Rayat Shikshan Sanstha's

Rajarshi Chhatrapati Shahu College, Kolhapur

Department of Computer Science

2021 2022

Celebrating 73rd Republic Day

TECHNOSAVY

Wednesday, 26th January 2022

Happy Day!

Editors

Miss. Zeba J.Shaikh.
(Head of Computer Science Department).

Miss. Prasangi P. Salokhe.
(Assistant Professor in Computer Science).

Miss. Namrata S. Yadav.
(Assistant Professor in Computer Science).

Miss. Snehal S.Patil
(Assistant Professor in Mathematics).

Special Thanks To

Major. Prof. Dr. R. S. Dubal

(I/C Principal, R.C.Shahu College, Kolhapur)

Dr. V.V.Killedar

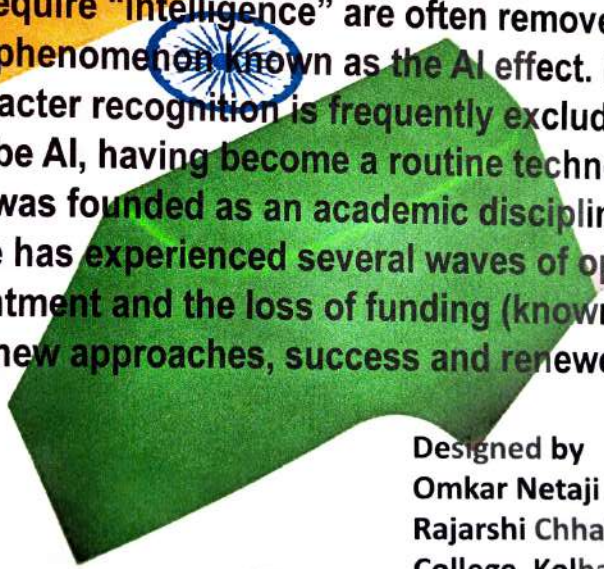
(Vice-Principal,R.C.Shahu.College)

Index

Artificial Intelligence

Artificial intelligence (AI) is intelligence demonstrated by machines, as opposed to natural intelligence displayed by animals including humans. Leading AI textbooks define the field as the study of "intelligent agents": any system that perceives its environment and takes actions that maximize its chance of achieving its goals. Some popular accounts use the term "artificial intelligence" to describe machines that mimic "cognitive" functions that humans associate with the human mind, such as "learning" and "problem solving", however, this definition is rejected by major AI researchers.

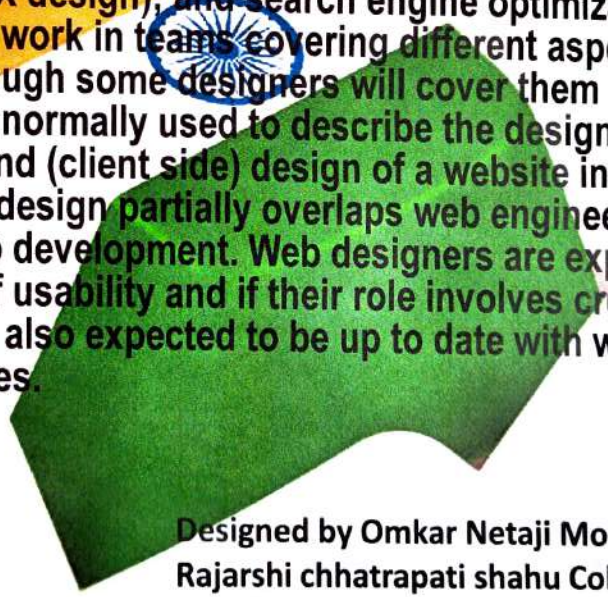
AI applications include advanced web search engines (e.g., Google), recommendation systems (used by YouTube, Amazon and Netflix), understanding human speech (such as Siri and Alexa), self-driving cars (e.g., Tesla), automated decision-making and competing at the highest level in strategic game systems (such as chess and Go).[citation needed] As machines become increasingly capable, tasks considered to require "intelligence" are often removed from the definition of AI, a phenomenon known as the AI effect. For instance, optical character recognition is frequently excluded from things considered to be AI, having become a routine technology. Artificial intelligence was founded as an academic discipline in 1956, and in the years since has experienced several waves of optimism, followed by disappointment and the loss of funding (known as an "AI winter"), followed by new approaches, success and renewed funding.



Designed by
Omkar Netaji Mohite B.c.s. F.Y
Rajarshi Chhatrapati Shahu
College, Kolhapur

Web Design

Web design encompasses many different skills and disciplines in the production and maintenance of websites. The different areas of web design include web graphic design; user interface design (UI design); authoring, including standardised code and proprietary software; user experience design (UX design); and search engine optimization. Often many individuals will work in teams covering different aspects of the design process, although some designers will cover them all.[1] The term "web design" is normally used to describe the design process relating to the front-end (client side) design of a website including writing markup. Web design partially overlaps web engineering in the broader scope of web development. Web designers are expected to have an awareness of usability and if their role involves creating markup then they are also expected to be up to date with web accessibility guidelines.



Designed by Omkar Netaji Mohite BCS F.Y
Rajarshi chhatrapati shahu College Kolhapur

CYBER SECURITY

What is cyber security:-

Cyber security consists of technologies,process & controls designed to protect systems,networks,programs,devices & data from *cyber attack*.
.It aims to reduce the risk of cyber attacks and protects against the unauthorised exploitation of systems,networks & technologies.

7 Types of Cyber Security Threats:-

Cyber security professionals should have an in-depth understanding of the following types of cyber security threats.

1. Malware :

Malware is malicious software such as spyware, ransomware, viruses and worms. Malware is activated when a user clicks on a malicious link or attachment,
which leads to installing dangerous software. Cisco reports that malware, once activated, can:

- Block access to key network components (ransomware)
- Install additional harmful software
- Covertly obtain information by transmitting data from the hard drive (spyware)
- Disrupt individual parts, making the system inoperable

2. Emotet :

The Cybersecurity and Infrastructure Security Agency (CISA) describes Emotet as "an advanced, modular banking Trojan that primarily functions as a downloader or dropper of other banking Trojans. Emotet continues to be among the most costly and destructive malware."

3. Denial of Service :

A denial of service (DoS) is a type of cyber attack that floods a computer or network so it can't respond to requests.

A distributed DoS (DDoS) does the same thing, but the attack originates from a computer network. Cyber attackers often use a flood attack to disrupt the "handshake" process and carry out a DoS. Several other techniques may be used, and some cyber attackers use the time that a network is disabled to launch other attacks. A botnet is a type of

DDoS in which millions of systems can be infected with malware and controlled by a hacker, according to Jeff Melnick of Netwrix, an information technology security software company. Botnets, sometimes called zombie systems, target and overwhelm a target's processing capabilities. Botnets are in different geographic locations and hard to trace.

4. Man in the Middle :-

A man-in-the-middle (MITM) attack occurs when hackers insert themselves into a two-party transaction. After interrupting the traffic, they can filter and steal data, according to Cisco. MITM attacks often occur when a visitor uses an unsecured public Wi-Fi network. Attackers insert themselves between the visitor and the network, and then use malware to install software and use data maliciously

5. Phishing :

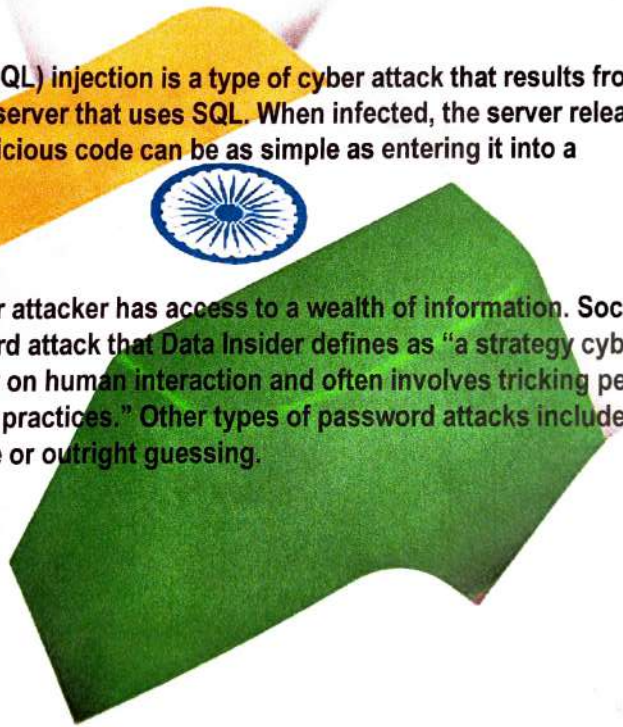
Phishing attacks use fake communication, such as an email, to trick the receiver into opening it and carrying out the instructions inside, such as providing a credit card number. "The goal is to steal sensitive data like credit card and login information or to install malware on the victim's machine," Cisco reports.

6. SQL Injection :

A Structured Query Language (SQL) injection is a type of cyber attack that results from inserting malicious code into a server that uses SQL. When infected, the server releases information. Submitting the malicious code can be as simple as entering it into a vulnerable website search box.

7. Password Attacks :

With the right password, a cyber attacker has access to a wealth of information. Social engineering is a type of password attack that Data Insider defines as "a strategy cyber attackers use that relies heavily on human interaction and often involves tricking people into breaking standard security practices." Other types of password attacks include accessing a password database or outright guessing.



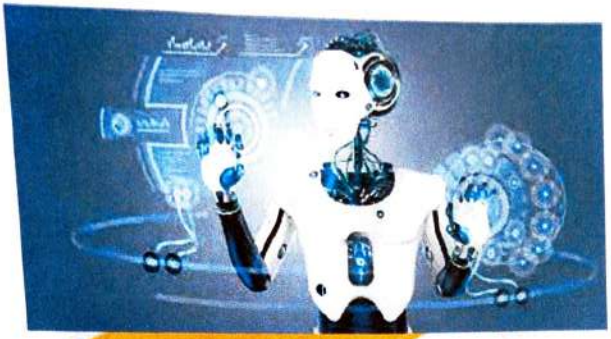
Cyber security is currently one of the fastest growing and most in-demand industries in terms of employment opportunities. There are several reasons for this quicker-than-average growth across nearly every type of cyber security career. This includes the fact that cyber attacks are increasing at an unprecedented rate, and the malicious actors behind these infiltrations are continuously coming up with new attack strategies. Often, all that stands between an organization and a full-scale, damaging data breach are internal cyber security professionals and the tactics they put in place for protection. Beyond just guarding against unauthorized access, these cyber security professionals are also responsible for maintaining continuous uptime of the organization's most crucial IT assets while supporting these platforms' top-notch performance for end users.

As cyberattacks increase and become more dangerous by the day, every company must have a solid cybersecurity game plan in place, then follow it closely.

Thank You

Designed By :-
Prasanna Shashikant Diwan.
B.C.S. F.Y.
Rajarshi Chhatrapati Shahu College, Kolhapur.

Robotics



Robotics is the intersection of science, engineering and technology that produces machines, called robots, that substitute for (or replicate) human actions. Pop culture has always been fascinated with robots. R2-D2. Optimus Prime. WALL-E. These over-exaggerated, humanoid concepts of robots usually seem like a caricature of the real thing...or are they more forward thinking than we realize? Robots are gaining intellectual and mechanical capabilities that don't put the possibility of a R2-D2- like machine out of reach in the future. ROBOT : A robot is the product of the robotics field, where programmable machines are built that can assist humans or mimic human actions. Robots were originally built to handle monotonous tasks (like building cars on an assembly line), but have since expanded well beyond their initial uses to perform tasks like fighting fires, cleaning homes and assisting with incredibly intricate surgeries. Each robot has a differing level of autonomy, ranging from human-controlled bots that carry out tasks that a human has full control over to fully-autonomous bots that perform tasks without any external influences.

By,
Sushant Jalindar Patil
FYBCS