AN ADMISSION CONTROL TECHNIQUE FOR MULTIPLE DATA OWNERS IN CLOUD COMPUTING ENVIRONMENT

B PRAKASH[1], Dr. A SATYANARAYANA[2]
[1]M.Tech Student, Dept of CSE, Siddhartha Institute of Technology & Sciences, Hyderabad, T.S, India
[2]Assistant Professor, Dept of CSE, Siddhartha Institute of Technology & Sciences, Hyderabad, T.S, India

ABSTRACT:

It can be overcome by storing information and knowledge of the computer in mobile Internet applications through mobile cloud computing problems. The new model can also conduct discussions based on cloud-based user data, complete geographic services, and efficiently handle tasks in real time. With integration in cloud computing, security problems that may arise from the confidentiality of data and user power in the mobile cloud computing system, which is affected by the initial constraints of the development of mobile cloud computing. In order to provide a safe and sufficient process, the Hierarchical Access Control method was proposed using file-based encryption to change the hierarchical attribute, along with the three-level structure modified in this document. The control method was modified in this study, it is suggested in the hierarchical hierarchy to encrypt modified files with a three-tier structure. The exact control of the ABE method is used to access many function labels that must be approved by the user. Under a particular model of mobile cloud computing, the system can control and control a large amount of data for all types of mobile devices, such as smart phones, mobile phones and PDAs, and data can respond to unauthorized users of mobile devices. Third parties. Who is also legal.

Keywords: Attribute-based access, access control. Mobile cloud computing.

1. INTRODUCTION:

In fact, most mobile devices have the ability to capture some atmospheric data at this time, for example, almost all smartphones are equipped with sensors, accelerometer, gyroscope, compass, pressure gauge, camera, GPS navigation system and microphone in Nearby. Some people using mobile devices and applications need mobile Internet to provide an easy-to-use, fast and stable service. In addition, security issues are related to portable peripherals and important Internet access. There is no precise meaning of mobile cloud computing, different concepts have been proposed. By confusing the idea of WSN, portable devices can be considered as mobile sensors that other mobile devices can offer when using cloud mobile services with little confidential information, including air traffic data, health surveillance data, and so on. The issue of access control concerns the use of authorized users and disables access to data by unauthorized users. Adding a summary of approved users to all information is the easiest way to fix access control. Cloud computing is definitely an Internet-based computer model where shared resources are provided with hardware when necessary. It is a growing but promising model for integrating mobile devices into cloud computing, as well as for integration within the cloud-based multi-data hierarchy [1]. In the suggested scenario, users with different levels of authorization have different legal rights to access data from the Neglect sensor in mobile devices. With specific tag sets, you can access and decrypt encrypted data. The new plan focuses primarily on processing, storage and access to information, [2] which is implemented to ensure that users with legal authority have access to corresponding disaggregated data as well as to reduce illegal users and unauthorized legal users. To access information, making it very suitable for calculating mobile device models.

2. EXISTING SYSTEM:

Senders are secure with a message that has certain properties for approved recipients. The ABE-based access control uses different tags to distinguish attributes that a particular user must have. You can access certain data that has been decrypted with certain sets of tags and decrypt them [3]. Much of the document presented the plan with regard to how to control access to file encryption based on attribute in cloud computing. In a noisy laptop environment, you'll find huge data to process and label with attributes to refer easier to store before you store it. At the same time, the application user hierarchy requires an authentication tool to manage its attributes. Disadvantages of the current system: Do not guarantee availability problems. Consumer data is not stored confidentially in cloud systems. Data integrity problem. There are no multiple controls.

3. VARIANT APPROACH:

In the proposed scenario, users with different levels of entitlement enjoy different legal rights to access data from the negligence sensor of mobile devices. Therefore, the same data must be encoded simultaneously in encrypted text, which must be decrypted by different users on multiple occasions. The new plan focuses primarily on information processing, storage and access, which are made to ensure that users of the application with government access to legal access to the corresponding sensor data, and to restrict illegal users and users [4]. Legal persons who do not have access to information, the proposed promising model, make it very suitable for this model based on mobile cloud computing. This article proposed the hierarchical access control method using hierarchically modified file encryption with modified three-layer structures. What needs to be emphasized is that the main feature of the proposed document can be defined as the three-layer structure that has been modified to solve the security problems described above. Advantages of the proposed system: encryption can be decoded with a number of keys. Both the exact level description and the user attribute must be supported within the access structure of the method.

Concerns in Mobile Cloud: Authority of information users: Different authority-level system to obtain access to sensing data for application users ought to be established because the paradigm is used within the hierarchical multi-user shared atmosphere, that also implies that you with greater authority level is deserving of all of the data the users with lower privilege level could obtain access to, as the lower privilege users can't obtain the data beyond his/her authority. Confidentiality of information: Even though the cloud services found in the scenario are supplied by private cloud which is designed to stay safe, it's still necessary to guarantee the sensing data protected against malicious organizations that don't fit in with the mobile cloud system. You will find mainly two techniques to enhance availability in cloud that are virtualization and redundancy. Presently, cloud technologies are mainly based virtual machine, since cloud providers can offer separated virtualized memory, virtualized storage, and virtualized CPU cycles, to ensure that users can invariably have them. Confidentiality is a huge barrier for cloud providers to popularize cloud to consumers because it arrives. There essentially exist two common approaches in current cloud infrastructures, say physical isolation and file encryption. Data integrity ensures people who their storing information is not modified by others or collapsing because of system failure. To be able to possess a secure control system, cloud vendors may require a specialized operating-system. Mobile cloud-computing model within this paper implies that mobile phone users run applications on remote cloud servers rather of cellular devices themselves, the paradigm performs nearly as good as normal cloud-computing with computers with the exception that mobile cloud model connects cellular devices and cloud servers through 3G or 4G while cloud-computing paradigm.

Updated model: It is crucial that you with lower privilege cannot obtain access to some good info the greater privilege user could possibly get to, as the greater authority user can obtain access to all of the data that's accessible for users in lower hierarchical position since different people that use the mobile cloud-computing system constitute a hierarchical authority system [5]. So a safe and secure and hierarchical access control method ought to be suggested to use within the mobile cloud-computing system. The dwelling of file encryption keys should performs just like the hierarchical structure from the mobile cloud-computing users. One encrypted data could be received by a number of users. An altered hierarchical attribute-based file encryption access control method used in mobile cloud-computing is suggested within this paper, which changes a suggested plan known as hierarchical attribute-based file encryption HABE. One benefit of IBE would be that the sender didn't need to search the general public keys info on certificate authority (CA) online, which reduced the problem of poor CA performance. This improved system relieved PKG of effective burden that has been enhanced the machine efficiency by authenticating identities and transporting keys within locality area rather of worldwide area [6]. The general public key of the user is explained some IDs made up of the general public key of father node and also the users own ID within the approach to G-HIBE, the most crucial feature from the proposal would be that the users public key could reflect precise position from the user within the hierarchical structure [6]. The main from the suggested plan is known as modified hierarchical attribute-based file encryption, which differs from the HABE plan. Each data user proven within the figure offers a distinctive ID that is a character string made to describe the characteristics of internal parties inside the system.

Access Controlling Methods:

Meteorological information is transferred to Tier 1, a cloud type of IaaS provided by the cloud provider. Applications can use the sensors specified in handheld devices to capture data required by applications, including temperature value, humidity information, atmospheric pressure, etc. The information model we provide is inspired by the proposed data model, where our data model consists of planning, device identifier, size, time, value, and time period. How weather information is widely based on the same raw weather data, which means just how large one weather information is. For some time, as long as the mobile phone records the data in the atmosphere where it is located, the delivery action will be performed because the time attribute comes from raw sensor data. Something is the most important signal of sensor data, meaning the device is different from coordination to coordination, and different types of cellular devices have different meanings. You can only access encrypted texts if they meet your needs.

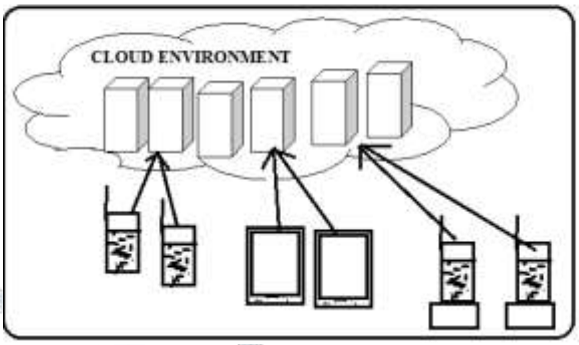

Fig.1.Mobile cloud computing overview

4. CONCLUSION:

The plan not only achieves hierarchical access rates for mobile sensor data in the mobile cloud computing model, but also protects information against an unreliable third party. The proposed access control is implemented using MHABE to be applied in a multi-hierarchical data environment and suitable for any laptop model to protect the privacy of information and to defend unauthorized access. The keys in the authentication center must have the same hierarchical structure as the user rights level structure. The article suggests a custom HABE scheme if it uses file-based encryption and encryption functions to control access to a hierarchical file encryption. Unlike the original HABE plan, the new plan can be further adapted to the cloud computing environment for processing, storing and storing large data and data, giving the new system a different privilege to access data and files allowed.

REFERENCES:

[1] S. Zittrower and C. C. Zou, “Encrypted phrase searching in the cloud,” in IEEE Global Communications Conference, 2012, pp. 764–770.

[2] Y. Tang, D. Gu, N. Ding, and H. Lu, “Phrase search over encrypted data with symmetric encryption scheme,” in International Conference on Distributed Computing SystemsWorkshops, 2012, pp. 471–480.

[3] M. Ding, F. Gao, Z. Jin, and H. Zhang, “An efficient public key encryption with conjunctive keyword search scheme based on pairings,” in IEEE International Conference on Network Infrastructure and Digital Content, 2012, pp. 526–530.

[4] F. Kerschbaum, “Secure conjunctive keyword searches for unstructured text,” in International Conference on Network and System Security, 2011, pp. 285–289.

[5] Z. Fu, X. Sun, N. Linge, and L. Zhou, “Achieving effective cloud search services: multi-keyword ranked search over encrypted cloud data supporting synonym query,” IEEE Transactions on Consumer Electronics, vol. 60, pp. 164–172, 2014.

[6] C. L. A. Clarke, G. V. Cormack, and E. A. Tudhope, “Relevance ranking for one to three term queries,” Information Processing and Management: an International Journal, vol. 36, no. 2, pp. 291–311, Jan. 2000.