IJERMS

International Journal of Engineering Researches and Management Studies

MOBILE CLOUD COMPUTING WITH A CHANGED HIERARCHIC ATTRIBUTE-BASED SECRET WRITING ACCESS MANAGEMENT METHOD

K. Venkatagurunatha[*1] Naidu & P.Sireesha[2]

[*1]Assistant Professor, School of Engineering &Technology, SPMVV, Tirupati

[2]Assistant Professor, Narayanadri Institute Of Engineering & Technology, Rajampet

ABSTRACT

Cloud computing is associate degree Internet-based computing pattern through that shared resources area unit provided to devices on- demand. Its associate degree rising however promising paradigm to group action mobile devices into cloud computing, and therefore the integration performs within the cloud primarily based gradable multi-user data-shared surroundings. With group action into cloud computing, security problems like knowledge confidentiality and user authority could arise within the mobile cloud computing system, and it's involved because the main constraints to the developments of mobile cloud computing. so as to give safe and secure operation, a gradable access management methodology exploitation changed gradable attribute-based coding and a changed three-layer structure is projected during this paper. during a specific mobile cloud computing model, monumental knowledge which can be from every kind of mobile devices, like good phones, functioned phones and PDAs so on will be controlled and monitored by the system, and therefore the knowledge will be sensitive to unauthorized third party and constraint to legal users additionally. The novel theme primarily focuses on the knowledge process, storing and accessing, that is meant to guarantee the users with legal authorities to induce corresponding classified knowledge and to limit criminal users and unauthorized legal users get access to the info, that makes it extraordinarily appropriate for the mobile cloud computing paradigms.

Keywords: Modified hierarchic attribute-based secret writing,Access management.

1. DEFINITION

Explosive growth of mobile devices as well as good phones, PDAs, and pill computers and therefore the applications put in them, the mobile-Internet can maintain the event growth trend as 4G communication network is extensively promoted to our lives. What users of the mobile devices and applications would like is that mobile-Internet will offer them with the service that is easy, high- speed, and steady. additionally, the protection problems with mobile terminals and therefore the web access hooked up importance to. And as a mixture of cloud computing, mobile devices and wireless networks, mobile cloud computing is associate rising however terribly promising paradigm that brings made procedure resources to mobile users, network operators, still as cloud computing suppliers . the issues of information storing and knowledge computing in mobile-Internet applications will be overcome by mobile cloud computing whereas the new paradigm can even accomplish cloud based mostly multi-user data sharing, finish geographical service limitation, and method time period tasks expeditiously at identical time.

There is no correct definition of mobile cloud computing, many ideas were planned, and 2 most well liked schemes may be delineate as follows:

a. Mobile cloud computing may be a quite theme that might run associate application like a weather monitor application on remote cloud servers as displayed in Figure one, whereas the mobile devices simply act like traditional PCs except that the mobile devices connect with cloud servers via 3G or 4G whereas PCs through web. And this thought is taken into account because the most well liked definition of mobile cloud computing
b. Taking benefits of leisure resources such as processor, memory, and storing disks, another model of mobile cloud computing exploits the mobile devices themselves as resources suppliers of cloud and therefore the theme supports user quality, and acknowledges the potential of mobile clouds to try and do collective sensing still.

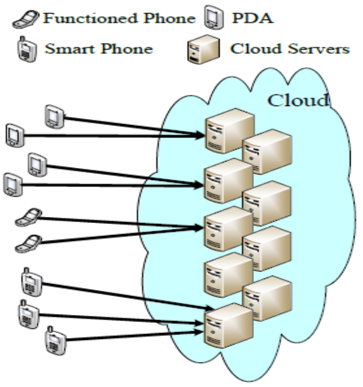

Fig. 1. A mobile cloud computing model

In this paper, we tend to in the main use the primary paradigm mentioned on top of, however the second conjures up USA to assume that what if the mobile devices don't offer computing resources or storing resources however sensing knowledge instead?

In fact, most mobile devices ar capable to capture some data from the atmosphere these days, for example, virtually each good phone ar equipped with sensors of proximity, measuring system, gyroscope, compass, barometer, camera, GPS, mike [6], etc. Combining the thought of WSN, mobile devices may be considered mobile sensors that able to offer alternative mobile devices WHO are users of the mobile cloud services with some sensing info as well as atmosphere watching knowledge, health watching knowledge, and so on.
We take a weather monitor application as associate example in this paper.

Assuming that an organization develops a weather monitor application that aims to share time period weather info like temperature, humidity, pictures, and precise location info then on to alternative users of the appliance .and therefore the application utilizes the user-cloud-user model rather than peer- to-peer model so the users will get classified and demanded info. Another feature of the appliance is that the users divided into totally different hierarchies, counting on that users will get totally different sensing knowledge, and users with higher privilege level will, of course, get access to additional specific and additional oftentimes updated info.

In order to meet what the application needs, security issues of the full system mustn't be neglected, among all security problems the foremost necessary 2 security problems in such model may be divided into 2 parts: authority of application users and therefore the confidentiality of sensing knowledge. Those problems may be resolved by providing strategies of access management . Attribute based mostly encoding (ABE) may be a recent cryptological primitive that has been used for access management . Access management issue deals with providing access to approved users and preventing unauthorized users to access knowledge. Attaching an inventory of approved users to every knowledge is that the simplest resolution to realize access management. However, this resolution is troublesome within the state of affairs with a sizable amount of users, like the appliance mentioned on top of at intervals the atmosphere of cloud. Public cryptological theme is another resolution, in that a public/secret key try is given to every user and cypher every message with public key of the approved user, so solely the particular users ar able to decode it. within the planned state of affairs, users with completely different privilege levels have different rights to access the a part of sensing knowledge coming back from the mobile devices. Therefore, one same knowledge must be encrypted into ciphertextonce, that got to be able to be decrypted multiple times by totally different approved users.

Based on such application demands, the thought of attribute based mostly encoding is introduced. Senders cypher message with sure attributes of the approved receivers. The ABE based mostly access management technique uses many tags to mark the attributes that a specific approved user desires to possess. The users with sure tag sets will get access to the spe-cific encrypted knowledge and decode it. In reference papers 12 to 15 introduced the theme concerning the attribute based mostly encoding access management technique within the cloud computing. within the mobile loud computing atmosphere, there are tremendous knowledge that has to be processed and marked with attributions for the convenient attributing access before storing. At identical time, the data structure of the application users would like associate authentication center entity to regulate their attributes.

In this paper, a stratified access management technique employing a changed stratified attribute- based encoding and a changed three-layer structure is planned. Differing from the prevailing paradigms like the HABE algorithmic rule and therefore the original three-layer structure, the novel theme in the main focuses on the information process, storing and accessing, that is meant to make sure the appliance users with legal access authorities to urge corresponding sensing knowledge and to limit users and unauthorized legal users get access to the information, the planned promising paradigm makes it very appropriate for the mobile cloud computing based mostly paradigm. What ought to be emphasised is that the foremost necessary highlight of bushed the planned paper may be delineate as that the changed three-layer structure is meant for finding the protection problems illustrated on top of.

2. MOBILE CLOUD COMPUTING SECURITY PROBLEMS

Most of the users started to use mobile cloud computing services like iCloud and One Drive services thanks to the poor storage and computation capability of current mobile devices. However, these reasonably mobile cloud services square measure thought of to be vulnerable in security and users could lose their hold on files or messages like photos, documents, contacts, and calendars, whats worse, those info could also be taken by third parties. In Sept, 2014, Apple admitted that iCloud was compromised by hackers and plenty of photos of celebrities leaked out.

Such outpouring event afraid North American nation that the safety problems with mobile cloud ought to be taken seriously. For finding such security challenges, knowledge authority and knowledge confidentiality ought to be paid additional attention.

Authority of information users: completely different authority-level system to urge access to sensing data for application users ought to be established since the paradigm is applied within the stratified multi-user shared surroundings, that conjointly means that that the users with higher authority level ought to get all the information that the users with lower privilege level may get access to, whereas the lower privilege users can’t get the information on the far side his/her authority.

Confidentiality of data: though the cloud services used within the state of affairs square measure provided by non-public cloud that is meant to be secure, it's still necessary to confirm the sensing knowledge protected against malicious third parties that don't belong to the mobile cloud system. thusit's vital for the system to herald a secure and economical coding theme.
In this section, we tend to primarily discuss the overall cloud com- puting security problems and mobile cloud computing problems.

Security problems for Cloud Computing

TABLEI

Cloud computing security Issues

Security Challenges	Descriptions
Availability	Cloud providers are supposed to guarantee to consumers that they can get and use their data any places and anytime.
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 be utilized in different occasions.

Security problems for Mobile Cloud Computing

Mobile cloud computing model during this paper implies that mobile device users run applications on remote cloud servers rather than mobile devices themselves, the paradigm performs nearly a similar as traditional cloud computing with computers except that mobile cloud model connects mobile devices and cloud servers through 3G or 4G whereas cloud computing paradigm via web, therefore, mobile cloud computing inherits the safety threats of ancient cloud computing. Whats more, the safety problems that area unit specific to mobile devices like battery exhaustion attacks, mobile bonnets and targeted attacks ought to fret still.

3. MODIFIED HIERARCHAL ATTRIBUTE BASED ENCRYPTION

We take a weather application on mobile devices as a state of affairs. As the mobile cloud computing defines, there would be most sensing knowledge from the mobile devices in bursting into the cloud infrastructures to method and store the info. The sensing knowledge happiness to a mobile cloud computing model will contain info of various hierarchies like temperature and humanity numbers, the weather dynamic trend, info update frequency then on. it's vital that the users with lower privilege will not get access to some info that the upper privilege user can get to, whereas the higher authority user will get access to all the info that's getable for users in lower hierarchal position since totally different users of the mobile cloud ADP system represent a hierarchal authority system. At an equivalent, all the knowledge ought to be encrypted suitably since the info isn't purported to be offered for a 3rd party that 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.

4. M-HABE ACCESS CONTROL METHOD APPLIED IN CLOUD-BASED SMART GRID

Applying M-HABE, the planned theme is illustrated in Figure 3.

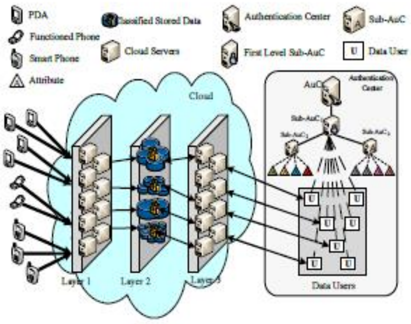

Fig. 3. General structure of M-HABE access control method for mobile cloud computing

The entire system works as following steps:

- Every kind of mobile devices that are put in with the mobile cloud computing based mostly weather application ar distributed into completely different locations everywhere the country with users. The applications will exploit the sensors put in within the mobile devices to capture the weather knowledge that the applications would like, together with temperature worth, wetness data, gas pressure so on.
- The sensing weather knowledge is transported to the layer1 which could be a quite IaaS cloud service provided by the cloud supplier .
- Before sent to layer two, the sensing weather knowledge is classed by its knowledge model in layer one with its wonderful ability of computing and storing, the step will be illustrated by figure four.

The knowledge model we have a tendency to gift is impressed by the knowledge model planned, based mostly on that our knowledge model is composed by format, device ID, size, time, worth and amount.

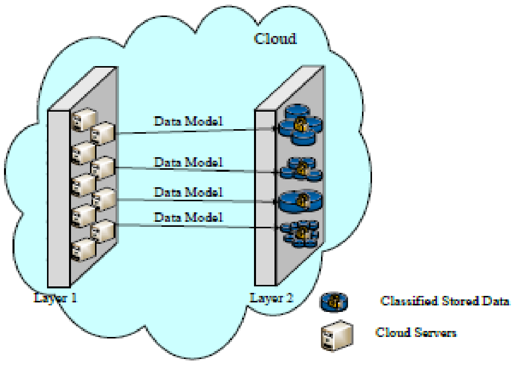

Fig. 4. Data model

Therefore, a information will be expressed as a vector knowledge format stands for the fundamental format of the raw whether data that a specific mobile device produces, there are completely different sorts of formats depended on different sorts of mobile devices, for example, JPEG, WMA, TXT, PNG, WMV, etc. Mobile device id is that the solely sign of the supply mobile device wherever raw weather knowledge comes from. the scale of sensing weather knowledge is outlined by the inclementness knowledge itself, that indicates the scale of 1 specific weather knowledge. As for time, as long as a mobile device captures knowledge from the surroundings wherever it's in, the time that the causation action happens are going to be regarded as the time attribute of the raw sensing knowledge. a price sign represents the foremost vital characteristic of sensing knowledge, the which means it stands for differs from format to format, and different sorts of mobile devices have different meanings. for instance, for a temperature detector, the worth means that specific numbers of the temperature, whereas the wetness sensors will solely manufacture the info with the worth attributes that indicate the particular numbers of wetness. A amount identification is a time cycle of the sensing knowledge, it is used to explain the life amount of 1 specific sensing information, and also the knowledge are going to be destroyed once the storing time in cloud of it's on the far side the amount time.

- The sensing weather knowledge is encrypted into ciphertext in layer two by M-HABE encoding algorithmic rule victimization the key and the cyphertext is sent to layer three that is conjointly a quite IaaS cloud service in cloud. The encoding step will be incontestible as Figure five.

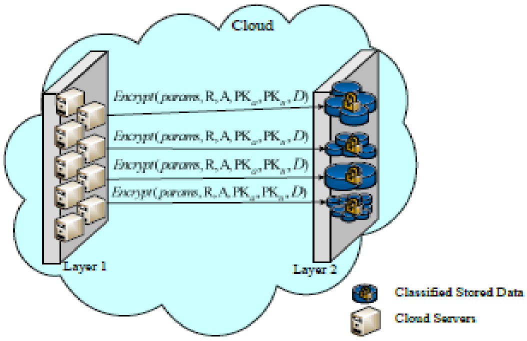
Cloud
$Encrypt(params, R, A, PK_{u}, PK_{a}, D)$
$Encrypt(params, R, A, PK_{u}, PK_{a}, D)$
$Encrypt(params, R, A, PK_{u}, PK_{a}, D)$
$Encrypt(params, R, A, PK_{u}, PK_{a}, D)$
Layer 1
Layer 2
Classified Stored Data
Cloud Servers

Fig. 5. Encryption procedure

- The knowledge users of the theme are in charge of simply like Figure two indicates.

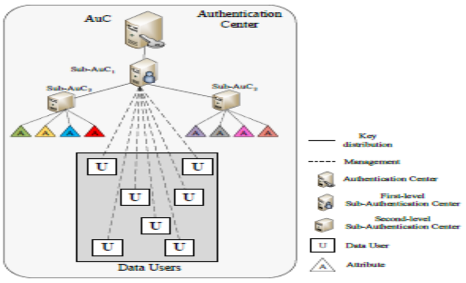

Fig. 2. M-HABE model

The users will get access to the ciphertexts provided that he/she satisfies the necessities of RDcrypt algorithmic rule or ADcrypt algorithmic rule that ar represented partly III.

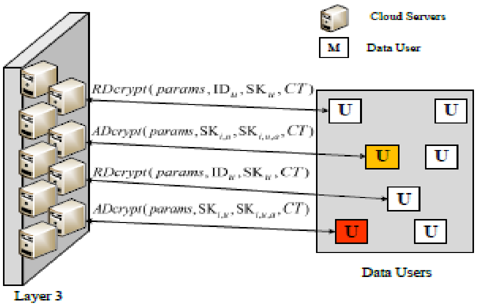
Cloud Servers
M
Data User
$RDcrypt(params, ID_{u}, SK_{u}, CT)$
$ADcrypt(params, SK_{i,u}, SK_{i,u,a}, CT)$
$RDcrypt(params, ID_{u}, SK_{u}, CT)$
$ADcrypt(params, SK_{i,u}, SK_{i,u,a}, CT)$
U
Data Users
Layer 3

Fig. 6. Decryption procedure

The secret writing procedure is shown in Figure 6.

5. CONCLUSION

The paper planned a changed HABE theme by tak- ing blessings of attributes primarily cryptography (ABE) and stratified identity based cryptography (HIBE) access management process. The planned access management methodology victimisation M-HABE is intended to be utilised among a stratified multi- user data-shared setting, that is extraordinarily appropriate for a mobile cloud computing model to safeguard the info privacy and defend unauthorized access. Compared with the initial HABE theme, the novel theme is a lot of adaptive for mobile cloud computing setting to method, store and access the big information and files whereas the novel system will let totally different privilege entities access their permissible information and files. The theme not solely accomplishes the stratified access management of mobile sensing information within the mobile cloud computing model, however protects the info from being obtained by Associate in Nursing 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, "cloud- based augmentation for mobile devices: motivation, taxonomies, and open challenges," communications surveys &amp; 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 confer- ence 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 com-munications (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 acces control in cloud storage services,"
9. C. Gentry and a. Silverberg, "hierarchical id- based cryptography," in advances in cryptologyasiacrypt2002.springer,2002.
10. J. Bethencourt, a. Sahai, and b. Waters, "ciphertext-policy attribute- based encryption," in security and privacy, 2007. Sp'07. Ieee sympo-sium on. Ieee, 2007, pp. 321–334.
11. A. Shamir, "identity-based cryptosystems and signature schemes," in advances in cryptology. Springer, 1985, pp. 47–53.
12. 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.
13. B. Grobauer, t. Walloschek, and e. Sto¨ cker, "understanding cloud computing vulnerabilities," security & privacy, ieee, vol. 9, no. 2, pp.50–57, 2011.
14. S. Ghemawat, h. Gobioff, and s.-t. Leung, "the google file system," in acm sigops operating systems review, vol. 37, no. 5. Acm, 2003,pp.29-43.
15. 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.
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," in communications and network security (cns), 2013 ieee conference on. Ieee, 2013, pp. 383–384.
17. R. Walters, "cyber attacks on us companies in 2014," heritage foun- dation issue brief, no. 4289, 2014.
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, vol. 28, p. 13, 2009.

19. *L. Sumter, "cloud computing: security risk," in 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, "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.*
21. *J. Oberheide and f. Jahanian, "when mobile is harder than fixed (and vice versa): demystifying security challenges in mobile environments," in 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," network, ieee, vol. 28, no. 6, pp. 67–73, 2014.*
23. *J. Horwitz and b. Lynn, "toward hierarchical identity-based encryption," in advances in cryptologyeurocrypt 2002. Springer, 2002, pp. 466–481.*
24. *V. Goyal, o. Pandey, a. Sahai, and b. Waters, "attribute-based encryp- tion 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.*
25. *M. Armbrust, a. Fox, r. Griffith, a. D. Joseph, r. Katz, a. Konwinski, g. Lee, d. Patterson, a. Rabkin, i. Stoica et al., "a view of cloud computing," communications of the acm, vol. 53, no. 4, pp. 50–58, 2010.*