Attribute-based Data Security with Obfuscated Access Policy for Smart Grid Applications

Kamalakanta Sethi[1], Ankit Pradhan*[1], Padmalochan Bera[1]
*ap36@iitbbs.ac.in
[1]School of Electrical Sciences, IIT Bhubaneswar, India

1. Introduction

- Smart grid employs intelligent transmission and distribution networks for effective and reliable delivery of electricity.
- It uses fine-grained electrical measurements to attain optimized reliability and stability by sharing these measurements among different entities of energy management systems of the grid.
- There are many stakeholders like users, PMUs, and other entities, with changing requirements involved in the sharing of the data. Therefore, data security plays a vital role in the correct functioning of a power grid network.
- Attribute-based encryption (ABE) can provide efficient and secure management of access control in smart grid.
- In this poster, we propose an attribute-based encryption (ABE) for secure data sharing in Smart Grid architectures as ABE enables efficient and secure access control. Also, the access policy is obfuscated to preserve privacy. We use Linear Secret Sharing (LSS) Scheme for supporting any monotone access structures, thereby enhancing the expressiveness of access policies. Finally, we also analyze the security, access policy privacy and collusion resistance properties along with efficiency analysis of our cryptosystem.

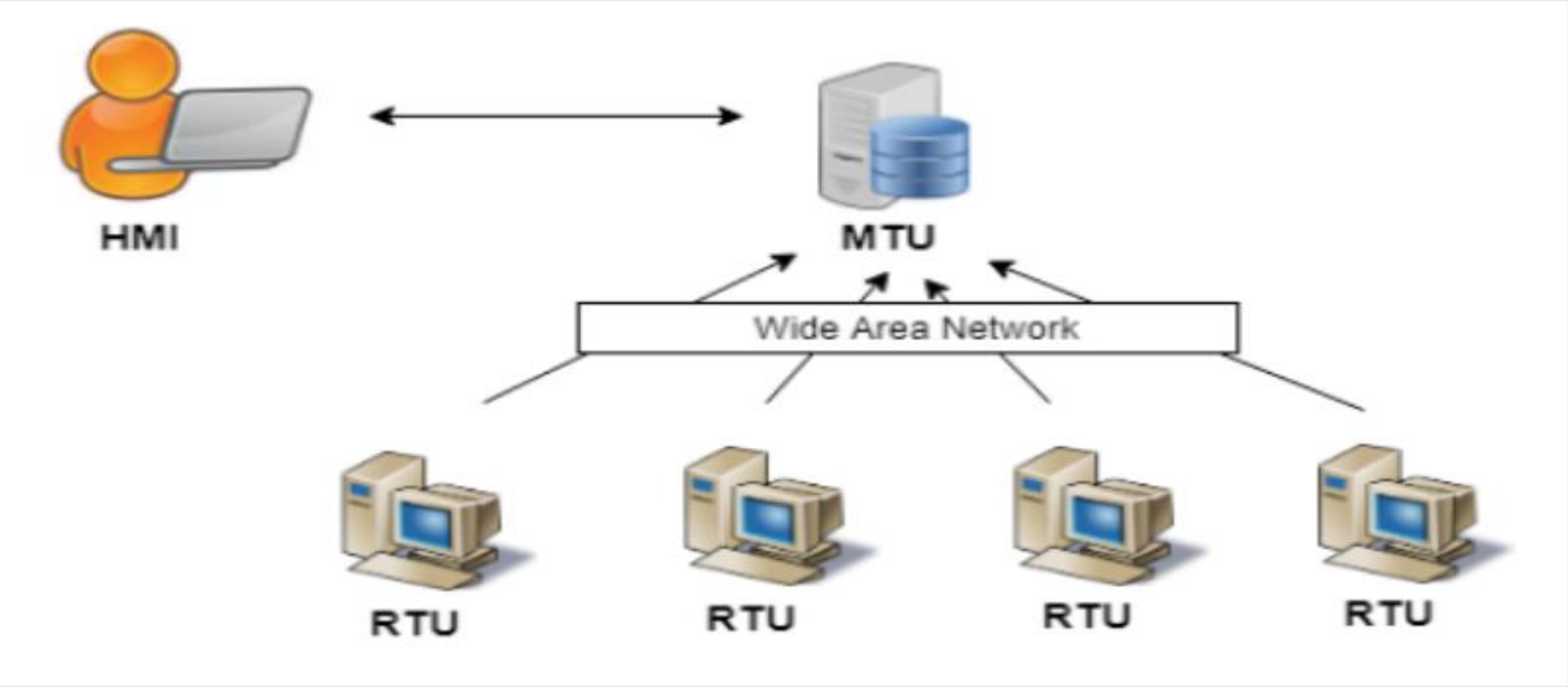
2, Background

- Prime Order Bilinear Groups: Our scheme is built on prime-order bilinear groups.
- Access Structure: We focus monotonic access structure in our construction.
- Anonymous Key Agreement Protocol: It helps in obfuscating access policy for smart grid application.
- Linear Secret Sharing (LSS) Schemes: Our proposed solution has access policies designed on linear secret sharing schemes (LSS) which improve not only the expressiveness of the policy but also computational efficiency.

3. System Model

- System model of our proposed cryptosystem consists of various entities namely Key generation center (KGC), Storage center (SC), Sender and User. The system is shown in the Figure.
- **Key Generation Server (KGC):** It is the primary authority for generating public and secret keys and other cryptographic parameters for various entities in the smart grid. Depending on attributes of each entity, it can grant requisite access rights and by itself has no access to the plaintext of the encrypted information of the smart grid.
- **Storage Center:** This is a repository center for data in the smart grid which controls data access from users. In the SCADA model, the role of storage center lies on the MTU for storing data generated by the RTUs and permit access to other users. Obfuscation of access policies becomes important when the storage center is semi-trusted. Storage center can also be relied upon taking action on ciphertext metadata like 'Critical' tag or 'Intended User' tag to forward message to appropriate recipient.
- **Sender:** It is an entity which generates and transfers the data to the storage center. In our model, the sender defines the access policy of our attribute-based model, encrypts the data using the policy, and obfuscates the policy before uploading the ciphertext to the storage center. As an illustration, we note that an RTU or power metering device can act a sender by defining the access policy for its metering data,
- **User:** User leverages the human-machine interface to access information from the storage center. As in attribute-based schemes, a user can decrypt those ciphertexts stored at the storage center for which the attributes in his attribute set satisfy the access policy of the ciphertext.

System Model Diagram



4. Algorithmic Definitions

- **GlobaSetup:** This algorithm generates global parameters (GP) by taking a security parameter.
- **KGCSetup:** This procedure is executed by KGC . It takes GP as input and produces public key and secret key for KGC.
- **SCSetup:** Storage Center with an identifier ID invokes this procedure by taking GP as input and produces public key and private key for SC
- **KeyGen:** This procedure generates secret key of user by taking attribute set S of user, secret key of KGC and GP.
- **Encrypt:** This procedure is called by data owner that wants to store the data in cloud. This step encrypts a message M with respect to a policy A, public key of KGC, public key of SC, and GP. It generates the ciphertext CT.
- **TokenGen:** This procedure is executed by user to generate token TK. After generation of token, user send it to SC for partial decryption of ciphertext CT. This procedure takes global parameter GP, ciphertext CT and secret key of the user as input.
- **PartialDecrypt:** This step is executed by SC to generate partial decrypt ciphertext CT'. It takes GP, CT and token TK as input
- **Decrypt:** This procedure is exected by user to generate plaintext message. It takes GP, partially decrypted ciphertext CT' and secret key of user as input

5. Performance Comparison

Schemes	Access Structure	Obfuscated policy	Ciphertext size	Secret key size	Public key Size
Hur's scheme [2]	AND-OR Threshold gates	Yes	(2r+1)a+b+A	(3s+1)a	2a+b
CP_ABSC Scheme[1]	AND-OR Threshold gates	No	(2r+3)a+b+A	(2s+1)a	2a+b
Our scheme	LSS	Yes	(2r+1)a+b+A	(3s+1)a	2a+b

6. Conclusion and Future Work

- We proposed a policy-obfuscated attribute-based encryption scheme which is suitable for the applications of smart grid. Our scheme is designed for the large attribute universe model with immediate implications for large scale scalability.
- It is also shown to be effective as our mathematical construction is based on groups of prime order.
- Our scheme preserves the privacy of access policies, and by modelling policies as monotonic access structures using linear secret sharing (LSS) scheme, it supports high expressiveness.
- Outsourcing decryption is inherently built in the construction, which relieves the computational load of the users.
- Apart from smart grids, we believe that this scheme can also be extended for secure data access control in areas like electric vehicular transportation.

7. References

[1] C. Hu, J. Yu, X. Cheng, Z. Tian, K. Akkaya, and L. Sun, "CP-ABSC: An attribute-based signcryption scheme to secure multicast communications in smart grids", Mathematical Foundations of Computing, 2018.

[2] J. Hur, "Attribute-Based Secure Data Sharing with Hidden Policies in Smart Grid", in IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 11, pp. 2171-2180, Nov. 2013.

[3] C. Hahn, H. Kwon, and J. Hur, "Efficient Attribute-Based Secure Data Sharing with Hidden Policies and Traceability in Mobile Health Networks", Mobile Information Systems, vol. 2016, Article ID 6545873, 13 pages, 2016.

[4] Z. Guan, J. Li, L. Wu, Y. Zhang, J. Wu and X. Du, "Achieving Efficient and Secure Data Acquisition for Cloud-Supported Internet of Things in Smart Grid," in IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1934-44, Dec. 2017.