Contents

Darshan
UNIVERSITY
योगः कर्मसु कौशलम्

Goals

Reason and Problem-solving :-

Early researchers developed algorithms that step-by-step reasoning that humans use when they solve puzzles or make logical deduction. By the late 1980s and 1990s, methods were developed for dealing.

Many of these algorithms are insufficient for solving large reasining problems because they experience a **“combinatorial explosion”**:they become exponentially slower as the problems grow.

Planning and decision-making :-

An “agent” is anything that perceives and takes actions in the world.A rational agent has goals or prefrance – there are some situatons it would prefer to be in, ad some situatuons it is trying to avoid.the decision-making agent assigns a number to each situation that measure how much the agent pregers it.

Perception :-

Machine preception is the ability to use input from sensor microphone, wireless signals,active lidars,sonar,radar to deduce aspects of the world.Computer vision is the ability to analye visual input.

The field includes speech recogination, image classification, facial recogination, and robotic perception.

Darshan
UNIVERSITY
योग: कर्मसु कौशलम्

Cybersecurity is the practice of protecting computer systems, networks, and data from unauthorized access, attacks, or damage. It is essential in today's digital world where personal information, financial data, and sensitive business details are stored and transmitted electronically. Effective cybersecurity involves using technologies, processes, and controls to safeguard digital assets from threats like malware, phishing, and hacking. It covers areas such as network security, application security, and identity management to ensure that information remains confidential, accurate, and accessible only to authorized users. With cyber threats becoming increasingly sophisticated, maintaining strong cybersecurity practices—such as using strong passwords, regularly updating software, and implementing multi-factor authentication—is critical to protect privacy, prevent financial losses, and ensure business continuity.

- Use strong, unique passwords.
- Enable two-factor authentication (2FA).
- Keep software and systems updated.
- Backup important data regularly.
- Be cautious with emails and links.
- Use firewalls and antivirus software.

Darshan
UNIVERSITY

Cybersecurity is crucial because it protects sensitive information from falling into the wrong hands, which can lead to identity theft, financial loss, and damage to personal or organizational reputation. In a world where so much of our personal and professional lives rely on digital technology, cybersecurity helps prevent unauthorized access to data and systems. It safeguards businesses from costly cyberattacks that can disrupt operations, steal intellectual property, or expose confidential customer information. Additionally, strong cybersecurity measures help maintain trust between companies and their customers by ensuring data privacy and security. As cyber threats continue to evolve and become more sophisticated, investing in cybersecurity is essential to protect individuals, organizations, and even national security from potentially devast

ing consequences.

Blockchain is a decentralized digital ledger technology that records transactions across many computers so that the recorded data cannot be altered retroactively. Each transaction is grouped into a “block,” and these blocks are linked together in chronological order to form a “chain.” This structure ensures transparency, security, and immutability of data.

Originally developed as the underlying technology for cryptocurrencies like Bitcoin, blockchain has since found applications in many fields including finance, supply chain management, healthcare, and voting systems. Because it operates without a central authority, blockchain enables trust and verification between parties without the need for intermediaries.

Key features of blockchain include decentralization, transparency, security through cryptographic hashing, and immutability. These make it useful for securely tracking ownership, verifying transactions, and enabling smart contracts—self-executing contracts with terms directly written into code.

If you want, I can dive deeper into how it works or its applications!

Darshan
UNIVERSITY
योग: कर्मसु कौशलम्

thical hacking, also known as **white-hat hacking**, is the practice of deliberately probing computer systems, networks, or applications to find security weaknesses before malicious hackers can exploit them. Ethical hackers use the same techniques as cybercriminals but with permission and legal authorization, aiming to improve security by identifying vulnerabilities and helping organizations fix them.

This process is often part of **penetration testing** or security assessments. Ethical hackers play a crucial role in cybersecurity by helping companies protect their systems from attacks, preventing data breaches, and ensuring overall safety. They follow strict rules and guidelines to avoid causing harm and report all findings responsibly.

In short, ethical hacking is a proactive way to strengthen defenses and keep digital systems safe from cyber threats. Want to know how someone becomes an ethical hacker or the tools they use?

DU
Darshan
UNIVERSITY
योगः कर्मसु कौशलम्

Darshan
UNIVERSITY
योग: कर्मसु कौशलम्