IJIEMR Transactions, online available on 7th Mar 2018. Link :http://www.ijiemr.org/downloads.php?vol=Volume-08&issue=ISSUE-03

Title: **M-HABE ACCESS CONTROL MECHANISM FOR RESTRICTING UN-AUTHORIZED ACCESS CONTROL IN CLOUD**

Volume 08, Issue 03, Pages: 104–108.

Paper Authors

MR.C.RAVI KISHORE REDDY, U.DURGA RANI

Vignan's Lara Institute of Technology & Science

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

M-HABE ACCESS CONTROL MECHANISM FOR RESTRICTING UN-AUTHORIZED ACCESS CONTROL IN CLOUD

MR.C.RAVI KISHORE REDDY[1], U.DURGA RANI[2]

Assistant Professor[1], Department of M.C.A, Vignan's Lara Institute of Technology & Science
M.C.A Student[2],Department of M.C.A Vignan's Lara Institute of Technology & Science

Abstract:

The Cloud computing is an Internet-based computing pattern through which shared resources are provided to devices on demand. The cloud computing is used to stored the data for the future use.It's an emerging but promising paradigm to integrating mobile devices into cloud computing.The integration performs in the cloud based hierarchical multi-user data-shared environment. With integrating into cloud computing, security issues such as data confidentiality and user authority may arise in the mobile cloud computing system. In cloud computing system the hierarchical model is used for the data sharing process. The hierarchical model is used to set the priority for each user depends their accessibility. A Modified Hierarchical Attribute-Based Encryption Access Control Method for Mobile Cloud Computing" application is used to encrypt the information and set the key for decrypt the data.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 this (M-HABE) method the Access control is set for the data, and priority is assign for the each user. High priority person only access the data, low priority user cannot access the data and done data sharing.

EXISTING SYSTEM:

In existing system the data is shared from one device to another is the difficult problem.the data may be losed while transferring is happens, In existing system the security purpose is not enhance for the data.so the data is hacked by anyone. Maintaining data is the difficult job. Anyone can get the data. The user cannot get the data from anywhere at anytime.so the timing consumption problem may be occur. These are the main issues in the existing system.

DISADVANTAGE:

- Timing consumption is high
- No security for the data
- Data losing may be happen
- Data transferring is difficult

PROPOSED SYSTEM:

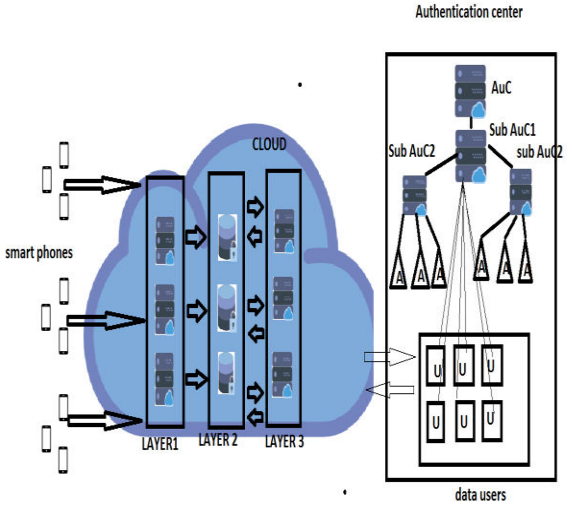
In proposed system the user can stored his data to the cloud, the user can get the data from anywhere at any time. In cloud computing process the security purpose is enhance for the data.Cloud providers are supposed to guarantee to consumers that they can get and use their data at any places and any time.Consumers' data should be kept secret in cloud systems.The data stored in cloud systems need a mechanism to ensure their data not lost or modified by unauthorized users. A secure control system

distributes appropriate resources to be utilized in
Different occasions.

ADVANTAGES:

- **Availability**- Cloud providers should offer services that consumers could get and use at any places and any time.
- **Confidentiality**-Consumers' data should be kept secret in cloud systems
- **Data integrity**-The data stored in cloud systems need a mechanism to ensure their data not lost or modified by unauthorized users.
- **Control**-A secure control system distributes appropriate resources to beUtilized in different occasions.

ARCHITECTURE:



MODULE DESCRIPTION

MODULES:

- Upload & View data module
- Data encryption &decryption module
- Data sharing module
- User priority module

UPLOAD & VIEW DATA MODULE:

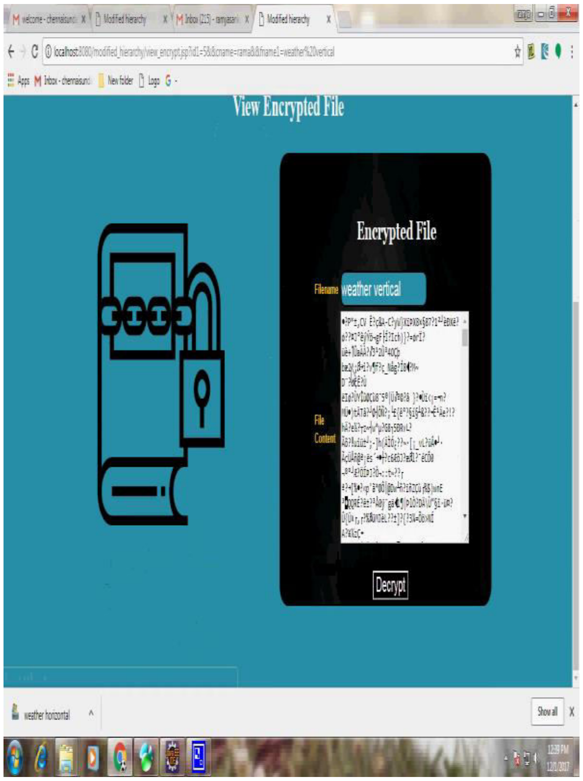
- In user side the user upload his data to the mobile cloud computing in level 1 cloud server.
- In level 2 the admin get the data and make encryption for this data and stored it in the classified cloud data.
- The other user wants to access the data. They have access permission from admin.if the user is the authorized person identified by the priority of the user.
- High priority user can access the data from cloud server.
- The admin generate key for the user and send it to the mailid.the user use the key to access the data.this is the level 3 process.

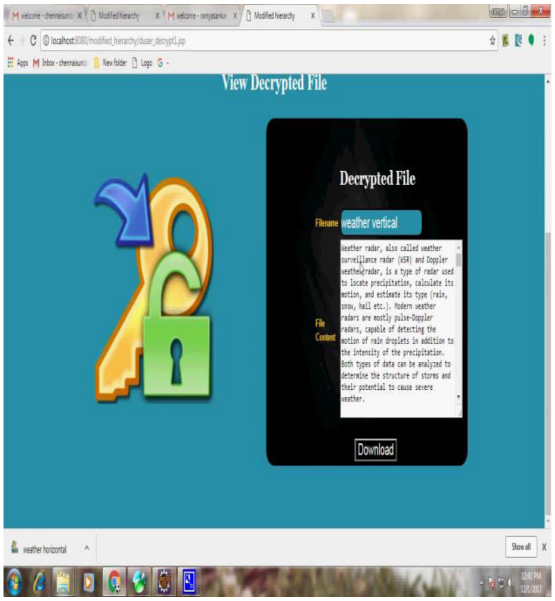
DATA ENCRYPTION & DECRYPTION:

- The user stored the data to the cloud server, the admin encrypt the data in the level 2 process. After encrypt the data they can stored the classified stored data.
- After encrypt the data the admin generate the key for decrypt the data. Theuser wants to access the data they have access permission from admin.
- The admin analyzing the priority of the user, after analyzing the priority the admin send the key to the user through mailid.
- The user can use the generated key to decrypt the data and access the data sharing.

Algorithm Implementation

- **RSA algorithm**
- Setup: Given a security parameter K that is huge enough, AUC will generate a system parameter params and a root master key MK0.
- CreateMK: Using system parameter params and their own master keys, AUC or Sub-AuCs can create master keys for lower-level Sub-AuCs.
- CreateSK: With its own master key MK——————————————— and system parameter params, Sub-AuC1 creates secret key SKu for each consumer if it is sure that the public key of the user is PKu, or there would be no secret key for the user.
- CreateUser: Sub-AuCs will create users' secret identity keys SKi;u and secret attribute keys SKi;u;a for them if the Aub- AuC makes sure that the attribute a is in charge of it and the user u satisfies a. And if not there would be no secret identity keys or secret attribute keys.
- Encrypt: With R denoting a set of users' IDs, A representing the attribute-based access structure, the pubic keys of all the users that are in R, and the public keys of all the attributes that are in A, the data provider, which is also a data user of the cloud computing in this case, can encrypt the sensing data D into ciphertext C.
- RDcrypt: Given the ciphertext C, a data user possessing the precise ID that is in R can decrypt the ciphertext C into plaintext D with params and the user's secret key SKu.
- ADcrypt: Given the ciphertext C, a data user possessing an attribute set fag that satisfies A, which means that the consumer owns at least an attribute key SKi;u;a, can also decrypt the ciphertext C into plaintext D with system parameter params, the user's secret identity key SKi;u, and the secret attribute key SKi;u;a.





View Decrypted File

Decrypted File

Filename: weather vertical

File Content: Weather radar, also called weather surveillance radar (WSR) and Doppler weather radar, is a type of radar used to locate precipitation, calculate its motion, and estimate its type (rain, snow, hail etc.). Modern weather radars are mostly pulse-Doppler radars, capable of detecting the motion of rain droplets in addition to the intensity of the precipitation. Both types of data can be analyzed to determine the structure of storms and their potential to cause severe weather.

Download

CONCLUSION

The paper proposed a modified HABE scheme by takingadvantages of attributes based encryption (ABE) and hierarchical identity based encryption (HIBE) access control processing. The proposed access control method using MHABE is designed to be utilized within a hierarchical multiuser data-shared environment, which is extremely suitable for a mobile cloud computing model to protect the data privacyand defend unauthorized access. Compared with the original HABE scheme, the novel scheme can be more adaptive for mobile cloud computing environment to process, store and access the enormous data and files while the novel system can let different privilege entities access their permitted data and files. The scheme not only accomplishes the hierarchical access control of mobile sensing data in the mobile cloud computing model, but protects the data from being obtained by an untrusted third party.

References

[1] N. Fernando, S. W. Loke, and W. Rahayu, “Mobile cloud computing:A survey,” Future Generation Computer Systems, vol. 29, no. 1, pp. 84–106, 2013.

[2] S. Abolfazli, Z. Sanaei, E. Ahmed, A. Gani, and R. Buyya, “Cloudbased augmentation for mobile devices: motivation, taxonomies, and open challenges,” Communications Surveys & Tutorials, IEEE, vol. 16, no. 1, pp. 337–368, 2014.

[3] R. Kumar and S. Rajalakshmi, “Mobile cloud computing: Standard approach to protecting and securing of mobile cloud ecosystems,” in Computer Sciences and Applications (CSA), 2013 International Conference on. IEEE, 2013, pp. 663–669.

[4] J. Carolan, S. Gaede, J. Baty, G. Brunette, A. Licht, J. Remmell,L. Tucker, and J. Weise, “Introduction to cloud computing architecture,”White Paper, 1st edn. Sun Micro Systems Inc, 2009.

[5] E. E. Marinelli, “Hyrax: cloud computing on mobile devices using mapreduce,” DTIC Document, Tech. Rep., 2009.

[6] Q. Han, S. Liang, and H. Zhang, “Mobile cloud sensing, big data, and 5g networks make an intelligent and smart world,” Network, IEEE, vol. 29,no. 2, pp. 40–45, 2015.

[7] I. Stojmenovic, “Access control in distributed systems: Merging theory with practice,” in Trust, Security and Privacy in Computing and

Communications(TrustCom), 2011 IEEE 10th International Conference on.IEEE, 2011, pp. 1–2.

[8] G. Wang, Q. Liu, and J. Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services," in Proceedings of the 17th ACM conference on Computer and communications security. ACM, 2010, pp. 735–737.

[9] C. Gentry and A. Silverberg, "Hierarchical id-based cryptography," in Advances in cryptologyASIACRYPT 2002. Springer, 2002, pp. 548–566.

[10] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in Security and Privacy, 2007. SP'07. IEEE Symposium on. IEEE, 2007, pp. 321–334.