International Journal of Engineering & Technology, 7 (3.10) (2018) 18-22

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper



An Advanced Hierarchical Attribute Based Encryption Access Control in Mobile Cloud Computing

Sreelesh N K[1], Santhosh Kumar B J[2]

[1, 2] *Department of Computer Science*
[1, 2] *Amrita Vishwa Vidyapeetham*
[1, 2] *Amrita School of Arts and Sciences*
Mysore, India
[*]*Corresponding author E-mail: sreeleshnk8003@gmail.com*[1]

Abstract

Cloud computing is a revolutionary computing technique, by which computing resources are provided dynamically via Internet is widely popular. Since the most attractive part of cloud computing is computation outsourcing, it is far beyond enough to just conduct access control. Unfortunately, the data in the cloud is out of user's control in most cases, privacy risks would rise dramatically due to the access of unauthorized users. The security of the data is the major concern. Coordinating mobile devices into cloud computing is a rising but encouraging illustration. The coordination happens in a cloud based multi-layered client information sharing condition. With the coordination of cloud computing with mobile devices may result in security issues such as information privacy and client rights.
The proposed work makes use of a technology using Advanced Hierarchical Attribute Based Encryption (A-HABE) architecture, in which the data storage will be in hierarchical structure and the retrieval of data will also be in the form of access level. Data confidentiality should be guaranteed and the system should be resilient. The secure storage and sharing of data without the fear of an unauthorized access in the cloud can result in growth in many sectors.

Keywords: *Attribute Based Encryption; A-HABE; Cloud Computing; Hierarchy; Mobile;*

1. Introduction

With the quick improvement of PC task and cell phone innovation, cloud computing has turned into the eventual fate of system correspondence. Portable stages will fundamentally depend on cloud computing in the days to come. Cell phones have restricted capacity limit and portable cloud computing stores process information outside of cell phones. Boundless registering force and capacity are fundamental telephone needs. Capacity should be acquired from the cloud. Gadgets, for example, top of the line guides store maps and courses locally. They require mists to get continuous data about course arranging and activity refreshes. Getting to portable information in the cloud is turning into the present developing interest.
As the mobile cloud computing defines there would be so much sensitive data from the mobile devices is bursting into the cloud infrastructures to process and store the data. The sensitive data belonging to a mobile cloud computing model can contain information of different hierarchies. It is important that the users with lower privilege cannot get access to some information that the higher privilege user can get to, while the higher authority user can get access to all the data that is obtainable for users in lower hierarchical position since different users of the mobile cloud computing system constitute a hierarchical authority system. At the same, all the information should be encrypted appropriately since the data is not supposed to be available for a third party which doesn't belong to the system. So, a secure and hierarchical access control method should be proposed to apply in the mobile cloud computing system.

2. Related Works

N. Fernando et.al [1] gave an expansive clarification of versatile distributed computing research. The examination done by them was about the difficulties that were not yet accomplished and they coordinated for the future work.

S. Abolfazli, Z. et al [2]The most developed versatile upgrade show that utilizations asset rich mists to include, improve and streamline the registering influence of cell phones intended to perform asset concentrated portable applications is a CMA. The examination is led to feature the effect of remote assets on the quality and dependability of the development procedure and to advance the difficulties and open doors for the better use of cloud based assets in cell phones.

R. Kumar, et al [3]The paper talks about the security and difficulties looked by versatile cloud through taking a gander at display cloud security issues, insufficiency in portable cloud gadgets and how to deal with these issues in future portable information insurance.

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

I. Stojmenovic [4] the latest encryption crude utilized for get to control is Attribute Based Encryption (ABE). This framework tends to a portion of the entrance control issues in circulated frameworks, for example, versatile specially appointed systems, in-vehicle systems and cloud computing, and so on. These applications have an alternate impediment and need us to indicate how variations of ABE can be tweaked.

G. Wang, et al [5] this article characterizes an answer which encourages organizations to share classified information adequately on cloud servers. This is executed by joining progressive character based encryption (HIBE) framework and a figure content characteristic based encryption (CP-ABE) framework and utilizing execution bargain lastly applying apathy re-encode to the program and intermediary re-encryption.

C. Gentry, et al [6]given a progressive character-based encryption conspire and a mark plot that can adjust the protection at any level and if there is a trouble of expecting a bilinear Diffie-Hellman issue, select arbitrary prophet demonstrate figure content security.

J. Bothencourt, et al [7] actualized a framework for complex access control for encoded information, which is generally known as figure content approaches-based encryption. This innovation can be utilized regardless of whether the server isn't trusted. The Encrypted information will be kept mystery, also forestalls impact assaults.

A. Zhou, et al [8] Learned about various distributed computing framework suppliers about their well-being and isolation concerns. They found that these worries are insufficient and should include more parts of security (convenience, privacy, information uprightness, control and reviewing).

Y. Xie, et al [9] proposed a structure in light of bar/sub, talked about the advantages and disadvantages, which incorporates the new cases of security challenges lastly a response to security will be started.

Ambrust, et al [10] they have a specific go for security and safe activity and gradually picking up specialist over innovation utilizing diverse level of qualities. The paper proposes a three-level structure in view of encryption (A-HABE).

Al-Haj, et al [11] Characterized security mindful asset designation as a Constraint fulfillment issue (CSP) which is settled utilizing a Satisfiable Model (SMT) solver. The exploratory investigation uncovers the effective approach in limiting danger and upgrading the tractability of cloud virtual machine security design.

B.R Moyers, et al [12] their exploration work was to diminish the impact of assaults on cell phones, the examination incorporates looking at the source codes and parallel documents of the versatile application.

The idea of Identity based Encryption (IBE) was presented by Shamir [13]. IBE utilizes discretionary strings to delineate the client's way of life as open key encryption information. The benefit of IBE is that the sender won't scrutinize the general population key data to the affirmation expert online to take care of the issue of execution of the accreditation specialist. One inconvenience of IBE is that all private keys produces client keys can be clog in the framework.

Horwitz [14] provided an idea of Hierarchical IBE, which works like the higher lever user of the system, can create a private key for the lower level user with his private key. This means that a private key generator only needs to create a first level user private key, while lower level user private key can be generated by ancestors. The improved system lessens the burden of PKG and increases the system effectiveness by validating the identity and transferring the key in the local area rather than global scope.

T. Shobana, et al [15] the task objective is to utilize AES 512 bits to upgrade the wellbeing of the cloud. As the data is put away in faraway areas, there are numerous sorts of gadgets getting to into it. In existing AES, 256 bits are utilized for security. In this examination, they utilize AES 512 bits to upgrade the cloud wellbeing, encode and decodes information with better security.

Ganesh, A.R, et.al [16] the current symmetric encryption guarantees better security, however keeping up the key is troublesome. Keeping up key is simple when utilizing topsy-turvy plans, however suppliers lesser security contrasted with symmetric plans. Proposed an improved variant of the half and half encryption plot named cross-encryption key that joined Advanced Encryption Standard (AES) with Elliptic Curve Cryptography (ECC) for trading the key securely, hub validation and blended encryption to upgrade figure content well-being.

S. Manishankar [17] Real issue staying for open frameworks and web is security. Absence of security is one of the constraints in receiving distributed computing. There are numerous security issues with respect to distributed computing like information security and looking at the cloud use by distributed computing clients. As the utilization of World Wide Web expanded, the security hazards additionally expanded alongside it. The security challenges incorporate when there is a mass or sudden customer demands, security check will be fizzled.

Sandhya.R, S. Manishankar, Bhagyasree.S [18] Learned about adjusting colossal information for the data administration industry. Proposed a calculation that tends to the difficulties happened while cloud stack administration chooses the best cloud segment for workload administration, including determination and booking calculation utilizing VISTA plan calculation and achieving the adjusted outcome with decreased use of preparing measurements.

3. Existing System

The literature survey portrays that the calculations and the security frameworks that are being utilized by the present frameworks are not that successful for the individual or a client to add classified data in the server/cloud. The information that is being added in the cloud or the server can be accessed to if the clients have a unique key with them. Yet, there is no security for the information which can be accessed to by the clients and further shared by them.

4. Proposed System

In proposed framework the user can store his information to the cloud. The user can get the information from anyplace anytime. The motivation behind this application is to improve security of information in cloud computing process.
Cloud suppliers should ensure the consumers that they can access and utilize their information at wherever and whenever. Customers' information ought to be kept secured in cloud frameworks. The information saved in cloud frameworks require a system to guarantee their information isn't lost or changed by unauthorized clients. A safe control framework disperses fitting assets to be used in various events.
The application gives facility to the consumer to offer authorization to the users who can get to the information saved in the cloud. When the consumer receives the user request to access the data, the permission will be given by generating a key and sending that key to users' mail according to the priority of the user only then the data can be accessed by the authorized users. RSA (Rivest

Shamir Adleman) algorithm is used for key generation, further will be explained in the implementation part.

5. Methodology

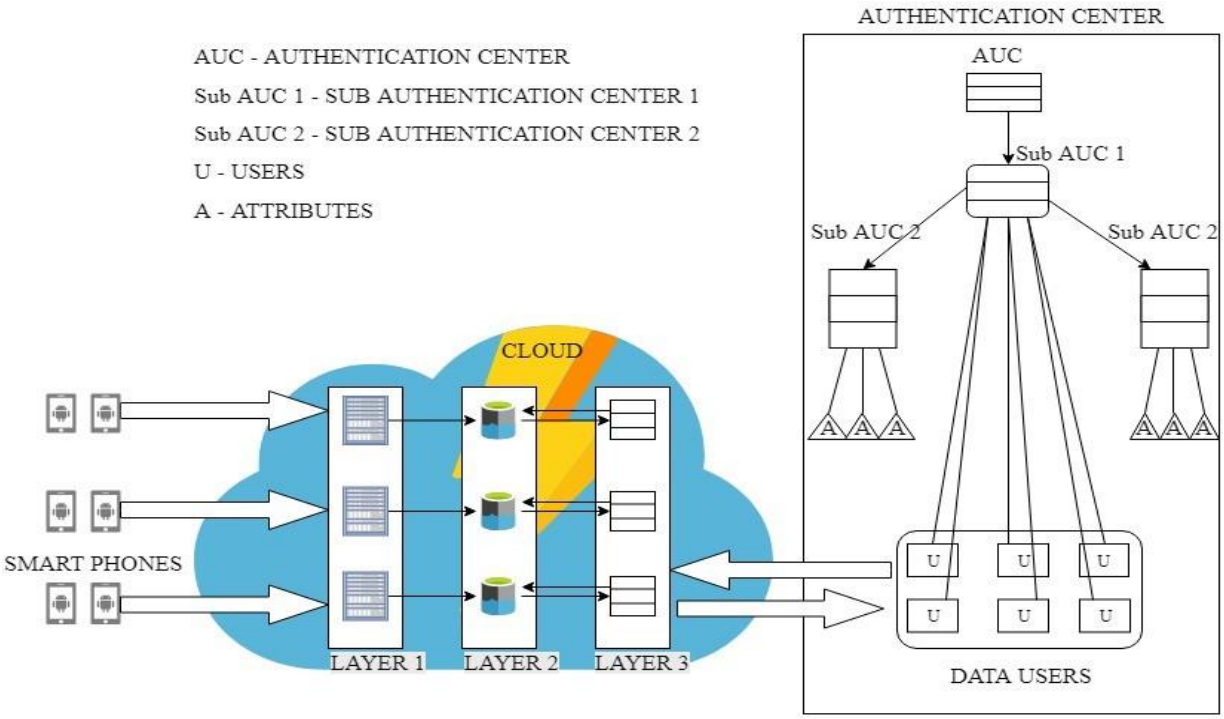


Fig. 1: Architecture Diagram

The above diagram shows theconsumer login by providing credentials. The consumer can access the files and upload the data to the cloud. Data stored by the consumer will be encrypted. The user will login to the cloud for accessing the data. The consumer will give permission to the users who have the priority to access the data. The user request will be send to the consuer's portal and the consumer will send the key for the user according to the priority.

5.1. Algorithm

Step 1: Given a security parameter K that is huge enough, AUC will generate a system parameter 'params' and a root master key MK.

Step 2: Create Master Key: Using system parameter 'params' and their own master keys, AUC or Sub-AUCs can create master keys for lower-level Sub-AUCs.

Step 3: Create Secret Key: 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.

Step 4: Create User: Sub-AUC 2 will create user's identity keys SKi;u and attribute keys SKi;u;a which is kept as secret. For them if the Sub- AUC makes sure that the attribute A is in charge of it and the user u satisfies a, if not there would be no secret identity keys or secret attribute keys.

Step 5: Encrypt: With R denoting a set of user's 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 sensitive data D into cipher text C.

Step 6:RDecrypt: Given the cipher text C, a data user possessing the precise ID that is in R is able to decrypt the cipher text C into plaintext D with params and the users secret key SKu.

Step 7: ADecrypt: Given the cipher text C, an attribute set {a} flag that is possessed by a data user that satisfies A, which means an attribute key SKi;u:a owned by a consumer can also decode the cipher text C into plaintext D using the system parameters with the user's secret identity key SKi;u, and the attribute key SKi;u;a.

As shown in the above algorithm the encryption and decryption takes place and the algorithm that is used here is the RSA Algorithm.

Table 1: Abbreviations of the terms

Key Name	Meaning
MK	Master Key(Authentication)
PKu	Public Key(Users)
SKu	Secret Key(Users)
SKi:u	Secret Identity key(Users)
SKi;u;a	Secret Attribute Key(Users)
AUC	Authentication Center
Sub-AUC1	Sub Authentication1
Sub-AUC2	Sub Authentication2

Table 2: Functional tests are based on the following:

Parameters	Description
Valid Input	Should accept identified classes with valid input
Invalid Input	Reject identified classes with invalid input.
Functions	The functions which are identified should be worked out
Output	Should work on an application output's identified classes.
System/procedures	Methods or interfacing frameworks should be conjured.

Association and readiness of practical tests are centered on prerequisites, key capacities, or uncommon experiments. Also, contemplation for testing are, deliberate scope relating to distinguish business process streams, information fields, predefined forms and progressive procedures. Prior to the fulfillment of functionality testing, extra tests are recognized and values of current tests are resolved.

6. Experimental Results

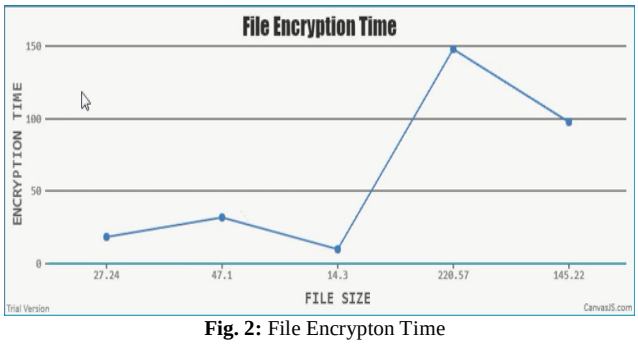


Fig. 2: File Encrypton Time

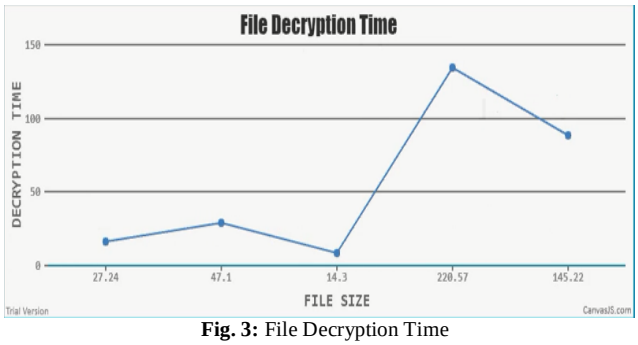


Fig. 3: File Decryption Time

The figures fig. 2 and fig. 3 demonstrates the time taken by the application to encrypt the information. There are numerous clients utilizing the cloud services with a specific end goal to spare their information. One of the fundamental parameters is the time taken to encode and decode the information. Availability of information is one of the benefits of the proposed application, along these lines, the application ought to give speedier transferring and getting to of information. For accomplishing this favorable position it is critical to figure the time required to encrypt and decrypt the information. The application will be more proficient on the off chance that it can give security and speedier transferring and getting to information. Unwavering quality gave by the cloud servers causes the clients to store their private information without the dread of unauthorized access.



Fig.4: Encrypted File

Fig. 4 shows how the data is encrypted at the application and how it is kept safe from unauthorized access. When the user clicks on decrypt button, the user request is sent to the consumer who uploaded the data, the consumer will send the key into the user's email and when the user enters the key he can access into the data. As mentioned in the previous sections, a user can only decode the encrypted file with the permission of the consumer who has the authority to provide permission, hence the data is safe from unauthorized access.



Fig. 5: Decrypted File

Fig. 5 portrays the decrypted document after the consumer allows the client to access the information. The user will have the capacity to download the document from the cloud.

7. Conclusion

This paper proposes the way the data has been encrypted in the cloud and the retrieval of data from the cloud using a multi hierarchical method, now the data can be accessed only by the consumers for whom the data Uploader gives permission to access. The proposed method is appropriate for the mobile cloud computing technique for the protection and guarding the illegal access. The suggested system prioritizes the users to access only the legitimate files. Hence the safety of the system is highlighted as there is no loss of data, illegal access, more control over the data stockpiled.

Acknowledgement

First of all, I thank Mata Amritanandamayi Devi for her support and inspiration in several ways.
Earnestly, I thank our Director, Br. Sunil Dharmapal and Correspondent Br. Venu Gopal for giving the imperative condition, system and encouragement for doing my project work at Amrita Vishwa Vidyapeetham University, Mysuru Campus, and Mysuru.
I offer my real on account of Prof. Vidya Pai C, Principal, Amrita School of Arts and Sciences, Amrita Vishwa Vidyapeetham-am, Mysuru for the reliable help and consolation.

References

[1] M. A. N. I. S. H. A. N. K. A. R. .S, "Integrated Security Service for on demand Services in IAAS Cloud Author", International Journal of Advances in Computer Science and Cloud Computing, vol. 2, no. 1, 2014.
[2] Stojmenovic, I. (2011, November). 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 (pp. 1-2). IEEE.
[3] Wang, G., Liu, Q., & Wu, J. (2010, October). 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 (pp. 735-737). ACM.
[4] Gentry, C., & Silverberg, A. (2002). Hierarchical ID-based cryptography. Advances in cryptology—ASIACRYPT 2002, 149-155.
[5] Bethencourt, J., Sahai, A., & Waters, B. (2007, May). Ciphertext-policy attribute-based encryption. In Security and Privacy, 2007. SP'07. IEEE Symposium on (pp. 321-334). IEEE.
[6] Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., ... &Zaharia, M. (2010). A view of cloud computing. Communications of the ACM, 53(4), 50-58.
[7] Al-Haj, S., Al-Shaer, E., & Ramasamy, H. V. (2013, June). Security-aware resource allocation in clouds. In Services Computing (SCC), 2013 IEEE International Conference on (pp. 400-407). IEEE.
[8] 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.
[9] Horwitz, J., & Lynn, B. (2002). Toward hierarchical identity-based encryption. In Advances in Cryptology—EUROCRYPT 2002 (pp. 466-481). Springer Berlin/Heidelberg.
[10] S. T., S., K., and V., S. K., "Enhancement of cloud security using AES 512 bits", Research Journal of Applied Sciences, Engineering and Technology, vol. 8, pp. 2116-2120, 2014.
[11] Ganesh, A. R., Manikandan, P. N., Sethu, S. P., Sundararajan, R., &Pargunarajan, K. (2011, June). An improved AES-ECC hybrid encryption scheme for secure communication in cooperative diversity based Wireless Sensor Networks. In Recent Trends in Information Technology (ICRTIT), 2011 International Conference on (pp. 1209-1214). IEEE.
[12] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proceedings of the 13th ACM conference on Computer and communications security. Acm, 2006, pp. 89–98.
[13] Grobauer, B., Walloschek, T., & Stocker, E. (2011). Understanding cloud computing vulnerabilities. IEEE Security & Privacy, 9(2), 50-57.
[14] Fernando, N., Loke, S. W., &Rahayu, W. (2013). Mobile cloud computing: A survey. Future generation computer systems, 29(1), 84-106.
[15] Abolfazli, S., Sanaei, Z., Ahmed, E., Gani, A., &Buyya, R. (2014). Cloud-based augmentation for mobile devices: motivation, taxonomies, and open challenges. IEEE Communications Surveys & Tutorials, 16(1), 337-368.
[16] Kumar, R., & Rajalakshmi, S. (2013, December). Mobile cloud computing: Standard approach to protecting and securing of mobile cloud ecosystems. In Computer Sciences and Applications (CSA), 2013 International Conference on (pp. 663-669). IEEE.
[17] Zhou, M., Zhang, R., Xie, W., Qian, W., & Zhou, A. (2010, November). Security and privacy in cloud computing: A survey. In Semantics Knowledge and Grid (SKG), 2010 Sixth International Conference on (pp. 105-112). IEEE.
[18] S. Manishankar, Sandhya, R., and Bhagyashree, S., "Dynamic load balancing for cloud partition in public cloud model using VISTA scheduler algorithm", Journal of Theoretical and Applied Information Technology, vol. 87, pp. 285-290, 2016.
[19] Shamir, A. (1984, August). Identity-based cryptosystems and signature schemes. In Crypto (Vol. 84, pp. 47-53)..Zhou, M., Zhang, R., Xie, W., Qian, W., & Zhou, A. (2010, November). Security and privacy in cloud computing: A survey. In Semantics Knowledge and Grid (SKG), 2010 Sixth International Conference on (pp. 105-112). IEEE.