Encrypted Data Sharing Using Proxy ReEncryption in Smart Grid

Anass Sbai, C. Drocourt, Gilles Dequen

Encrypted data sharing using Proxy ReEncryption in smart grid

Anass Sbai, Cyril Drocourt, and Gilles Dequen

University Of Picardie Jules Verne
https://www.mis.u-picardie.fr/
MIS Laboratory, 14 Quai de la Somme, 80080 Amiens, France

Abstract. In a rapidly changing territory, energy networks must be increasingly responsive and flexible. New models of multi-fluid management and energy production are being created and developed on national and international level. This involves the use, monitoring and supervision of many sensors that reports lot of data. This paper deals with the secure management of large amounts of data within the context of smart grid. We propose a solution based on proxy re-encryption designed primarily to allow decryption delegation, which allow a neat management of large amount of data while respecting the GDPR (General Data Protection Regulation) and security standards.

Keywords: Smart Grid, Cloud Computing, Security, Proxy Re-Encryption

1 Introduction

The fight against global warming led to the emergence of new energy markets and great challenges. It involves the installation of a whole infrastructure and communication networks which requires a great deal of attention at the security level. In 2010, the discovery of the STUXNET virus [1] triggered debates on security in the energy industry. Standardization organisms and agencies were the first to be involved. The European Council entrusted the standardization organisms (CEN, CENELEC and ETSI) with the mandate M490 [2] to adopt security standards for smart grids. Various norms and security methods already existed, the challenge was how to make them combined and harmonized. CEN offers the Smart-Grid Architecture Model (SGAM) which gives a three-dimensional projection of the entire system in form of layers, areas, and domains. This conceptual representation allows to model the use cases, identify required standards and identify the gaps and standards needs. Thus we can focus on end to end security, from the component layer to the business layer. In the context of VERTPOM project, the goal is to deploy a decision support tool called BANK of ENERGY (BE) that help the transition to positive energy territories. Thus, by maintaining an optimized balance between the produced energy with regard to usage and energy storage means [3]. The energy networks must be more responsive, flexible, and thus foster interactions between market players. As illustrated in figure 1,

the BE need the consumption data transmitted by smart meters via data concentrators and stored by the NEM (Network Energy Manager). Also production data handled by the EP (Energy Provider) and other data collected by sensors that could be stored and handled by an other NEM. In 2014, a compliance pack for smart meters which provides a regulation for personal data was proposed by the CNIL (Commission Nationale de l'Informatique et des Libertés) [4]. To sum up, they define the consumption data, precisely the load curves, as the property of the consumer and above all as a sensitive data. From the CNIL's point of view, the provider could have access to theses data only if the consumer gives his consent, which is done in general via the contracts. For commercial prospecting, data processing or sales to subcontractors, the data must be anonymized. In this paper, we propose a novel approach to preserve privacy in the context of smart grids. Instead of anonymizing the data, we opted for an encrypted data storage in the cloud. Only data owners will be able to access the appropriate data and entities to which we have delegated decryption's right. For this purpose we use the concept of proxy re-encryption. In the next section we will present some related works, then we will detail our approach and show its compatibility with the CNIL's regulation. Finally, we will conclude with a discussion regarding the advantages and limitations of our solution.

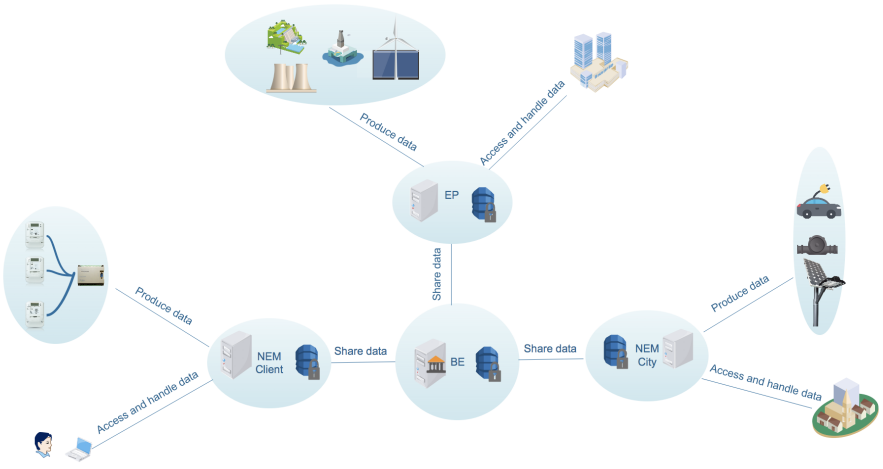

Fig. 1. Architectural model for the Bank of energy.[5]

2 Related Works

The main inconvenient of todays Cloud Storage Provider (CSP) solutions (e.g iCloud, OVH, GoogleDrive ...), is that they are considered as an all-trusted

part. Either the data are encrypted under a key known by the cloud or stored in plaintext. Several works aim to enforce confidentiality while allowing efficient data sharing. Starting with the broadcast encryption designed by Fiat [6]. Another similar approach was introduced by Sahai in 2005 [7] which is Attribute Based Encryption. Inspired by [8] system, their idea was to create a new type of IBE that they called fuzzy IBE to combine encryption and access control. But none of these solutions allow for a selective sharing. As an alternative to these solutions, we choose to use the proxy re-encryption(PRE). It allows the transformation of ciphers intended to Alice into new ciphers that can be decrypted by Bob. First appeared in 1998, it was designed by the trio BBS [9], where instead of recovering, decrypting then encrypting the data to bob, Alice generate a re-encryption key and rely on a semi-trusted proxy to convert the ciphers using the key created by Alice. One of the drawbacks of their method is that the system is bidirectional. That is to say, if Alice delegate decryption rights to Bob, the latter would consequently delegate decryption rights to Alice. Y.Dodis [10] formalizes the design of proxy re-encryption schemes by categorizing these systems in two types: unidirectional and bidirectional. In [11] proposes a cloud based solution for file sharing called SkyCryptor using PRE. The idea is to use a unique symmetric key for each file to be encrypted with AES and then encrypt the key with the asymmetric public key of the user generated thanks to the PRE algorithm. The solution is dedicated device and now marketed under the name of BeSafe. Each user's device have it's own key pair and the re-encryption is used to share the files between different devices or users. But above all, the users must install the BeSafe software and use it to encrypt the data. Instead, we proposed in [5] the PREaaS which doesn't need any heavy client and which is more flexible, modular and transparent.

3 Our Contribution

3.1 PREaaS

In figure 1, we illustrate an architectural model for the BE, were it interacts with two NEMs and one EP. We can classify all entities into three main actors :

- *Data producers* : Devices generating data (sensors, smartmeters ...).
- *Data owners* : Entities that owns the data produced.
- *Data consumers* : Entities that need to use these data .

The idea is that the data produced must be encrypted before storage, in such a way that only the data owner (DO) could decrypt and delegate access rights to data consumers. The DO could retrieve the data directly from the CSP and DO's authentication would be preferable but not mandatory. Because, even if we give access to every one. Only the holder of the appropriate secret could decrypt it or entities to which the DO has delegated decryption rights. So, authentication will not add any warranty in terms of confidentiality but above all could be used by the CSPs to avoid DDos-attacks. There are several

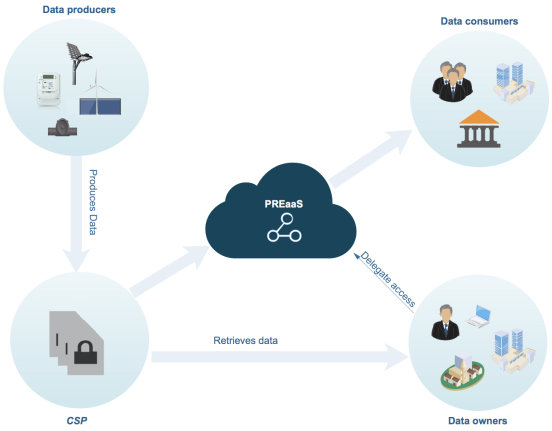

Fig. 2. Tasks distribution between different environments

ways to implement such a mechanism, which we discussed in [5]. To reduce the costs, instead of having each entity implementing a PRE, we proposed the PRE as a service. The PREaaS, has the advantage to manage only encrypted data and handle only public keys and Re-encryption keys. Even if CSPs or users are corrupted and collude with the PREaaS, it won't affect the confidentiality. This is guaranteed by careful choice on the algorithms used by the service. We assume that a shared secret exists between Data Owner (DO) and Data Producer (DP) which encrypt data. This secret will be encrypted by the DO's public key as any other KEM/DEM mechanism. This already exist and known as hybrid encryption, but the novelty as in SkyCryptor is that the asymmetric encryption scheme used will be a unidirectional proxy re-encryption scheme. That way, when the DC wants to access to some data that does not belong to him, the CSP will forward his request to the DO including the DC's public key. As a response, the data owner creates a re-encryption key and transmit it to the CSP. The latter calls the PREaaS to re-encrypt the corresponding cipher of the session key and send the encrypted data.

If we take over the CNIL's obligations, our solution is compatible and allows to have a real consent from an interface and not via contracts with pre-checked box. It can be proposed in addition to the anonymization solution, knowing that anonymization is a difficult task specially for dynamic databases.

3.2 Implementation

Many solution exist that implement PRE, like BeSafe presented later in the paper, but their main inconvenient is the need to install a software in the client side. We chose to use JavaScript as a core technologie, and thus to be executed in the client side directly by navigator or even mobile devices without any software and also in the server side thanks to NodeJs. For scalability and flexibility

purpose, the PREaaS must allow the use of different PRE algorithm. We already implemented one of the most efficient unidirectional PRE which is Chow's algorithm. But the security of the scheme is still a concern where the security proof of the latter are based on random oracle. It is better to use schemes that are proven CCA-secure in the standard model. But all these schemes uses pairing based solution which is expensive in terms of computation. We proposed the first CCA-secure unidirectional PRE in the standard model without pairings in [12] and present the result of its implementation below. Our scheme is based on the Cramer-Shoup encryption system which is by design CCA-secure in the standard model, while Chow's algorithm is based on ElGamal encryption scheme and rely on Schnorr signature to reach the CCA security. First we use a generic group with prime order length 3072-bit, and the second one using NIST Standard ECC p-256 [13] thanks to SJCL [14]. Both correspond to the same security level that is 128-bit. For the tests we used a 2,5 GHz intel core i7, with 16 GB RAM. Table 2. shows the time resources consumed by the different function of

	Chow		Our schceme	
Function	$\mathbb{F}_p$	Ecc	$\mathbb{F}_p$	Ecc
KeyGen	515	68	1653	163
ReKeyGen	502	48	2450	235
Encrypt	1000	95	2313	216
ReEncrypt	967	89	2372	229
Decrypt	979	78	1649	137

Table 1. Computational efficiency of Chow and our algorithm in (ms)

both algorithms. We can see that our scheme is more expensive than Chow's which is normal. If we take for example the key generation of our scheme, even before implementing it we can see that it will cost almost 3 times more than Chow's algorithm since we generate 7 elements for the secret key against 2 for Chow. The most important information that we must take into account, is that encryption and re-encryption functions consumes the most compared to keys generation and decryption. Practically, encrypt and key generation functions wont be so called. Generating re-encryption keys, depends on the number of delegations needed, but still not constraining in terms of time consuming. On the other side, re-encryption function is called for each new user, new delegation and changed session key. Having an independent service that do the re-encryption work is lightening.

4 Conclusion

In the context of smart grid we proposed the PREaaS to manage large data flows. However, data producers remain limited and constrained in terms of resources.

Fig. 3. Tasks distribution between different environments

But the implementation of this type of solution based on asymmetric encryption remains possible. Several works aim to optimize FPGA implementation of elliptic curve and now there is even implementation of Weil and Tate pairing. The PREaaS will allow the use of different PRE algorithm in future such as BBS with ephemeral keys, Ateniese scheme... As a part of the VERTPOM's project, we will work on authentication issues in multi cloud systems which we haven't treated in this work.

References

1. Aleksandr Matrosov, Eugene Rodionov, David Harley, and Juraj Malcho. Stuxnet under the microscope. *ESET LLC (September 2010)*, 2010.
2. Smart Grid Coordination CEN-CENELEC-ETSI. Group sgcg/m490. *B_Smart Grid Report First set of standards Version*, 2, 2014.
3. Jean-Paul Boronat. Véritable énergie du territoire positif et modulaire, 2017.
4. A compliance package for smart meters. https://www.cnil.fr/en/innovative-home-energy-management-compliance-package-smart-meters.
5. Anass Sbai, Cyril Drocourt, and Gilles Dequen. Pre as a service within smart grid cities. In *16th International Conference on Security and Cryptography*, 2019.
6. Amos Fiat and Moni Naor. Broadcast encryption. In *Annual International Cryptology Conference*, pages 480–491. Springer, 1993.
7. Amit Sahai and Brent Waters. Fuzzy identity-based encryption. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 457–473. Springer, 2005.
8. Dan Boneh and Matt Franklin. Identity-based encryption from the weil pairing. In *Annual international cryptology conference*, pages 213–229. Springer, 2001.
9. Matt Blaze, Gerrit Bleumer, and Martin Strauss. Divertible protocols and atomic proxy cryptography. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 127–144. Springer, 1998.
10. Anca-Andreea Ivan and Yevgeniy Dodis. Proxy cryptography revisited. In *NDSS*, 2003.
11. Aram Jivanyan, Roland Yeghiazaryan, Armen Darbinyan, and Azat Manukyan. Secure collaboration in public cloud storages. In *CYTED-RITOS International Workshop on Groupware*, pages 190–197. Springer, 2015.
12. Anass Sbai, Cyril Drocourt, and Gilles Dequen. Cca secure unidirectional pre with key pair in the standard model without pairings. In *6th International Conference on Information Systems Security and Privacy*, 2020.
13. Shay Gueron and Vlad Krasnov. Fast prime field elliptic-curve cryptography with 256-bit primes. *Journal of Cryptographic Engineering*, 5(2):141–151, 2015.
14. Emily Stark, Mike Hamburg, and Dan Boneh. Stanford javascript crypto library, 2013.