Achieving Efficient and Secure Data Acquisitionfor Cloud-supported Internet of Things in SmartGrid

ABSTRACT:

Cloud-supported Internet of Things (Cloud-IoT)has been broadly deployed in smart grid systems. The IoTfront-ends are responsible for data acquisition and statussupervision, while the substantial amount of data is stored andmanaged in the cloud server. Achieving data security and systemefficiency in the data acquisition and transmission process are ofgreat significance and challenging, because the powergrid-related data is sensitive and in huge amount. In this paper,we present an efficient and secure data acquisition scheme basedon CP-ABE (Ciphertext Policy Attribute Based Encryption).Data acquired from the terminals will be partitioned into blocksand encrypted with its corresponding access sub-tree in sequence,thereby the data encryption and data transmission can beprocessed in parallel. Furthermore, we protect the informationabout the access tree with threshold secret sharing method,which can preserve the data privacy and integrity from userswith the unauthorized sets of attributes. The formal analysisdemonstrates that the proposed scheme can fulfill the securityrequirements of the Cloud-supported IoT in smart grid. Thenumerical analysis and experimental results indicate that ourscheme can effectively reduce the time cost compared with otherpopular approaches.

EXISTING SYSTEM:

- Sahai and Waters proposed the Attribute-BasedEncryption (ABE) to realize fine-grained access control onencrypted data. In ABE, the encryption policy

is associatedwith a set of attributes, and the data owner can be offline afterdata is encrypted.

- VipulGoyal et al developed a newcryptosystem for fine-grained sharing of encrypted databased on Sahai's work, called Key-Policy Attribute-BasedEncryption (KP-ABE). In their scheme, the ciphertext'sencryption policy is associated with a set of attributes, but theattributes that organized into a tree structure (named accesstree) are specified by data receivers.
- Bethencourt et alproposed the Ciphertext Policy Attribute Based Encryption(CP-ABE).

DISADVANTAGES OF EXISTING SYSTEM:

- First, the efficiency of data acquisition should be considered due to the large amount of data to be encrypted/decrypted and transferred. It's critical to ensure an acceptable the data acquisition time.
- Second, the protection of data security and privacy must be kept in mind.
- Achieving data security and system efficiency in the data acquisition and transmission process are of great significance and challenging. Existing related schemes cannot deal with this challengingissue well

PROPOSED SYSTEM:

- In this paper, we present an efficient and secure data acquisition scheme based on CP-ABE.
- We propose a parallel data processing method. Data acquired from the terminals will be partitioned into blocks and encrypted with its corresponding access sub-tree in sequence, thereby the data encryption and

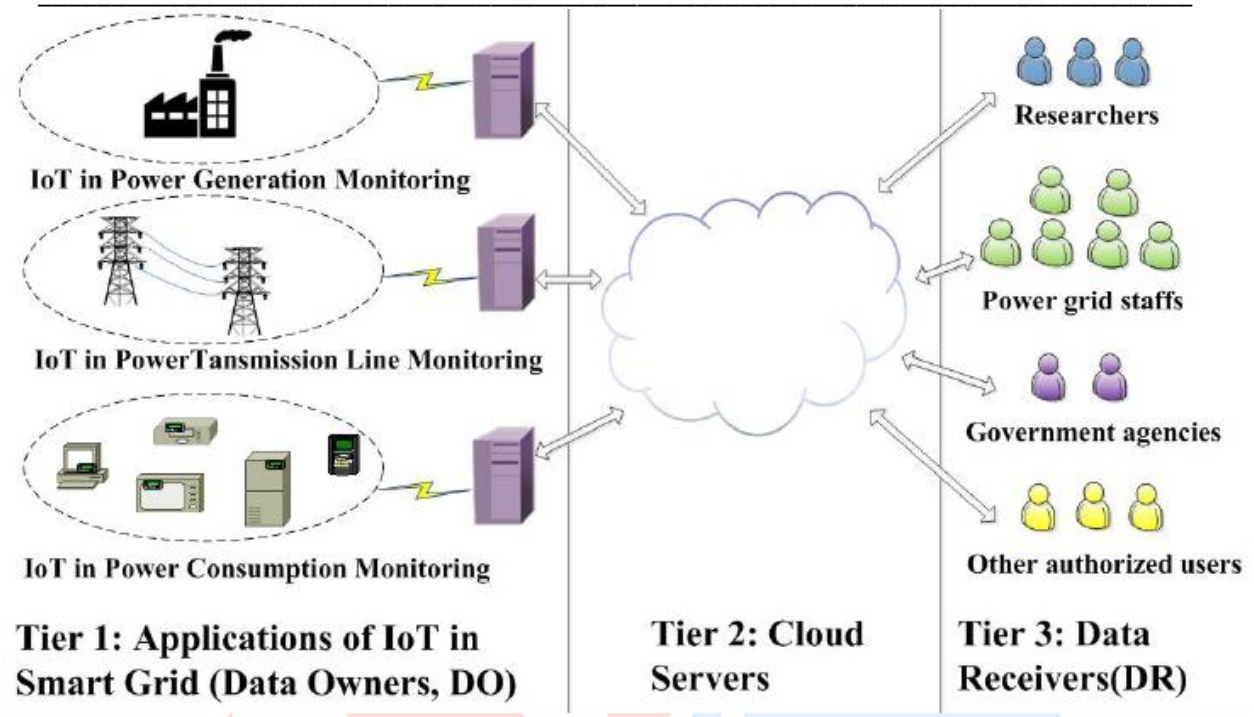
data transmission can be processed in parallel. The data decryption process is similar to the process of data encryption.

- ❖ We introduce the dual secret sharing scheme to protect the access tree information. Only when all of the shares are combined can the secret be recovered. Each of the data blocks holds a share. While the last one share is protected with the other secret sharing scheme. If the user's attributes satisfy the threshold function of root node, then the last share will be retrieved.
- ❖ In addition, some users with the unauthorized attributes sets will be filtered out. We realize the privacy-preserving, the data integrity check and the attributes check simultaneously.

ADVANTAGES OF PROPOSED SYSTEM:

- ❖ We give the security analysis and performance evaluation, which prove that the security of our scheme is no weaker than that of the traditional scheme, and that our scheme can reduce the system response time and users' waiting time notably.
- ❖ Reduces response time overhead significantly compared to other popular schemes.

SYSTEM ARCHITECTURE:



SYSTEM REQUIREMENTS:

HARDWARE REQUIREMENTS:

- System : Pentium Dual Core.
- Hard Disk : 120 GB.
- Monitor : 15'' LED
- Input Devices : Keyboard, Mouse
- Ram : 1 GB

SOFTWARE REQUIREMENTS:

- Operating system : Windows 7.
- Coding Language : JAVA/J2EE

- Tool : Netbeans 7.2.1
- Database : MYSQL

REFERENCE:

Zhitao Guan, Jing Li, Longfei Wu, Yue Zhang, Jun Wu, Xiaojiang Du, "Achieving Efficient and Secure Data Acquisitionfor Cloud-supported Internet of Things in SmartGrid" ,**IEEE Internet of Things Journal, IEEE 2017.**