POSTER: Reliable and Efficient Protection of Consumer Privacy in Advanced Metering Infrastructure

Vitaly Ford and Ambareen Siraj

Computer Science Department, Tennessee Tech University
Cookeville, TN 38505, USA
vford42@students.tntech.edu, asiraj@tntech.edu

Abstract. We are investigating a novel approach towards reliable and efficient protection of consumer privacy in the Advanced Metering Infrastructure (AMI). In the smart grid, one of the main concerns of consumers is associated with the usage of the smart meters and how utility companies handle energy consumption data, which can potentially reveal sensitive and private information about consumers. Current solutions provide privacy-preserving protocols using zero-knowledge proofs and homomorphic encryption, which work on aggregated smart meter data. There is still lack of an integrated solution that enables privacy preservation with access to fine-grained data such that opportunities of making energy consumption more efficient are not sacrificed. Such access will also enable other forms of advanced intelligent analysis like energy fraud detection. In this regard, we propose a three-tier privacy preservation model that includes secure communication among smart meters, utility company, and a Trusted Third Party (TTP) using Certificateless Public Key Encryption and AES 128. It is a flexible framework allowing protection of consumer privacy such that only consumers can securely retrieve their fine-grained readings through the TTP's web-portal. This protocol supports dynamic rate utilization as well as data mining for advanced analysis. In addition, the proposed secure framework satisfies computational resource limitations in the Advanced Metering Infrastructure and provides a scalable solution for efficient consumer privacy-preserving billing.

Keywords: Security, AMI, privacy-preserving protocol.

1 Introduction

We introduce a three-tier model for secure smart meter communication that enables consumer's privacy preservation as well as retention of fine grained data analysis capability. The model comprises of Smart Meters (SMs), Utility Companies (UCs), and a Trusted Third Party (TTP). TTP has direct access to fine-grained consumer data and has the capability to include additional advanced analysis features, such as fraud detection. The data are secured in such a way that TTP cannot link energy consumption readings with any particular consumer. In the proposed model, SMs encrypt all the energy consumption data and send the encrypted traffic to TTP through a separate collector entity in the UC's smart metering network. However, UC can only relay the energy measurements to TTP without having the ability to decrypt them.

Many existing solutions [2, 3, 4] propose different protocols that have to be used in the smart grid at the same time for load monitoring, aggregation, billing and fraud detection. Instead of using varied protocols for the above-mentioned operations, the proposed architecture utilizes one protocol with minimal overhead to SMs.

2 Approach

The following describes the proposed model for the AMI infrastructure. The three-tier system consists of SMs, UCs, and TTP storage system. TTP is an independent private organization, whose service is purchased by UCs. TTP can manage meter data from several different electricity providers and thus release the AMI infrastructure from unnecessary computations, such as aggregation, fraud detection, and energy consumption analysis. There is also a collector(s) installed by UC, which facilitates collection of energy consumption data from various SMs. Fig. 1 shows the high-level architecture (solid lines correspond to an internal UC network and dashed lines correspond to the Internet connectivity).

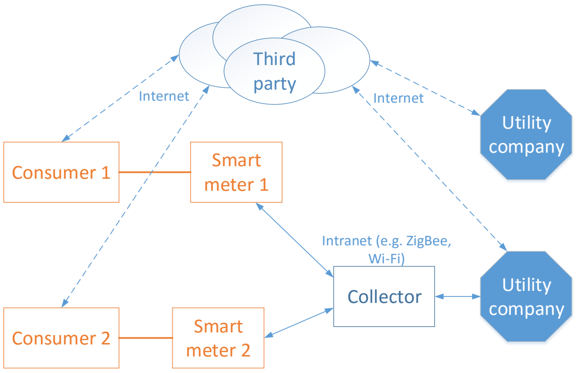

Fig. 1. Proposed architecture.

In the proposed model (Fig. 1), TTP is connected to UC via the IP-based communication line in the Internet. SMs are not directly connected with the TTP and instead connected through UC. This is because SMs connect with their UCs via an internal network to decrease the possibility of attacks that are common in the Internet.

In this model, UC deploys SMs and has limited control over them. The control is restricted for preserving consumer privacy and UCs are only allowed to provide administrative support for AMI, such as verifying SMs availability.

When UC deploys SM, it generates a random identification number (ID) for SM in the household. SM and TTP initiate a Certificateless Public Key Exchange Protocol (CLPKE) [1], where UC serves as the Key Generation Center. Once public/private keys are distributed to both parties, TTP generates a session key for securely communicating energy consumption data from SM to TTP and sends it via an encrypted connection (using public/private keys) to SM. SM stores the session key in its TPM and uses it for sending energy readings to TTP via UC.

SM encrypts energy consumption (*EC*) measurements and sends them to the collector. The main responsibility of the collector is to temporarily store the encrypted *EC* data and send them to UC in a predefined time interval. UC forwards the encrypted *EC* data to TTP. Without knowledge of the key, UC cannot decrypt the data and thus, privacy is preserved for their clients. TTP decrypts all received data and stores them in its database.

At the time of billing, UC sends TTP a request for *EC* readings to be billed, including the anonymized meter's ID and price ranges for different periods of time. TTP authenticates UC, queries the requested data from its database, and aggregates energy on a daily/monthly basis depending on the policy and bill calculation requirements.

When a consumer receives the bill, he/she can check the correctness of the billing computations. Consumers can connect to the TTP web-service, authenticate without revealing their real identity, and gain access to their fine-grained data.

The features of the proposed protocol are as follows:

- Energy data are encrypted by SMs and anonymized by UC prior to being sent to TTP.
- Lightweight efficient encryption is used for the main parts of communication. We use Advanced Encryption Standard (AES) 128-bit keys for securing communication between SM and UC as well as SM and TTP.
- UC forwards the anonymized and encrypted data to TTP via a wide area network. UC cannot decrypt the data, preserving consumer privacy.
- UC can acquire aggregated decrypted data from TTP on request for billing purposes.
- TTP cannot identify real consumers because of anonymization of SM's ID.
- Additional consumer energy consumption analysis can be done at TTP without disclosure of any sensitive information about consumers.
- UC cannot ask a consumer to pay a fee different from the one that was produced by TTP for billing.

3 Protocol Phases

There are three main phases in the proposed protocol: *registration phase* (Fig. 3), *session key exchange phase* (Fig. 4), and *data transmission phase* (Fig. 5). The *registration phase* describes the steps that SMs and TTP have to follow for receiving their public/private key pairs from UC based on the CLPKE [1]. Those keys will allow SM and TTP to establish a secure and private connection for exchanging a session key used for further communication between SM and TTP at the *data transmission phase*.

1) *Registration phase.*

UC serves as a Key Generation Center. SMs and TTP communicate with UC in order to obtain public/private keys. Any communication between SM and UC is encrypted with the pre-shared key $S_{SM\text{-}UC}$. When SM sends UC an encrypted (with $S_{SM\text{-}UC}$) message, it concatenates its $\mathrm{ID}_{\mathrm{SM}}$ so that UC can identify the meter upon receiving the message and decrypt it accordingly. The message consists of a request to generate keys and a timestamp against replay attacks. UC generates the keys and sends them to SM. UC and TTP have to establish a *TLS* connection before UC sends the keys for TTP.

2) *Session key exchange phase.*

When SM and TTP complete the registration phase, they initiate a session key exchange phase in order to share a secret key used for encrypting/decrypting fine-grained meter readings. SM uses TTP's public key for encrypting the message containing a request to share a key and a random number used as an extra security measure against man-in-the-middle attacks. In addition, SM sends an HMAC to preserve integrity. Upon receiving the message, TTP generates the session key $S_{SM\text{-}TTP}$, concatenates the random number, encrypts the packet with SM's public key, and forwards it to SM via UC.

3) *Data transmission phase.*

The session key established at the *session key exchange* phase is used for sending meter readings from SM to TTP. Thus, only SM and TTP can decrypt the fine-grained measurements. SM sends energy consumption (EC) along with a timestamp t to UC by encrypting the data with $S_{SM\text{-}TTP}$. It also concatenates an HMAC to the message by hashing $EC \mid\mid t$ and its real $\mathrm{ID}_{\mathrm{SM}}$. UC verifies HMAC and forwards the received data to TTP, replacing $\mathrm{ID}_{\mathrm{SM}}$ with an-$\mathrm{ID}_{\mathrm{SM}}$ found in its table mapping real $\mathrm{ID}_{\mathrm{SM}}$ with the anonymized an-$\mathrm{ID}_{\mathrm{SM}}$. TTP decrypts $EC \mid\mid t$ by using $S_{SM\text{-}TTP}$ and retrieves the data.

4 Conclusion and future work

Proposed secure AMI preserves consumer privacy in terms of billing and advanced fine-grained data analysis, such as fraud detection. It takes into account the limited capabilities of Smart Meters and can be implemented with minimum changes to the current grid. Also, consumers can access their own fine-grained data stored at TTP. We are currently working on formal and empirical evaluation of the proposed privacy preserving protocol for AMI infrastructure.

Acknowledgements. This work is supported by the Center for Energy Systems Research of Tennessee Tech University. We are thankful to Michael Pyle, Chief Security Officer and VP of Cyber Security at Schneider Electric, Nashville TN, for his invaluable comments and feedback.

References

1. Sun, Y., Zhang, F., Baek, J.: Strongly Secure Certificateless Public Key Encryption without Pairing. Cryptology and Network Security Lecture Notes in Computer Science. 194--208.
2. Joye, M., Libert, B.: A Scalable Scheme for Privacy-Preserving Aggregation of Time-Series Data. Financial Cryptography and Data Security LNCS. 111--125.
3. Lin, H.-Y., Tzeng, W.-G., Shen, S.-T., Lin, B.-S.P.: A Practical Smart Metering System Supporting Privacy Preserving Billing and Load Monitoring. Applied Cryptography and Network Security Lecture Notes in Computer Science. 544--560.
4. Ruj, S., Nayak, A., Stojmenovic, I.: A security architecture for data aggregation and access control in smart grids, arxiv.org/pdf/1111.2619.pdf.