Asia-pacific Journal of Convergent Research Interchange
Vol.2, No.1, March 31 (2016), pp. 13-19
http://dx.doi.org/10.21742/apjcri.2016.03.03

Proposal for Advanced Attribute-based Encryption in Mobile Cloud Computing

Jung Hyun Kim[1)]

Abstract

Cloud computing is an Internet-based computing design through which shared resources are given to gadgets on request. Its a rising yet encouraging worldview to incorporating cell phones into distributed computing, and the reconciliation performs in the cloud based progressive multi-client information shared environment. With coordinating into distributed computing, security issues, for example, information privacy and user authority may arise in the mobile cloud computing system, and it is worried as the fundamental requirements to the advancements of portable distributed computing. With a specific end goal to give protected and secure operation, a progressive get to control technique utilizing altered various leveled trait based encryption (M-HABE) and a changed three-layer structure is proposed in this paper. In a particular portable distributed computing model, colossal information which might be from a wide range of cell phones, for example, advanced cells, worked telephones and PDAs thus on can be controlled and observed by the system, and the information can be touchy to unapproved outsider and imperative to legitimate clients too. The novel plan fundamentally concentrates on the information handling, putting away and getting to, which is intended to guarantee the clients with lawful experts to get relating characterized information and to confine unlawful clients and unapproved legitimate clients access the information, which makes it to a great degree appropriate for the mobile cloud computing paradigms..

Keywords : mobile, cloud computing, M-HABE, access control, attribute-based encryption.

1. Introduction

With explosive growth of mobile devices including advanced mobile phones, PDAs, and tablet PCs and the applications introduced in them, the versatile Internet will keep up the improvement development incline as 4G correspondence system is widely elevated to our lives[1-5]. What clients of the cell phones and applications need is that portable Internet can furnish them with the administration which is easy to understand, highspeed, and enduring. Likewise, the security issues of portable terminals and the Internet get to are joined significance to[6-7]. What's more, as a mix of distributed computing, cell phones and remote systems, versatile distributed computing is a rising yet extremely encouraging worldview which conveys

Received(November 17, 2015), Review Result(1st: November 20, 2015, 2nd: December 8, 2015), Accepted(December 10, 2015)

[1](Corresponding Author) Conversing Technology, Hoseo Graduate School of Venture, Seoul
email: hyun2@hanmail.net

ISSN: 2508-9080 APJCRI

rich computational assets to portable clients, arrange administrators, and also distributed computing suppliers[8-11]. The flaws of data storing and data computing in mobile-Internet applications can be overcome by mobile cloud computing while the new worldview can likewise finish cloud based multi-client information sharing, end geographical service limitation, and process real-time tasks proficiently in the meantime[12-15].

There is no precise meaning of portable distributed computing, a few ideas were proposed, and two most prevalent plans can be depicted as takes after:

1. Mobile cloud computing is a sort of plan which could run an application, for example, a climate screen application on remote cloud servers as showed in Figure 1, while the cell phones simply act like ordinary PCs with the exception of that the cell phones interface with cloud servers by means of 3G or 4G while PCs through Internet. What's more, this idea is considered as the most prominent meaning of versatile distributed computing[4].

2. Taking focal points of recreation assets, for example, CPU, memory, and putting away plates, another model of versatile distributed computing misuses the cell phones themselves as assets suppliers of cloud[5]. What's more, the plan underpins client versatility, and perceives the capability of portable mists to do aggregate detecting too.

In this paper, authors for the most part utilize the main worldview said above, however the second one rouses us to expect that imagine a scenario where the cell phones don't give figuring assets or putting away assets yet detecting information. Truth be told, most cell phones are competent to catch a few information from the earth these days, for instance, practically every PDA are outfitted with sensors of proximity, accelerometer, gyroscope, compass, barometer, camera, GPS, microphone[6], etc. Combining the idea of WSN, cell phones can be viewed as portable sensors that can give other cell phones who are clients of the versatile cloud administrations with some sensing information including environment monitoring data, health monitoring data, and so on.

2. Proposed System

2.1 Related Works

2.1.1 Hierarchical identity-based encryption

The idea of Identity Based Encryption (IBE) was proposed by Shamir[11] first in 1984, varying from traditional symmetrical encryption system, IBE took subjective character strings that can speak to the personalities of clients, for example, ID numbers, email addresses, as open keys to scramble information[16-18]. One favorable position of IBE is that the sender didn't need to look people in general keys data on declaration specialist (CA) on the web, which tackled the issue of poor CA execution[19-22]. The lack of IBE framework was that all clients keys were created by the private key era (PKG), which would turn into the bottleneck in the framework.

Horwitz [23-26] proposed the possibility of various leveled IBE (HIBE) in 2002, a client in the higher progressive position of the system could make private keys for lower position clients with his/her private keys. Which imply that exclusive the main level clients private keys need be made by PKG, while bring down level clients private keys could be created and overseen by their progenitors. This enhanced system eased PKG of incredible weight and improved the system proficiency by confirming personalities and transporting keys inside region range rather than worldwide zone.

People in general key of a client is depicted by an arrangement of IDs made out of the general population key of father hub and the clients claim ID in the technique for G-HIBE [9], the most imperative component of the proposition is that the clients open key could reflect exact position of the client in the hierarchical structure.

2.2.2 Ciphertext-policy attribute-based encryption

Characteristic based encryption (ABE) [24] is viewed as the IBE technique with a get to structure bringing into the ciphertext or private key, the access structure figures out what ciphertext can be acquired by which clients. Two major branches of ABE system are key-approach ABE (KP-ABE) [24] and ciphertext-strategy ABE (CP-ABE) [10], the later one is used in numerous standards including this proposed paper. The get to structure specified above in CP-ABE is put in ciphertext, which implies that the information sender can be initiative to the point that he/she can decide the beneficiary. Clients are depicted by an arrangement of properties in CP-ABE, just when the quality set fulfills the get to structure can the client gets the ciphertext.

The core of the proposed plan is called changed various leveled characteristic based

encryption (M-HABE), which is not quite the same as the HABE scheme. HABE was proposed in light of G-HIBE [9] and CP-ABE [10] by Wang [8] in 2010, it was composed essentially for the use inside a venture. We altered the proposition to adjust the situations of portable distributed computing framework, which could be delineated as figure 2, with the point of making it suit to the system in light of mobile cloud computing.

2.3 Existing System

Senders encrypt message with specific properties of the approved collectors. The ABE based get to control technique utilizes a few labels to stamp the characteristics that a particular approved client needs to have. The clients with certain label sets can access the particular encrypted data and decrypt it.

Lots of paper presented the plan about the characteristic based encryption get to control strategy in the distributed computing. In the portable uproarious registering environment, there are enormous information which should be prepared and set apart with attributions for the helpful crediting access before putting away. In the meantime, the various leveled structure of the application clients require a confirmation focus substance to control their attributes.

2.4 Disadvantages in Existing System

- Does not guarantee Availability
- Issues of Confidentiality. Consumers' data were not kept secret in cloud systems
- Data Integrity Issue
- No Multiple Controls

2.5 Proposed System

In the proposed scenario, clients with various benefit levels have diverse rights to get to the piece of detecting information originating from the cell phones. In this way, one same information must be scrambled into ciphertext once, which should have the capacity to be unscrambled numerous circumstances by various approved clients.

In this paper, a various leveled get to control strategy utilizing a changed progressive trait based encryption (M-HABE) and an altered three-layer structure is proposed.

Differing from the existing paradigms such as the HABE algorithm and the first three-layer

structure, the novel plan basically concentrates on the information preparing, putting away and getting to, which is intended to guarantee the application clients with legitimate get to specialists to get comparing detecting information and to confine unlawful clients and unapproved lawful clients access the information, the proposed promising worldview makes it amazingly reasonable for the versatile distributed computing based worldview.

What ought to be accentuated is that the most critical highlight of all in the proposed paper can be portrayed as that the altered three-layer structure is intended for illuminating the security issues illustrated previously.

2.6 Summary: Advantages of Proposed System

(1) One ciphertext can be decrypted by several keys.

(2) Both precise level description and user attribute should be supported in the access structure of the method.

(3) The keys in the authentication center ought to have the same hierarchical structure just as the structure of users privilege levels.

3. Conclusion

The paper proposed a modified HABE scheme by taking focal points of attributes based encryption (ABE) and hierarchial identity based encryption (HIBE) access control handling. The proposed get to control strategy utilizing MHABE is intended to be used inside a hierarchial multiuser information shared environment, which is extremely suitable for a mobile cloud computing model to secure the information protection and safeguard unapproved get to. Contrasted and the first HABE plot, the novel plan can be more versatile for portable distributed computing environment to process, store and get to the colossal information and documents while the novel framework can give distinctive benefit substances a chance to get to their allowed information and records. The plan not just fulfills the various leveled get to control of versatile detecting information in the portable distributed computing model, yet shields the information from being gotten by an untrusted third party.

ISSN: 2508-9080 APJCRI

References

[1] N. Fernando, S. W. Loke, and W. Rahayu, Mobile cloud computing:A survey, Future Generation Computer Systems, **(2013)**, Vol.29, No.1, pp.84-106.

[2] S. Abolfazli, Z. Sanaei, E. Ahmed, A. Gani and R. Buyya, Cloudbasedaugmentation for mobile devices: motivation, taxonomies, andopen challenges, Communications Surveys & Tutorials, IEEE, **(2014)**, Vol.16, No.1, pp.337 – 368**.**

[3] R. Kumar and S. Rajalakshmi, Mobile cloud computing: Standardapproach to protecting and securing of mobile cloud ecosystems, Computer Sciences and Applications (CSA), 2013 International Conference. 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 5gnetworks make an intelligent and smart world, IEEE Network, **(2015)**, Vol.29, No.2, pp.40-45.

[7] I. Stojmenovic, Access control in distributed systems: Merging theorywith practice, 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 forfine-grained access control in cloud storage services, 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, Advances in cryptology ASIACRYPT 2002. Springer, (**2002),** pp.548-566.

[10] J. Bethencourt, A. Sahai and B. Waters, Ciphertext-policy attribute based encryption, Security and Privacy, 2007. SP'07.IEEE Symposium. IEEE, **(2007)**, pp.321-334.

[11] A. Shamir, Identity-based cryptosystems and signature schemes, Advances in cryptology. Springer, **(1985)**, pp.47-53.

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

[13] B. Grobauer, T. Walloschek and E. Stöcker, Understanding cloudcomputing vulnerabilities, Security & privacy, IEEE, **(2011)**, Vol.9, No.2, pp.50-57.

[14] S. Ghemawat, H. Gobioff and S. T. Leung, The google file system, ACM SIGOPS operating systems review, **(2003)**, Vol.37, No.5, pp.29-43.

[15] M. Zhou, R. Zhang, W. Xie, W. Qian and A. Zhou, Security andprivacy in cloud computing: A survey,

Semantics Knowledge and Grid (SKG), 2010 Sixth International Conference on. IEEE, **(2010)**, pp.105-112.

[16] Y. Xie, J. Zhang, G. Fu, H. Wen, Q. Han, X. Zhu, Y. Jiang and X. Guo, The security issue of wsns based on cloud computing, Communications and Network Security (CNS), 2013 IEEE Conference. IEEE, **(2013)**, pp.383-384.

[17] R. Walters, Cyber attacks on us companies in 2014, Heritage Foundation Issue Brief, (2014), No.4289.

[18] A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin and I. Stoica, Above the clouds: A Berkeley view of cloud computing, Dept. Electrical Eng. and Comput. Sciences, University of California, Berkeley, Rep. UCB/EECS, **(2009)**, Vol.28, p.13.

[19] L. Sumter, Cloud computing: security risk, Proceedings of the 48th Annual Southeast Regional Conference. ACM, **(2010)**, p.112.

[20] B. R. Moyers, J. P. Dunning, R. C. Marchany and J. G. Tront, Effectsof wi-fi and bluetooth battery exhaustion attacks on mobile devices, System Sciences (HICSS), 2010 43rd Hawaii International Conferenceon. IEEE, **(2010)**, pp.1-9.

[21] J. Oberheide and F. Jahanian, When mobile is harder than fixed (andvice versa): demystifying security challenges in mobile environments, Proceedings of the Eleventh Workshop on Mobile Computing Systems& Applications. ACM, **(2010)**, pp.43-48.

[22] W. Zhang, Y. Wen and H. H. Chen, Toward transcoding as a service:energy-efficient offloading policy for green mobile cloud, IEEE Network, **(2014)**, Vol.28, No.6, pp.67-73.

[23] J. Horwitz and B. Lynn, Toward hierarchical identity-based encryption, Advances in Cryptology EUROCRYPT 2002. Springer, **(2002)**, pp.466-481.

[24] V. Goyal, O. Pandey, A. Sahai and B. Waters, Attribute-based encryptionfor fine-grained access control of encrypted data, Proceedings of the 13th ACM conference on Computer and communications security. ACM, **(2006)**, pp.89-98.

[25] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica and M. Zaharia, A View of Cloud Computing, Communications of the ACM, **(2010)**, Vol.53, No. 4, pp.50-58.

[26] T. D. Nguyen and E. N. Huh, An efficient key management forsecure multicast in sensor-cloud, Computers, Networks, Systems and Industrial Engineering (CNSI), 2011 First ACIS/JNU International Conference on. IEEE, **(2011)**, pp.3-9.