BIOGRAPHICAL SKETCH

Mahmoud Badr is currently a Graduate Research Assistant in the Department of Electrical and Computer Engineering, Tennessee Tech. University, USA since August 2019 and pursuing his Ph.D. degree in the same department. He works under the supervision of Dr. Mohamed Mahmoud. His research interests include several topics in the area of security and privacy in smart grid AMI networks, privacy-preserving machine learning, machine learning for cyber-security, and cyber-physical Systems Security. He has five years of academic and teaching experience in different topics. He is an active reviewer in top IEEE journals/conferences.

EDUCATION

Doctor of Philosophy, Engineering, Tennessee Technological University, August 2022 (expected), Cookeville, Tennessee

Master of Science, Electrical and Computer Engineering, Benha University, Cairo, Egypt, 2018

Bachelor of Science, Electrical and Computer Engineering, Benha University, Cairo, Egypt, 2013

College of Engineering

TENNESSEE TECH

The Department of

Electrical and Computer Engineering

Announces the Dissertation Defense of

Mahmoud Badr

In Partial

Fulfillment of the Requirements

For the degree of

Doctor of Philosophy in Engineering

June 29, 2022

9:00 a.m.

Tennessee Tech University

Join Zoom Meeting

https://tntech.zoom.us/j/8978016564

FIELD OF STUDY

Security and Privacy Preservation

DISSERTATION TOPIC

Security and Privacy Preservation for Smart Grid AMI using Machine learning and Cryptography

EXAMINING COMMITTEE

Mohamed Mahmoud, Committee Chair
Associate Professor, Electrical and Computer Engineering

Allen MacKenzie
Chair & Professor, Electrical and Computer Engineering

Tarek Elfouly
Associate Professor, Electrical and Computer Engineering

Sheikh Ghafoor
Professor, Computer Science

Douglas Talbert
Professor, Computer Science

AN ABSTRACT OF A DISSERTATION

In the smart grid's advanced metering infrastructure (AMI), smart meters (SMs) are deployed at the customers' premises to report their electricity consumption readings to the electric utility (EU). These readings are used for billing, load monitoring, and energy forecasting. Despite the benefits of the AMI, it is vulnerable to security and privacy attacks. **First**, malicious customers compromise their SMs to report false readings to achieve financial gains illegally. This causes hefty financial losses to the EU and degrades the power grid performance. To detect the false-reading attacks, various solutions have been proposed in the literature. However, *none of the existing works has studied the problem in net-metering systems*. The problem is more challenging in these systems because the readings not only depend on the customers' consumption patterns, but also on other factors such as the solar irradiance and the generation capacity of the solar panels. Therefore, in this dissertation, we propose a multi-data-source hybrid deep learning-based detector to identify the false-reading attacks in net-metering systems. Our detector is trained on net meter readings of all customers besides data from trustworthy sources, such as the solar irradiance and temperature, to enhance the detector performance by learning the correlations between them. The rationale here is that although an attacker can report false readings, he cannot manipulate the solar irradiance and temperature values because they are beyond his control. The results of our experiments indicate that our detector achieves a high detection rate of 98.59 % and a low false alarm of 2.92 %. **Second**, federated learning (FL) can be used to build a global energy predictor for smart grids without revealing the customers' raw data to preserve privacy. However, it is still vulnerable to privacy attacks because it reveals local models' parameters during the training process. Although privacy-preserving data aggregation schemes can be used to hide the local models' parameters and enable the utility company and customers to compute a global model, the existing schemes are not communication-efficient. Therefore, in this dissertation, we propose a privacy-preserving and communication-efficient FL-based energy predictor for net-metering systems. In particular, we design an efficient data aggregation scheme to preserve the customers' privacy by encrypting their models' parameters during the FL training. To ensure communication efficiency, we use a change and transmit approach to update local model's parameters, where only the parameters with sufficient changes are updated. Our extensive evaluations demonstrate that our approach accurately predicts future readings while providing privacy protection and high communication efficiency. **Third**, most of the existing electricity theft detectors are global in the sense that they are trained on different consumption levels, including low and high consumptions, to be used for all consumers. In this dissertation, we introduce a novel type of evasion attacks against global detectors as follows. A malicious consumer who has a high consumption level trains a generative adversarial network (GAN) to generate false readings for a low consumption profile (that is indistinguishable from the profiles the detector trained on) to evade the detector, i.e., steal electricity without being detected. To thwart this attack, we divide the consumers into clusters of close electricity consumption levels and train one detector for each cluster. The results of our experiments indicate that our countermeasure significantly reduces the attack's success rate.