MAKING ELECTRICITY GRIDS SMART *AND* SECURE

Xuemin (Sherman) Shen, Rongxing Lu, Xiaohui Liang, Hao Liang

Electricity grids are getting smarter. Today, electricity distributors are taking advantage of sophisticated meters and two-way communication systems to match power production to demand in real time. Thanks to this technology, utilities can base their prices on usage patterns or even remotely dial down home air conditioners when the grid faces peak loads.

But there are big privacy concerns around transmitting consumer data over the Internet: data such as the amount of electricity each house uses, when it was used and what it was used for.

Grid managers need some way of encrypting it so, for example, thieves cannot figure out when someone is away from home by monitoring their electricity patterns. At the same time, the encryption process cannot require too much computing power or slow down the speed of data transfer — a problem with many encryption techniques.

To solve that issue, WISE researcher Xuemin (Sherman) Shen and his colleagues have developed an approach they call EPPA: Efficient and Privacy-Preserving Aggregation. EPPA uses a technique called Pallier's homomorphic cryptosystem to encrypt the multidimensional consumer data and then send it to local data gateways.

The beauty of homomorphic encryption is that it allows the local gateways to merge data from different consumers without decrypting it, keeping the process highly efficient. Each gateway can then compact the aggregated data and forward it to grid managers. When Shen and his colleagues tested their system against a range of security threats, the EPPA-encrypted data stayed safe and secure.

As a result, EPPA allows the kind of real-time communications that the smart grid requires yet still protects all-important consumer privacy.

Partners: Natural Science and Engineering Research Council of Canada