A MODIFIED HIERARCHICAL ATTRIBUTE-BASED ENCRYPTION ACCESS CONTROLMETHOD FOR MOBILE CLOUD COMPUTING

PADAKANDL A BABY SHALINI*1, Mr. K HARI BABU*2, NAGARAJU KAVITHA*3

* 1,3 B. Tech Students, *2 Assistant Professor
Dept. of Computer Science and Engineering,
RISE Krishna Sai Gandhi Group of Institutions

ABSTRACT

Cloud computing is an Internet-based computing pattern through which shared resources are provided to devices on demand. It is 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 cloudcomputing system, and it is concerned as the main constraints to the developments of mobile cloud computing. 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.

Keywords: Integration, Computing, Internet

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, highspeed, and steady. In addition, the security issues of mobile terminals and the Internet access are attached importance to. The flaws of data storing and data computing in mobile-Internet applications can be overcome by mobile cloud computing while the new paradigm can also accomplish cloud based multi-user data sharing, end geographical service limitation, and process real-time tasks efficiently at the same time. There is no accurate definition of mobile cloud computing, several concepts were proposed, and two most popular schemes can be described as follows:

1) Mobile cloud computing is a kind of scheme which could run an application such as a weather monitor application on remote, while the mobile devices just act like normal PCs except that the mobile devices connect to cloud servers via 3G or 4G while PCs through Internet. And this concept is considered as the most popular definition of mobile cloud computing [4].

2) Taking advantages of leisure resources such as CPU, memory, and storing disks, another model of mobile cloud computing exploits the mobile devices themselves as resources providers of cloud [5]. And the scheme supports user mobility, and recognizes the potential of mobile clouds to do collective sensing as well. In this paper, we mainly use the first paradigm mentioned above, but the second one inspires us to assume that what if the mobile devices do not provide computing resources or storing resources but sensing data instead? In fact, most mobile devices are capable to capture some data from the environment nowadays, for example, almost every smart phone are equipped with sensors of proximity, accelerometer, gyroscope, compass, barometer, camera, GPS, microphone [6], etc. Combining the concept of WSN, mobile devices can be regarded as mobile sensors that are able to provide other mobile devices who are users of the mobile cloud services with some sensing information including environment monitoring data, health monitoring data, and so on. In order to meet what the application requires, security issues of the whole system should not be ignored, among all security issues the most important two security issues in such model can be divided into two parts: authority of application users and the confidentiality of sensing data. Those issues can be solved by providing methods of access control [7]. Attribute Based Encryption (ABE) is a recent cryptographic primitive which has been used for access control [8]–[11]. Access control issue deals with providing access to authorized users and preventing unauthorized users to access data. In this paper, a hierarchical access control method using a modified hierarchical attribute-based

encryption (M-HABE) and a modified three-layer structure [16] is proposed. Differing from the existing paradigms such as the HABE algorithm and the original three-layer structure, the novel scheme mainly focuses on the data processing, storing and accessing, which is designed to ensure the application users with legal access authorities to get corresponding sensing data and to restrict illegal users and unauthorized legal users get access to the data, the proposed promising paradigm makes it extremely suitable for the mobile cloud computing based paradigm.

Objective

A user 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. The flaws of data storing and data computing in mobile-Internet applications can be overcome by mobile cloud computing while the new paradigm can also accomplish cloud based multi-user data sharing, end geographical service limitation, and process real-time tasks efficiently at the same time.

LITERATURE SURVEY

A cloud storage administration enables data proprietor to re-appropriate their statistics to the cloud as well as during which give the statistics admittance toward the user. Since the cloud server as well as the statistics proprietor be not in a similar belief space, the semiconfided in cloud server can't be depended to authorize the entrance strategy. To tackle this test, conventional strategies as a rule necessitate the statistics proprietor to scramble the information as well as convey unscrambling key to approved user. These techniques, notwithstanding, typically include confounded key administration as well as elevated transparency on statistics proprietor. In this manuscript, we structure an entrance manage structure pro cloud storage frameworks so as to accomplishes fine-grained get to manage base on an adjusted Ciphertext-Policy Attribute-base Encryption (CP-ABE) loom.

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.

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).

SYSTEM ANALYSIS

The Systems Development Life Cycle (SDLC), or Software Development Life Cycle in systems engineering, information systems and software engineering, is the process of creating or altering systems, and the models and methodologies that people use to develop these systems. In software engineering the SDLC concept underpins many kinds of software development methodologies.

Existing System

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.

Disadvantages of Existing System:

1. Data confidentiality is less.

Proposed System

In this paper 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 a specific mobile cloud computing model, enormous data which may be from all kinds of mobile devices, such as smart phones, functioned phones and PDAs and so on can be controlled and monitored by the system, and the data can be sensitive to unauthorized third party and constraint to legal users as well. The novel scheme mainly focuses on the data processing, storing and accessing, which is designed to ensure the users with legal authorities to get corresponding classified data and to restrict illegal users and unauthorized legal users get access to the data, which makes it extremely suitable for the mobile cloud computing paradigms.

Advantages of Proposed System:

1. Strictly restrict illegal users and unauthorized legal users get access to the data.
2. More efficient.

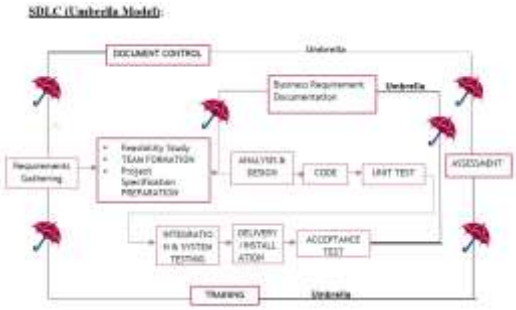

Fig 1: SDLC (Umbrella Model)

SDLC is nothing but Software Development Life Cycle. It is a standard which is used by software industry to develop good software.

SYSTEM DESIGN

UML diagrams

The Unified Modeling Language allows the software engineer to express an analysis model using the modeling notation that is governed by a set of syntactic semantic and pragmatic rules.A UML system is represented using five different views that describe the system from distinctly different perspective. Each view is defined by a set of diagram, which is as follows.

- User Model View

i. This view represents the system from the user's perspective.

ii. The analysis representation describes a usage scenario from the end- users perspective.

- Structural Model view

i. In this model the data and functionality are arrived from inside the system.

ii. This model view models the static structures.

- Behavioral Model View

It represents the dynamic of behavioral as parts of the system, depicting the interactions of collection between various structural elements described in the user model and structural model view.

- Implementation Model View

In this the structural and behavioral as parts of the system are represented as they are to be built.

- Environmental Model View

In this the structural and behavioral aspects of the environment in which the system is to be implemented are represented.

Class diagram:

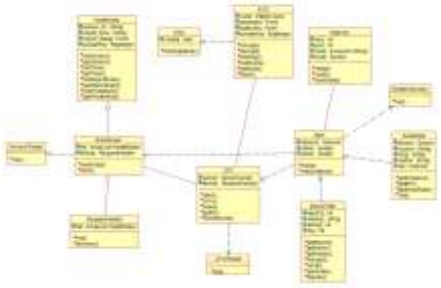

Fig 2: Class diagram

Apart from class diagram the case, sequence, collaboration, Component diagram etc

Component Diagram for user:

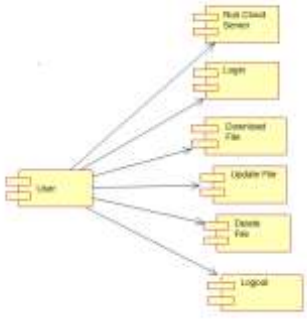

Fig 3: Component Diagram for User

SOURCE CODE

CloudServer.java:

```
package com;
import java.awt. Border Layout; import java.awt.Color;
```

```
import java.awt.Container; import java.awt.Font;
import javax.swing.JFrame; import
javax.swing.JLabel; import javax.swing.JPanel;
import javax.swing.UIManager; import
javax.swing.JTextArea; import
javax.swing.JScrollPane; import java.net.Socket;
import java.net.ServerSocket; import
java.net.InetAddress; import
javax.swing.JOptionPane;
public class CloudServer extends JFrame
implements Runnable{

JLabel l1; Font f1,f2;
JPanel p1,p2,p3; Thread thread; JTextArea area;
JScrollPane jsp; ServerSocket server;
RequestHandler rh; static double time;
public void start(){ try{
server = new ServerSocket(1111);
area.append("Cloud Server Services Started\n\n");
while(true){
Socket socket = server.accept();
socket.setKeepAlive(true);
InetAddress address=socket.getInetAddress();
String ipadd=address.toString();
area.append("ConnectedComputers
:"+ipadd.substring(1,ipadd.length())+"\n");
rh = new RequestHandler(socket,area); rh.start();
}
}catch(Exception e){
e.printStackTrace();
}
}
public CloudServer(){
setTitle("Cloud Server");
getContentPane().setLayout(new BorderLayout());
f1 = new Font("Courier New",Font.BOLD,20);
p1 = new JPanel();
l1 = new
JLabel("<HTML><BODY><CENTER>C
loud Server
Screen</CENTER></BODY></HTML>".toUpper
Case());
l1.setFont(this.f1); l1.setForeground(new
Color(125,54,2));
p1.setBackground(Color.pink); p1.add(l1);
f2 = new Font("Times New
Roman",Font.PLAIN,16); p2 = new JPanel();
p2.setLayout(new BorderLayout()); area = new
JTextArea(); area.setFont(f2);
area.setEditable(false);
jsp = new JScrollPane(area);
p2.add(jsp,BorderLayout.CENTER);
getContentPane().add(p1, BorderLayout.NORTH);
getContentPane().add(p2,
BorderLayout.CENTER);
thread = new Thread(this); thread.start();
}
public void run(){ try{
while(true){
```

TEST CASES

Test Case Id	Test Case Name	Test Case Desc.	Test Steps			Test Case Status	Test Priority
			Step	Expected	Actual		
01	Run Cloud Server	Verify the either Cloud server is running or not	Without start Cloud Server	We cannot store the data	Cloud server started	High	High
02	Admin Login	Verify either the Admin can login or not	Without having the authenticate details	Admin cannot login to the system	Admin can login to the system	High	High
03	Add Users	Test whether the Users are added or not	Without selecting the authenticated level	User cannot add to the system	User added successfully	High	High
04	UploadFile	Test whether the file is uploaded or not	Without selecting any file	Admin cannot upload the file	File uploaded successfully	High	High
05	User Login	Verify user can login ornot	Without having authentication	User cannot login	User login successfully	High	High

06	Download File	Verify file is downloaded or not	Without having the access control	File cannot be downloaded	File downloaded successfully	High	High

EXPERIMENTAL RESULTS

Fig. 3: Cloud Server

MHABE: put this folder inside tomcat WEBAPP directory and start tomcat andrun in browser to get below screen

Fig.4: MHABE Web Application Home Page

In above screen click on 'Admin' link and then login as admin and admin

Fig.5: Home pageAfter admin login will get below screen

Fig.6: Admin Screen

In above screen click on 'Add Users/Employees' link to add new users

Fig.7: New user registration screen

In above screen based on user give access control as High, Medium or Low. Now click on 'Upload File' link to upload file

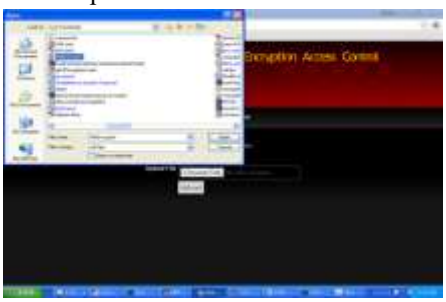

Fig.8: File Uploading from system

In above I am uploading one file, after upload will get below screen

Fig.9: File Uploding ScreenNow click on 'View Users' link to view all users

Fig.10: User details Screen

In above screen we can see aaa user has HIGH access so he can delete and download file and bbb user has Medium access so he can download and update file and ccc user has Low access so he can only download file. Now logout and login as user.

access ScreenIn above screen user ccc has got only download option

Screen at cloud server

Fig.11: Screen at cloud server

CONCLUSION

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.

FUTURE ENHANCEMENT

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. 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.*