The Data Privacy and Integrity with Threshold Secret Sharing Method in Cloud Supporting Internet

[1]Gujjula Srinu, Mtech Student [2]P.V.Kishore Kumar, Assistant Professor.
[1,2]Dept of CSE, Eluru College of Engineering and Technology,
Duggirala(V), Pedavegi(M), Eluru, Andhra Pradesh.

ABSTRACT

Cloud-supported Internet of Things (Cloud-IoT) has been broadly deployed in smart grid systems. The IoT front-ends are responsible for data acquisition and status supervision, while the substantial amount of data is stored and managed in the cloud server. Achieving data security and system efficiency in the data acquisition and transmission process are of great significance and challenging, because the power grid-related data is sensitive and in huge amount. In this paper, we present an efficient and secure data acquisition scheme based on CP-ABE (Cipher text Policy Attribute Based Encryption).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. Furthermore, we protect the information about the access tree with threshold secret sharing method, which can preserve the data privacy and integrity from users with the unauthorized sets of attributes. The formal analysis demonstrates that the proposed scheme can fulfill the security requirements of the Cloud-supported IoT in smart grid. The numerical analysis and experimental results indicate that our scheme can effectively reduce the time cost compared with other popular approaches.

INTRODUCTION

With the support of modern information technologies like the Internet of Things (IoT) and cloud computing, smart grid has emerged as the next-generation power supply network, in which the electricity is generated according to the real-time demands of electric equipment or household appliances. To make the smart grid more intelligent, a great number of IoT terminals are deployed to gather the status of the power grid timely for the control center. Some sample applications are shown in Fig. 1, such as the power transmission line monitoring, power generation monitoring, substation state monitoring, smart metering, electric energy data acquisition, smart home. For instance, in power transmission line monitoring scenario, using preplaced sensors, the status parameters of the transmission line and power towers can be gathered in real time, so that any fault can be diagnosed and located in a timely manner.

In smart grid, the different kinds of applications mentioned above all generate an enormous amount of data, which needs to be stored and managed efficiently. Cloud-IoT is proposed to address this

issue, with the support of cloud computing, mass data from different IoT terminals can be collected and processed by local front-end servers, then transferred and stored in the cloud servers. The data in cloud can be accessed by various types of data users. The power grid staff can continually monitor the status of power grid. Researchers and government agencies can analyze the data for research or policymaking.

EXISTING SYSTEM

- Recently, various techniques have been proposed to address the problems of data security and fine-grained access control. In, Sahai and Waters proposed the Attribute-Based Encryption (ABE) to realize fine-grained access control on encrypted data. In ABE, the encryption policy is associated with a set of attributes, and the data owner can be offline after data is encrypted.
- Vipul Goyal et al developed a new cryptosystem for fine-grained sharing of encrypted data in based on Sahai's work, called Key-Policy Attribute-Based Encryption (KP-ABE).
- To improve system efficiency and protect the user privacy, some researchers study on the multiple authorities.

DISADVANTAGES OF EXISTING SYSTEM:

- Efficiency of data acquisition is not considered due to the large amount of data to be encrypted/ decrypted and transferred.
- In existing smart grid system, the different kinds of applications mentioned above all generate an enormous amount of data, which are not stored and managed efficiently.

PROPOSED SYSTEM:

- We present an efficient and secure data acquisition scheme based on CP-ABE. The main Contributions of our work can be summarized as the following:
- 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.
- We adopt the dual secret sharing scheme, which realizes the privacy-preserving, the data integrity check and the attributes check simultaneously.
- The analysis shows that the proposed scheme can meet the security requirements of data acquisition in smart grid,

IMPLEMENTATION

MODULES

- Data Owner
- Data Receiver
- Cloud Server
- Attribute Authority

MODULES DESCRIPTION

Data Owners (*DO*) *DO* decides the access policy and encrypts the data with CP-ABE. The encrypted data will be uploaded to the Cloud Servers. *DO* are assumed to be honest in the system.

Data Requester/Receivers (*DR*) *DR* sends the decryption request to Cloud and obtain the cipher texts over the internet. Only when their attributes satisfy the access policies of the ciphertext, can they get access to the plaintexts. Data requester/receivers may collude to access the data that is otherwise not accessible individually.

Cloud Servers (*CS*) *CS* is responsible for storing massive volume of data. They cannot be trusted by *DO*. Hence, it is necessary for *DO* to define the access policy to ensure the data confidentiality. CS is assumed not to collude with *DR*.

Attribute Authority (AA) AA is responsible for registering users, evaluating their attributes and generating their secret key *SK* accordingly. It runs the *Setup* algorithm, and issues public key *PK* and master key *MK* to each *DO*. It is considered as fully trusted.

SCREENS

Fig: Home Page

Fig: AA Home

Fig: Owner Home

Fig: Data Receiver Home

Fig: Key Verification

Fig: Cloud Home

CONCLUSION

Cloud-IoT techniques are widely deployed in Smart Grid. Huge amount of data is gathered by IoT front-end devices and stored in the back-end cloud servers. However, 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 challenging issue well. To tackle with this problem, we propose a secure and efficient data acquisition scheme for Cloud-IoT in smart grid. In the proposed scheme, the large data is partitioned into several blocks, and the blocks are encrypted/decrypted and transmitted in sequence. In addition, we adopt the dual secret sharing scheme, which realizes the privacy-preserving, the data integrity check and the attributes check simultaneously.

The analysis shows that the proposed scheme can meet the security requirements of data acquisition in smart grid, and it also reduces response time overhead significantly compared to other popular schemes. The data of the proposed scheme is not uploaded in real time, it is offline before encryption. The research on data timeliness will be our future work.

REFERENCES

[1] X. Fang, S. Misra, G. Xue, and D. Yang, “Smart grid—The new andimproved power grid: A

survey", *IEEE communications surveys &tutorials*, vol. 14, no. 4, pp. 944-980, Dec. 2012.

[2] J. Singh, T. Pasquier, J. Bacon, and H. Ko, "Twenty SecurityConsiderations for Cloud-Supported Internet of Things", *IEEE Internetof Things Journal*, vol. 3, no. 3, pp. 269-284, Dec. 2016.

[3] L. Jiang, L. D. Xu, H. Cai, Z. Jiang. "An IoT-Oriented Data StorageFramework in Cloud Computing Platform", *IEEE Transactions onIndustrial Informatics*, vol. 10, no. 2, pp. 1443-1451, Feb. 2014.

[4] X. Du, Y. Xiao, M. Guizani, and H. H. Chen, "An effective keymanagement scheme for heterogeneous sensor networks", *Ad Hoc Networks*, vol. 5, no. 1, pp. 24-34, Jan. 2007.

[5] X. Du, and H. H. Chen, "Security in wireless sensor networks", *IEEEWireless Communications*, vol. 15, no. 4, pp. 60-66, Aug. 2008.

[6] X. Du, M.Guizani, Y. Xiao, and H. H. Chen, "Defending DoS Attacks onBroadcast Authentication in Wireless Sensor Networks", *in proc. IEEEICC*, 2008, pp. 1653-1657.

[7] X. Hei, X. Du, J. Wu, and F. Hu, "Defending Resource DepletionAttacks on Implantable Medical Devices", *in proc. IEEE GLOBECOM*,2010, pp. 1-5.

[8] X. Hei, and X. Du, "Biometric-based two-level secure access control forImplantable Medical Devices during emergencies", *in proc. IEEEINFOCOM*, 2011, pp. 346-350.

[9] W Yu, G Xu, Z Chen, P Moulema, "A Cloud Computing BasedArchitecture for Cyber Security Situation Awareness", *in proc.International Workshop on Security and Privacy in Cloud Computing(SPCC)*, 2013, pp. 488-492.

[10] A. Sahai, and B. Waters, "Fuzzy Identity-Based Encryption", *in proc. EUROCRYPT*, 2005, pp. 457-473.

[11] V. Goyal，O. Pandey，A. Sahai，and B. Waters, "Attribute-basedencryption for fine-grained access control of encrypted data", *in proc.CCS*, 2010, pp. 89-98.