International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 09 | Sept - 2021 ISSN: 2582-3930

Improving Privacy and Security in Decentralizing Multi-Authority Attribute-Based Encryption in Cloud Computing

Srihari Rao B[1], Dr. P Pedda Sadhu Naik[2]
[1]M. Tech(CSE), [2]Professor & HOD, Dept. of CSE
Dr. Samuel George Institute of Engineering & Technology, Markapur, A.P., India.

ABSTRACT: 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.
Keywords: *Attribute-based encryption, decentralizing multi-authority attribute-based encryption, dual system encryption*.

1. INTRODUCTION

Cloud computing enables users to store their sensitive data into un trusted remotely cloud service providers to achieve scalable services on-demand. Prominent security requirements arising from this means of data storage and management include data security and privacy and require the use of strong encryption techniques with fine-grained access control for data security in cloud computing. Attribute-based Encryption (ABE) is an efficient encryption system with fine-grained access control for encrypting out-sourced data in cloud computing. With the emergence of sharing confidential corporate data on cloud servers, data are generated by several organizations, and access policies can be defined by several authorities. Single-authority ABE cannot meet the demands of decentralized distribution, and decentralizing multi-authority ABE have been proposed to solve those problems.

For basic Identity-based encryption (IBE) and ABE, all private keys are managed by an authorized centre. However, in practice, this will present a performance bottle-neck requiring evaluation due to the huge numbers of requests. In addition, concentrated attacks seem to be more easily from happening. Therefore, Hierarchical IBE (HIBE) [1-7] and Hierarchical ABE (HABE) [8-11] are now being used. HIBE and HABE are also called levelled multi-authority IBE and ABE. According to the main concept, the authorized centre is managed at different levels, and domains or users at higher levels can use their private keys to generate private keys for the domain or users at lower levels. HIBE or HABE, when applied at various levels, can solve the key distribution load problem. Because roots are ultimately trusted sources, authorized centres at each level are based on a single trusted root. In addition, system efficiency can be improved dynamically because

identity authentication and key transmission can be performed locally. In basic ABE systems, the information shared is always within one domain or organization. However, in reality, information such as drivers' licenses and registration information in universities are organized by different government departments. The management of attributes and key distributions cannot be undertaken by the same attribute authority. Moreover, access strategies may be distributed based on attributes of different authorities. Therefore, leveled multi-authority ABE cannot meet distribution demands. Decentralizing multi-authority ABE is used to solve the access problem in which user attributes belong to different authorities.

Those authorities differ from that for a leveled In basic ABE systems, the information shared is always within one domain or organization. However, in reality, information such as drivers' licenses and registration information in universities are organized by different government departments. The management of attributes and key distributions cannot be undertaken by the same attribute authority. Moreover, access strategies may be distributed based on attributes of different authorities. Therefore, levelled multi-authority ABE cannot meet distribution demands. Decentralizing multi-authority ABE is used to solve the access problem in which user attributes belong to different authorities. Those authorities differ from that for a leveled multi-authorized ABE, for which the levelled multi-authority ABE has one trust root. There is no trust between organizations, and attribute management and key distribution always are performed separately from each other. For some specified work reasons such as sharing confidential corporate data on cloud servers, trust relationships can be made between organizations. Single-authority ABE primarily randomizes private keys, and the secret values are separated based on the part in the users' private keys (referring to a different attribute), and decryption is performed by reconstructing the secret values. In Single-authority ABE, each user's keys are generated using different random and secretly shared values such that keys generated for different users cannot be combined, which prevents collusion attacks. For decentralizing multi-authority ABE, the private keys of users can be generated by different authorities that do not communicate. Thus, the crucial technical challenge for decentralizing multi-authority ABE is constructing a secret-sharing value to resist collusion attacks The Global Identifier (GID) and central authority originated to solve the resist collusion attacks.

All early schemes used central authority to deliver secret splitting, thereby assuring collusion resistant under circumstances wherein authorities do not trust one another. However, a central authority should be globally trustworthy. Therefore, in order to avoid the security weaknesses resulting from the use of central authorities, schemes that do not employ central authorities have been published. There is no reliance on single trust centres, and although each authority distributes its own attributes and keys, they still need common support parameters for distribution by related organizations, or complicated trust relationships need to be formed between each authority. User's GID is published globally in early schemes will breach the user privacy. In order to solve the question, some schemes used anonymous key issuing protocol to enhance user privacy, but the protocols usually are complex.

2. EXISTINGSYSTEM

For theChase07 scheme [14],Chaseillustrated a method that allows multi-independent attribute authorities to manage attributes and distribute keys. A message is encrypted such that a user can only decrypt it if he has at least dk of the given attributes from each authority $k$and those attributes belong to different authorities. The Global Identifier (GID) and central authority originated in the Chase07 scheme to solve the decentralizing multi-authority ABE collusion resistant problem. A trustable central authority can ensure correct secret splitting among different authorities, which leads to collusion resistant. Moreover, trustable relationships do not need to be made between each authority. Each user only has the request attributes offered by all

authorities; therefore, the entire secret value can be obtained, and the ciphertext can be decrypted. This was the first presentation of the idea of using GID binding with users' private keys, and the user tends to be unique globally. The disadvantages of the Chase07scheme can be summarized by the following three points. First, the central authority needs to be trustable under all circumstances. Second, there is a stable access policy whereby each user needs to be offered a constant number of the attributes that are authorized by the authority. Third, the extensibility is weak, and once an authority needs to be added, the keys need to be replaced throughout the entire network. Lastly, users need to submit their own GID information to each authority will cause privacy disclosure.

Müller,Katzenbeisser, and Eckert offered a different system with a centralized authority that realizes any LSSS access structure in the Müller-Katzenbeisserscheme[15]. Unlike the Chase07 scheme, the central authority here is mainly used to generate the public and private keys for each user and bind those keys to the identities of the users. For decryption, privatekeys and secret attribute keys are needed. A user's private key is generated by a central authority that is unique within the network, which ensures that the attributes are related to the same user. Thus, the full process of decryption can be performed. In addition, the collusion resistance problem can be solved for each user, who applies a different relativesecretattribute key from the authority.

3. PROPOSED SYSTEM

The proposed scheme is a decentralized multi-authority ABE that will dynamically enhance privacy and security. Acentral authority is not relied on to manage users and keys. Our scheme offers some improvements bycombining a user's identity with the identity of the Attribute Authority (AA) where the user is located. This leads to unique user identifiers globally, and the problem of collusion resistance is also solved. In addition, user identity management does not require support from a new management organization. In our scheme, when the user requests an attribute secret key, if the attributes are located outside the domain, the request by the source AA in the domain to the target AA is used rather than by requests by usersthemselves.So, user identities remain private to the AAs outside the domain, thus avoiding privacy disclosure. The key issuing protocol between AAs is simple as result of the trust relationship of AAs. On the other hand, using the AA instead of users to initialize attribute requests can greatly improve efficiency and security. In addition, some simple parameter exchanges only occur at the very early stage of the construction of each attribute authority.The trust relationship can also only be made by sharing the public key between each AA.User management and key distribution are conducted by the AA within the domain, and, therefore, the dynamic joining of AA is supported in our scheme. Dual system encryption has been used to test the security of our scheme.

4. IMPLEMENTATION

DATA OWNER

In this module, data owner has to register to Authentication Center and Authentication Center checks and authorizes the data owner login . Data owner browse the file , encrypt and upload file with its mac. Once uploaded the file all the authentication center must provide the storage access for the file store on the cloud. Data owner can also delete the file after the uploading of the file to the cloud.

Authentication Center

In this module Authentication Center checks user &owner login and authorizes the registration. Authentication center list all other sub-authentication centers and provide authorization (Activate OR Deactivate). Authentication center provides the storage access to cloud for every file uploaded by the data owner.

AA 1: In this module the AA1 shows all the private key requests from the users and generates. And also provides the storage access for the file uploaded by the data owner.

AA 2: In this module the AA2 shows all the public key requests from the users and generates. And also provides the storage access for the file uploaded by the data owner.

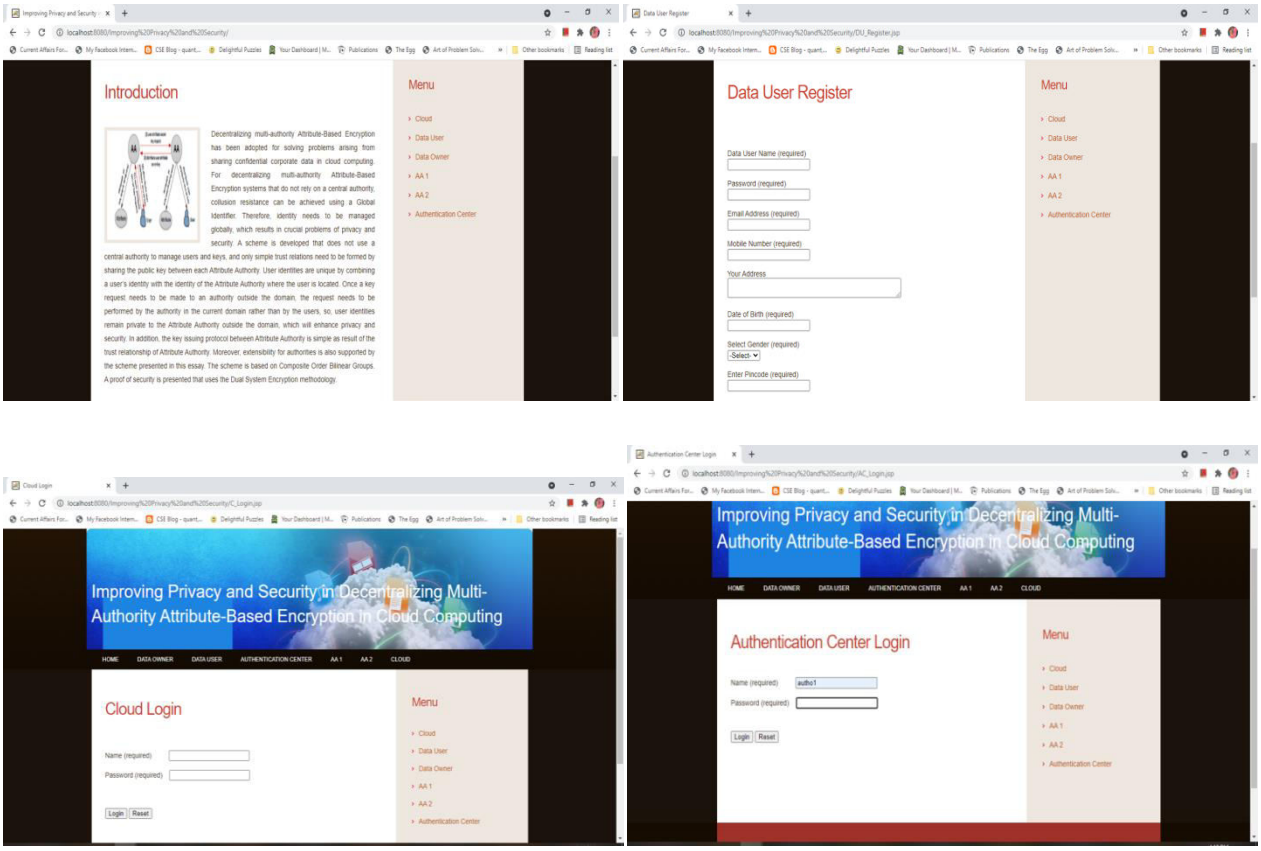
Cloud Server

Receive all files from the data owner and store all files, user details. Provide files to end user after verifying Private key and secret key provided by the authentication center. Maintain file transaction details and forward the file download request from the user to the authentication centre.

End User (Receiver)

In this module end user has to register and login, and the user is authorized by the authentication center, user will request private key from the AA1 and the secret key from the AA2 to download the file from cloud server.

5. OUTPUT TEST SCREENS



6. CONCLUSIONS

Decentralizing multi-authority ABE can solve problems arising from security requirements of sharing confidential corporate data on cloud servers. For decentralized multi-authority ABE schemes with non-central authority, the collusion resistant can be solved using the GID. Therefore, the uniqueness of user identities

needs to be managed globally, which results in crucial problems of privacy and security. In this essay, a scheme without a central authority to manage keys and users has been proposed, and privacy and security have been enhanced dynamically. (1) User identities tend to be unique globally to achieve collusion resistant, but identities need not be published globally. Privacy has been enhanced. Moreover, user identity management does not need to be offered by related organizations.(2) When a user requests a user attribute key from an attribute authority outside the domain, the current authority, not the user, performs the task. Efficiency is improved and user privacy is protected. In addition, the possibility of cheating suffered by users is also decreased. (3) To build trust relations, only global parameters and public key information need to be swapped between attribute authorities. (4) Each attribute authority manages its own keys and users, and the attribute authorities therefore can be flexibly expanded.For future work, once the attribute authorities in each domain belong to a hierarchical multi-authority ABE, the focus must be on devising a method that combines the scheme designed in this essay with hierarchical multi-authority ABE.

REFERENCES

[1]J. Horwitz,B. Lynn, "Towards hierarchicalidentity-based encryption,"inProc.EUROCRYPT, Amsterdam, The Netherlands, April.2002, pp.466-481.
[2]C. Gentry, A. Silverberg, "Hierarchical ID-based cryptography,"inProc.ASIACRYPT, Singapore, December. 2002, pp. 548-566.
[3]D. Boneh, X. Boyen, "Efficient Selective-ID secure identity based encryption without random oracles,"inProc.EUROCRYPT, Interlaken, Switzerland, May.2004,pp. 223-238.
[4]D. Boneh, X. Boyen, E. Goh, "Hierarchical identity based encryption with constant size ciphertext,"inProc.EUROCRYPT, Aarhus, Denmark, May.2005, pp. 440-456.
[5]X. Boyen, B. Waters, "Anonymous hierarchical identity-based encryption(without random oracles),"inProc.CRYPTO, Santa Barbara, California, USA, August.2006, pp. 290-307.
[6]B. Waters, "Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions,"inProc.CRYPTO,Santa Barbara, CA,August. 2009, pp.619-636.
[7]A. Lewko, B. Waters, "New techniques for dual system encryption and fully secure HIBE with short ciphertexts,"inProc.TCC,Zurich, Switzerland, February.2010, pp. 455-579.
[8]G. Wang, Q. Liu, J. Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services,"inProc.CCS, Chicago,Illinois, USA, October.2010, pp. 735-737.
[9] 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.
[10]Zhiguo Wan, Jun'e Liu, Robert H. Deng, "HASBE: A Hierarchical attribute-based solution for flexible and scalable access control in cloud computing,"IEEE Transactions on Information Forensics and Security, 7(2),pp. 743-753, April.2012.
[11] Q. Huang, L.Wang, Y.Yang, "DECENT: Secure and fine-grained data access controlwith policy updating for constrained IoTdevices,"World Wide Web, 2017 (11), pp. 1-17, 2017.
[12]A. Beimel, "Secure Schemes for secret sharing and key distribution[Ph.D. Thesis],"Haifa: Israel Institute of Technology, 1996.
[13]D. Boneh, E. Goh, K. Nissim, "Evaluating 2-dnf formulas on ciphertexts,"inProc.TCC,Cambridge, MA, USA, February.2005, pp.325-341.
[14]M. Chase, "Multi-authority attribute based encryption,"inProc.TCC, Amsterdam, The Netherlands, February.2007, pp. 515-534.

[15]S. Müller, S. Katzenbeisser, C. Eckert,"Distributed attribute-based encryption,"inProc.ICISC, Seoul, Korea, December. 2008,pp. 20-36.
[16]A. Lewko, B.Waters, "Decentralizing attribute-based encryption,"inProc.EUROCRYPT, Tallinn, Estonia, May. 2011, pp.568-588.
[17]H. Lin, Z. Cao, X. Liang, J. Shao, "Secure threshold multi authority attribute based encryption without a central authority,"inProc.INDOCRYPT[18]M. Chase, S. Chow, "Improving privacy and security in multi-authority attribute-based encryption,"inProc.CCS, Chicago, Illinois, USA, November.2009, pp. 121-130.
[19]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.
[20]A. Lewko, T. Okamoto, A. Sahai, K. Takashima, B. Waters, "Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption,"inProc.EUROCRYPT, Monaco and Nice, France,May.2010, pp.62-91.
[21]A. Beimel, "Secret-sharingschemes: A Survey.In: Coding and Cryptology-Third International Workshop