Hierarchical Access Control for Multi Users based on Hybrid Encryption in Mobile Cloud Computing

Satish
M.Tech (IT), Dept of ISE
SDM College of Engineering
& Technology, Dharwad
Karnataka, India.

Dr. S. R. Biradar
Dept. of ISE
SDM College of Engineering
& Technology, Dharwad
Karnataka, India.

Abstract:- **The mobile devices and applications need is that mobile-Internet can provide them with the service which is user-friendly, high speed, and steady. In addition, the security issues of mobile terminals and the Internet access are attached importance to. And as a combination of cloud computing, mobile devices and wireless networks, mobile cloud computing is an emerging but very promising paradigm which brings rich computational resources to mobile users, network operators, as well as cloud computing providers. Cloud computing is an Internet-based computing pattern through which shared resources are provided to devices on demand. It's an emerging but promising paradigm to integrating mobile devices into cloud computing, and 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, and it is concerned as the main constraints to the developments of mobile cloud computing.**

1. INTRODUCTION

With explosive growth of mobile devices including smart phones, PDAs, and tablet computers and the applications installed in them, the mobile-Internet will maintain the development growth trend as 4G communication network is extensively promoted to our lives. What users of the mobile devices and applications need is that mobile-Internet can provide them with the service which is user-friendly, high-speed, and steady. In addition, the security issues of mobile terminals and the Internet access are attached importance to. And as a combination of cloud computing, mobile devices and wireless networks, mobile cloud computing is an emerging but very promising paradigm which brings rich computational resources to mobile users, network operators, as well as cloud computing providers.

2. LITERATURE SURVEY

2.1 S. Abolfazli, Z. Sanaei, E. Ahmed, A. Gani, and R. Buyya

The paper "Cloud based augmentation for mobile devices: motivation, taxonomies, and open challenges," the effects of remote resources on the quality and reliability of augmentation processes and discuss the challenges and opportunities of employing varied cloud-based resources in augmenting mobile devices. We present augmentation definition, motivation, and taxonomy of augmentation types, including traditional and cloud-based.

We critically analyze the state-of-the-art CMA (Cloud-based Mobile Augmentation) approaches and classify them into four groups of distant fixed, proximate fixed, proximate mobile, and hybrid to present taxonomy. Vital decision making and performance limitation factors that influence on the adoption of CMA approaches are introduced and an exemplary decision making flowchart for future CMA approaches are presented. Impacts of CMA approaches on mobile computing is discussed and open challenges are presented as the future research directions.

2.2 N. Fernando, S. W. Loke, and W. Rahayu

The paper "Mobile cloud computing: A survey," Future Generation Computer Systems. The resource demands of specific services develop as well along with the increase of mobile. Nonetheless, mobile certainly will often be restricted performance that is regarding computation, storage, battery life, context adaptation of connectivity, scalability, and heterogeneity included security issue. An outstanding solution to address these limitations is definitely to offload computation is mobile cloud computing (MCC).

However, present approaches don't address the complexity which results from quickly and context that is constantly changing in mobile user scenarios and accordingly developing effective and efficient MCC applications continues to be demanding. Consequently, this paper demonstrates a summary of demands for MCC applications along with a classification of present solutions. Additionally, it brings a design lead to the collection of appropriate concepts for various classes of common applications which are cloud augmented tend to be mobile. Finally, we offer open issues that guideline to researchers take into consideration when designing MCC.

3. EXISTING SYSTEM

The public key of a user is described by a set of IDs composed of the public key of father node and the users own ID in the method of G-HIBE, the most important feature of is that the users public key could reflect precise position of the user in the hierarchical structure. The higher hierarchical position of the system could create private keys for lower position users with his/her private keys. The

public key of a user is described by a set of IDs composed of the public key of father node and the users own ID in the method. The most important feature of is that the users public key could reflect precise position of the user in the hierarchical structure. Attribute based encryption (ABE) is regarded access structure bringing into the cipher text or private key, the access structure determines what cipher text can be obtained by which users. Each data user possesses a unique ID which is a character string designed to describe the features of internal parties within the system, and so do (authentication center)AuC, Sub-AuCs, and users attributes, especially, the ID of each user contains an integer for describing the privilege level of the user. Additionally, data users also own a set of attributes while other internal parties do not.

4. PROPOSED SYSTEM

The paper proposed a modified HABE scheme by taking advantages 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 privacy and 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 un trusted third party.

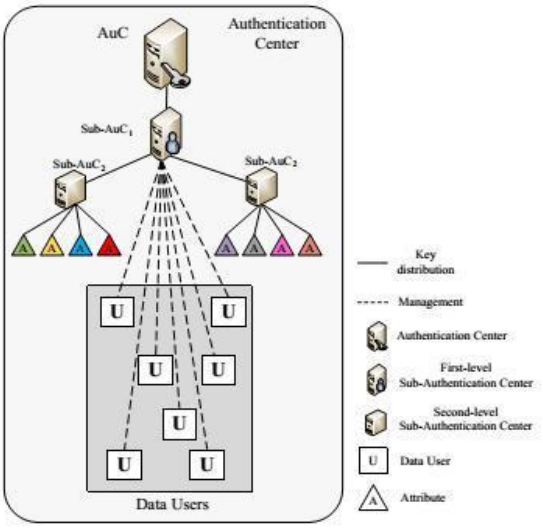

Fig: Hierarchical Access Control Model

5. ADVANTAGES

5.1 Protect the data privacy.

5.2 Defend unauthorized access.

5.3 We can process, store and access the enormous data.

5.4 Protect the data from being obtained by an untrusted third party.

6. CONCLUSION

We proposed a modified HABE scheme by taking advantages 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 privacy and 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.

7. REFERENCES

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

[2] 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.

[3] 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.

[4] A. Shamir, "Identity-based cryptosystems and signature schemes," in Advances in cryptology. Springer, 1985, pp. 47–53.

[5] M. Zhou, R. Zhang, W. Xie, W. Qian, and A. Zhou, "Security and privacy in cloud computing: A survey," in Semantics Knowledge and Grid (SKG), 2010 Sixth International Conference on. IEEE, 2010, pp. 105–112.

[6] B. R. Moyers, J. P. Dunning, R. C. Marchany, and J. G. Tront, "Effects of wi-fi and Bluetooth battery exhaustion attacks on mobile devices," in System Sciences (HICSS), 2010 43rd Hawaii International Conference on. IEEE, 2010, pp. 1–9.

[7] W. Zhang, Y. Wen, and H.-H. Chen, "Toward transcoding as a service: energy-efficient offloading policy for green mobile cloud," Network, IEEE, vol. 28, no. 6, pp. 67–73, 2014. E. E. Marinelli, "Hyrax: cloud computing on mobile devices using map reduce," DTIC Document, Tech. Rep., 2009.

[8] 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.

[9] 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.

[10] 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.