Research Presentation for
Assistant Professor Position in Cyber Engineering
at Gannon University

Shayan (Sean) Taheri, Ph.D.

Florida Institute for Cybersecurity (FICS) Research Center

Electrical and Computer Engineering (ECE) Department

University of Florida (UF)

Overview

- Personal Introduction.
- Research Statement.
- Research Plans.
- Research Sample (RS) 1: Evaluation of Tracking Regimes for, and Security of PLI Systems.
- RS 2: Security of Analog to Digital Converter.
- RS 3: Leveraging Transfer Learning and Data Transformation in Botnet Detection.
- Conclusions and Questions.

Personal Introduction

- Name: Shayan (Sean) Taheri.
- Date of Birth: July/28/1991.
- Current Position: Postdoctoral Fellow.
  - Location: Florida Institute for Cybersecurity (FICS) Research.
  - Supervisors: Dr. Navid Asadi and Dr. Mark Tehranipoor.
  - Research Projects: Physical Inspection of Electronics, Medical Hardware Security, and Post-Quantum Cryptography.
  - Duration Time: May/2020 to May/2021 (Research Internship) and May/2021 to Present (Postdoctoral Fellow).
- Ph.D. Degree: Electrical Engineering from the University of Central Florida. Defense Date: April/2020. Completion Date: May/2021.
- M.S. Degree: Computer Engineering from the Utah State University. Completion Date: August/2015.
- B.S. Degree: Electrical Engineering from the National University of Iran. Completion Date: July/2013.
- General Research Interests: Computer Hardware, Cybersecurity, Artificial Intelligence, and Data Science.
- Engineering Experience: 12 years, from 2009 to 2022 (present). Education, research, and teaching are all included.

Research Statement

- Research Philosophy:
  - Planning to gain experience and knowledge quickly and continuously in the areas of interest.
  - Achieving and improving my skills and abilities in programming and hardware languages, hardware tools, artificial intelligence-based resources, individual and teamwork, technical written and oral presentations, and interpersonal skills.
  - My main research experiences and interests are within the areas of Hardware Security and Security Aspects of Artificial Intelligence.
- Research Projects:
  - Developing tracking regimes and security evaluation framework for physical layer identification systems (in master’s program).
  - Security analysis of analog to digital converter (in doctoral program).
  - Design and development of modern systems for Internet of Things (in doctoral program).
  - Detection of anomaly in data from different domains namely, “network traffic data, semiconductor manufacturing data, electrocardiogram signals, software data (e.g., system calls), biometric (fingerprint and iris) data, and pharmaceutical (pill) image data” using the state-of-the-art machine/deep learning techniques (in doctoral program).
  - Physical inspection and assurance of electronics (in postdoctoral program).

Research Plans

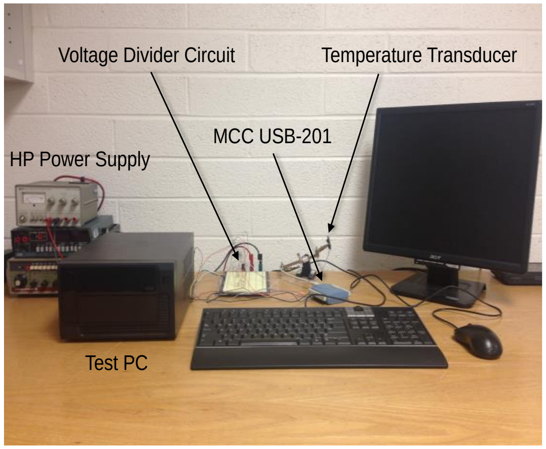
- Areas of Contributions:
  - ✓ Computer Hardware: Computer Architecture and VLSI Design.
  - ✓ Cybersecurity: Hardware Security.
  - ✓ Artificial Intelligence: The intersection of area with hardware and cybersecurity.
- Activities:
  - ✓ Updating and enhancing the department research laboratories.
  - ✓ Improving the student and department organizations from research perspective.
  - ✓ Strengthening the program specializations of ***Electrical and Computer Engineering***, ***Cyber Engineering***, and ***Cybersecurity*** from research perspective.
  - ✓ Growing connections with the academic, industrial, and government agencies.
  - ✓ Writing technical and educational proposals for funding agencies.
  - ✓ Recruiting graduate and undergraduate students.
  - ✓ Making collaborations with the faculty members (across the departments). Possible collaborators: ***Dr. Wookwon Lee, Dr. Ramakrishnan Sundaram, Dr. Fong K. Mak, Dr. Yong-Kyu Jung***, ***Dr. Lin Zhao***, and ***Dr. Richard Matovu***.
  - ✓ Creating my own laboratory inside the ***Institute for Health and Cyber Knowledge (I-HACK)*** with research focuses on all directions of "***Hardware Security***" and "***Security Aspects of Artificial Intelligence***".
  - ✓ Contributing into the programs of ***Computer Science*** department.

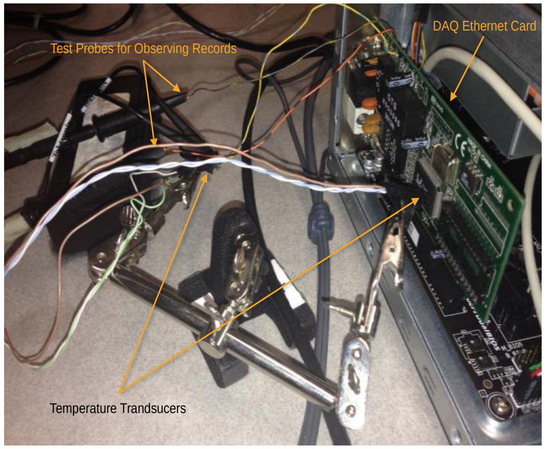
Research Plans (Cont.)

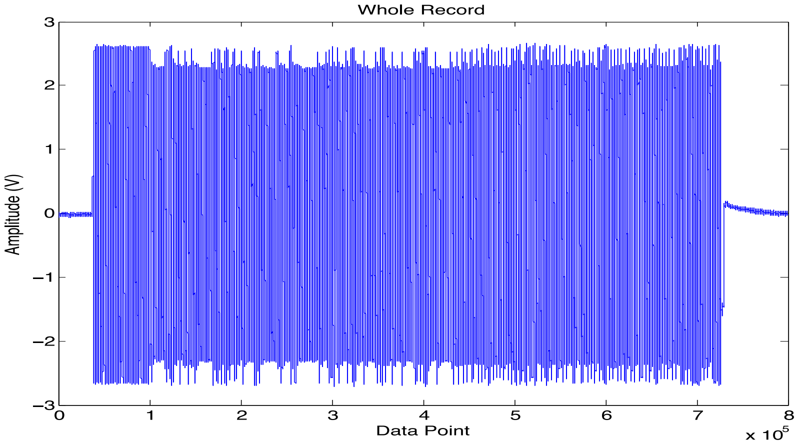
- Agencies, Institutions, and Companies of Interest:
  - ✓ National Science Foundation.
  - ✓ Department of Commerce, Department of Defense, and Department of Energy.
  - ✓ Air Force Office of Scientific Research, Defense Advanced Research Projects Agency (DARPA), and U.S. Army.
  - ✓ Pennsylvania Department of Community and Economic Development, and Pennsylvania Department of Labor and Industry.
  - ✓ National Aeronautics and Space Administration.
  - ✓ Advanced Micro Devices, Apple Inc., Intel Corporation, Meta Platforms, Microsoft Corporation, Nvidia Corporation, and Qualcomm.
- Software and Tools:
  - ✓ Cadence, Synopsys, and Xilinx Suites (for VLSI Design).
  - ✓ GEM5, CACTI, SimpleScalar, Structural Simulation Toolkit, and HTCondor (for Computer Architecture).
  - ✓ Graphics Processing Unit support for TensorFlow, Keras, PyTorch, OpenCV, and TensorBoard (for Deep Learning).

RS 1: Evaluation of Tracking Regimes for, and Security of PLI Systems

- Physical Layer Identification (PLI): Using the first layer of the Open Systems Interconnection (OSI) model for identification of the devices.
- PLI System: Any systematic approach for accomplishment of the PLI operation, including equipment, algorithm, etc.
- PLI Methodology:
  - ✓ Identify and acquire a certain signal (i.e., Fingerprint).
  - ✓ Extract a set of meaningful features from the signal.
  - ✓ Compare the test feature set with the reference feature set.
  - ✓ Determination of the device identity.
- Ethernet card record – Example for fingerprint (m5c1 card – Experiment 4 , Dataset 8).

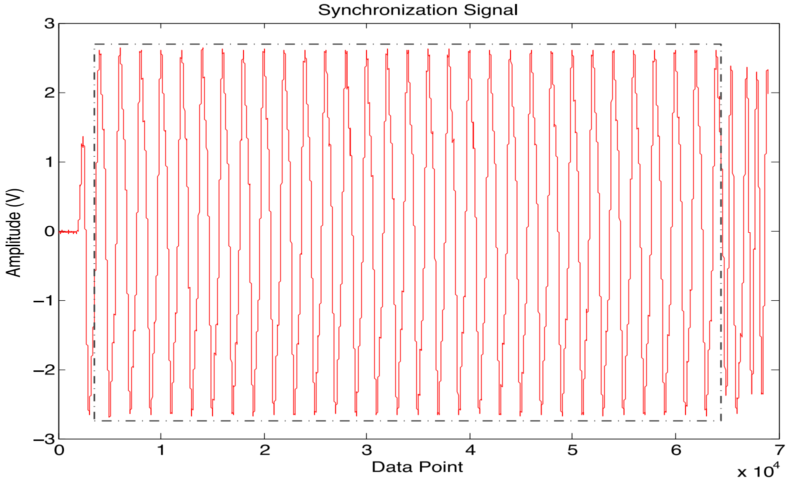


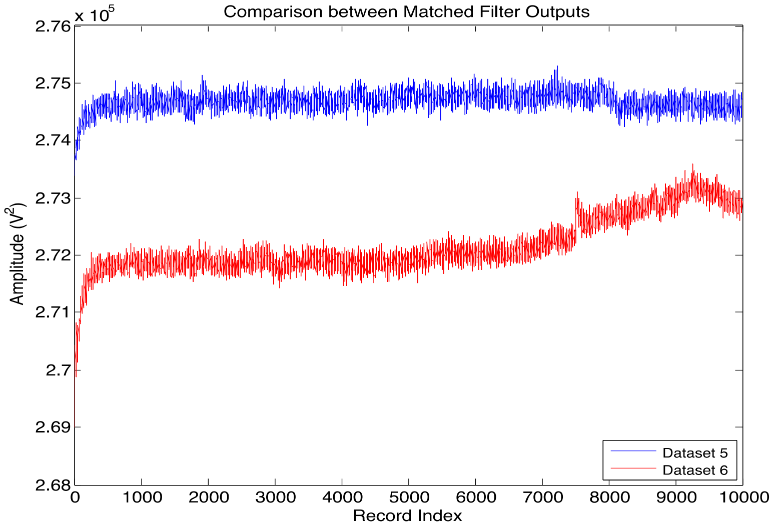




RS 1: Evaluation of Tracking Regimes for, and Security of PLI Systems

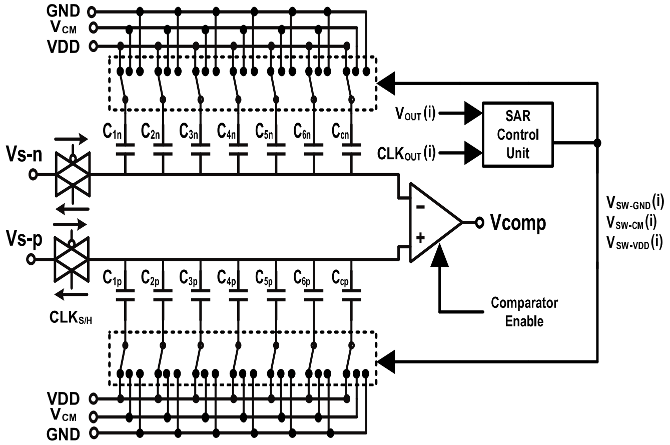
- Employing a PLI system, used for wired Ethernet cards:
  - ✓ Information profiles for identification of the devices.
  - ✓ Using profiles for understanding the device behavior over time.
  - ✓ Using the steady-state portion of the device's record for identification.
- Three main components in each information profile:
  - ✓ Matched Filter.
  - ✓ Matched filter outputs for all of the collected records.
  - ✓ All of the calculated threshold ranges for acceptance of the upcoming data.
- The PLI system problem:
  - ✓ Lack of identification of the devices in different conditions.
  - ✓ Significant changes in the features of the device's signal.
  - ✓ Solution: Tracking these changes.
- Developing a Tracking System (a.k.a. tracking regime):
  - ✓ Capable of explaining the amount of variations of a device's signal.
  - ✓ A Transductive Transfer Learning problem.
  - ✓ System performance: Similarity between the predicted and actual data.
- Security Evaluation of the PLI System:
  - ✓ Exposing the system to different types of attack.
  - ✓ Attack Type: Generating the forged version of a device's signal using an arbitrary waveform generator (AWG).





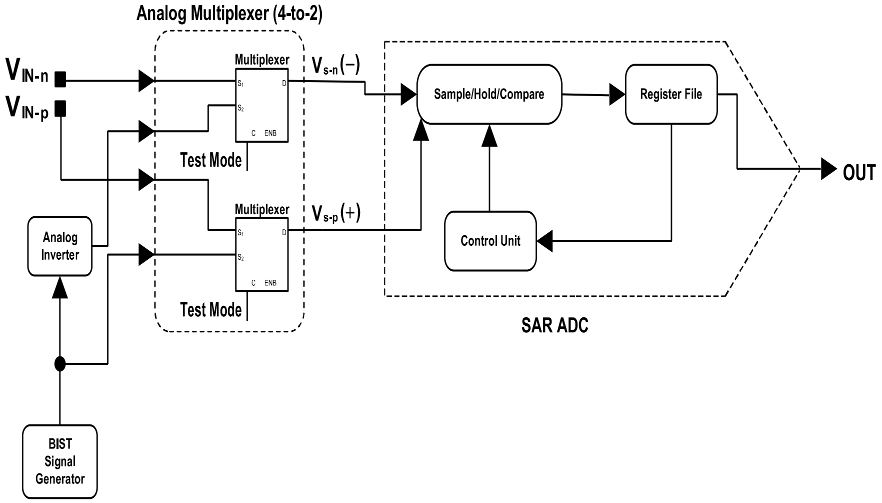
RS 1: Evaluation of Tracking Regimes for, and Security of PLI Systems

- Hardware is not secure and protected anymore as opposed to the traditional view that saw it entirely without malicious flaws.
- The concept of hardware security was formally introduced after emergence of hardware Trojans and the following proposing countermeasures for them.
- Making the hardware secure is associated with cost, power consumption, performance, and reliability concerns.
- A hardware Trojan is defined as a malicious and intentional modifications of a circuit design that results in undesired behavior when the circuit is deployed.
- Data converters are a fundamental building block for many circuits.
- Applications of data converters are in certain functions such as digitizing voice, image, and wireless telecommunications signals.
- Here, we have the first attempt in the literature on the security of data converters.

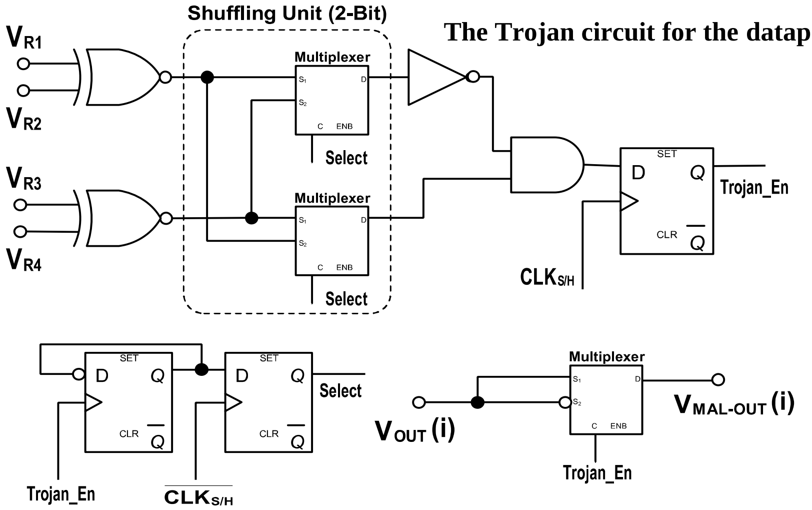


The sample/hold/compare block circuit.

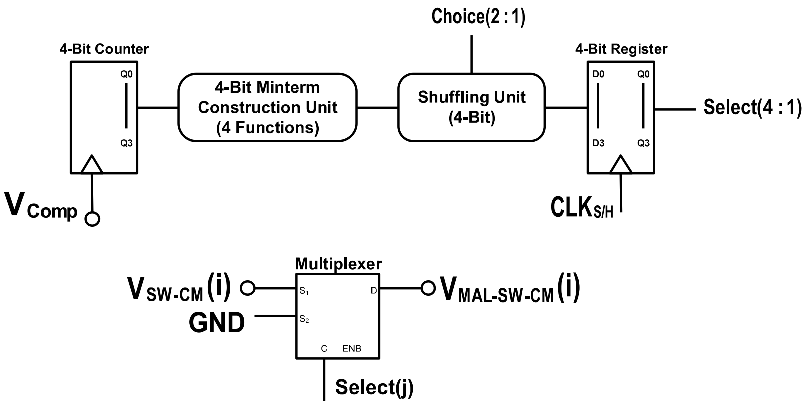
The top-level architecture of an ultra-low power six-bit successive approximation register analog-to-digital converter with a built-in-self-test (BIST)-based input mechanism.



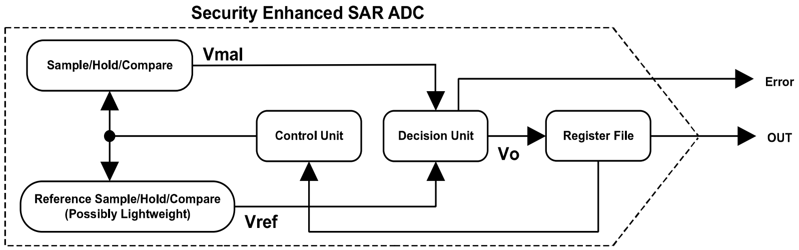
RS 2: Security of Analog to Digital Converter (Cont.)

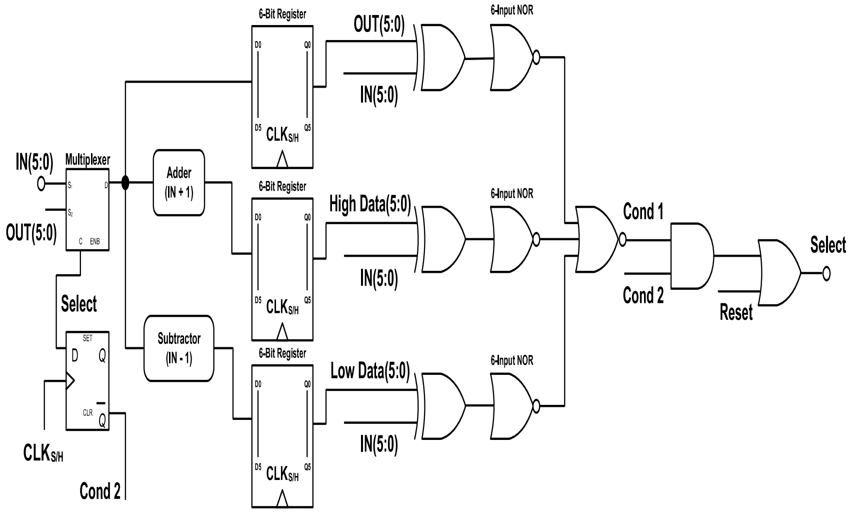


The Trojan circuit for the datapath-based threat.

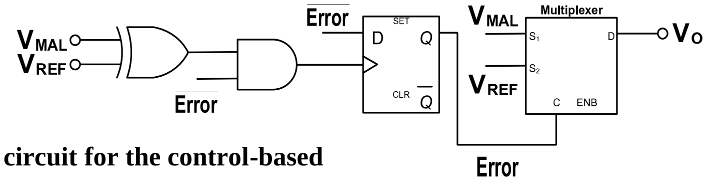


The Trojan circuit for the control-based threat.


Security Enhanced SAR ADC
Sample/Hold/Compare
Vmal
Error
Control Unit
Decision Unit
Register File
OUT
Vo
Reference Sample/Hold/Compare (Possibly Lightweight)
Vref

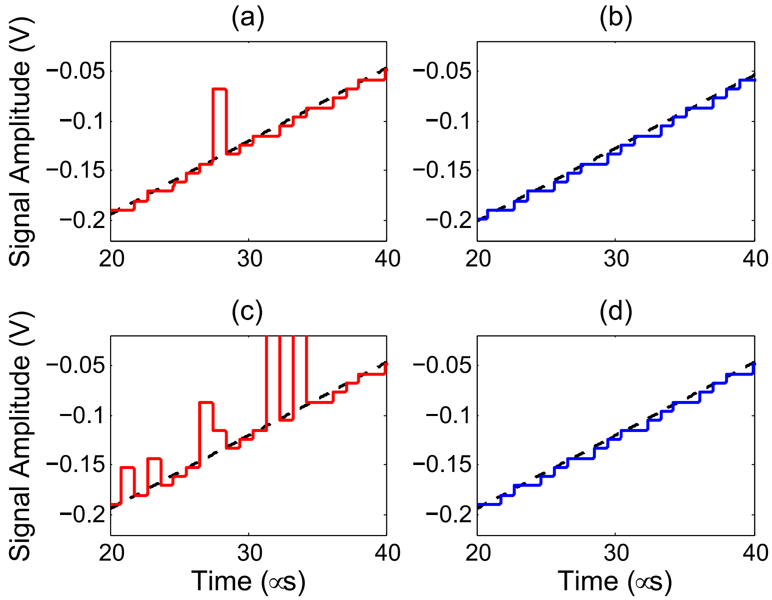


The defense circuit for the datapath-based countermeasure.

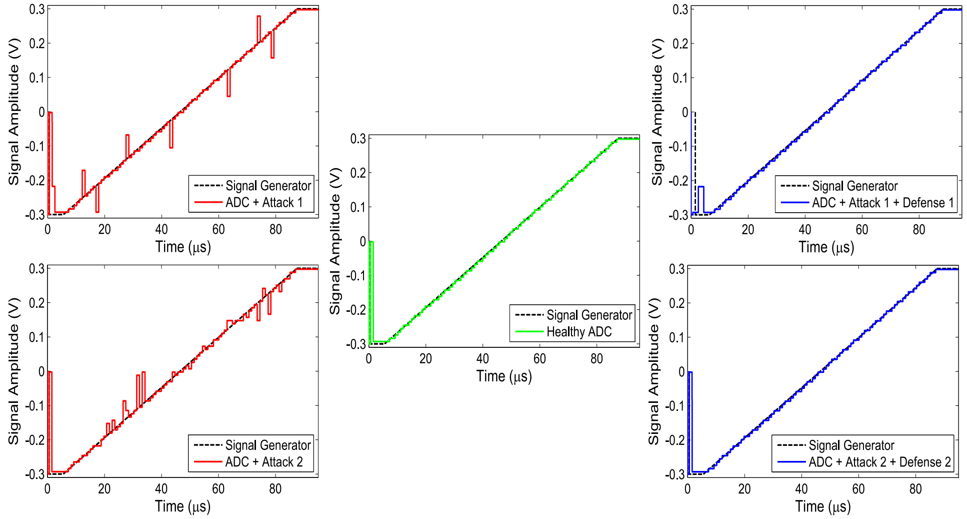


The defense circuit for the control-based countermeasure.

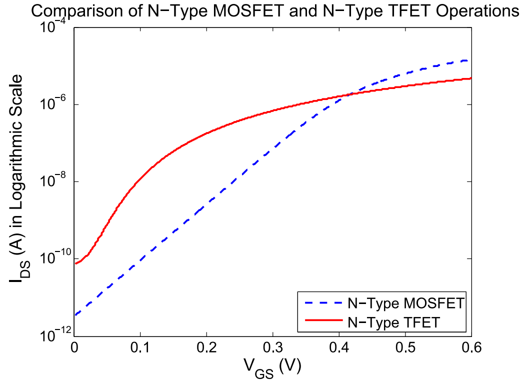
RS 2: Security of Analog to Digital Converter (Cont.)

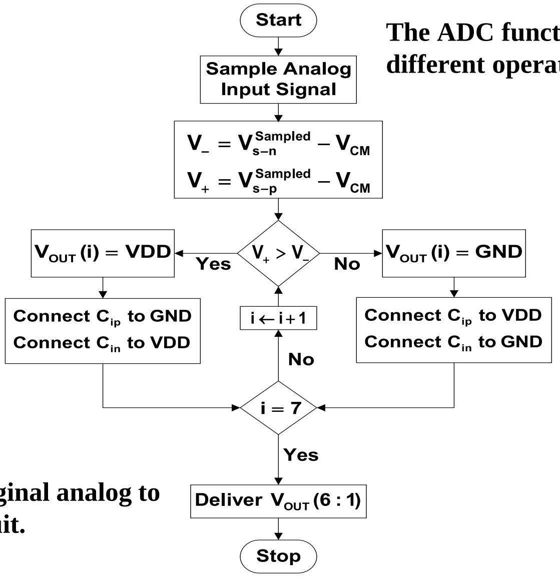


Behavior of Normal and Infected SAR ADC using Tunnel Field-Effect Transistor (TFET).



The ADC functionality evaluation in five different operating conditions.





Start

Sample Analog Input Signal

$V_- = V^{Sampled}_{s-n} - V_{CM}$

$V_+ = V^{Sampled}_{s-p} - V_{CM}$

$V_+ > V_-$

Yes: $V_{OUT}(i) = VDD$ → Connect C_{ip} to GND, Connect C_{in} to VDD

No: $V_{OUT}(i) = GND$ → Connect C_{ip} to VDD, Connect C_{in} to GND

$i = 7$

No: $i \leftarrow i+1$

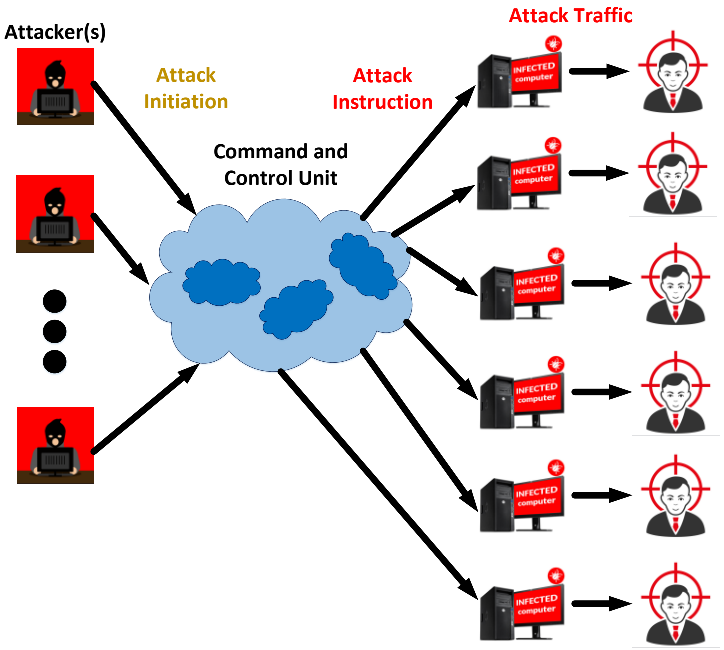
Yes: Deliver $V_{OUT}(6:1)$

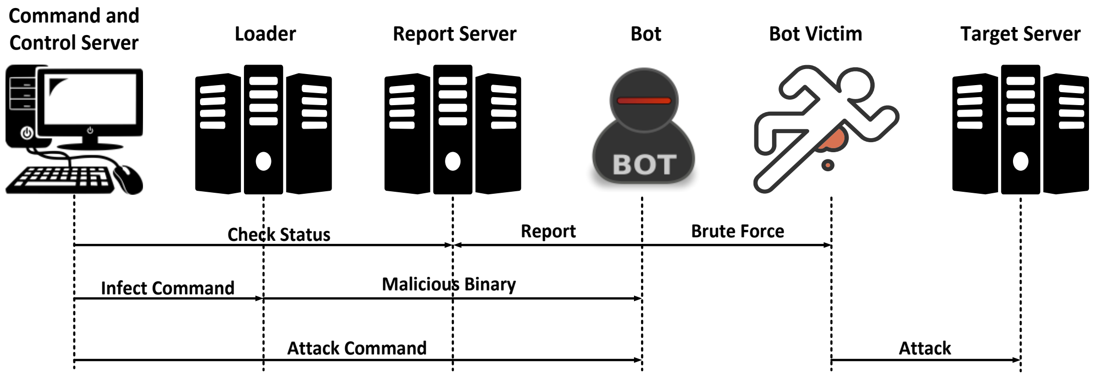
Stop

The operation flow of the original analog to digital converter (ADC) circuit.

RS 3: Leveraging Transfer Learning and Data Transformation in Botnet Detection

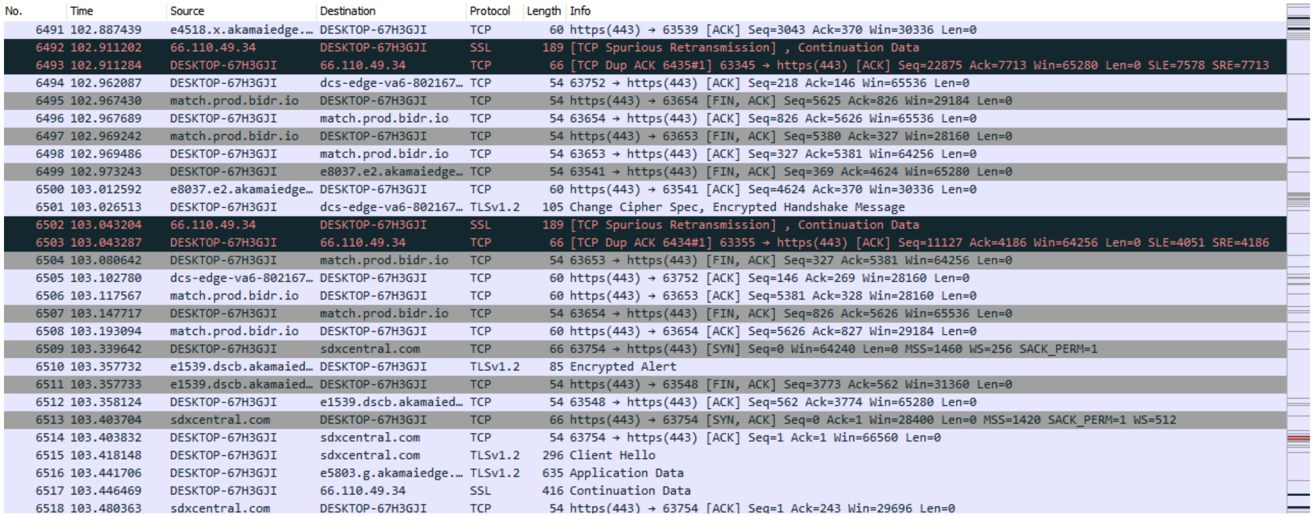
- Artificial Intelligence has a broad variety of applications some of which we already know and encounter in our everyday life.
- AI has a wide range of applications, such as facial recognition, speech recognition, and robotics, but its application scope goes far beyond the three aspects of image, voice, and behavior.
- Security issues of AI software and hardware systems need attention and finding possible solutions for them is challenging.
- Possible security issues can be stated as: bad training mechanism, a bug in the system, the training data is not a representative of the given environment, and attacks in adversarial environments.
- Possible applications of AI is the Cybersecurity domain can be named as: malware monitoring, intrusion detection, bypassing possible threats, intelligence analysis, and botnet detection.





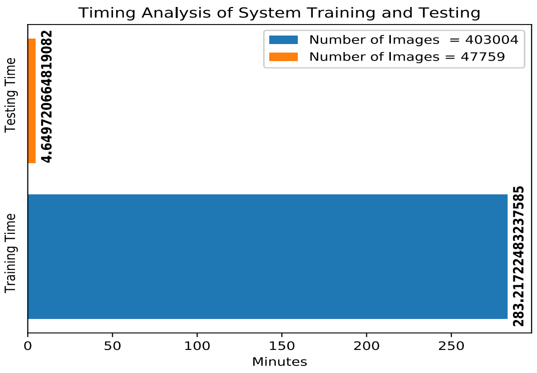
The operations of the Mirai botnet and the network architecture for a typical botnet.

RS 3: Leveraging Transfer Learning and Data Transformation in Botnet Detection (Cont.)



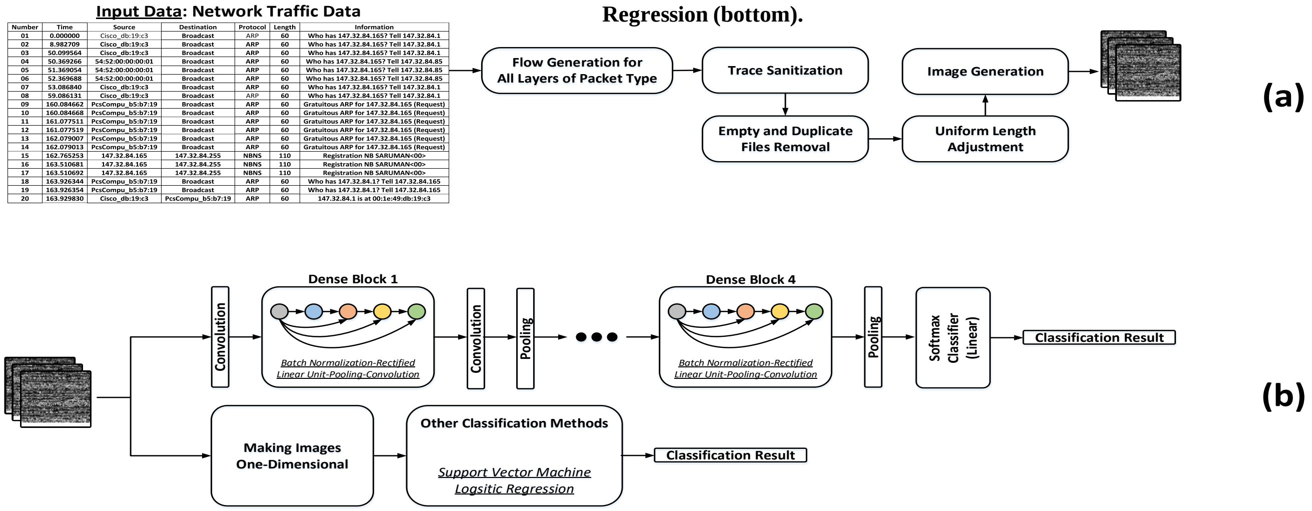
```
No.   Time       Source                Destination           Protocol  Length Info
 6491 102.887439 e4518.x.akamaiedge.… DESKTOP-67H3GJI       TCP          60 https(443) → 63539 [ACK] Seq=3043 Ack=370 Win=30336 Len=0
 6492 102.911202 66.110.49.34          DESKTOP-67H3GJI       SSL         189 [TCP Spurious Retransmission] , Continuation Data
 6493 102.911284 DESKTOP-67H3GJI       66.110.49.34          TCP          66 [TCP Dup ACK 6435#1] 63345 → https(443) [ACK] Seq=22875 Ack=7713 Win=65280 Len=0 SLE=7578 SRE=7713
 6494 102.962087 DESKTOP-67H3GJI       dcs-edge-va6-802167… TCP          54 63752 → https(443) [ACK] Seq=218 Ack=146 Win=65536 Len=0
 6495 102.967430 match.prod.bidr.io    DESKTOP-67H3GJI       TCP          54 https(443) → 63654 [FIN, ACK] Seq=5625 Ack=826 Win=29184 Len=0
 6496 102.967689 DESKTOP-67H3GJI       match.prod.bidr.io    TCP          54 63654 → https(443) [ACK] Seq=826 Ack=5626 Win=65536 Len=0
 6497 102.969242 match.prod.bidr.io    DESKTOP-67H3GJI       TCP          54 https(443) → 63653 [FIN, ACK] Seq=5380 Ack=327 Win=28160 Len=0
 6498 102.969486 DESKTOP-67H3GJI       match.prod.bidr.io    TCP          54 63653 → https(443) [ACK] Seq=327 Ack=5381 Win=64256 Len=0
 6499 102.973243 DESKTOP-67H3GJI       e8037.e2.akamaiedge… TCP          54 63541 → https(443) [FIN, ACK] Seq=369 Ack=4624 Win=65280 Len=0
 6500 103.012592 e8037.e2.akamaiedge… DESKTOP-67H3GJI       TCP          60 https(443) → 63541 [ACK] Seq=4624 Ack=370 Win=30336 Len=0
 6501 103.026513 DESKTOP-67H3GJI       dcs-edge-va6-802167… TLSv1.2     105 Change Cipher Spec, Encrypted Handshake Message
 6502 103.043204 66.110.49.34          DESKTOP-67H3GJI       SSL         189 [TCP Spurious Retransmission] , Continuation Data
 6503 103.043287 DESKTOP-67H3GJI       66.110.49.34          TCP          66 [TCP Dup ACK 6434#1] 63355 → https(443) [ACK] Seq=11127 Ack=4186 Win=64256 Len=0 SLE=4051 SRE=4186
 6504 103.080642 DESKTOP-67H3GJI       match.prod.bidr.io    TCP          54 63653 → https(443) [FIN, ACK] Seq=327 Ack=5381 Win=64256 Len=0
 6505 103.102780 dcs-edge-va6-802167… DESKTOP-67H3GJI       TCP          60 https(443) → 63752 [ACK] Seq=146 Ack=269 Win=28160 Len=0
 6506 103.117567 match.prod.bidr.io    DESKTOP-67H3GJI       TCP          60 https(443) → 63653 [ACK] Seq=5381 Ack=328 Win=28160 Len=0
 6507 103.147717 DESKTOP-67H3GJI       match.prod.bidr.io    TCP          54 63654 → https(443) [FIN, ACK] Seq=826 Ack=5626 Win=65536 Len=0
 6508 103.193094 match.prod.bidr.io    DESKTOP-67H3GJI       TCP          60 https(443) → 63654 [ACK] Seq=5626 Ack=827 Win=29184 Len=0
 6509 103.339642 DESKTOP-67H3GJI       sdxcentral.com        TCP          66 63754 → https(443) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 6510 103.357732 e1539.dscb.akamaied… DESKTOP-67H3GJI       TLSv1.2      85 Encrypted Alert
 6511 103.357733 e1539.dscb.akamaied… DESKTOP-67H3GJI       TCP          54 https(443) → 63548 [FIN, ACK] Seq=3773 Ack=562 Win=31360 Len=0
 6512 103.358124 DESKTOP-67H3GJI       e1539.dscb.akamaied… TCP          54 63548 → https(443) [ACK] Seq=562 Ack=3774 Win=65280 Len=0
 6513 103.403704 sdxcentral.com        DESKTOP-67H3GJI       TCP          66 https(443) → 63754 [SYN, ACK] Seq=0 Ack=1 Win=28400 Len=0 MSS=1420 SACK_PERM=1 WS=512
 6514 103.403832 DESKTOP-67H3GJI       sdxcentral.com        TCP          54 63754 → https(443) [ACK] Seq=1 Ack=1 Win=66560 Len=0
 6515 103.418148 DESKTOP-67H3GJI       sdxcentral.com        TLSv1.2     296 Client Hello
 6516 103.441706 DESKTOP-67H3GJI       e5803.g.akamaiedge.… TLSv1.2     635 Application Data
 6517 103.446469 DESKTOP-67H3GJI       66.110.49.34          SSL         416 Continuation Data
 6518 103.480363 sdxcentral.com        DESKTOP-67H3GJI       TCP          54 https(443) → 63754 [ACK] Seq=1 Ack=243 Win=29696 Len=0
```

A snapshot of the captured traffic data from a local residential network.



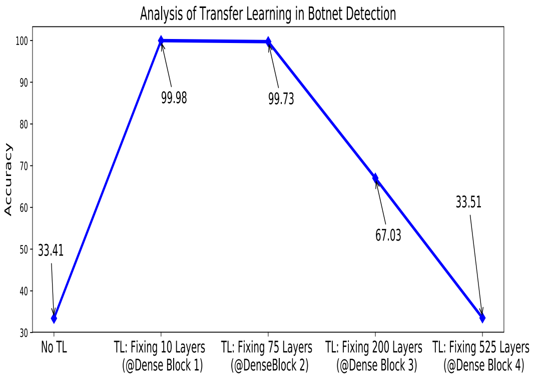
System performance and results.

The flow of botnet detection using DenseNet, Support Vector Machine (SVM), and Logistic Regression: (a) transformation of network traffic data into image and (b) classification of transformed network traffic data into image using DenseNet (top) and SVM along with Logistic Regression (bottom).



Input Data: Network Traffic Data

Number	Time	Source	Destination	Protocol	Length	Information
01	0.000000	Cisco_db:19:c3	Broadcast	ARP	60	Who has 147.32.84.165? Tell 147.32.84.1
02	8.982709	Cisco_db:19:c3	Broadcast	ARP	60	Who has 147.32.84.165? Tell 147.32.84.1
03	50.099564	Cisco_db:19:c3	Broadcast	ARP	60	Who has 147.32.84.165? Tell 147.32.84.1
04	50.369266	54:52:00:00:00:01	Broadcast	ARP	60	Who has 147.32.84.165? Tell 147.32.84.85
05	51.369054	54:52:00:00:00:01	Broadcast	ARP	60	Who has 147.32.84.165? Tell 147.32.84.85
06	52.369688	54:52:00:00:00:01	Broadcast	ARP	60	Who has 147.32.84.165? Tell 147.32.84.85
07	53.086840	Cisco_db:19:c3	Broadcast	ARP	60	Who has 147.32.84.165? Tell 147.32.84.1
08	59.086131	Cisco_db:19:c3	Broadcast	ARP	60	Who has 147.32.84.165? Tell 147.32.84.1
09	160.084662	PcsCompu_b5:b7:19	Broadcast	ARP	60	Gratuitous ARP for 147.32.84.165 (Request)
10	160.084668	PcsCompu_b5:b7:19	Broadcast	ARP	60	Gratuitous ARP for 147.32.84.165 (Request)
11	161.077511	PcsCompu_b5:b7:19	Broadcast	ARP	60	Gratuitous ARP for 147.32.84.165 (Request)
12	161.077519	PcsCompu_b5:b7:19	Broadcast	ARP	60	Gratuitous ARP for 147.32.84.165 (Request)
13	162.079007	PcsCompu_b5:b7:19	Broadcast	ARP	60	Gratuitous ARP for 147.32.84.165 (Request)
14	162.079013	PcsCompu_b5:b7:19	Broadcast	ARP	60	Gratuitous ARP for 147.32.84.165 (Request)
15	162.765253	147.32.84.165	147.32.84.255	NBNS	110	Registration NB SARUMAN<00>
16	163.510681	147.32.84.165	147.32.84.255	NBNS	110	Registration NB SARUMAN<00>
17	163.510692	147.32.84.165	147.32.84.255	NBNS	110	Registration NB SARUMAN<00>
18	163.926344	PcsCompu_b5:b7:19	Broadcast	ARP	60	Who has 147.32.84.1? Tell 147.32.84.165
19	163.926354	PcsCompu_b5:b7:19	Broadcast	ARP	60	Who has 147.32.84.1? Tell 147.32.84.165
20	163.929830	Cisco_db:19:c3	PcsCompu_b5:b7:19	ARP	60	147.32.84.1 is at 00:1e:49:db:19:c3



Conclusions and Questions

- An introduction with respect to the applied position and the university.
- Discussion on academic background, educational and technical skills, and interests in research.
- Explanation of ideas and plans for making theoretical and practical contributions on all undergraduate and graduate programs in the department.
- Provision of research statement along with the respective plans.
- Presentation of three research samples.
- It will be a great pleasure and honor for me to join the Gannon University, and make significant contributions for improving the department objectives, missions, outcomes, resources, programs, diversity and inclusion, facilities, and laboratories.
- Please let me know if you have any questions and/or comments.
- Thank you very much for your understanding, valuable time, and considerations.