

INNOWAVE

ISSUE 8



THE WALL MAGAZINE OF IT DEPARTMENT



PATRONS

Shri Vinod Vats

Dr. Payal Pahwa

EDITORIAL BOARD

Dr. Varsha Sharma

STUDENT COORDINATOR

Karan Joshi



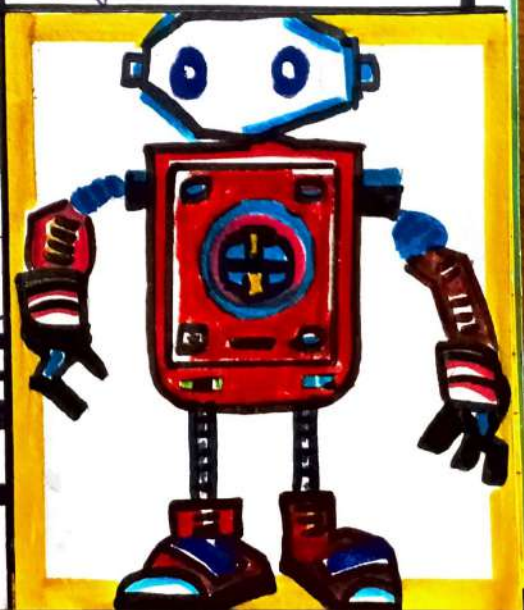
ROBOTICS PROCESS AUTOMATION...

* WHAT IS ROBOTIC PROCESS AUTOMATION?

Robotic process automation (RPA) is a software technology that makes it easy to build, deploy, and manage software robots that emulate humans actions interacting with digital systems and software. Just like people, software robots can do things like understand what's on a screen, complete the right keystrokes, navigate systems, identify and extract data, and perform a wide range of defined actions. But software robots can do it faster and more consistently than people, without the need to get up and stretch or take a coffee break.

THE BUSINESS BENEFITS OF RPA...

Robotics process automation streamlines workflows, which makes organisations more profitable, flexible and responsive. It also increases employee satisfaction, engagement, and productivity by removing mundane tasks from their workdays. RPA is noninvasive and can be rapidly implemented to accelerate digital transformation. And it's ideal for automating workflows that involve legacy systems that lack APIs.



Cyber Security

"Quantum Encryption is essential to protect our digital assets and infrastructure from attackers."

In last year, cyber criminals delivered a wave of cyber attacks that were not just highly coordinated, but far more advanced than ever before seen. Simple endpoint attacks became complex, multi-stage operations. Ransomware attacks hit small businesses and huge corporations alike. Cryptomining attack gave cyber criminals an easy foothold in the company networks. It sounds like something out of a movie, but unfortunately it is true and a very common occurrence in today's landscape. These days we attested massive data leaks, expensive ransomware payouts, and a vast, new, complicated threat landscape. And in today's world we often witness the cyber criminals up their threat game in a big way. This is why cyber security has become such a vital part of any individual life - and Cyber security specialists are in demand now more than ever.

The world of cyber security revolves around the industry standard of confidentiality, integrity, and availability. Privacy means data can be accessed only by the authorized party; integrity means information can be added, altered or removed only by authorized parties and availability means that data must be available on-demand according to agreed-upon parameters. Cyber Security is a process that's designed to protect networks and devices from external threats. The practice is used by individuals and enterprises to protect against unauthorized access to data centers and other computerized systems. The main element of cyber security is the use of authentication mechanisms.

With an increasing number of users, devices and programs in the modern enterprise, combined with the increased deluge of data much of which is sensitive or confidential, the importance of cybersecurity continues to grow. The growing volume and sophistication of cyber attacks and attack technique compound the problem even further. Traditional reactive approaches, in which resources were put toward protecting systems against the bigger known threats were undefended. To keep up with changing security risks, a more proactive and adaptive approach is necessary. There are many benefits of implementing and maintaining cybersecurity. Some of them are:- benefits for business as they remain protected against data breaches, regulatory compliance, protection of network, improved recovery after a breach. Therefore, cyber security is really very important, thus, one must use internet with utmost alertness.

Be aware ... Connect with Care

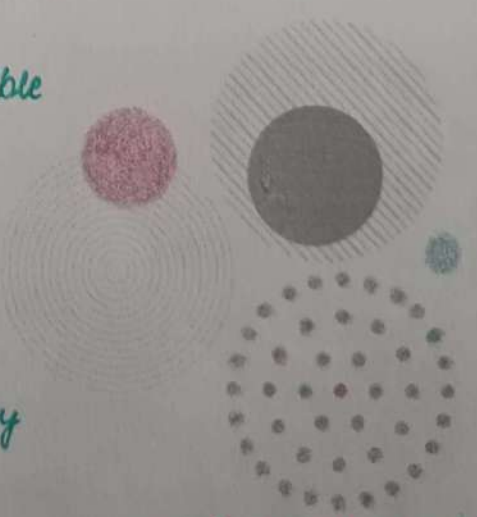


Revolutionizing Our Digital Experience

Smarter devices have emerged as game-changers, re-defining the way we engage with technology. These devices embody crucial aspects that justify their importance in our lives.

Smarter devices effortlessly connect with other devices and networks, fostering seamless communication and information access. Advanced AI algorithms and machine learning capabilities enable personalized experiences, adapting to user preferences and delivering tailored solutions. Smarter devices collect and analyze extensive data, providing valuable insights for informed decision-making and lifestyle optimization. These devices automate tasks, streamlining daily routines and enhancing productivity. Intuitive interfaces, voice commands, and regular updates ensure user satisfaction and functionality.

Smarter devices have become indispensable tools, revolutionizing our lives through enhanced connectivity and superior user experiences, shaping our future interactions with the world as technology advances.



CYBER SECURITY

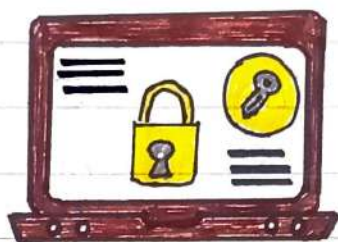
In today's interconnected world, where digital technology permeates every aspect of our lives, ensuring cyber security and fostering digital trust have become paramount. Cyber threats pose significant risks to individuals, organizations, and even nations. As we embrace the benefits of digitalization, it is crucial to prioritize cybersecurity measures to protect sensitive data, maintain privacy, and build trust in the digital ecosystem. Cybersecurity encompasses a range of practices and measures designed to protect computer systems, networks and data from unauthorized access, disruption or damage.

"Cybersecurity is a race without a finish line" - Howard Schmidt

Cyber threats continue to evolve in sophistication and scale, posing a substantial challenge to individuals and organizations alike. These attacks range from data breaches and ransomware attacks to phishing scams and identity theft.

The future of cybersecurity will be shaped by emerging technologies and the increasing interconnectedness of devices. Artificial Intelligence and machine learning can revolutionize threat detection and response, enabling more proactive and adaptive cybersecurity measures. By implementing robust cybersecurity measures, fostering international collaboration & promoting education and awareness we can build a trusted environment that enables benefits of digital age.

As our reliance on digital infrastructure continues to expand the risks associated with cyber threats are growing at an alarming rate. Cyber attacks can result in financial losses, reputational damage, and even compromise national security. From individuals falling victim to phishing attacks to large scale data breaches, the need for robust cybersecurity measures is undeniable.



TYPES OF SECURITY THREATS:-

- a) **MALWARE:** Malware is a malicious software such as spyware, ransomware, viruses and worms, its activated through a malicious link or email attachment that a user clicks leading to installing dangerous software.
- b) **PHISHING:** Phishing attacks use fake communication, such as an email, to trick the receiver into opening it and providing sensitive information like usernames, passwords, credit card numbers etc.
- c) **SQL INJECTION:** This results from inserting malicious code into the server that uses SQL. When infected the server releases information.
- d) **Denial-of-service (DOS) attack:** Floods a server with traffic, making a website or resource unavailable for intended users.
- e) **Distributed Denial of Service (DDoS):** The computer network gets flooded with superfluous requests from hundreds of IP addresses to overload and crash the target system like website.
- f) **Social Engineering:** It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

Best Practices for Cyber Protection include 2FA, Antivirus Programs, Firewall, Internet Security Suite, Identity Theft Protection, Trainings etc.

Cybersecurity: Protecting digital world from threats

In today's interconnected world, where technologies play an increasingly vital role in our lives ensuring robust cybersecurity measures has become more crucial than ever before. With the exponential growth of internet and the threat to digital lives have multiplied. Cyber threats have evolved at an alarming pace, necessitating a proactive approach to cybersecurity. Hackers and cybercriminals constantly seek innovative ways to exploit vulnerability, causing financial losses, reputational damage and compromising personal privacy.

Cybersecurity is vital in safeguarding vital information such as personal data, financial records. Breaches can result in severe consequences including financial losses and legal implications. With digital footprint we leave behind ensuring privacy has become challenging. Cyberattacks can disrupt operations leading to losses in business. Despite technological advancements human errors remain a significant factor contributing cybersecurity breaches. Phishing attacks and social engineering techniques exploit human vulnerability emphasizing the need for education and awareness. The interconnected nature of digital system poses challenges in identifying and securing potential vulnerabilities across the entire infrastructure. Organisations must navigate complex networks, multiple devices and various software application while prioritizing cybersecurity.

Some proactive measures must be taken to ensure cybersecurity. A robust password should be used and it should be complex, unique and regularly updated. Keeping software and system up to date is essential in preventing vulnerability, regular updates include security fixes. Employing firewalls intrusion, detection and prevention systems and virtual private networks and strengthen network security protecting external threats. Encrypting sensitive data adds an extra layer of security making it unreadable and unusable if intercepted by unauthorised individuals. Regularly testing and updating the plan is essential to address emerging threats. In conclusion in increasingly digitised world cybersecurity is not an option but necessity.

Topic

Date :

ROBOTICS PROCESS AUTOMATION GENOMICS

Introduction :-

In recent years, the convergence of robotic process automation (RPA) and genomics has sparked a transformative revolution in the field of genetics research and healthcare. The integration of robotic systems and automation technologies into genomics has significantly improved the efficiency, accuracy, and speed of various processes, unleashing a new era of discovery and innovation.

Streamlined laboratory process :- RPA has revolutionized genomics laboratory workflow by automating repetitive error-prone tasks. Robots excel in delicate procedures like DNA extraction, purification, and sample handling, improving data accuracy.

Enhancing Data Analysis :- Robots can automatically analyze and interpret genomic data, reducing human bias and increasing result reproducibility.

Enabled Precision medicine :- RPA has propelled precision medicine by identifying genetic markers associated with diseases and drug response.

Addressing Ethical and Regulatory challenges :- While RPA offers tremendous benefits, it also presents ethical and regulatory concerns. Ensuring privacy and data security is crucial for genomics.

Conclusion :- The integration of robotic process automation in genomics has revolutionized the field, streamlining laboratory processes, accelerating high-throughput sequencing, enhancing data analysis, and enabling precision medicine. While ethical and regulatory challenges exist.

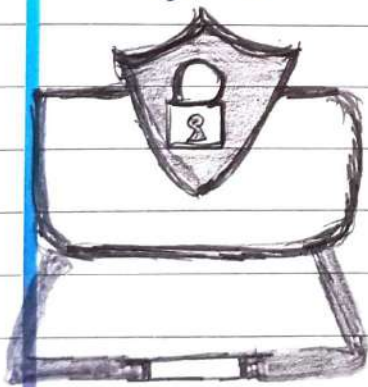
By :- VIKASH KUMAR

Art Designer

CYBER SECURITY

In today's interconnected world, where technology plays a vital role in every aspect of our life. The need for robust cybersecurity measures has become more critical than ever before. Cybersecurity is a practice of protecting computer systems, networks and data from unauthorized access, damage, or theft.

It encompasses a range of strategies, technologies and best practices aimed at safeguarding digital assets and mitigating the risks posed by cyber threats. With the increasing reliance on technology in our daily life, cybersecurity has become a critical concern. It involves implementing measures such as strong passwords, encryption, firewalls and regular software updates to prevent unauthorized access and ensure the confidentiality, integrity and availability of information.



Cybersecurity is an ongoing effort that requires awareness between individuals and governments to create a secure digital environment.

Submitted By —
Divyansh
Rampal

Robotic Process Automation

In recent years, Robotic Process Automation (RPA) has emerged as a revolutionary technology that is reshaping the landscape of business operations. RPA utilizes software robots or bots to automate rule based or repetitive tasks.

The benefits of RPA extend beyond operational improvements. It enables organisations to achieve high accuracy and compliance by ensuring consistent adherence to predefined rules and regulations. Additionally, RPA can enhance user experience by including fast responses, service quality and friendly interactions.

Although, organisations must analyse their existing processes, identify suitable automation opportunities and develop a robust governance framework. Moreover, collaboration between business and IT teams is crucial to align automation initiatives with strategic objectives and ensure seamless integration with existing systems.

As technology continues to advance, RPA is poised to play an increasingly significant role in reshaping business operations. RPA is set to revolutionize the way companies operate, paving the way for more efficient and innovative future.

- By Daksh Sardana (121-IT-C)

GOOD WRITE

Topic.....

Date. / /

★ ROBOTIC PROCESS AUTOMATION ★

Robotic Process Automation (RPA) revolutionizes business operations by automating repetitive using software robots or bots. This technology enhances efficiency, revolutionises costs, and minimise errors, freeing up human resources for higher-value initiatives. RPA seamlessly integrates with existing systems, offering rapid implementation and adaptability to market demands.

RPA tirelessly handles rule-based tasks, accelerating processes, improving productivity and enhancing customer satisfaction. It harmoniously complements legacy systems, producing previous technology investments and ensuring data accuracy and regulatory compliance. With its agility, RPA enables businesses to quickly adapt to market demands and scale operations effectively.

Embracing RPA enables businesses to optimize operations, drive innovation and gain a competitive edge, freeing human potential for growth in the digital era. Robotic Process Automation represents a strategic move towards business efficiency and staying ahead in a rapidly evolving landscape.

- Jyotiraditya
IT 2nd Yr

11720803/21

GOOD WRITE
A Mark of Quality

Teacher's Sign.

CYBER SECURITY

In today's interconnected world, where information flows seamlessly across borders and technology pervades every aspect of our lives, cybersecurity has become a critical concern. Cyber security refers to the practices and technologies used to protect computer systems, networks, and data from unauthorized access, theft, or damage. It encompasses various aspects, including information security, network security, application security, and more. The prime goal of cybersecurity is to ensure the confidentiality, integrity, and availability of digital assets. The consequences of a successful cyber attack can be severe. Individuals may lose personal information leading to identity theft and financial loss. Organizations face the risk of data breaches, which can result in reputational damage, legal liabilities, and financial repercussions. Critical infrastructure systems, such as power grid and transportation networks, are also vulnerable to cyber attacks that could have far-reaching societal consequences. By understanding the evolving threat and implementing effective practices, we can build a safer and more secure cyberspace for everyone.



To emerge as a centre of excellence producing globally competent and morally sound professionals in the field of Information Technology who will practice commitment to their profession and dedicate themselves to the service of mankind.



- To develop state-of-art laboratories providing relevant practical inputs to students.
- To provide strong knowledge base to students in the area of Information Technology and to train them as per the requirement of industries and research organizations.
- To facilitate institute industry interaction to the benefit of stake holders and motivate teachers for the continuous improvement of their academic standards.

