VTECH VOL 13 ISSUE 2 2026

VTECH

IT SEEMS IMPOSSIBLE UNTIL IT IS DONE ..!

"The main aim of education should be to develop character, mental strength, and a spirit of philanthropy."

INDEX

Editorial Team:
Mrs. Sheetal Kokate (Faculty)
Abhishek Yadav (Student)
Radha Kharat (Student)

Contact us at:

Vespolytechnic_0004
VESP-Diploma Engineering

VTECH

DEPARTMENT OF ELECTRONICS & TELECOMMUNICATION

VISION:

To promote excellence in Tele- communication & Information Technology education and prepare our students to face fast growing challenges of the competitive world

MISSIONS:

- **To provide excellent education by balancing both theoretical and practical aspects Engineering. of Tele-communication**
- **Department is dedicated to equip students with strong foundation to enable them for continuing education.**
- **To promote Professional skills, Ethical and Spiritual values resulting in service to the community.**

IT SEEMS IMPOSSIBLE UNTIL IT IS DONE ..!

PROGRAM EDUCATIONAL OUTCOMES

- Engage in testing, operating and maintaining systems in the field of Electronics & Tele-Communication engineering and allied engineering industries.
- Provide socially responsible, environmental friendly solutions for broad-based problem by applying the knowledge of Electronics & Tele Communication engineering or pursue higher education.
- Work effectively as individuals and as team members in multidisciplinary environments
- Engage in lifelong learning, career enhancement and adapt to changing Professional and societal needs.

PROGRAM SPECIFIC OUTCOMES

• Electronics and Telecommunication Systems maintain various types of Electronics and Telecommunication systems.

• EDA Tools Usage: Use EDA tools to develop simple Electronics and Telecommunication engineering related circuits.

DEPARTMENTAL AREAS OF SPECIALZATION

- Embedded System
- Mobile & Wireless Communication
- Entrepreneurship Development &Startups
- Advanced power Electronics
- IoT Applications
- Emerging Trends in Electronics
- Computer Networks and Data Communication
- Optical Networks and Satellite Communication
- Automation and PLC
- Drone technology
- VLSI Applications

MOU's

- PRACHI ELECTRONICS
- JOHN GALT INTERNATIONAL
- CLEAR POINT INSTRUMENTATION PVT. LTD
- ANUP ENGINEERING & ALUMINIUM INDUSTRIES
- SHRISTI WIRELESS SOLUTIONS

RESULT ANALYSIS 2025-26

EJ T.Y

KEER SARVESH SUMANT
89.88%

GUPTA KESAR ANANTLAL
89.29

MAKHIJA DISHIKA SUMIT
88.35

EJ S.Y

PATKAR NEIL VIVEK
92.78%

SPANDANAPRASHANT NALAWADE
90.11%

GAIKWAD MANSI ARUN
84.11

EJ F.Y

GAIKWAD NIRAMAY JITESH
90.59%

MOHD ASHHAD
89.53%

LAD YASH YOGESH
86%

STUDENT'S ACTIVITIES

GUEST LECTURE

Expert Lecture A.Y.2024-25

Sr. No .	Date	Program code	Topic	Name of Expert	Designation	Organization
1	29/07/2025	EJ3K	Artificial intelligence and github	Rudraksh Lamba	Director	Qubotron electratag technology

STUDENT'S ACTIVITIES

INDUSTRIAL VISIT

Sr. No.	Date	Program Code	Industry Name
1	03/10/2025	EJ3K	Clearpoint Instrumentation Pvt.Ltd
2	01/10/2025	EJ3K	Dr. Babasaheb Ambedkar Memorial Bhavan


भारतरत्न डॉ. बाबासाहेब आंबेडकर स्मारक

STUDENT'S IN OTHER ACTIVITIES

Academic Year 2025-26 (Co-Curricular/ Extra Co-Curricular)

Name of students	Event	Details	Organized by	Date	Achievement
Sunsit Gundal,Khushi Thakula,Atharva Mhatre,Abhishekh Singh	TPP	Engineers Day	V.E.S.P	24/09/2025	FIRST
Sarvesh Keer, Ketan Nachre, Chowan Aishwarya,Vedant Gajmal	TPP	Engineers Day	V.E.S.P	24/09/2025	SECOND
Nair Tejas,Varve Sarthak,Padate Omkar,Pawar Dhanshree	TPP	Engineers Day	V.E.S.P	24/09/2025	THIRD

STUDENT'S IN OTHER ACTIVITIES

Drones for Disaster Management: Revolutionising Crisis Response.

Atharva Mhatre
Department of Electronics and Telecommunication Engineering
ej2023.atharva.mhatre@ves.ac.in

Sunisht Gundal
Department of Electronics and Telecommunication Engineering
ej2023.sunisht.gundal @ves.ac.in

Khushi Thakulla
Department of Electronics and Telecommunication Engineering
ej2023.khushi.thakulla@ves.ac.in

Aashish Singh
Department of Electronics and Telecommunication Engineering
ej2023.Aashish.singh@ves.ac.in

Abstract—

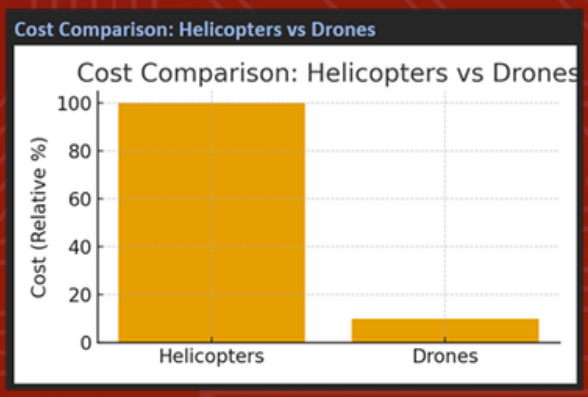
This paper explores the transformative role of drones in disaster management, focusing on their applications, technological advancements, challenges, and future innovations. As disasters increase in frequency and intensity, drones offer rapid deployment, advanced sensing, and safe accessibility to hazardous zones. Through real-world case studies, this paper highlights how drones enhance search and rescue, damage assessment, and aid delivery. While challenges such as regulation, training, and ethical considerations persist, the integration of AI, swarm technology, and 5G promises a more resilient disaster management framework.

Keywords—Disaster management, Drones, UAV, Rescue, Artificial Intelligence, IoT, 5G, Blockchain, Swarm Intelligence

I. INTRODUCTION

Disasters are increasing in frequency and severity, demanding faster and safer response strategies. Traditional rescue operations are slowed by inaccessible terrain and hazardous environments. UAVs (Unmanned Aerial Vehicles) are classified into nano, micro, tactical, and MALE/HALE drones, with rotary UAVs commonly used in disaster zones due to vertical take-off/landing and hover capability. Drones are cost-effective, often 90% cheaper than helicopters for reconnaissance, and provide rapid situational awareness.

II. WHY DRONES? – THE GAME CHANGERS



Drones combine accessibility, speed, and advanced sensing. They employ LiDAR for terrain mapping, SAR (Synthetic Aperture Radar) for cloud/smoke penetration, multispectral sensors for flood and vegetation assessment, and thermal imaging for survivor detection at night. They provide real-time, high-resolution aerial intelligence within minutes compared to satellites, which may take days.

III. REAL-WORLD IMPACT & CASE STUDIES

Case studies validate drone effectiveness. During the Nepal Earthquake (2015), UAVs mapped destruction and delivered aid. In Typhoon Hagibis (2019), drones carried medical supplies to trapped residents. In California Wildfires (2020), thermal drones identified hotspots 30% faster than ground teams. Hurricane Dorian (2019) saw drones map 500 km² in 48 hours, far quicker than satellite revisits. In Turkey-Syria Earthquake (2023), drones with thermal imaging aided in locating over 100 survivors.

IV. DIVERSE DISASTER APPLICATIONS

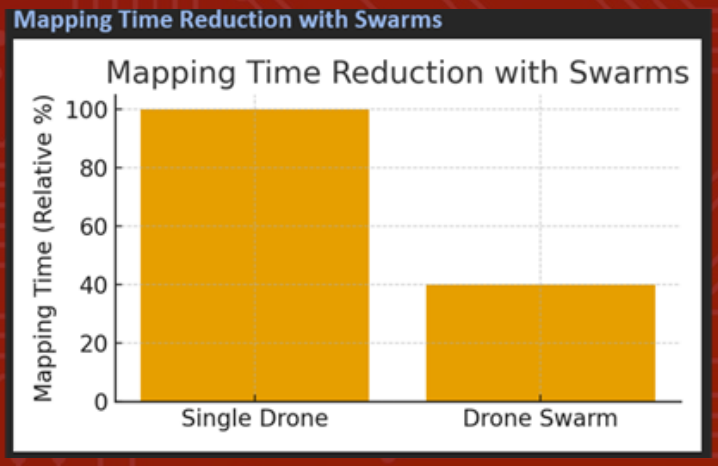
UAVs serve both tactical and strategic roles. Tactical uses include search and rescue, localized mapping, and real-time victim detection. Strategic uses include risk monitoring of landslides, evacuation route planning, and long-term recovery analysis. They can restore communication by acting as airborne LTE/5G base stations, and their high-resolution data supports faster insurance and policy decisions.

V. CUTTING-EDGE FEATURES & TECHNOLOGIES

Modern UAVs feature endurance improvements with hybrid-fuel drones lasting up to 10 hours. GPS/INS systems ensure navigation in GPS-denied zones such as tunnels. Edge computing reduces bandwidth needs by processing imagery onboard. Payload modularity enables drones to switch between sensors, loudspeakers, or medical kits. Collision-avoidance systems using radar and computer vision improve safety in crowded airspaces.

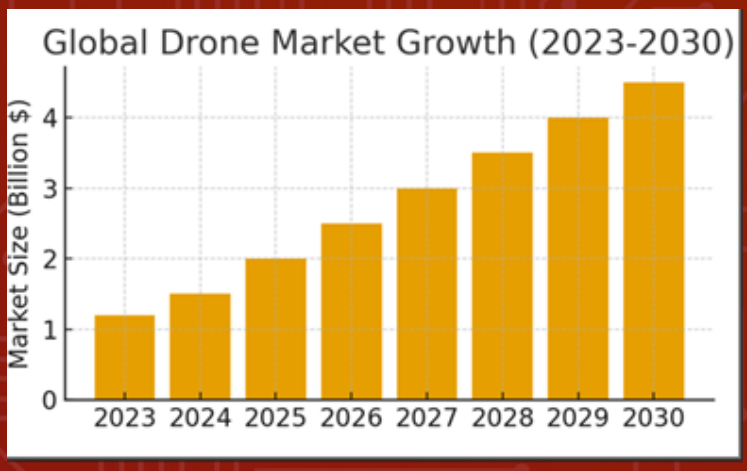
VII. FUTURE DIRECTIONS & INNOVATIONS

Emerging trends include AI-driven survivor detection and predictive analytics, drone swarms inspired by natural systems, and integration with IoT and ground sensors for predictive disaster management. Satellite-drone collaboration will allow beyond-line-of-sight operations in remote regions. Block chain can secure aerial data for disaster claims and inter-agency trust. Bio-inspired micro drones and solar-powered hybrids promise ultra-long endurance beyond 24 hours.



VIII. CONCLUSION

Drones are indispensable for modern disaster management. Standardization by ICAO, ISO, and IEEE is vital for cross-border operations. Inter-agency collaboration among defense forces, NGOs, and governments ensures resource sharing. Future integration with AI, IoT, and advanced communication will further enhance resilience. Ultimately, UAVs represent a transformative leap toward faster, safer, and smarter disaster responses.



IX. Literature Review & Background

Historical Context:

Early disaster response efforts used limited aerial imaging methods. The 1906 San Francisco earthquake marked one of the first documented cases where a camera on a kite was deployed for damage assessment.

Recent Advancements:

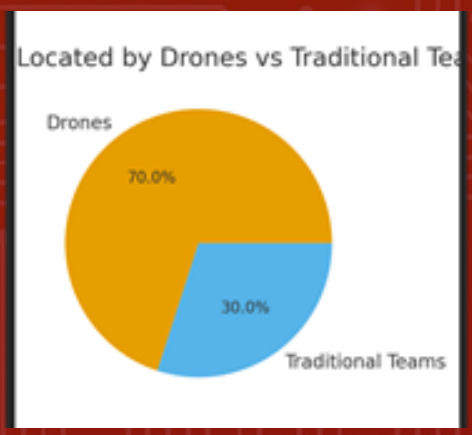
The integration of advanced sensors (thermal, LiDAR) and AI-based image processing has enabled automated, data-rich missions. For instance, drones in the 2015 Nepal earthquake and the 2023 Türkiye-Syria earthquake provided real-time situational data for search and rescue operations.

Technical Precedents:

Research on network topology for multi-drone swarms, energy-efficient flight paths, and reinforcement learning for autonomous navigation has laid the foundation for scalable disaster management systems.

Key References:

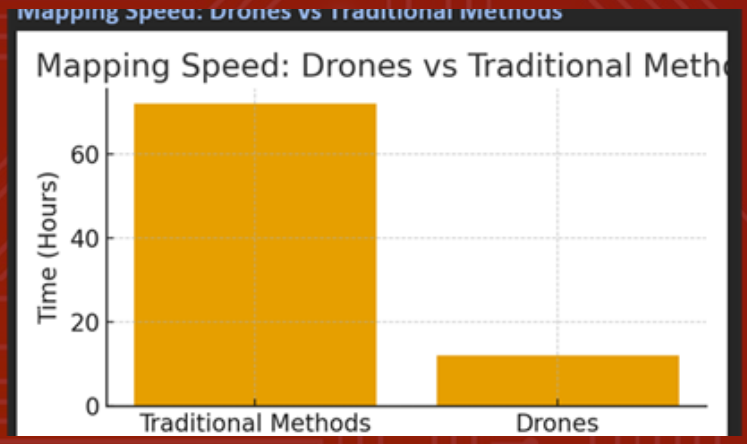
- Daud, S. M. S. M. et al. (2022)
- Ray, P. P. et al. (2017)
- Ho, Y.-H. & Tsai, Y.-J. (2022)



X. Proposed System Architecture

Core Components:

- UAS Platform: Multi-rotor drone optimized for stable flight and heavy payload delivery.
- Onboard Processing: STM32F4 series microcontroller for real-time flight control and sensor fusion.
- Sensor Suite: MPU6050 IMU, high-resolution RGB camera, thermal camera for heat detection.



Communication Subsystem:

- Onboard Bus: I2C/SPI protocols for low-latency sensor integration.
- Long-Range Control: LoRa SX1278 module for 10–20 km range in disaster-affected areas with limited infrastructure.
- High-Bandwidth Link: Wi-Fi/5G for live video streaming and situational awareness.

XI. Methodology & Implementation Details

Autonomous Navigation:

- SLAM for robust navigation in GPS-denied environments.
- Obstacle avoidance using LiDAR/stereo cameras with PID control.

Data Processing & Fusion:

- Kalman filter for IMU–GPS data fusion.
- YOLO-based machine learning for automated victim detection and structural damage assessment.

System Prototype:

Arduino-based flight controller tested in a simulated disaster scenario, validating integrated hardware and communication protocols.

XII. References

Daud, S. M. S. M., et al. "Applications of drone in disaster management: A scoping review." Science & Justice, 2022.

Ray, P. P., et al. "Internet of things for disaster management: State-of-the-art and prospects." IEEE Access, 2017.

Ho, Y.-H., & Tsai, Y.-J. "Open collaborative platform for multi-drones to support search and rescue operations." Drones, 2022.

United Nations Report on Disaster Impact, 2012.

Nepal Earthquake Drone Deployment, IEEE Spectrum, 2015.

Japan Typhoon Hagibis Disaster Response, Journal of Field Robotics, 2019.

California Wildfire UAV Applications, National Fire Protection Agency Report, 2020.

Hurricane Dorian Mapping with UAVs, Remote Sensing Journal, 2019.

Turkey-Syria Earthquake UAV Case Study, UN Disaster Relief Report, 2023.

STUDENT'S IN OTHER ACTIVITIES

IoT-Based Smart Water Quality Detection.

Sarvesh Keer
Dept. of Electronics & Tele-Communication,
VES Polytechnic,
Chembur-71
ej2023.sarvesh.keer@ves.ac.in

Anushka Panchal
Dept. of Electronics & Tele-Communication,
VES Polytechnic,
Chembur-71
ej2023.anushka.panchal@ves.ac.in

Vedant Gajmal
Dept. of Electronics & Tele-Communication,
VES Polytechnic,
Chembur-71
ej2023.vedant.gajmal@ves.ac.in

Abstract--

The rapid urbanization and industrial growth have significantly strained freshwater resources, resulting in contamination of water bodies. Monitoring and ensuring the quality of water have become critical tasks for public health, ecosystem sustainability, and industrial processes. Traditional methods of water quality detection, while effective, are often costly, time-consuming, and impractical for real-time monitoring. The integration of Internet of Things (IoT) technology offers a promising solution to overcome these challenges. This paper explores the development and implementation of an IoT-based smart water quality detection system, which uses sensors to monitor key water quality parameters such as pH, turbidity, dissolved oxygen (DO), and temperature. The system provides real-time data, enabling remote monitoring and early detection of water quality issues.

I.INTRODUCTION

Water quality monitoring is vital for ensuring safe drinking water, protecting aquatic ecosystems, and managing industrial water usage. Traditional water quality testing methods often involve manual collection and laboratory analysis, which is time-intensive and prone to delays. With the increasing demand for real-time monitoring and continuous data collection, there is a growing need for automated solutions that can deliver accurate, timely, and actionable insights. IoT-based water quality detection systems address these needs by integrating sensors with cloud computing to provide a cost-effective, scalable, and efficient approach.

This paper discusses the IoT-based smart water quality detection system, its components, working principles, and its application in real-world scenario.

The system's objectives are:

1. To continuously monitor critical water quality parameters in real-time.
2. To transmit and store data securely on a cloud platform for historical analysis.
3. To provide an accessible interface for data visualization.
4. To implement an automated alert system for proactive intervention.

II. IOT-BASED SMART WATER QUALITY DETECTION SYSTEM

- Sensors: These are the core components used to collect water quality data, such as pH sensors, turbidity sensors, temperature sensors, and dissolved oxygen sensors.
- Microcontroller/Processor: This unit processes the data collected from sensors. It converts raw sensor data into usable information, typically in digital form, which is then transmitted to a cloud platform.
- Connectivity Modules: These modules, such as Wi-Fi, LoRa, or GSM, allow the data to be transmitted from the microcontroller to a remote server or cloud platform in real time.
- Cloud Platform: This is where the data is stored, processed, and analyzed. It allows for remote monitoring and provides the interface for users to view and analyze water quality parameters.

Key Parameters Monitored:

- pH Level: Indicates the acidity or alkalinity of the water. Extreme values can harm aquatic life and indicate contamination.
- Turbidity: Measures the cloudiness of water, which is caused by suspended particles. High turbidity is often associated with pollutants or sediments.
- Dissolved Oxygen (DO): Essential for aquatic life. Low levels of DO can indicate poor water quality and the presence of pollutants.
- Temperature: Affects the rate of chemical reactions and the solubility of gases in water. It can also be an indicator of thermal pollution from industrial activities.

System Design:

- Sensor Integration: Various sensors are integrated with a microcontroller such as ESP8266/ESP32, which collects data on water quality parameters.
- Data Transmission: The microcontroller uses connectivity modules (e.g., Wi-Fi, GSM) to send the sensor data to a cloud platform for further processing and storage.

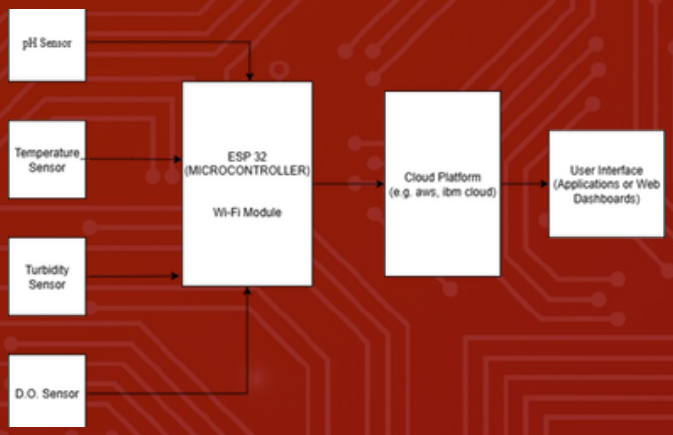


Fig.1 Block Diagram of Smart Water Quality Detection System

Cloud Computing & Analysis: The cloud platform processes the data using analytical tools and algorithms to detect anomalies or deviations from acceptable water quality standards.
User Interface: A web-based or mobile application provides a user-friendly interface for real-time monitoring, notifications, and reporting.

III. TECHNOLOGIES USED

Sensor Technologies Used:
This system employs various sensors to measure different water quality parameters:

- pH Sensor: A potentiometric sensor that measures the hydrogen ion concentration in water.

Fig.2 Gravity Analog pH Sensor

- Turbidity Sensor: A light scattering sensor that measures the scattering of light as it passes through the water, indicating the concentration of suspended particles.

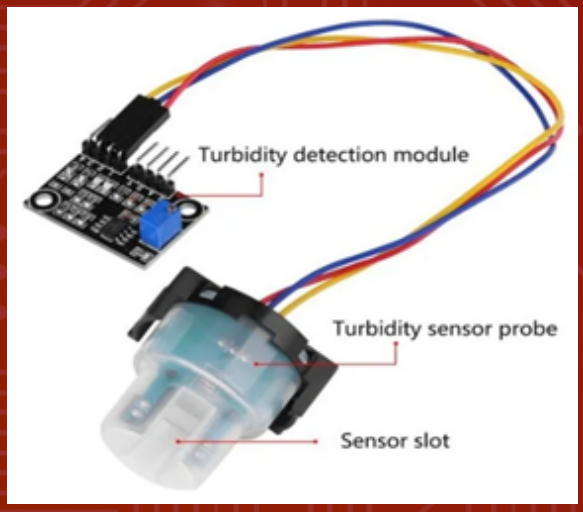


Fig.3 Suspended Turbidity Value Detection Module Kit

- DO Sensor: An electrochemical sensor that detects the amount of dissolved oxygen in water.

Fig.4 SN-3001-LDO-N01-20 (RS485), Fluorescence dissolved oxygen sensor

- Temperature Sensor: A thermistor-based sensor that measures the water temperature.

Fig.5 NTC Thermistor Temperature Sensor

Microcontroller Used:

- ESP32: They are low-cost, energy-efficient, and have built-in Wi-Fi connectivity for easy integration with cloud platforms.

Cloud Computing & Data Analytics

The IoT system relies on cloud computing for data storage, processing, and real-time monitoring. Popular cloud platforms include:

- ThingSpeak: An open-source IoT platform for real-time data analytics.
- AWS IoT Core: A robust cloud solution for securely connecting devices and processing data.
- Microsoft Azure IoT Suite: Provides a comprehensive set of tools for device management, data analytics, and machine learning.

Fig.6 Notable Cloud Services

Data analytics techniques, including machine learning, can be used to predict water quality trends, detect anomalies, and send alerts when water quality parameters deviate from predefined thresholds.

Connectivity and Communication

- Wi-Fi: Suitable for applications in urban areas where reliable internet access is available.
- GSM: Used in remote areas without reliable Wi-Fi or broadband connections.
- LoRaWAN: Ideal for long-range, low-power communication in rural or agricultural regions.

IV. ADVANTAGES OF IOT-BASED WATER QUALITY DETECTION

Real-time Monitoring

One of the significant advantages of IoT-based water quality detection is the ability to monitor water quality in real time. Traditional methods provide only periodic measurements, which may miss rapid changes in water quality. Real-time data collection allows for immediate identification of contamination or other issues.

Cost-Effectiveness

IoT-based systems can be more affordable than traditional water quality monitoring methods. They require minimal manual intervention, reduce the need for lab-based tests, and lower operational costs over time.

Automation and Alerts

The system can automatically trigger alerts or notifications when water quality parameters fall outside acceptable ranges. This automation reduces human error and ensures timely responses to water quality issues.

Scalability

The IoT-based system can be easily scaled to monitor multiple water bodies simultaneously. New sensors and devices can be added without significant infrastructure changes, making it ideal for large-scale deployments.

V. APPLICATIONS

Drinking Water Monitoring

IoT-based water quality detection systems can be used to monitor the quality of drinking water.

Environmental Monitoring

These systems can monitor rivers, lakes, and reservoirs, providing data on pollution levels and helping authorities detect harmful contaminants, illegal dumping, and other environmental hazards.

Industrial Applications

IoT-based water quality detection can help these industries meet regulatory standards and minimize environmental impact.

Aquaculture

In aquaculture, maintaining optimal water quality is crucial for the health of fish and other aquatic organisms. An IoT-based system can monitor DO levels, temperature, and pH to ensure a healthy environment for aquatic life.

VI. CHALLENGES AND FUTURE DIRECTIONS

Sensor Calibration and Maintenance

Sensors used in water quality monitoring can degrade over time, requiring regular calibration and maintenance to ensure accurate readings. Research into low-maintenance, long-lasting sensors is ongoing

Data Security

The transmission of water quality data over the internet raises concerns about data privacy and security. Implementing strong encryption protocols and secure cloud services is essential to mitigate risks.

Power Consumption

Many IoT devices rely on battery power, and continuous monitoring can drain battery life quickly. Developing low-power sensors and energy-efficient communication protocols is an ongoing challenge.

Integration with Regulatory Systems

For large-scale adoption, IoT-based water quality systems need to be integrated with existing regulatory frameworks. Standardization of data formats and communication protocols will facilitate this integration.

VII. CONCLUSION

IoT-based smart water quality detection systems represent a transformative approach to monitoring and ensuring water quality. They offer real-time, scalable, and cost-effective solutions to address the challenges of traditional water quality monitoring methods. As technology continues to evolve, IoT-based systems are expected to play an increasingly critical role in ensuring clean and safe water for both human consumption and environmental protection.

VIII. REFERENCES

[1] "Smart Water Quality Monitoring with IoT Wireless Sensor Networks" — Sensors (2024) by Y. Singh & T. Walingo.

[2] "Smart Water Quality Monitoring with IoT Wireless Sensor Networks" Volume 24, Issue 9, Article 2871 by Kofi Sarpong Adu-Manu.

[3] "IoT Based Smart Water Quality Monitoring: Recent Techniques, Trends and Challenges for Domestic Applications" Volume 13, Issue 13, Article 1729 by Farmanullah Jan

[4] https://www.mouser.com/pdfDocs/ProductOverview_DFRobot-Gravity-Analog-pH-

[5] https://www.scribd.com/document/889704590/JXBS-3001-DO-RS485-Dissolved-oxygen-Sensor-Manual-Fluorescence-method-Electrode

[6] https://www.vishay.com/docs/29053/ntcappnote.pdf

[7] https://www.farnell.com/datasheets/33552.pdf

[8] https://robu.in/product/fluorescence-dissolved-oxygen-sensor/

[9]https://robu.in/product/turbidity-sensor-suspended-turbidity-value-detection-module-kit/

[10] https://ieeexplore.ieee.org/document/8821742

STUDENT'S CORNER

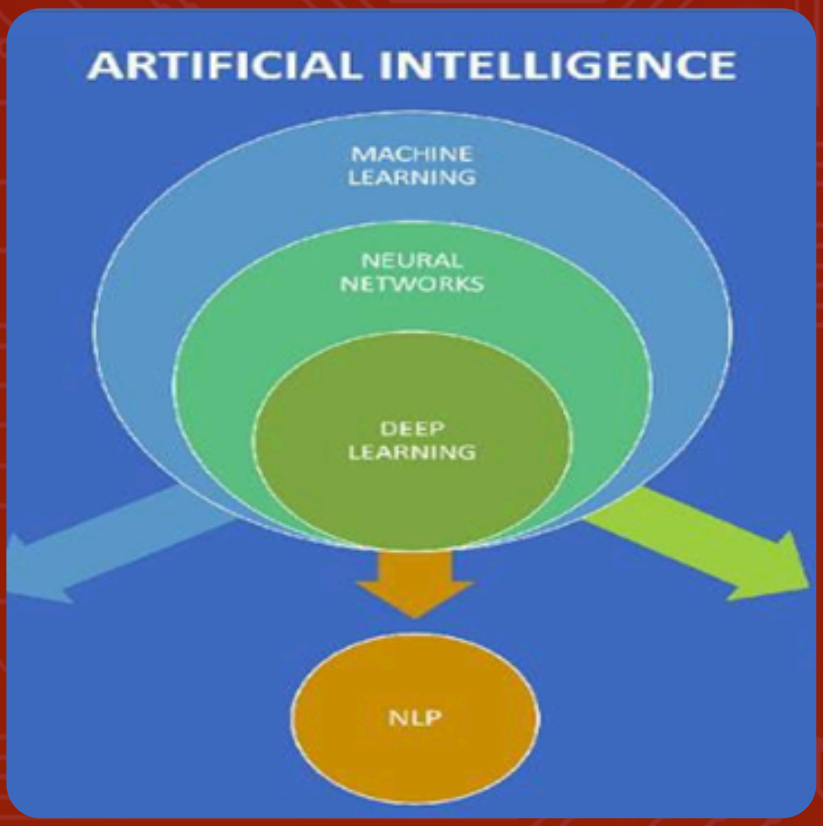
Introduction to Artificial Intelligence

Artificial Intelligence (AI) is one of the most powerful technologies in the modern world. It refers to machines and computer systems that can think, learn, and make decisions like humans. AI is used in many areas such as smartphones, healthcare, education, and transportation. It helps make work faster, smarter, and more efficient, improving our daily lives in many ways.

How Artificial Intelligence Works

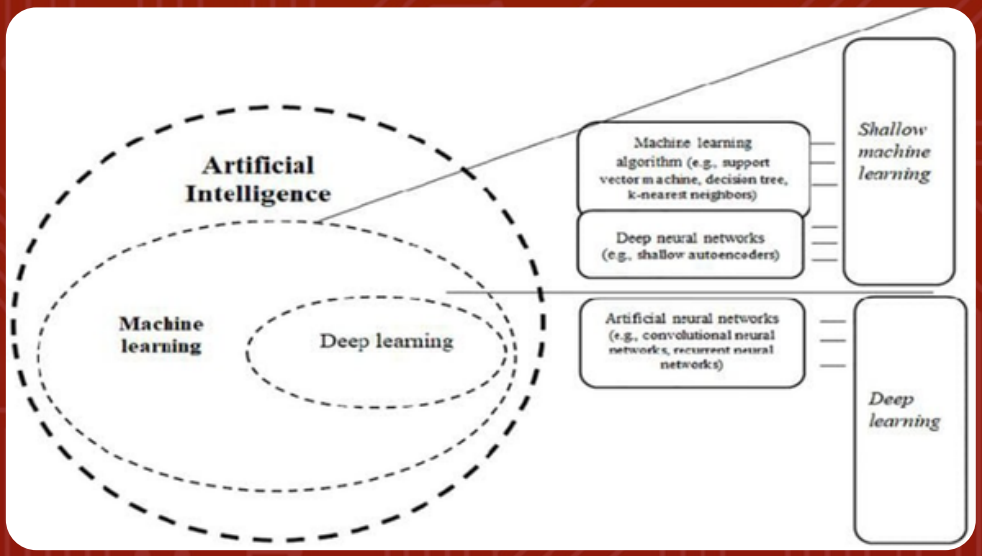
AI works by using data, algorithms, and machine learning techniques. Machines learn from large amounts of data and improve their performance over time. Technologies like machine learning, deep learning, and neural networks allow AI systems to recognize patterns, understand speech, and even predict future outcomes. This ability makes AI very powerful in solving complex problems.

STUDENT'S CORNER



Importance of AI in Daily Life

AI plays an important role in our everyday activities. Voice assistants, face recognition, online recommendations, and navigation apps all use AI. These technologies save time, improve accuracy, and make life more comfortable. AI also helps people with disabilities through speech recognition and smart assistance tools.



STUDENT'S CORNER

AI in Healthcare

In healthcare, AI helps doctors diagnose diseases more accurately and at an early stage. It is used in medical imaging, robotic surgeries, and patient monitoring. AI can analyze large amounts of medical data quickly, helping doctors provide better treatment. This improves patient care and saves lives.

AI in Education

AI is transforming education by offering personalized learning experiences. Smart learning apps help students learn at their own pace. AI also helps teachers by checking assignments, tracking student progress, and identifying learning gaps. This makes education more effective and accessible.

AI in Business and Industry

Businesses use AI to improve productivity and decision-making. AI helps in customer service through chatbots, predicts market trends, and automates repetitive tasks. This reduces costs and increases efficiency. Industries also use AI to improve safety and quality control.

Impact of AI on Jobs

AI is changing the job market by automating certain tasks. While some jobs may be reduced, many new job opportunities are being created in technology and innovation fields. People need to learn new skills and adapt to work alongside AI. Reskilling and continuous learning are very important.

Challenges and Ethical Issues of AI

Despite its benefits, AI also raises concerns such as data privacy, job loss, and misuse of technology. Ethical use of AI is important to ensure fairness and safety. Governments and organizations must create rules to control how AI is developed and used responsibly.

STUDENT'S CORNER

Future of Artificial Intelligence

The future of AI is bright and full of possibilities. It will continue to improve industries, solve global problems, and support human life. When used wisely, AI can create a smarter, safer, and more advanced world. Responsible development and human control will ensure AI benefits everyone

Written by:

Priya Singh
EJ2K

STUDENT'S CORNER

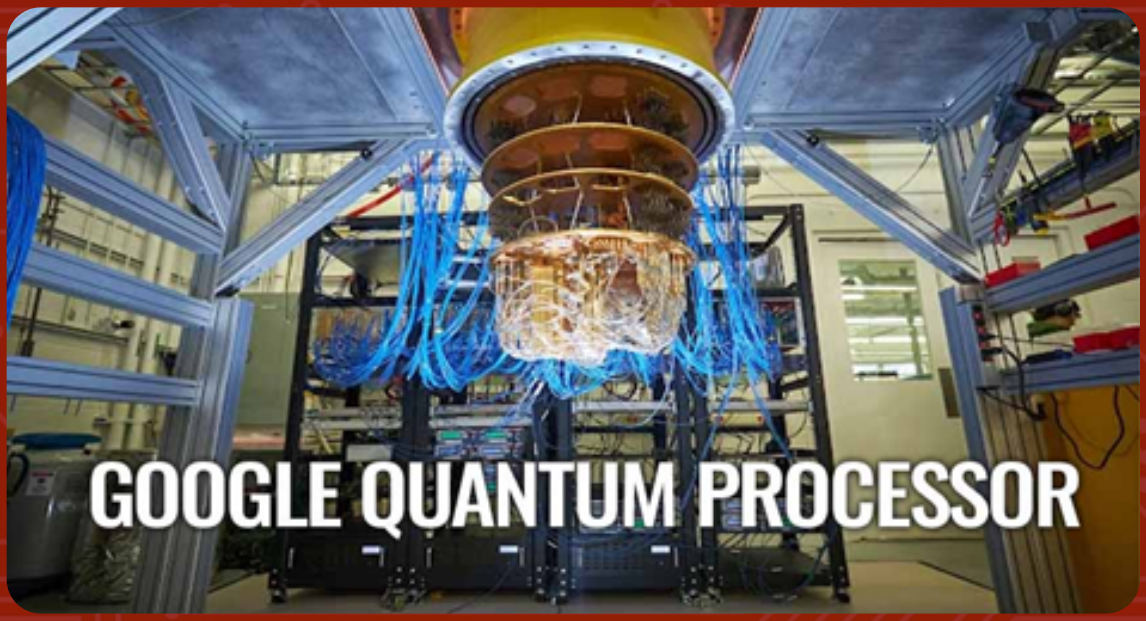
Quantum Computers : A Transformative Frontier in Modern Computing.

Quantum computing is considered one of the most revolutionary technological developments of the 21st century. Unlike traditional computers, it uses principles of quantum mechanics to solve complex problems more efficiently. Although still in the early stages of development, quantum computing has attracted global attention due to its potential impact on science, industry, and society.

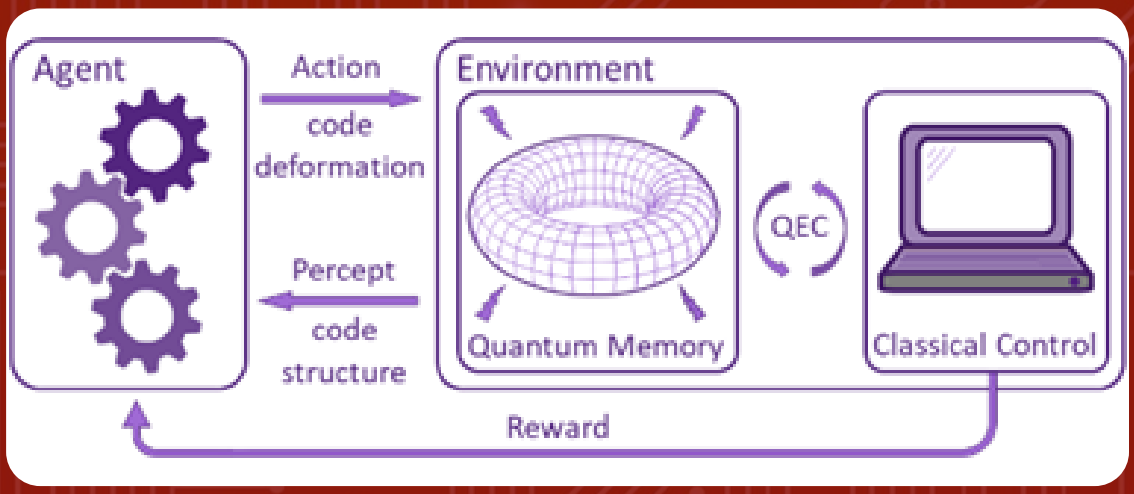
Quantum computing is based on qubits, which differ from classical bits. While a classical bit can be either 0 or 1, a qubit can exist in multiple states at the same time through superposition. Another key principle is entanglement, where qubits remain strongly connected and influence each other instantly. These properties allow quantum computers to process many possibilities simultaneously, making them powerful for solving complex problems.

STUDENT'S CORNER

Qubits can be implemented using different technologies such as superconducting circuits, trapped ions, photonic systems, and topological qubits. Companies like IBM and Google use superconducting qubits that operate at extremely low temperatures. Despite progress, scaling quantum computers remains difficult due to qubit sensitivity and decoherence, which causes loss of quantum information.

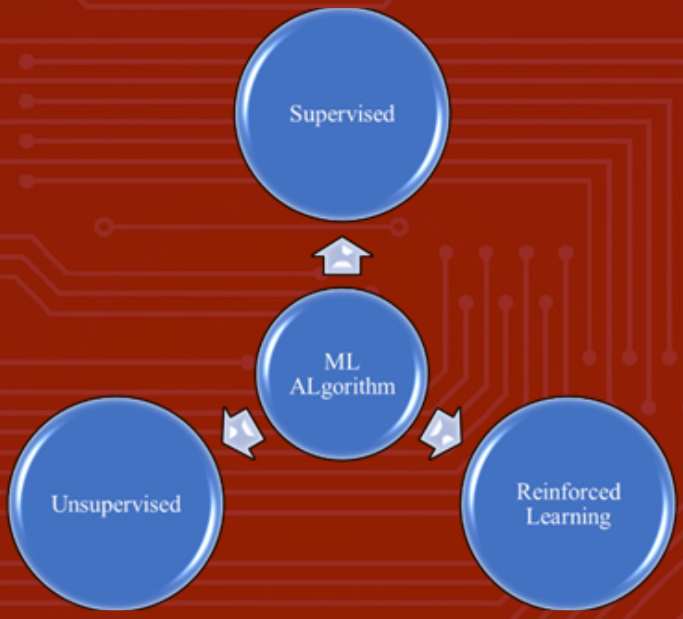


Error correction is a major challenge in quantum computing. Since qubits cannot be copied, classical error correction methods cannot be applied directly. Instead, quantum error correction codes are used to detect and correct errors without disturbing qubit states. Advances in this area are moving quantum systems closer to fault-tolerant and reliable computation.



STUDENT'S CORNER

Quantum algorithms such as Shor's algorithm and Grover's algorithm demonstrate how quantum computers can outperform classical systems in specific tasks. Quantum computing is especially useful for simulating molecules and materials, which can benefit drug discovery, material science, and chemical research. Applications are also being explored in optimization, machine learning, and data analysis.

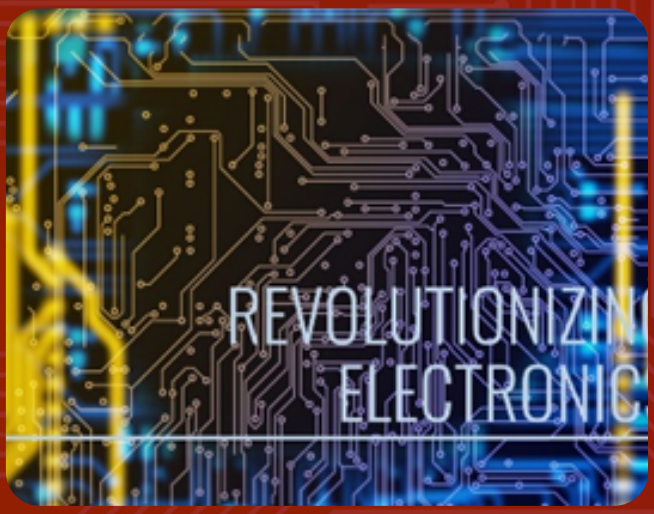


Recent achievements show steady progress in quantum technology. Google's 105-qubit processor demonstrated quantum simulations much faster than classical methods for certain tasks. IBM and other research organizations continue to improve quantum hardware, software, and error reduction, indicating that practical quantum systems may emerge in the coming decades.

Quantum computing still faces several limitations, including limited scalability, qubit instability, high error-correction requirements, and hardware complexity. Due to these challenges, large-scale universal quantum computers are expected to develop gradually, with early applications focused on specialized problems.

STUDENT'S CORNER

Quantum computing could significantly influence cybersecurity, finance, climate research, and national security. While it may weaken current encryption systems, it also drives the development of quantum-safe cryptography. Governments, academic institutions, and industries worldwide are investing heavily in quantum research, highlighting its strategic importance.



Quantum computing represents a major change in how difficult computing problems are solved, offering abilities that go far beyond traditional computers. By using ideas from quantum science such as superposition and entanglement, quantum computers have the potential to bring big changes in areas like data security, healthcare, finance, and climate studies. Although there are still major challenges—especially in increasing system size, reducing errors, and improving machine stability—continuous research and technological progress are helping overcome these limits. Future developments, including error-resistant systems, improved qubit designs, quantum communication networks, and combined quantum-classical systems, are expected to move quantum computing from laboratory research to real-world use. With growing global investment and teamwork across fields, quantum computing is likely to become a powerful technology, shaping the future of science and industry while creating new opportunities for research and innovation

STUDENT'S CORNER

Written by:

RIDDHI KURJEKAR
EJ2K

STUDENT'S CORNER

Cyber Crime: A Growing Threat in the Digital Age

Introduction to Cyber Crime

In today's digital world, the internet has become an essential part of daily life. People use computers and smartphones for communication, banking, education, shopping, and entertainment. However, along with these benefits, the misuse of technology has given rise to a serious problem known as cybercrime. Cybercrime is increasing rapidly and poses a major threat to individuals, organizations, and even governments. Understanding cybercrime is necessary to stay safe in the modern digital environment.

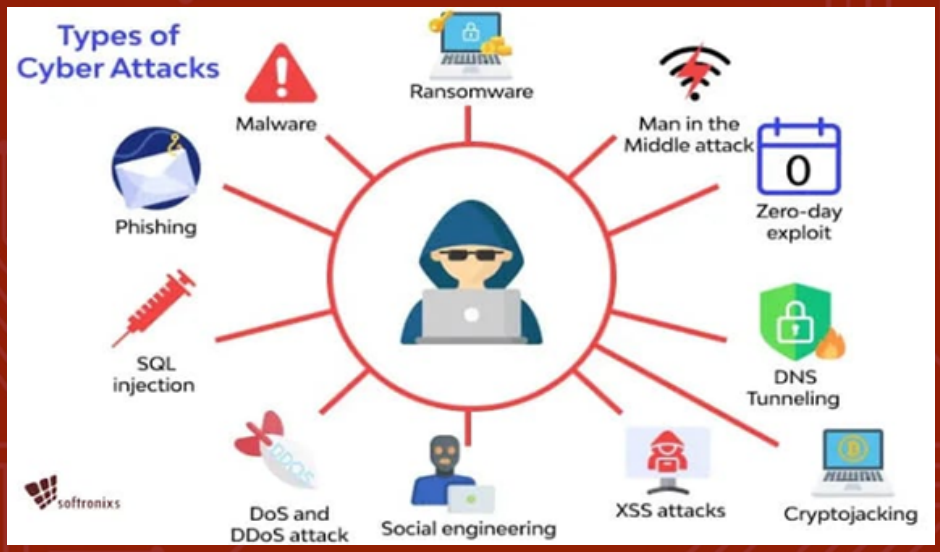
What Is Cyber Crime?

Cybercrime refers to illegal activities carried out using computers, mobile devices, networks, or the internet. In these crimes, technology may be used as a tool, a target, or both. Cyber criminals exploit digital systems to steal data, commit fraud, spread malware, or harm people online.

STUDENT'S CORNER

How Cyber Crime Works ?

Cybercrime works by taking advantage of technology and human trust. Cyber criminals use fake emails, messages, or websites to trick people into sharing personal or financial information. Once access is gained, they steal data or money and hide their identity online.



Importance of Cyber Crime Awareness in Daily Life

- Protects Personal Information – Secures passwords, bank details, and sensitive data.
- Prevents Financial Loss – Reduces the risk of fraud, scams, and phishing attacks.
- Ensures Privacy – Guards personal messages, photos, and online accounts.
- Promotes Safe Internet Use – Encourages responsible use of social media, emails, and apps.
- Supports Law Enforcement – Informed citizens can report crimes promptly to authorities. Reduces Stress and Fear – Awareness increases confidence and online safety

STUDENT'S CORNER

Prevention of Cyber Crime

- Use strong and unique passwords for all accounts.
- Enable two-factor authentication (2FA).
- Avoid clicking unknown links or downloading suspicious files.
- Keep software and devices updated.
- Educate yourself and family about online safety and scams.

STUDENT'S CORNER

Future of Cyber Crime

- Advanced Technology Exploitation – Cyber criminals may use AI, machine learning, and automation to create smarter attacks.
- IoT Vulnerabilities – With more smart devices (home appliances, cars, wearable tech), criminals may target Internet of Things (IoT) devices.
- Rise in Ransomware Attacks – Ransomware may become more frequent and sophisticated, targeting businesses, hospitals, and governments.
- Cyber Terrorism Threats – Hackers may attempt to disrupt critical infrastructure like power grids, transportation, and banking systems.
- Increased Phishing and Social Engineering – Fraudsters will use highly personalized messages to trick victims.
- Global and Cross-Border Crimes – Cybercrimes will continue to be international, making law enforcement more challenging.
- Data Breaches and Identity Theft – Large-scale data theft will increase, putting personal, financial, and corporate data at risk.
- Cyber Crime Against Emerging Technologies – New areas like virtual reality, augmented reality, and blockchain may be exploited. Bottom of Form

Cybercrime is no longer just a threat—it has become a part of our digital reality. Every click, download, or online transaction carries some risk, and criminals are constantly finding smarter ways to exploit technology. The good news is that awareness, strong laws, and personal responsibility can turn the tide. By staying informed, practicing safe online habits, and embracing cybersecurity measures, individuals and organizations can enjoy the benefits of the digital world without falling victim to crime. In the end, the fight against cybercrime is not just a technical battle—it is a shared responsibility for a sa fer, smarter, and more secure digital future

STUDENT'S CORNER

Written by:

Gayatri Shete.
EJ4K

STUDENT'S CORNER

cyber security and digital safety

A single security weakness is all it takes for data, privacy, and trust to collapse.

In an age where personal data is more valuable than money, weak cyber security has become one of the most dangerous threats of the digital era. Every day, millions of users unknowingly expose their private information-bank details, passwords, identities-to cyber criminals due to poor security practices and lack of digital awareness. Without strong cyber security measures, a single click on a malicious link or the use of an easy password can lead to data breaches, financial loss, identity theft, and even large-scale disruption of businesses and public services.The absence of better security does not just affect individuals; it creates a vulnerable digital environment where trust, privacy, and safety are constantly at risk.

The consequences of neglecting cyber security extend beyond financial loss. Personal reputations can be permanently damaged, sensitive corporate data can fall into the wrong hands, and critical infrastructure-such as healthcare systems, power grids, and government networks-can be disrupted, affecting millions of people. Cyber criminals are constantly developing new methods, from sophisticated phishing schemes to ransomware attacks, making it clear that staying passive is not an option. Building strong digital defenses, practicing safe online behavior, and staying informed about emerging threats are no longer optional—they are essential for protecting both personal and societal well-being in the digital age.

STUDENT'S CORNER

Digital safety is the practice of protecting yourself and your personal information while using the internet and digital devices. It involves being aware of online risks such as cyberbullying, scams, phishing attacks, and exposure to inappropriate content. Staying digitally safe means using strong passwords, enabling privacy settings on social media, thinking carefully before sharing personal information, and verifying the authenticity of online sources. By practicing digital safety, individuals—especially children and teenagers—can navigate the online world confidently, avoid potential threats, and maintain control over their personal data and online reputation.

· Core Components of Digital Safety

1. Personal Data Protection: Safeguard sensitive information by using strong, unique passwords, password managers, and enabling two-factor authentication (2FA).
2. Secure Networking: Avoid using unsecured public Wi-Fi for sensitive transactions, and protect home networks with firewalls and secure routers.
3. Malware Prevention: Keep operating systems and applications up to date to fix vulnerabilities, and use reliable antivirus or anti-malware software to block threats.
4. Safe Online Behavior: Be cautious with links, email attachments, and messages from unknown sources, and always verify the authenticity of online communications.

STUDENT'S CORNER

· Key Threats to Digital Safety

1. Cybercrime and Fraud: Increasing cases of financial fraud, identity theft, and ransomware attacks that target both individuals and organizations.
2. Data Breaches: Unauthorized access to sensitive personal, financial, or educational information, often resulting in privacy violations and financial loss.
3. Social Engineering: Manipulative tactics, such as phishing and pretexting, designed to trick users into revealing confidential information.

Digital safety requires smart and responsible behavior while using the internet. It begins with protecting personal information by avoiding the sharing of sensitive details such as home addresses, phone numbers, or passwords online. Adjusting privacy settings on social media is also essential to control who can view your content. Being aware of cyberbullying and reporting or blocking abusive users helps maintain a safe online environment. Additionally, it is important to verify information before trusting it, as not everything on the internet is true, and to think carefully before posting, since once shared, content can be difficult to remove. Practicing these habits ensures a safer and more secure online experience.

Written by:

Shreya Jadhav
EJ4K

ARTWORKS

{Art by}

Spandana nalawade

EJ4K

{Art by}

Saurabh Panchal

EJ4K

ARTWORKS

{Art by}

Ashok Navle Sir

ELECTRONICS AND TELECOMMUNICATION

EDITORIAL TEAM

Mrs. SHEETAL KOKATE.
FACULTY INCHARGE

ABHISHEK YADAV

RADHA KHARAT

It Always Seems Impossible Until It Is Done ...!