Teaching 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

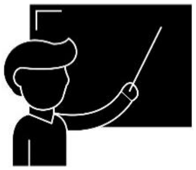
- Personal Introduction.
- Teaching Statement.
- Diversity Statement.
- Teaching Plans.
- Teaching Sample (TS) 1 : Introduction to Operating System (OS).
- TS 2: Introduction to Data Structures and Algorithms.
- TS 3: Introduction to Artificial Intelligence (AI).
- Conclusions and Questions.

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.

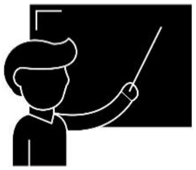
Teaching Statement

- <u>Teaching Philosophy</u>:
  - ✓ Explain context before concept.
  - ✓ Emphasize learning more than scoring.
  - ✓ Evaluate and update.
  - ✓ Encourage open-ended projects and assignments.
  - ✓ Research-based outcome.
  - ✓ Technology-dependent teaching.
  - ✓ Career-oriented meetings.
  - ✓ Teaching to and learning from the students.
- <u>Teaching Areas</u>:
  - ✓ Electronics and Computer Hardware.
  - ✓ Cybersecurity.
  - ✓ Artificial Intelligence and Data Science.
  - ✓ Physics.



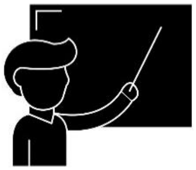
Diversity Statement

- Diversity Philosophy:
  - ✓ Teaching and guiding a diverse body of students, regardless of students' ethnic, cultural, social, economic, racial, and sexual status in order to create a rich and productive academic environment.
  - ✓ Being sensitive to the differences in students' diverse background as well as any obstacle that might stem from those differences.
  - ✓ Promoting oneness as a collective community for all university students and close the cultural gap between the majority and the minority students.
- Diversity Activities:
  - ✓ Online availability of all course material for easy access.
  - ✓ Invitation to my research group for lunch/dinner.
  - ✓ Comfortable office environment with flexible working hours.



Teaching Plans

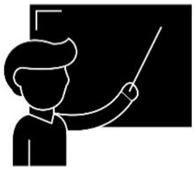
- Areas of Contributions:
  - ✓ Computer Hardware: Computer Architecture and VLSI Design.
  - ✓ Cybersecurity: Hardware Security.
  - ✓ Artificial Intelligence: The intersection of area with hardware and cybersecurity.
- Activities:
  - ✓ Offering the required courses determined by the ECE department.
  - ✓ Developing new courses related to the areas of contributions.
  - ✓ Updating and enhancing the department teaching laboratories.
  - ✓ Productive utilization of resources from the university teaching laboratories in the homework, assignments, projects, and exams.
  - ✓ Improving the student and department organizations from teaching perspective.
  - ✓ Strengthening the program specializations of ***Electrical and Computer Engineering***, ***Cyber Engineering***, and ***Cybersecurity*** from teaching perspective.
  - ✓ Contributing into the programs of ***Computer Science*** department.



GANNON UNIVERSITY

Teaching Plans (Cont.)

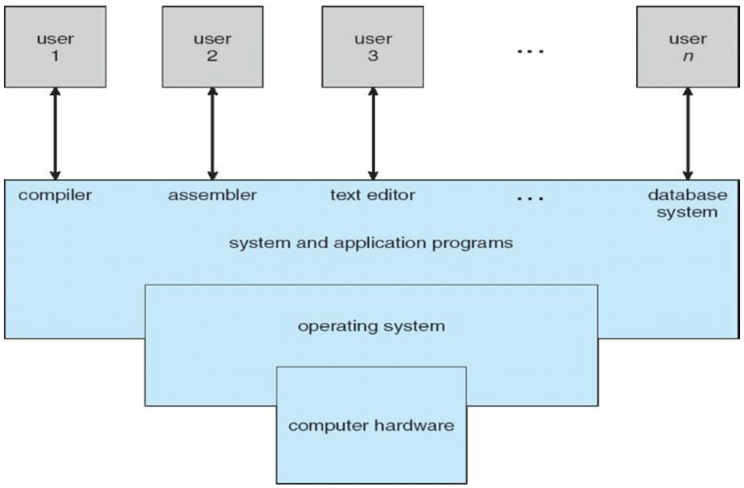
- Courses of Interest to Teach:
  - ✓ Computer Architecture Track:
    - ➢ Introduction to Programming – Python and MATLAB.
    - ➢ Digital Systems.
    - ➢ Embedded Systems.
    - ➢ Hardware Description Languages.
    - ➢ Computer System and Software.
    - ➢ Advanced Computer Architecture.
    - ➢ Parallel Computer Architecture.
  - ✓ VLSI Track:
    - ➢ Introduction to VLSI Design.
    - ➢ VLSI Testing and Verification.
    - ➢ Advanced VLSI Design. Inclusion of ASIC-based Laboratory Assignments and Full Custom-based Projects.
    - ➢ VLSI Physical Design Automation.
    - ➢ Mixed-Signal VLSI Design.
  - ✓ Cybersecurity Track:
    - ➢ Hardware Security.
    - ➢ Advanced Hardware Security.
    - ➢ Introduction to Security Aspects of Artificial Intelligence.
  - ✓ All courses of interest from the department related to Electrical and Computer Engineering, Cyber Engineering, and Computer Science.

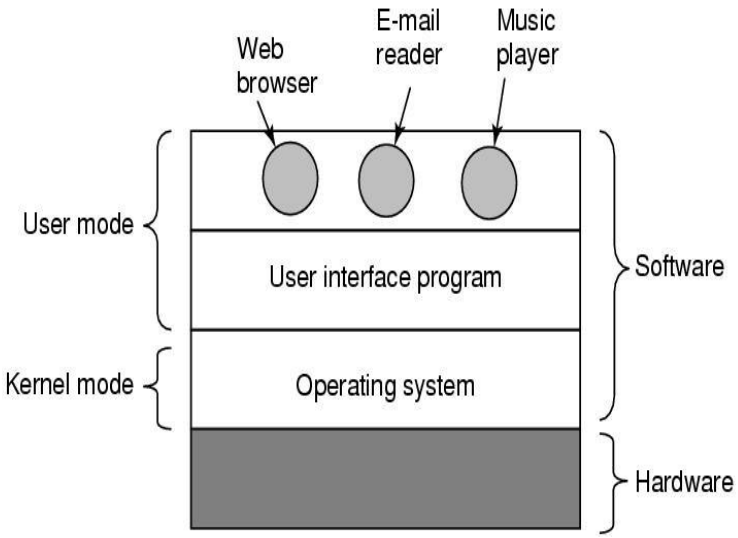


Teaching Plans (Cont.)

- Student and Department Organizations of Interest:
  - ✓ Association for Computing Machinery (ACM).
  - ✓ Campus Ministry for Catholicism.
  - ✓ Engineers Without Borders.
  - ✓ Engineering Student Council.
  - ✓ Eta Kappa Nu (HKN).
  - ✓ Institute of Electrical and Electronics Engineers (IEEE).
  - ✓ Programs for “Diversity, Equity, and Inclusion”.
  - ✓ Programs for K-12.
  - ✓ Society of Women Engineers (SWE).
  - ✓ Undergraduate Research Opportunities Program.

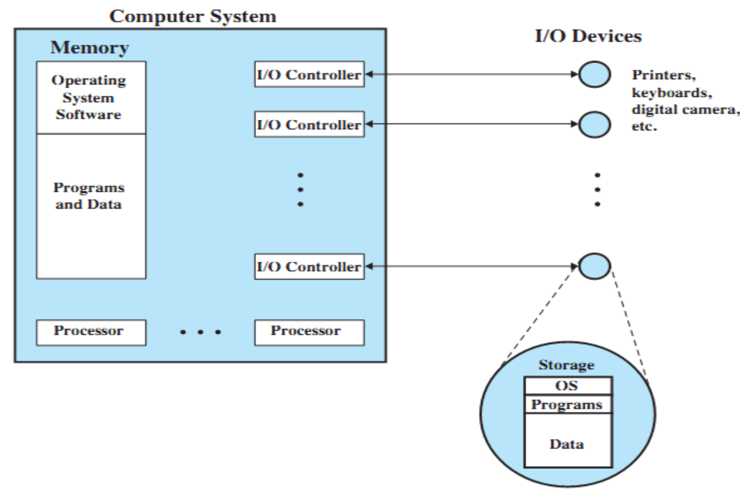
- A program that acts as an intermediary between a user of a computer and the computer hardware.
- Operating system goals:
  - ✓ Execute user programs and make solving user problems easier.
  - ✓ Make the computer system convenient to use.
  - ✓ Use the computer hardware in an efficient manner.
- Computer system can be divided into four components:
  - ✓ Hardware – provides basic computing resources.
    - ❖ *Central Processing Unit (CPU), memory, Input/Output (I/O) devices.*
  - ✓ Operating system.
    - ❖ *Controls and coordinates use of hardware among various applications and users.*
  - ✓ Application programs – define the ways in which the system resources are used to solve the computing problems of the users.
    - ❖ *Word processors, compilers, web browsers, database systems, video games.*
  - ✓ Users.
    - ❖ *People, machines, and other computers.*

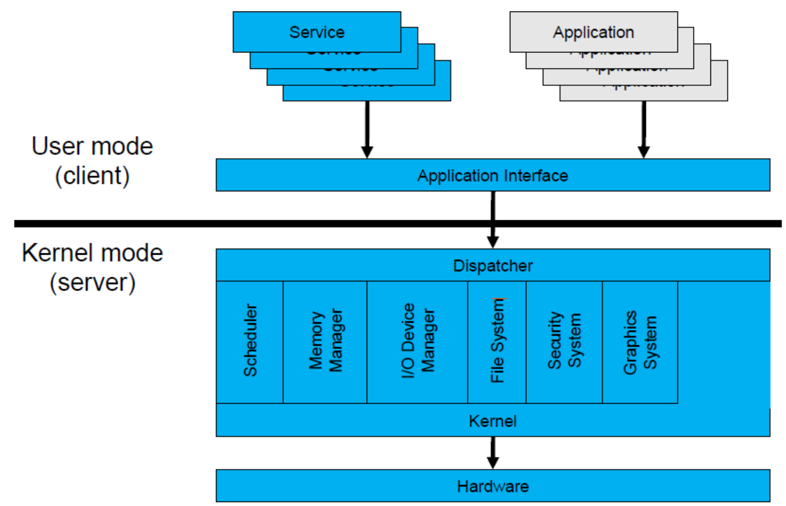


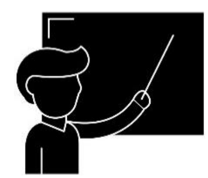


TS 1: Introduction to Operating System (Cont.)

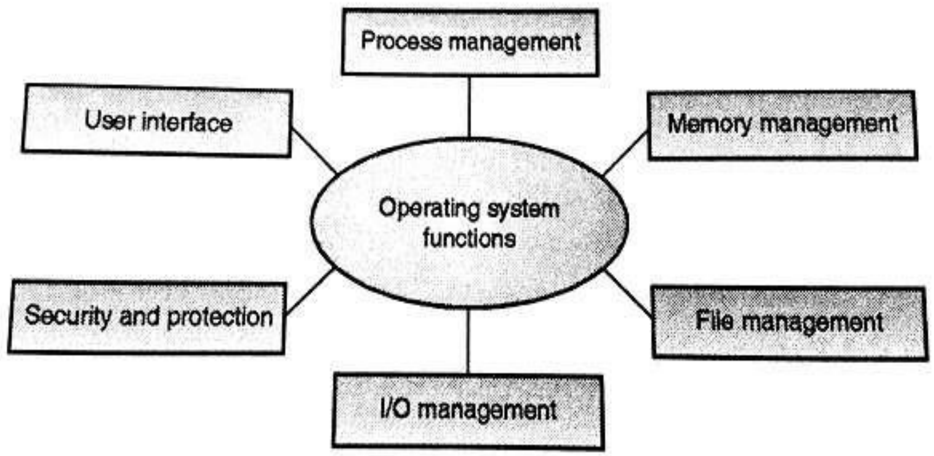
- Users want convenience, **ease of use**, and **good performance**.
  - ✓ Don’t care about **resource utilization**.
- Shared computer such as **mainframe** or **minicomputer** must keep all users satisfied.
- Users of dedicate systems such as **workstations** have dedicated resources but frequently use shared resources from **servers**.
- Handheld computers are resource poor, optimized for usability, and battery life.
- Certain computers have little or no user interface, such as embedded computers in devices and automobiles.
- OS is a **resource allocator**.
  - ✓ Manages all resources.
  - ✓ Decides between conflicting requests for efficient and fair resource usage.
- OS is a **control program**.
  - ✓ Controls execution of programs to prevent errors and improper use of the computer.
- No universally accepted definition: “Everything a vendor ships when you order an operating system” is a good approximation but varies wildly.
- “The one program running at all times on the computer” is the **kernel**.
- Everything else is either:
  - ✓ A system program (ships with the operating system).
  - ✓ An application program.
- **Bootstrap program** is loaded at power-up or reboot:
  - ✓ Typically stored in ROM or EPROM, generally known as **firmware**.
  - ✓ Initializes all aspects of system.
  - ✓ Loads operating system kernel and starts execution.

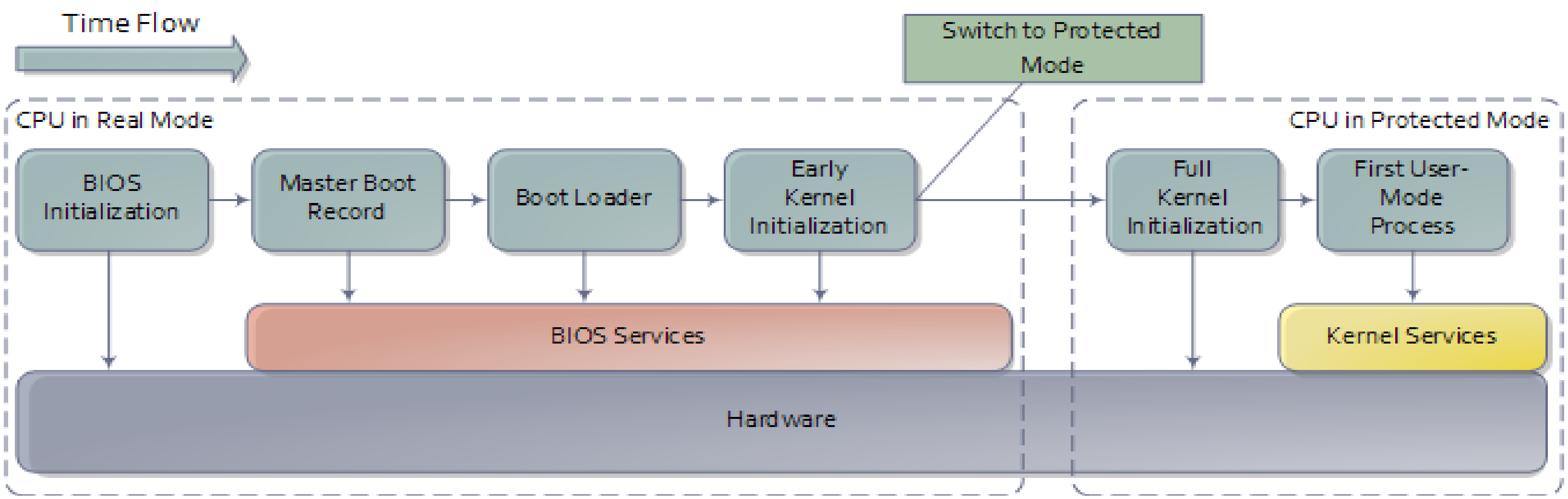




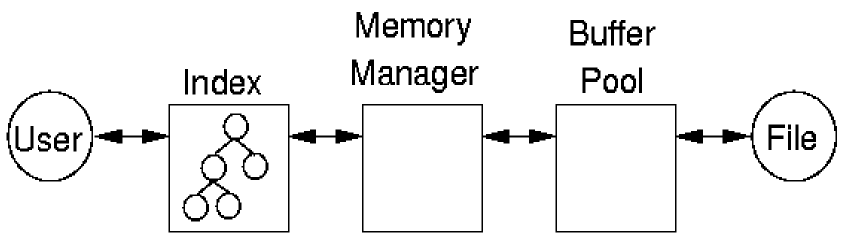


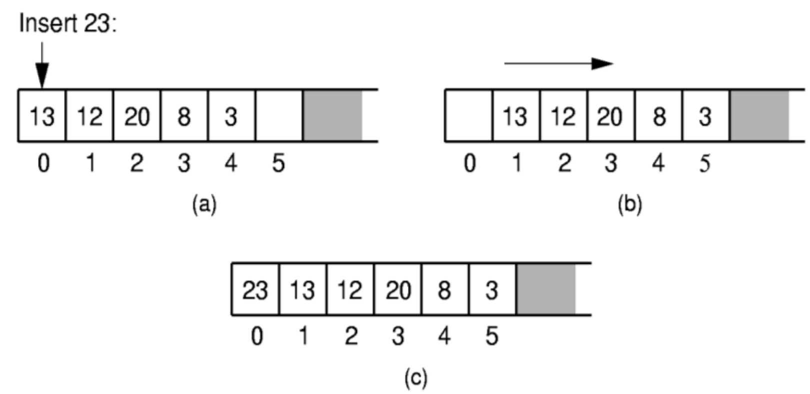
TS 1: Introduction to Operating System (Cont.)





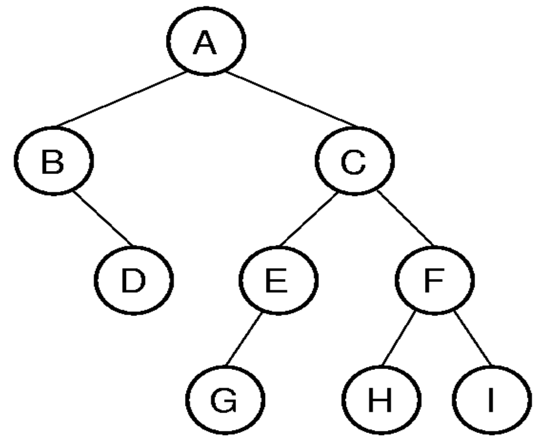
- Data structures organize data: More efficient programs.
- More powerful computers: More complex applications.
- More complex applications demand more calculations.
- Complex computing tasks are unlike our everyday experience.
- Choice of data structure or algorithm can make the difference between a program running in a few seconds or many days.
- A solution is said to be efficient if it solves the problem within its resource constraints: Space and Time.
- The cost of a solution is the amount of resources that the solution consumes.
- Select a data structure as follows:
  - ✓ Analyze the problem to determine the basic operations that must be supported.
  - ✓ Quantify the resource constraints for each operation.
  - ✓ Select the data structure that best meets these requirements.
- Each data structure has costs and benefits.
- Rarely is one data structure better than another in all situations.
- Any data structure requires:
  - ✓ Space for each data item that it stores.
  - ✓ Time to perform each basic operation.
  - ✓ Programming effort.
- Each problem has constraints on available space and time.
- Only after a careful analysis of problem characteristics, then we will be able to know the best data structure for a certain task.

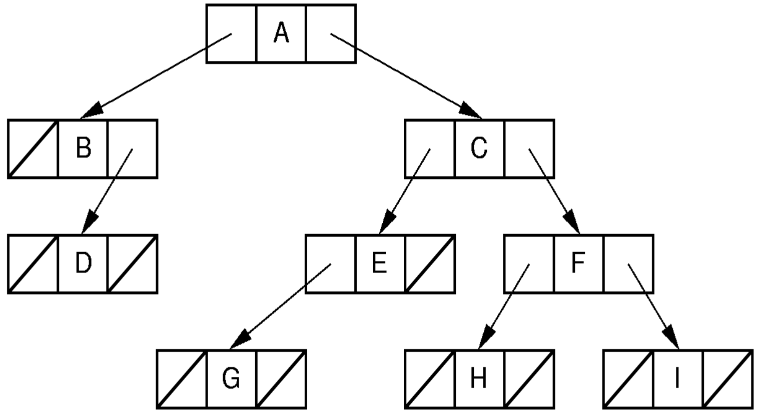




TS 2: Introduction to Data Structures and Algorithms (Cont.)

- Abstract Data Type (ADT): A definition for a data type solely in terms of a set of values and a set of operations on that data type.
- Each ADT operation is defined by its inputs and outputs.
- Encapsulation: Hide implementation details.
- A data structure is the physical implementation of an ADT.
  - ✓ Each operation associated with the ADT is implemented by one or more subroutines in the implementation.
- Data structure usually refers to an organization for data in main memory.
- File structure: An organization for data on peripheral storage, such as a disk drive.
- An ADT manages complexity through abstraction: metaphor, based on Hierarchies of labels.
- Data items have both a logical and a physical form.
- Logical form: Definition of the data item within an ADT.
  - ✓ *Example*: Integers in mathematical sense.
- Physical form: Implementation of the data item within a data structure.
  - ✓ *Example*: 16- and 32-bit integers as well as overflow.





- **What is Artificial Brain/Mind?**

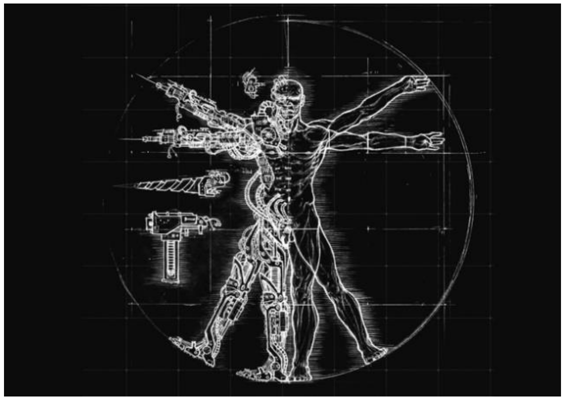
- "You, your joys, and your sorrows, your memories and your ambitions, your sense of personal identity and free will, are in fact no more than the behavior of a vast assembly of nerve cell and their associated molecules."

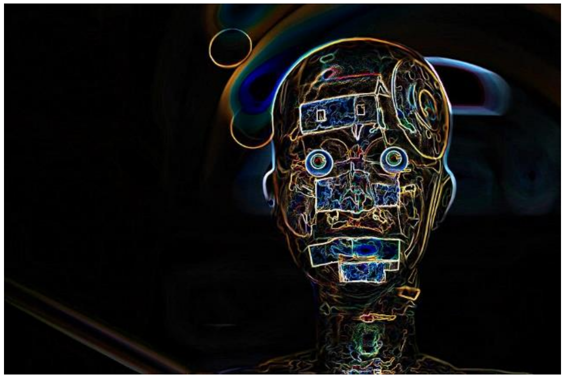
  Francis Crick

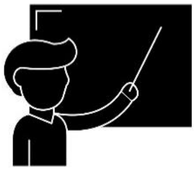
- Because we do not understand the brain very well, we are constantly tempted to use the latest technology as a model for trying to understand it. In my childhood we were always assured that the brain was a telephone switchboard ('What else could it be?').

  John R. Searle

- **How to theorize the artificial modeling of human feelings, thoughts, and actions?**







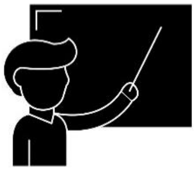
TS 3: Introduction to Artificial Intelligence (Cont.)

- **The Physical Symbol System Hypothesis (PSSH).**
- *<u>Intelligence actions can be modeled by a system manipulating symbols</u>*.
- "A **physical symbol system** consists of a set of entities, called **symbols**, which are physical patterns that can occur as components of another type of entity called an **expression** (or symbol structure).
- A **physical symbol system** has the necessary and sufficient means for performing **intelligent actions**. So, it is a modelling platform. At any instant of time the system will contain a collection of these symbol structures.
- A **symbol structure** is composed of a number of **instances** (or tokens) of symbols related in some physical way (such as one token being next to another).
- Besides these structures, the system also contains a collection of **processes** that operate on expressions to produce other expressions: processes of *<u>creation, modification, reproduction, and destruction</u>*."
- **How to implement the artificial modeling of human feelings, thoughts, and actions?**

Formal Logic/Algebra

Digital Computer

Chess



TS 3: Introduction to Artificial Intelligence (Cont.)

- **Can Machines Think?**

- "*The new problem has the advantage of drawing a fairly sharp line between the physical and the intellectual capacities of a man.*" (**Turing**, **1950**)

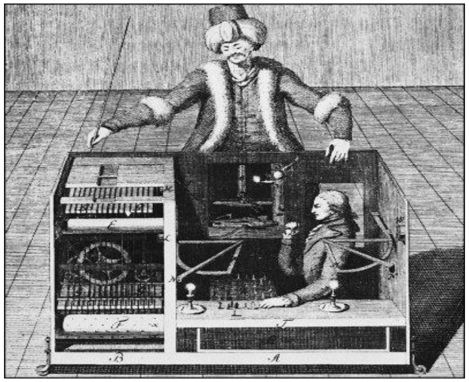
- **Machines with Thinking Abilities:**
  - ✓ A Turing machine is a mathematical model of a physical computing device.
  - ✓ Any given problem for which a Turing machine can provide solution, it can be provided by the physical machine as well.
  - ✓ Formulation: Every function that can be naturally regarded as computable can be computed by a Turing machine.
  - ✓ Can we create intelligence using machines?

- **The Arguments about Questioning the Thinking Ability of Machines?** Given that the nervous system is not a discrete-state machine, you cannot mimic the behavior of nervous system with a discrete-state machine (*Continuity in the Nervous System*).

- Machines with thinking capabilities: Ctesibius of Alexandria - Water Clock with a Regulator and Thermostat of Wiener - Controller of the Environment Temperature.

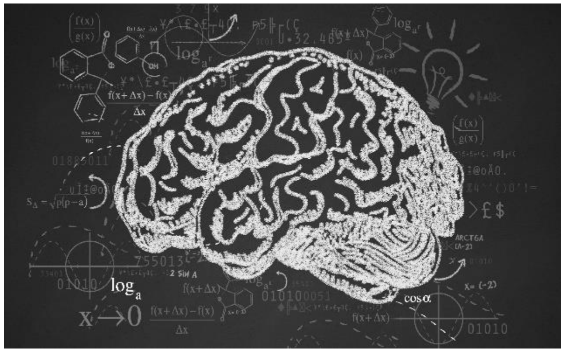
- **How to define artificial intelligence of a machine capable of having human feelings and thoughts, and performing actions?**

Alan Turing depicted on the Loebner Prize Gold Medal.



Automated device for playing chess and performing arts .

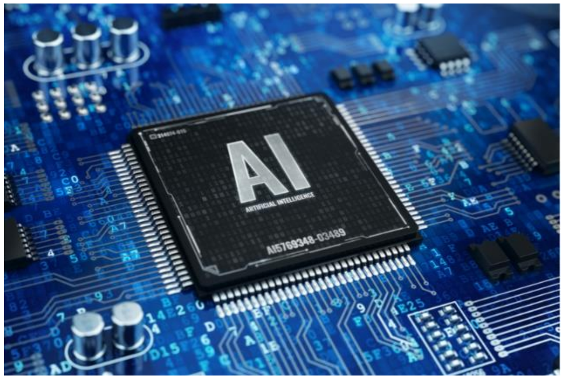
TS 3: Introduction to Artificial Intelligence (Cont.)



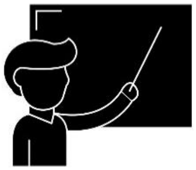
- **How to Define AI?**

- **AI Definition:** ***We can define artificial intelligence as the computational part of the ability to achieve goals in the world. Varying kinds and degrees of intelligence occur in humans, many animals and some machines. It is the capacity to learn and solve problems in particular tacking novel problems, act rationally, and act like humans***.

- **Major Goals**:
  - ✓ Understand the principles that make intelligence possible (in humans, animals, and artificial agents).
  - ✓ Developing intelligent machines or agents (no matter whether they operate as humans or not).
  - ✓ Formalizing knowledge and mechanizing reasoning in all areas of human endeavor.
  - ✓ Making the working with computers as easy as working with people.
  - ✓ Developing human-machine systems that exploit the complementariness of human and automated reasoning.



- **How should scientists from different areas of science view AI and what technical elements (i.e., models, libraries, and etc.) should we have inside AI?**



TS 3: Introduction to Artificial Intelligence (Cont.)

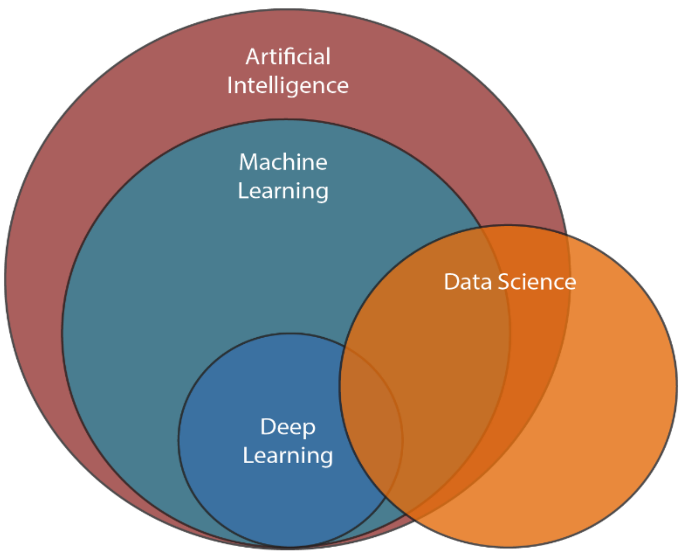
- **What is Inside AI?**

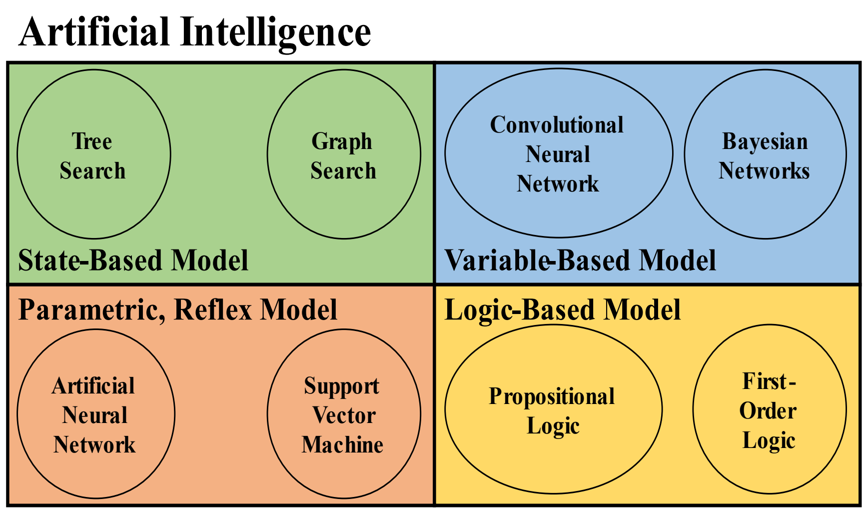
- **Applications**:
  - ✓ Image and Speech Recognition
  - ✓ Natural Language Processing
  - ✓ Autonomous Driving

- **Types of Models**:
  - ✓ Artificial Intelligence
  - ✓ Machine Learning
  - ✓ Deep Learning

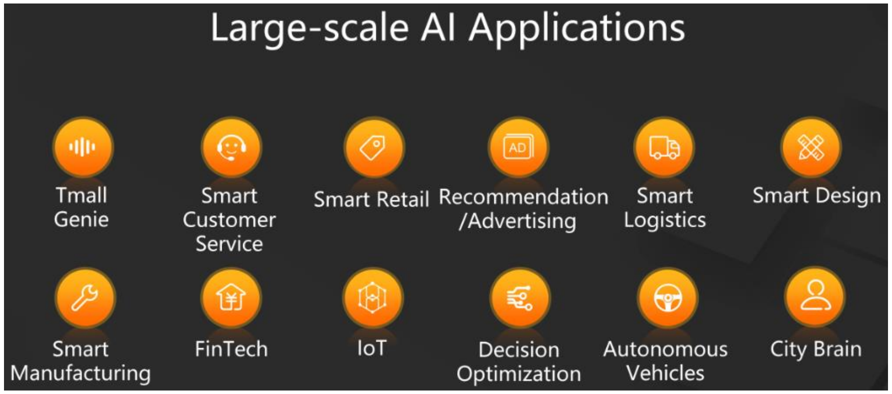
- **Software/Hardware**:
  - ✓ Graphical Processing Unit
  - ✓ Parallel Processing Tools (e.g., Spark)
  - ✓ Cloud Data Storage and Computing System

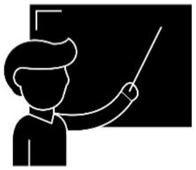
- **Programming Languages and Libraries**:
  - ✓ Python, MATLAB, Java, and C++
  - ✓ TensorFlow, Keras, PyTorch, OpenCV, and Caffe





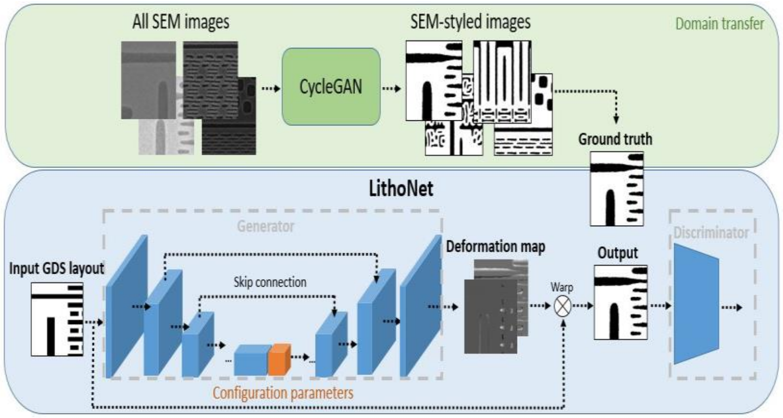
- **AI Successful Applications:**
  - ✓ Language Translation Services (Google)
  - ✓ Translating Telephone (Skype)
  - ✓ News Aggregation and Summarization (Google)
  - ✓ Speech Recognition (Nuance)
  - ✓ Song Recognition (Shazam)
  - ✓ Face Recognition (Google)
  - ✓ **Image Classification/Recognition** (Google)
  - ✓ Question Answering (Apple Siri, IBM Watson, and etc.)
  - ✓ Chess Playing (IBM Deep Blue)
  - ✓ 3D Scene Modeling from Images (Microsoft Photosynth)
  - ✓ Driverless Cars – Autonomous Driving (Google)
  - ✓ Traffic Prediction (Inrix)
  - ✓ **Cybersecurity**: Deep vulnerable code analysis, malware detection, intrusion detection, antispam, vulnerability management, normal and malicious data classification, insider attack prediction, adversarial AI (i.e., adversarial inputs, data poisoning, model stealing, and feedback weaponization), malware creation, smart botnets, spear phishing, conditional attacks, classify victims, security incident prediction, threat intelligence, and intelligent network networking.

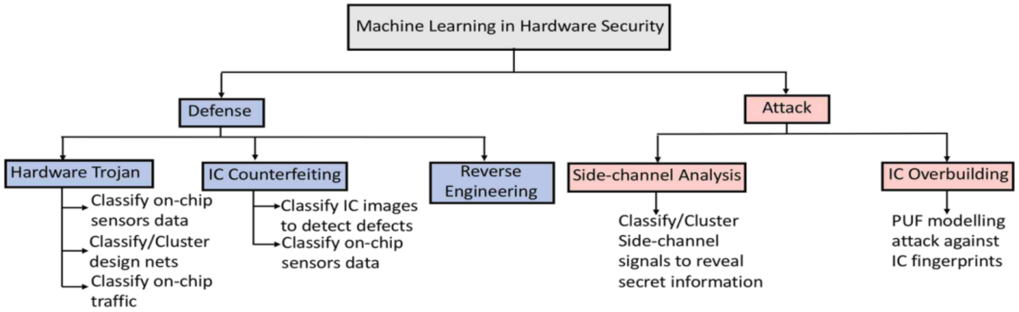




TS 3: Introduction to Artificial Intelligence (Cont.)

- **Cybersecurity Application - AI Meets Hardware Security:**
  - ✓ AI techniques are applied to various hardware security problems.
  - ✓ They can be incorporated both for attack and defense mechanisms.
  - ✓ Possible defense candidate are Hardware Trojan Detection.
  - ✓ Possible attack candidates are: (a) side-channel analysis; and (b) launching modeling attacks on physically unclonable functions.
  - ✓ **Circuit Recognition**: A deep learning framework using Convolutional Neural Networks (CNNs) for recognizing circuit functionalities based on a new circuit representation suitable for network computing processes.
  - ✓ **Physical Inspection of Electronics**: Developing a CNN-based approach that learns the parametric model of physical and chemical phenomena of a fabrication process directly from a training dataset containing pairs of Integrated Circuit (IC) layouts and their corresponding scanning electron microscope (SEM) images. Based on the learned CNN model, we can predict a fabricated circuit shape and structure more accurately and efficiently than traditional methods along with evaluating the trustiness of the ICs.





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 teaching.
- Explanation of ideas and plans for making theoretical and practical contributions on all undergraduate and graduate programs in the department.
- Provision of teaching and diversity statements along with the respective plans.
- Presentation of three teaching 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.