BIOGRAPHICAL SKETCH

Hawzhin Mohammed was born in Kirkuk city, Iraq. He graduated from Barzabi Namer high school, Erbil city, where he obtained his high school diploma in 1996. On discovering his passion for applied sciences, he proceeded to study Electrical Engineering at the Salahaddin University-Erbil, Erbil city, Iraq. He received a Bachelor of Engineering in Electrical Engineering in July of 2000. He attended Tennessee Technological University from January 2015 to May 2017 from where he obtained a Master of Science degree in Electrical and Computer Engineering. He attended Tennessee Technological University from May 2017 to August 2021 from where he obtained a Ph.D. degree in Electrical and Computer Engineering.

EDUCATION

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

M.S. Electrical & Computer Engineering
Tennessee Tech University, May 2017
Cookeville, Tennessee

B.Eng. Electrical Engineering
Salahaddin University - Ebril, July 2000
Ebril City, Iraq

College of Engineering

TENNESSEE TECH

The Department of

Electrical and Computer Engineering

Announces the Dissertation Defense of

Hawzhin Raoof Mohammed

In Partial

Fulfillment of the Requirements

For the degree of

Doctor of Philosophy in Engineering

July 22, 2021

1:30 p.m.

Tennessee Tech University

Zoom Link: https://tntech.zoom.us/j/89296339931

FIELD OF STUDY

Computer Engineering, Hardware Security

DISSERTATION TOPIC

Hardware Intrinsic Attacks on IoT Based Network: A Secure Edge Intelligence Perspective

EXAMINING COMMITTEE

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

Dr. William Eberle
Professor, Computer Science

Dr. Ghadir Radman
Professor, Electrical and Computer Engineering

Dr. Ismail Fidan
Professor, Manufacturing and Engineering Technology

Dr. J. W. Bruce
Associate Professor, Electrical and Computer Engineering

FUNDING

Funding for the graduate studies provided by

Carnegie Funding.

ABSTRACT

Internet of Things (IoT) devices have connected millions of houses around the globe via the internet. Running Artificial Intelligence (AI) on IoT devices is popular nowadays. Sending the data to the cloud for classification or decision making, introduce some problems like delay, power consumption, bandwidth occupation, privacy issue among others. To avoid these problems, the classification or decision-making has been pushed toward the edge of the network or to the IoT devices. This lead to edge intelligence or IoT device with AI. In the recent past, threats due to hardware Trojan in the integrated circuits (IC) have become a serious concern that affects IoT devices. In this dissertation, we discuss the possibility of the IoT device with embedded hardware Trojan that can cause serious security, privacy, and availability problems to the IoT-based Network. Conventional network attack detection techniques work at the network protocol layers. Whereas, IoT devices with hardware Trojan can lead to the peculiar manifestation of attack at the physical and/or firmware level. On the other hand, in the IC design, most of the hardware Trojan-based attack detection techniques require design time intervention, which is expensive for many of the IoT and cannot guarantee 100\% immunity. In this dissertation, we argue that the health of modern IoT devices requires a final line of defense against possible hardware Trojan-based attacks that go undetected during IC design and test. One of our approaches is to utilize power profiling (PP) data and network traffic (NT) data without intervening in the IC design to detect malicious activity in an IoT-based network. The technique is effective to identify multiple attacks concurrently and also able to differentiate between different types of attacks. Data fusion has been leveraged by combining the PP data and NT data and able to detect, without design time intervention, each of the five attacks individually with high accuracy. Another approach is to utilize the PP data of IoT devices for machine learning to detect untrusted IoT devices with the data `only' from the trusted IoT device. The machine learning algorithm efficiently detected the untrusted IoT device from the PP data collected from the trusted IoT device. On the other hand, Utilizing Convolutional Neural Networks (CNN) in IoT devices may be vulnerable to malicious users at hardware and firmware levels. Since most CNN cannot achieve the required throughput on a single IoT device due to the heavy computation and memory requirement, therefore, we propose a pipeline-based technique to distribute the CNN among multiple IoT devices, i.e., Distributed CNN (DCNN). The DCNN improves the throughput of the inference process. Verifying the integrity of the IoT device that is participating in the DCNN is a challenging task. Next, we explore the security of IoT devices in the DCNN. Then several kinds of attacks on CNN's layers have been examined Two novel stealthy attacks have been implemented.