MAGAZINE

ISSUE NO: 127
Mar 6, 2023

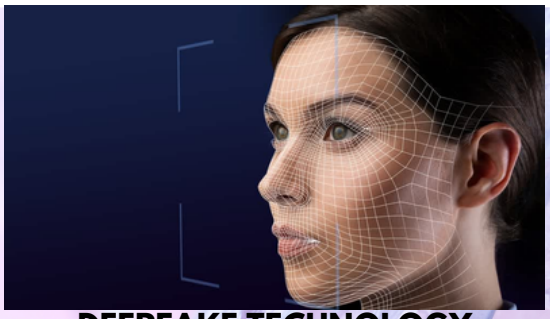
Byte Quest

Department of CSE

CYBER-PHYSICAL SYSTEMS

BIOMETRIC SECURITY SYSTEMS

CHALLENGES IN QUANTUM COMPUTING



DEEPFAKE TECHNOLOGY

Department Vision

To be a center for academic excellence in the field of Computer Science and Engineering education to enable graduates to be ethical and competent professionals.

Department Mission

To enable students to develop logic and problem solving approach that will help build their careers in the innovative field of computing and provide creative solutions for the benefit of society.

FACULTY COORDINATORS

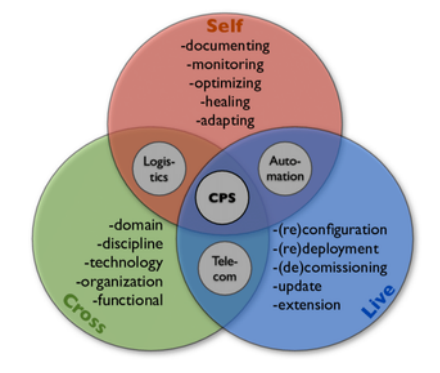
KOMAL KAUR
ASSISTANT PROFESSOR
DR. BHARGAVI PEDDIREDDY
ASSOCIATE PROFESSOR

STUDENT COORDINATORS

TALLURI CHANDRA KIRAN (3/4) CSE C
AMOGHA KANDURI (3/4) CSE C

Byte Quest

CYBER-PHYSICAL SYSTEMS



A Cyber-Physical System (CPS) is a system that integrates physical and computational components to monitor and control the physical processes seamlessly.
In other words, A cyber-physical system is a collection of computing devices communicating with one another and interacting with the physical world via sensors and actuators in a feedback loop.
These systems combine the sensing, actuation, computation, and communication capabilities, and leverage these to improve the physical systems' overall performance, safety, and reliability.
Examples: CPS includes self-driving cars, The STARMAC is a small quadrotor aircraft.
So in the above, we have done a basic intro part about Cyber-Physical systems. CPS systems have various kinds of functionality to improve Automation, Healthcare, Infrastructure development, and many more fields. Cyber-Physical Systems (CPS) are a complex combination of physical and computational elements that interact in real-time to achieve specific goals.

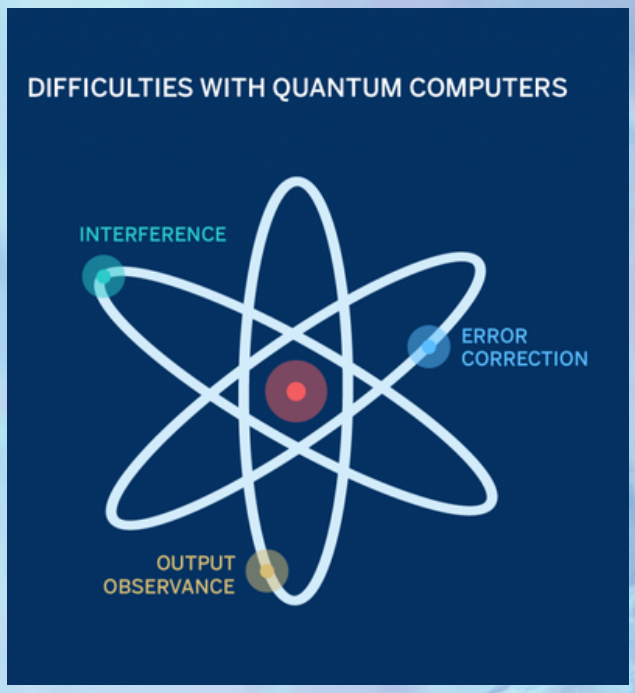
BIOMETRIC SECURITY SYSTEMS

The rapid development of biometric recognition technology has led to biometric security systems being used increasingly more for physical access control. Not just in high-security locations such as banks, but also in environments needing lower security levels such as office complexes. Biometric systems are opening up whole new opportunities to improve the protection of people.
It involves using biometric security software to automatically recognise people based on their behavioural or biological characteristics. The biometric technology currently used most often in physical access control is fingerprint recognition because of its lower price. Among 2D fingerprint sensors, multispectral sensors are often a better choice over optical sensors. They're slightly more expensive but offer higher accuracy and more reliable performance. Other identifiers used include finger veins, palm veins, faces and irises. For high-security environments, iris recognition provides the best accuracy, followed by palm vein recognition.

Byte Quest

CHALLENGES IN QUANTUM COMPUTING

Challenges of quantum computingThe three main challenges we'll look at include quantum decoherence, error correction, and scalability. Each is a major hurdle on the road to quantum computing, and must be overcome if the technology is to reach full potential.



Quantum computing has great potential, but its unique challenges hinder mainstream adoption. These mainly revolve around the inherent properties of quantum mechanics, and the practical difficulties of translating them into a computational context.

CHALLENGE 1: QUANTUM DECOHERENCE

Quantum decoherence is a fundamental challenge in quantum computing. It refers to the loss of quantum behaviour when a system interacts with its environment. This causes a quantum state to transition into a classical state—a significant obstacle because the time before decoherence occurs limits coherence time, or how long quantum information can be processed and stored.

CHALLENGE 2: QUANTUM ERROR CORRECTION

Quantum error correction (QEC) is vital component to the development of quantum computing. As you've seen, quantum states are inherently fragile, but implementing QEC presents its own issues.

CHALLENGE 3: SCALABILITY

As the number of qubits in a quantum computer increases, so does its computational power. But scaling quantum computers isn't as straightforward as adding more transistors to a classical computer chip.

Byte Quest

DEEPFAKE TECHNOLOGY

Deepfakes (portmanteau of "deep learning" and "fake"[1]) are synthetic media[2] that have been digitally manipulated to replace one person's likeness convincingly with that of another. Deepfakes are manipulations.

Deepfakes have garnered widespread attention for their potential use in creating child sexual abuse material, celebrity pornographic videos, revenge porn, fake news, hoaxes, bullying, and financial fraud. The spreading of disinformation and hate speech through deepfakes has the potential to undermine core functions and norms of democratic systems by interfering with people's ability to participate in decisions that affect them, determine collective agendas, and express political will through informed decision-making. This has elicited responses from both industry and government to detect and limit their use.
From traditional entertainment to gaming, deepfake technology has evolved to be increasingly convincing and available to the public, allowing the disruption of the entertainment and media industries.

BROUGHT TO YOU BY

Department of
Computer Science and Engineering

Vasavi College of Engineering