BIOGRAPHICAL SKETCH

Mr. Mohamed I. Ibrahem is currently a Ph.D. candidate in the Department of Electrical & Computer Engineering at Tennessee Tech University, USA. While pursuing his Ph.D. he was also the recipient of the Eminence Award for the Doctor of Philosophy Best Paper. His research interests include cybersecurity, security and privacy in smart grid AMI networks, privacy-preserving machine learning, secure federated learning, machine learning for cyber-security, and traffic analysis attacks and countermeasures.

EDUCATION

Ph.D. Engineering
Tennessee Tech University, August 2021 *(expected)*
Cookeville, Tennessee

M.Sc. Electrical Engineering
Benha University, 2018
Cairo, Egypt

B.Eng. Electrical Engineering
Benha University, 2014
Cairo, Egypt

FUNDING

Funding for the graduate studies provided by Tennessee Tech University through the Department of Electrical and Computer Engineering.

College of Engineering

TENNESSEE TECH

The Department of

Electrical and Computer Engineering

Announces the Dissertation Defense of

Mohamed I. Ibrahem

In Partial

Fulfillment of the Requirements

For the degree of

Doctor of Philosophy in Engineering

July 2, 2021

10:00 a.m.

Tennessee Tech University

Zoom Link:

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

FIELD OF STUDY

Cyber Security and Privacy Preservation

DISSERTATION TOPIC

Privacy-Preserving and Efficient Electricity Theft Detection and Data Collection for AMI Using Machine Learning

EXAMINING COMMITTEE

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

Dr. Syed Rafay Hasan
Associate Professor, Electrical and Computer Engineering

Dr. Ghadir Radman
Professor, Electrical and Computer Engineering

Dr. Douglas Talbert
Associate Professor, Computer Science

Dr. Muhammad Ismail
Assistant Professor, Computer Science

ABSTRACT

Smart grid (SG) is an advanced upgrade to the traditional power grid that aims to create a reliable and efficient power system. Advanced metering infrastructure (AMI) is one of the most important components of the SG. It enables bi-directional communication between the smart meters (SMs) and the system operator (SO) to collect fine-grained power consumption readings periodically (every few minutes) for energy management and load monitoring.

However, fraudulent customers may launch electricity theft cyber-attacks by reporting false readings to reduce their bills illegally. In addition, reporting such fine-grained readings periodically results in transmitting a massive amount of data by each SM. Change and transmit (CAT) is an efficient approach to collect the fine-grained readings, where SMs do not need to report their consumption when there is no enough change in the consumption compared to the last reported reading. In this case, we refer to this AMI by ``CAT AMI'', while we use the term periodic transmission (PT) AMI to refer to the AMI that collects the SMs' power consumption readings periodically. Although this approach is efficient, by analyzing the transmission pattern of an SM, sensitive information on the house dwellers can be inferred, e.g., whether the dwellers are absent from home ``presence-privacy attack (PPA)''. Moreover, all the existing works study only the electricity theft detection in PT AMI networks and none of the existing works have studied the problem in the CAT AMI networks.

In this thesis, we first propose an efficient scheme that enables the SO to detect electricity theft cyber-attacks that are launched by malicious customers, compute customers' bills, and monitor load while preserving the customers' privacy. We adapted a functional encryption scheme so that the encrypted readings are aggregated for billing and load monitoring and only the aggregated value is revealed to the SO. Also, we exploited the inner-product operations on encrypted readings to evaluate a machine-learning model to detect malicious customers. Then, we propose a scheme, called ``STDL'', for efficient collection of power consumption readings in CAT AMI networks while preserving the customers' privacy by sending spoofing transmissions using a deep-learning approach. Finally, we investigate the problem of electricity theft detection for CAT AMI network, in which some readings may not be received by the SO due to using CAT approach.