Accepted Manuscript

Design and implementation of a secure cloud-based billing model for smart meters as an Internet of things using homomorphic cryptography

Vu Mai, Ibrahim Khalil

PII: S0167-739X(16)30183-2
DOI: http://dx.doi.org/10.1016/j.future.2016.06.003
Reference: FUTURE 3069

To appear in: *Future Generation Computer Systems*

Received date: 16 November 2015
Revised date: 6 April 2016
Accepted date: 5 June 2016

Please cite this article as: V. Mai, I. Khalil, Design and implementation of a secure cloud-based billing model for smart meters as an Internet of things using homomorphic cryptography, *Future Generation Computer Systems* (2016), http://dx.doi.org/10.1016/j.future.2016.06.003

Design and Implementation of a Secure Cloud-based Billing Model for Smart Meters as an Internet of Things Using Homomorphic Cryptography

Vu Mai[a,*], Ibrahim Khalil[a]

[a]*Department of Computer Science and Information Technology, RMIT University, Melbourne, Australia*

Abstract

Smart grids introduce many outstanding security and privacy issues, especially when smart meters are connected to public networks, creating an Internet of things in which customer usage data is frequently exchanged and processed in large volumes. In this research, we propose a cloud-based data storage and processing model with the ability to preserve user privacy and confidentiality of smart meter data in a smart grid. This goal is achieved by encrypting smart meter data before storage on the cloud using a homomorphic asymmetric key cryptosystem. By applying the homomorphic feature of the cryptographic technique, we propose methods to allow most of the computing works of calculating customer invoices based on total electricity consumption to be done directly on encrypted data by the cloud. One of the outstanding features in our model is the aggregation of encrypted smart meter readings using fixed-point number arithmetic. To test the feasibility of our model, we conducted many experiments to estimate the number of homomorphic additions to be performed by the cloud and the computation time in different billing periods using data from the Smart project, in which smart grid readings were continuously collected from different households in every second within two months and electricity usage data collected every minute from 400 anonymous houses in one day. We also propose a parallel version of our billing algorithm to utilise the processing capability of multi-core processors in cloud servers so that computation time is reduced significantly compared to using our sequential algorithm. Our research works and experiments demonstrate clearly how cloud services can strengthen the security, privacy and efficiency of privacy-sensitive data frequently exchanged and processed in an Internet of things where smart meters communicate directly with public networks.

Keywords: smart grid, IoT, Internet of Things, homomorphic encryption

*Corresponding author
Email addresses: huyvumai@gmail.com (Vu Mai), ibrahim.khalil@rmit.edu.au (Ibrahim Khalil)