time.

We let Gpi denote the subgroups of order pi in G,∀hi∈Gpi and ∀hj∈Gpj and if i≠j , then e(hi,hj)=1

IV. PREVOIUS STUDY

For theChase07 scheme, Chase illustrated a a mechanism for allocating keys and managing attributes via many independent attribute authorities. A message is encrypted in such a way that a user can only decrypt it if he possesses at least dk of the provided qualities from each authority, and those attributes come from several authorities. The Chase07 method, designed to address the decentralising multi-authority ABE collusion resistance problem, is where the Global Identifier (GID) and central authority first appeared. Correct secret splitting among several authorities can be ensured by a reliable central authority, which results in collusion resistance. Furthermore, there is no requirement that each authority establish reliable connections with one another. Each user only has access to the request attributes provided by all authorities, making it possible to retrieve the complete secret value and decrypt the ciphertext. Since users typically have distinct global identities, this was the first time the concept of leveraging GID binding with users' private keys had been presented. The following three points serve as a summary of the drawbacks of the Chase07scheme. First, the central authority must always be able to be trusted. The second is a stable access policy, according to which each user must have access to a fixed number of the attributes that have been approved by the authority. Third, the extensibility is poor, necessitating network-wide key replacement whenever an authority needs to be added. The users' personal GID information must be sent to each authority, which will result in privacy disclosure.

V. RESULTS



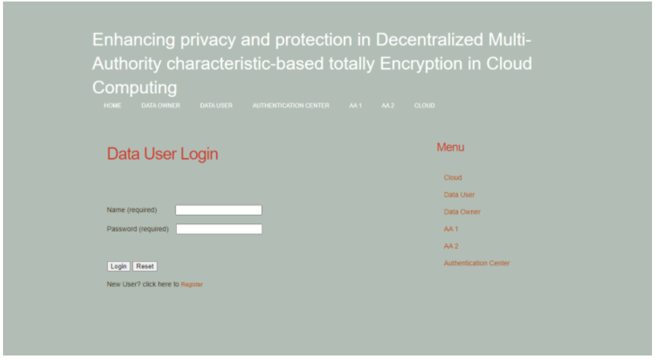
Enhancing privacy and protection in Decentralized Multi-Authority characteristic-based totally Encryption in Cloud Computing

Introduction

Decentralizing multi-authority Attribute-Based Encryption has been adopted for solving problems arising from sharing confidential corporate data in cloud computing. For decentralizing multi-authority Attribute-Based Encryption systems that do not rely on a central authority, collusion resistance can be achieved using a Global Identifier. Therefore, identity needs to be managed globally, which results in crucial problems of privacy and security. A scheme is developed that does not use a central authority to manage users and keys, and only simple trust relations need to be formed by sharing the public key between each Attribute Authority. User identities are unique by combining a user's identity with the identity of the Attribute Authority where the user is located. Once a key request needs to be made to an authority outside the domain, the request needs to be performed by the authority in the current domain rather than by the users, so, user identities remain private to the Attribute Authority outside the domain, which will enhance privacy and security. In addition, the key issuing protocol between Attribute Authority is simple as result of the trust relationship of Attribute Authority. Moreover, extensibility for authorities is also supported by the scheme presented in this essay. The scheme is based on Composite Order Bilinear Groups. A proof of security is presented that uses the Dual System Encryption methodology.

Fig.1. Home page of encryption page

From the above fig we can see the home page that contains introduction of project, data user, data owner, authentation, aa1 aa2, etc.



Enhancing privacy and protection in Decentralized Multi-Authority characteristic-based totally Encryption in Cloud Computing

Data User Login

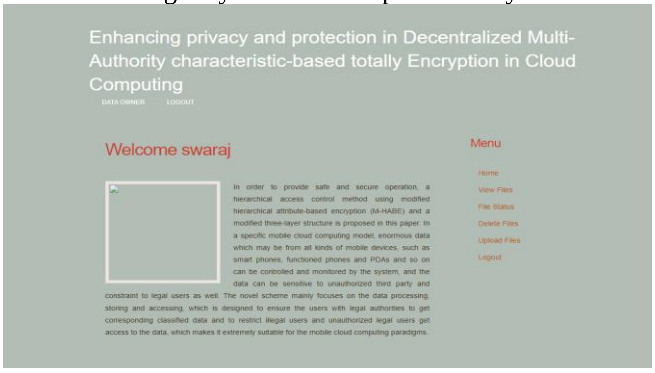
Name (required)

Password (required)

New User? click here to Register

Fig.2. Data User

Here we can login by the data user persons only



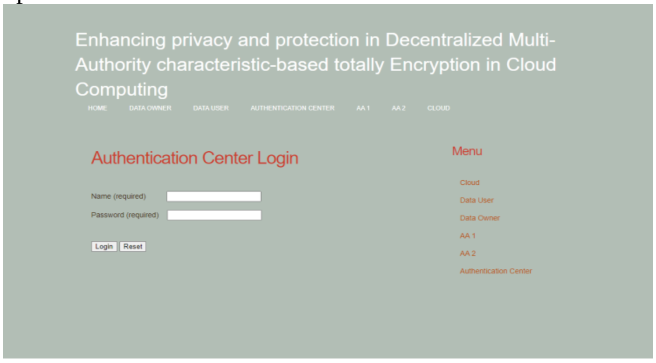
Enhancing privacy and protection in Decentralized Multi-Authority characteristic-based totally Encryption in Cloud Computing

Welcome swaraj

In order to provide safe and secure operation, a hierarchical access control method using modified hierarchical attribute-based encryption (M-HABE) and a modified three-layer structure is proposed in this paper. In a specific mobile cloud computing model, enormous data which may be from all kinds of mobile devices, such as smart phones, functioned phones and PDAs and so on can be controlled and monitored by the system, and the data can be sensitive to unauthorized third party and constraint to legal users as well. The novel scheme mainly focuses on the data processing, storing and accessing, which is designed to ensure the users with legal authorities to get corresponding classified data and to restrict illegal users and unauthorized legal users get access to the data, which makes it extremely suitable for the mobile cloud computing paradigms.

Fig.3. Login page of data owner

Here after the login of data owner page the page will be appeared in this formate here we will have the multiple options as the data owner can do



Enhancing privacy and protection in Decentralized Multi-Authority characteristic-based totally Encryption in Cloud Computing

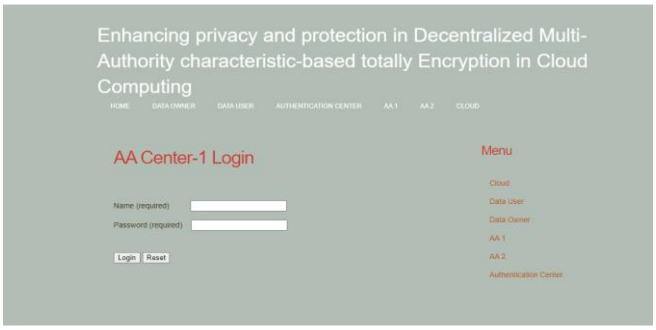
Authentication Center Login

Name (required)

Password (required)

Fig.4. Authentation center Login

Here the only authentication users can login and has multiple option to give the accesss to orginal person followed by AA1 and AA2 Centers



Enhancing privacy and protection in Decentralized Multi-Authority characteristic-based totally Encryption in Cloud Computing

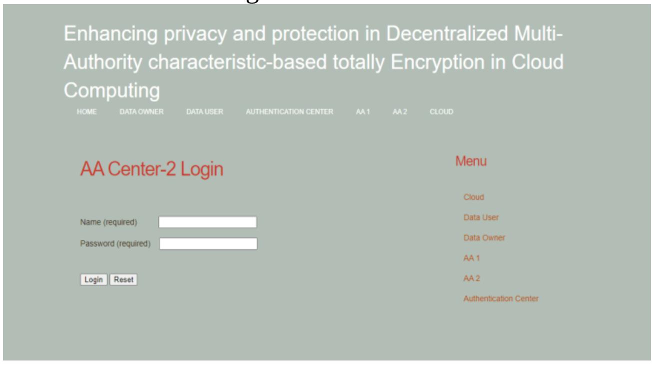
AA Center-1 Login

Name (required)

Password (required)

Fig.5. AA Center-1 Login

The authentication center sends the data to the AA1 center after the review the user then it will be sent to the AA2 after that the access will be given



Enhancing privacy and protection in Decentralized Multi-Authority characteristic-based totally Encryption in Cloud Computing

AA Center-2 Login

Name (required)

Password (required)

Fig.6. AA Center-2 Login

After the all access passed from the authentication center and aa1 then aa2 has rights to check the data is encrypted or not.

VI. CONCLUSION

The Decentralizingmulti-authority ABE can break problems arising from security conditions of participating nonpublic commercial data on pall waiters. For decentralized multi-authority ABE schemes with non-central authority, the conspiracy resistant can be answered using the GID. thus, the oneness of stoner individualities needs to be managed encyclopedically. stoner individualities tend to be unique encyclopedically to achieve conspiracy resistant, but individualities need not be published encyclopedically. sequestration has been enhanced. also, stoner identity operation doesn't need to be offered by affiliated associations.(2) When a stoner requests a stoner trait key from an trait authority outside the sphere, the current authority, not the stoner, performs the task. effectiveness is bettered and stoner sequestration is defended. In addition, the possibility of cheating suffered by druggies is also dropped. Only universal criteria and widely known vital information need to be transferred across trait authority in order to establish confidence. Since each trait authority is responsible for managing its own keys and drug users, the trait authorities can be enlarged as needed. The focus must be on developing a system that combines the scheme proposed in this essay with hierarchicalmulti-authority ABE for unborn work after the trait authorities in each sphere belong to a hierarchicalmulti-authority ABE.

Retrieval Number: 100.1/ijrte.C72780911322
DOI: 10.35940/ijrte.C7278.0911322
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

REFERENCES

1. J. Horwitz,B. Lynn, “Towards hierarchical identity-based encryption,”in Proc. EUROCRYPT, Amsterdam, The Netherlands, April.2002, pp.466-481. [CrossRef]
2. C. Gentry, A. Silverberg, “Hierarchical ID-based cryptography,” in Proc. ASIACRYPT, Singapore, December. 2002, pp. 548-566. [CrossRef]
3. D. Boneh, X. Boyen, “Efficient Selective-ID secure identity based encryption without random oracles,”in Proc .EUROCRYPT, Interlaken, Switzerland, May.2004,pp. 223-238. [CrossRef]
4. D. Boneh, X. Boyen, E. Goh, “Hierarchical identity based encryption with constant size ciphertext,”in Proc. EUROCRYPT, Aarhus, Denmark, May.2005, pp. 440-456. [CrossRef]
5. X. Boyen, B. Waters, “Anonymous hierarchical identity-based encryption(without random oracles),”inProc.CRYPTO, Santa Barbara, California, USA, August.2006, pp. 290-307. [CrossRef]
6. G. Wang, Q. Liu, J. Wu,M. Guo, “Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers,”Computers&security, 30 (5), pp. 320-331, July.2011. [CrossRef]
7. M. Chase, “Multi-authority attribute based encryption,”inProc.TCC, Amsterdam, The Netherlands, February.2007, pp. 515-534. [CrossRef]
8. M. Chase, S. Chow, “Improving privacy and security in multi-authority attribute-based encryption,”inProc.CCS, Chicago, Illinois, USA, November.2009, pp. 121-130. [CrossRef]
9. Y.Rahulamathavan, S.Veluru, J.Han, F.Li, M.Rajarajan and R.Lu, “User Collusion Avoidance Scheme for Privacy-Preserving Decentralized Key-Policy Attribute-Based Encryption,”IEEE Transactions on Computers, 65(9), pp. 2939-2946,September. 2016. [CrossRef]
10. A. BEIMEL, “SECRET-SHARINGSCHEMES: A SURVEY.IN: CODING AND CRYPTOLOGY-THIRD INTERNATIONAL WORKSHOP

AUTHORS PROFILE

G. Swaraj Reddy, Received B.Tech Degree on Computer Science Engineering in CMR Engineering College ,Hyderabad and pursing M.Tech on Computer Science Engineering in CMR Engineering College. My Research interest is on web development, mobile application and Cloud Computing.

Dr. Rajesh Tiwari, Received the Ph.D degree from CSVTU, Bhilai. He has a long years of experience in teaching field .Research areas are parallel computing and its enhancement. His research papers are published in many national and international journals

Mr. Mrutyunjaya S Yalawar, working as Assistant Professor at CMR Engineering College, Medchal, Hyderabad, India and having more than 3 years of experience in IT-Industries as Software Developer and more than 6 years of Experience in Teaching Field. His Research area includes Artificial Intelligence, Machine Learning, NLP, Cyber Security, Blockchain. He published about more than 15 Papers in various National and International Journals.