Smart Grid Data Security using Practical CP-ABE with Obfuscated Policy and Outsourcing Decryption

Ankit Pradhan, Punith R., Kamalakanta Sethi, and **Padmalochan Bera**

IIT Bhubaneswar

June 15, 2020

Introduction

- Efficient, scalable and secure solutions are needed for accessing data over various entities of power distribution systems and the smart grid.

- Traditional public key infrastructure is inefficient in handling the current scenario where billions of devices are connected through Internet of Things and data compromise might lead to substantial financial losses.

- Attribute-based encryption (ABE) can provide efficient and secure management of access control in smart grid enabling smart meters to encrypt data using a set of attributes and construct an access policy for preventing potential adversaries from accessing critical information.

Introduction

Requirements in the context of smart grid:

1. Improve scalability of current ABE designs to encompass large number of attributes.
2. Improve computational time of encryption and decryption algorithms.
3. Access policy privacy for players in smart grid related business corporations.
4. Improve expressiveness of access policies to cater to various changing requirements of data access.
5. Reduce burden on end users for decryption of large ciphertexts collected from smart meters.

Related Work and Background

Related Work:

1. *Attribute-Based Secure Data Sharing with Hidden Policies in Smart Grid* by J. Hur in IEEE Transactions on Parallel and Distributed Systems, 2013.
2. *CP-ABSC: An attribute-based signcryption scheme to secure multicast communications in smart grids* by C. Hu, J. Yu, X. Cheng, Z. Tian, K. Akkaya, and L. Sun in Mathematical Foundations of Computing, 2018.

Background:

1. Prime Order Bilinear Groups [1]
2. Monotonic Access Structures [2]
3. Linear Secret Sharing Schemes (LSS) [2]
4. Anonymous Key Agreement Protocol [3]

SCADA Architecture

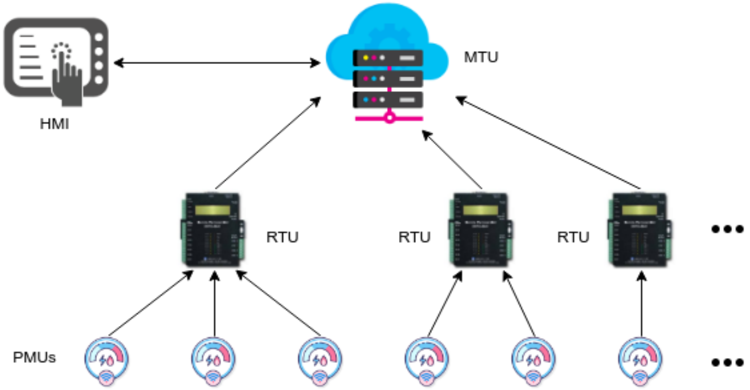

Figure 1: Simplified SCADA Architecture

Smart Grid entities from security perspective

1. **Key generation center (KGC)**: Primary entity for generating public and private keys for all units of the system.

2. **Storage center (SC)**: Repository center for data in the smart grid controlling data access. MTUs can act as SC for storing data generated by the RTUs and permitting access to other users.

3. **Sender**: Entity generating and transferring data to the SC. It defines the access policy for the data, encrypts the data using the policy, and obfuscates the policy before uploading the ciphertext to the SC.

4. **User**: Entity leverages the HMI to access information from the SC.

System Model

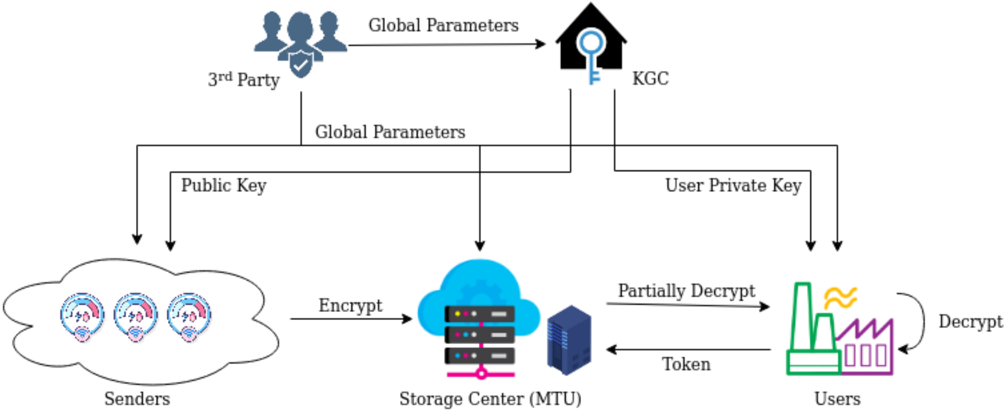

Figure 2: Representative System Model

Construction

Our scheme consists of the following probabilistic polynomial time (PPT) algorithms, categorized into the groups:

1. Setup (*GlobalSetup*, *KGCSetup*, *SCSetup*)
2. Key Generation (*KeyGen*)
3. Encryption (*Encrypt*)
4. Token Generation (*TokenGen*)
5. Partial Decryption (*PartialDecrypt*)
6. Decryption (*Decrypt*)

Details are presented in the paper!

Security Analysis

We analyze the security of our design from three perspectives:

1. **Data Confidentiality**: Trivially by design (Data Encryption)
2. **Access Policy Privacy**: Special design for obfuscating access policy during data encryption (Anonymous one-way key agreement)
3. **Collusion Resistance**: Attackers colluding with each other and pooling respective attributes cannot recover the message from the ciphertext. Ensured by design (blinding $e(g, g)^{s\alpha}$ in case of attack)

Efficiency Analysis

We compare the theoretical efficiency of Obfuscated Policy ABE with Hur's scheme [4] and CP-ABSC scheme [5] using the following notations in the theoretical analysis.

- $\mathbb{A}$ - Size of access policy
- α - storage overhead of an element in G
- β - storage overhead of an element in G_T
- l - Number of rows in in the LSS scheme matrix
- s - Number of attributes used in private key of an user.
- r - number of attributes in access policy associated with ciphertext.

Efficiency Analysis

Table 1: Key features

Schemes	Access structure	Obfuscated Policy
Hur [4]	AND-OR Threshold gates	Yes
CP_ABSC [5]	AND-OR Threshold gates	No
Obfuscated Policy ABE	LSS	Yes

Table 2: Efficiency Comparison

Schemes	Secret key size	Public key size	Ciphertext size
Hur's scheme [4]	$(3s+1)\alpha$	$2\alpha+\beta$	$(2r+1)\alpha+\beta+\mathbb{A}$
CP_ABSC scheme [5]	$(2s+1)\alpha$	$2\alpha+\beta$	$(2r+3)\alpha+\beta+\mathbb{A}$
Obfuscated Policy ABE	$(3s+1)\alpha$	$2\alpha+\beta$	$(2l+1)\alpha+\beta+\mathbb{A}$

Obfuscated Policy ABE vs. Hur [4] and CP_ABSC [5]

Experimental Analysis

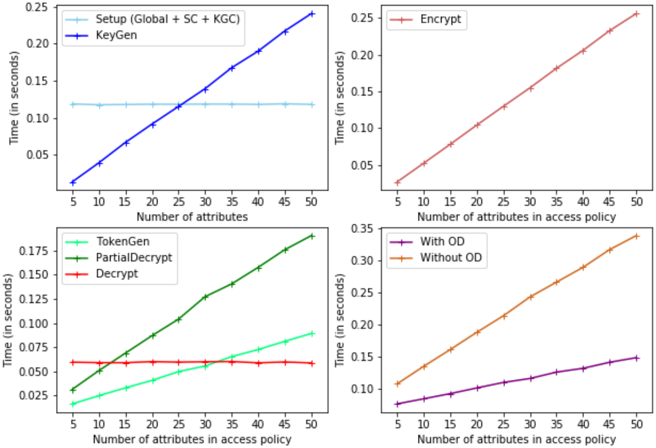

Figure 3: Execution time for various algorithms and the efficiency of Outsourcing Decryption (OD)

Conclusion and Future Work

Designed a practical policy-obfuscated ABE scheme suitable for the applications in Smart Grid:

1. Scalable (Large attribute universe design)
2. Faster (Construction on prime order groups)
3. Privacy preserving (Access Policy obfuscated)
4. Expressive and efficient access policy (LSS)
5. Less burden on users (Outsourcing decryption)

Future work aims at:

1. Reduce Sender encryption overhead by partial encryption and outsourcing full encryption to semi-trusted remote server followed by a secure verification of the full encryption.
2. Designing highly expressive constant ciphertext size ABE scheme with obfuscated policy benefit for Smart Grid.

Bibliography

Jae Hong Seo and Jung Hee Cheon.
Beyond the Limitation of Prime-Order Bilinear Groups, and Round Optimal Blind Signatures
In *Theory of Cryptography Conference*, Berlin, Springer, LNCS, vol. 7194, pp. 133-150, 2012.

Amos Beimel.
Secure schemes for secret sharing and key distribution
Ph.D. dissertation, Faculty Comput. Sci., Technion–Israel Inst. Technol., Haifa, Israel, 1996.

Aniket Kate, Greg Zaverucha, and Ian Goldberg.
Pairing-Based Onion Routing
In *Proceedings of Privacy Enhancing Technologies Symposium*, PET 2007, pp. 95-112, 2007.

Junbeom 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.

Chunqiang Hu, Jiguo Yu, Xiuzhen Cheng, Zhi Tian, Kemal Akkaya, and Limin Sun.
CP-ABSC: An attribute-based signcryption scheme to secure multicast communications in smart grids
In *Mathematical Foundations of Computing*, 2018.