AICTE Training and Learning (ATAL)

Faculty Development Program

On

CYBER SECURITY

(Application No. 1716803856)

From 20th to 25thJanuary 2025

Organized by

Department of Bachelor of Computer Application (BCA)

Guru Gobind Singh Educational Society’s Technical Campus

Chas, Bokaro – 827013, Jharkhand, India

Contents

Faculty Development Program

Hon’ble Chief Patrons

Prof. (Dr.) D. K. Singh , Hon’ble VC, JUT, Ranchi, Jharkhand

Shri Tarsem Singh, Hon’ble President, GGES, Bokaro, Jharkhand

Hon’ble Patron

Shri S. P. Singh, Secretary, GGES, Bokaro, Jharkhand

Convener

Prof. (Dr.) Priyadarshi Jaruhar, Director, GGSESTC

Coordinator

Dr. A. P. Burnwal, Associate Professor, BSH, GGSESTC

Co-Coordinator

Prof. Apurba Sinha, Assistant Professor, CSE, GGSESTC

Co-Convenor

Dr. Akash Arya , Assistant Professor, EEE, GGSESTC

Editorial Board

Ms. Pallavi Prasad, Administrative Officer, GGSESTC

Dr. Deepak Kumar, Assistant Professor, BSH, GGSESTC

Prof. Annupriya, Assistant Professor, BSH, GGSESTC

Dr. Vaibhav Gupta, Assistant Professor, FT, GGSESTC

Organizing Members

Prof. Mahmood Alam, Assistant Professor, ME, GGSESTC

Dr. R.P. Verma, Associate Professor, CE, GGSESTC

Prof. (Dr.) D.K Singh
Chief Patron, ATAL Faculty Development Program (FDP) on Cybersecurity
Honorable VC, JUT, Ranchi

Dear Faculty Members and Participants,

It is with great pride and enthusiasm that ATAL Faculty Development Program (FDP) on Cybersecurity organizing by Guru Gobind Singh Educational Society's Technical Campus (GGSESTC), Bokaro. This initiative reflects our commitment to fostering academic excellence and promoting professional growth among our faculty members and participants from across the nation.

In today's rapidly evolving world, staying ahead in fields like Cybersecurity is not just important—it is imperative. As educators and researchers, we hold the responsibility of equipping ourselves with the latest knowledge, tools, and methodologies so that we can empower our students to meet the challenges of tomorrow. This FDP serves as a platform to exchange ideas, explore innovations, and build a community of like-minded professionals striving for excellence.

I commend the organizing team for their efforts in curating a program that brings together distinguished speakers, engaging sessions, and hands-on experiences. I am confident that this FDP will prove to be a transformative journey for all participants, enhancing their expertise and expanding their perspectives.

I extend my best wishes to the participants and encourage you to make the most of this opportunity by actively engaging, sharing your insights, and embracing new learning experiences. Let us continue to build a culture of academic collaboration and innovation that benefits not only our institution but also society at large.

Warm Regards,

Prof. (Dr.) D.K. Singh
Vice Chancellor
JUT, Ranchi

Shri Tarsem Singh
Chief Patron, ATAL Faculty Development Program (FDP) on Cybersecurity
Hon’ble President, GGES, Bokaro, Jharkhand

I am very happy that our college is organising an ATAL Faculty Development Program (FDP) on Cybersecurity. This program aims to empower our faculty with advanced knowledge and skills in this critical domain, enabling us to stay ahead in the rapidly evolving digital landscape.

Your active participation will be invaluable in making this initiative a success. Let us work together to enhance our expertise and contribute to shaping a secure digital future.

Warm regards,

Shri Tarsem Singh
President, GGES

Shri Surendra Pal Singh
Patron, ATAL Faculty Development Program (FDP) on Cybersecurity
Hon’ble Secretary, GGES, Bokaro, Jharkhand

In today’s digitally interconnected world, cybersecurity is not just a necessity but a cornerstone for ensuring trust and resilience in all aspects of our lives. As educators and thought leaders, it is imperative for us to stay ahead of the curve in this ever-evolving field, equipping ourselves with the knowledge and tools to shape the next generation of professionals.

With this vision, I am delighted to announce the Faculty Development Program (FDP) on Cybersecurity, aimed at fostering excellence in teaching, research, and practice in this critical domain. This program will bring together experts, thought leaders, and practitioners to provide you with insights into cutting-edge technologies, emerging threats, and innovative solutions in cybersecurity.

I strongly encourage your active participation in this initiative. Together, let us enhance our capabilities and contribute meaningfully to the field of cybersecurity, empowering our students and advancing the mission of our institution.

Looking forward to your enthusiastic involvement in making this program a resounding success!

Warm regards,
Shri Surendra Pal Singh
Secretary, GGES

Dr. Priyadarshi Jaruhar
Convener, ATAL Faculty Development Program
Director, GGSESTC, BOKARO

Director’s Message

I am delighted to extend my warm greetings to all eminent resource persons and participants of the ATAL Faculty Development Program on Cyber Security. This initiative is a testament to our shared commitment to fostering a culture of excellence in education and empowering educators with the knowledge and skills required to navigate the complexities of the digital age.

In today’s interconnected world, where technological advancements are reshaping every aspect of our lives, cybersecurity has emerged as a critical area of focus. The increasing reliance on digital platforms has brought with it unprecedented challenges, including data breaches, privacy concerns, and cyber threats that demand immediate and effective solutions. It is imperative for academic institutions and educators to lead the charge in addressing these challenges by equipping themselves with the expertise necessary to build a secure digital future.

The ATAL FDP on Cyber Security provides a unique platform for faculty members to gain a comprehensive understanding of cybersecurity principles, best practices, and emerging trends. Through this program, participants will not only learn from expert practitioners and researchers but also engage in meaningful discussions that can drive innovative approaches to cybersecurity education and research.

I encourage all participants to make the most of this opportunity by actively engaging in the sessions, collaborating with fellow educators, and applying the insights gained to inspire their students and institutions. Let us collectively contribute to building a resilient and secure digital ecosystem that benefits society as a whole.

I would like to extend my heartfelt gratitude to AICTE for their visionary leadership in organizing such initiatives and to all the resource persons for their invaluable contributions. My best wishes to all participants for a fruitful and enriching learning experience.

I am writing to express my heartfelt gratitude for your unwavering support and visionary leadership of Prof. (Dr.) T G. Sitharam, Chairman AICTE, New Delhi; Prof. Rajiv Kumar, Member Secretary AICTE, New Delhi; Dr. Sunil Luthra, Director, AICTE (ATAL), New Delhi; Dr. D. K. Singh, Vice Chancellor, JUT, Ranchi; Shri Tarsem Singh, President, GGES; Shri S.P Singh, Secretary, GGES;. Your guidance has been instrumental in steering our organization toward success and fostering a culture of innovation and collaboration.

Thank you for your trust, encouragement, and the invaluable opportunities you continue to provide. Please know that your efforts and contributions are deeply appreciated and respected.

Looking forward to continuing this journey of success and growth under your exemplary leadership.

Together, let us advance the frontiers of knowledge and strengthen the foundation of a secure digital future.

Warm regards,

Dr. Priyadarshi Jaruhar

Director
GGSESTC, BOKARO

Dr. A.P. Burnwal
Coordinator, ATAL Faculty Development Program
HOD, Basic Science and Humanities, GGSESTC, BOKARO

Dear Participants, It gives me immense pleasure to welcome you to the Faculty

Development Program on
Cybersecurity by AICTE. This program has been thoughtfully designed to foster a deeper understanding of cybersecurity challenges, advanced teaching methodologies, emerging technologies and to equip educators with the tools to enhance their academic and professional endeavors.

In an era where cybersecurity is integral to every facet of our lives, it is vital that we, as educators, not only stay informed about the latest trends but also inspire our participants to contribute meaningfully to this field. Through this program, we aim to provide a platform for knowledge-sharing, skill-building, and collaborative learning with the help of eminent experts and practitioners.

I would like to express my gratitude to the leadership of Director of GGSESTC, our distinguished resource persons, and the organizing team for their unwavering support in making this initiative a reality. I am confident that this FDP will serve as a stepping stone to enhancing our collective expertise and fostering innovation in cybersecurity.

Wishing you an insightful and productive learning experience.

Warm regards,

Dr. A.P. Burnwal
HOD, Basic Science and Humanities
GGSESTC, BOKARO

Prof. Apurba Sinha
Co-Coordinator, ATAL Faculty Development Program
Assistant Professor, Dept. of CSE., GGSESTC, BOKARO

Dear Participants, It is with great enthusiasm that I extend a warm welcome to all of you

to the ATAL
Faculty Development Program on Cybersecurity. This program is a unique opportunity to engage with the latest developments, challenges, and innovations in the ever-evolving domain of cybersecurity.

As a co-coordinator, it has been a privilege to collaborate with the organizing team and esteemed experts to curate a program that blends theory with practice. In today's interconnected world, where the threats to digital assets are increasing exponentially, this FDP seeks to empower educators with the skills and knowledge to address these challenges effectively. Our focus is not only on understanding current trends but also on inspiring a culture of proactive security and resilience.

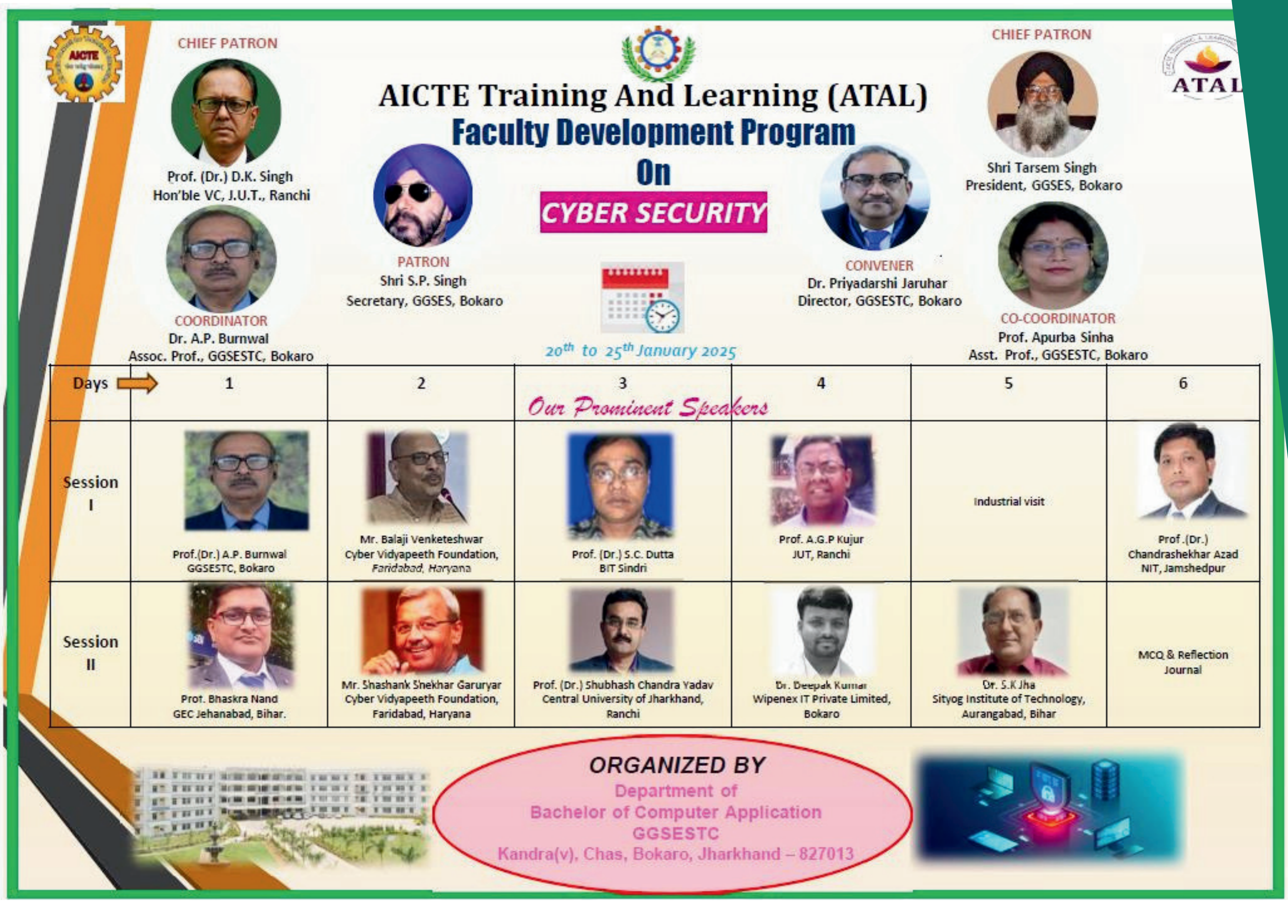
I extend my heartfelt thanks to ATAL for providing this platform, to our eminent speakers for their valuable contributions, and to all participants for their eagerness to learn and grow. I am confident that this FDP will pave the way for meaningful academic and professional advancements in cybersecurity.

Wishing you an enlightening and rewarding experience!

Warm regards,

Prof. Apurba Sinha
Co-coordinator, ATAL Faculty Development Program
Department of Computer Science and Engg.
GGSESTC, BOKARO

Summary of Faculty Development Program (FDP)



CHIEF PATRON
Prof. (Dr.) D.K. Singh
Hon'ble VC, J.U.T., Ranchi

COORDINATOR
Dr. A.P. Burnwal
Assoc. Prof., GGSESTC, Bokaro

AICTE Training And Learning (ATAL)

Faculty Development Program

On

CYBER SECURITY

PATRON
Shri S.P. Singh
Secretary, GGSES, Bokaro

20th to 25th January 2025

CONVENER
Dr. Priyadarshi Jaruhar
Director, GGSESTC, Bokaro

CHIEF PATRON
Shri Tarsem Singh
President, GGSES, Bokaro

CO-COORDINATOR
Prof. Apurba Sinha
Asst. Prof., GGSESTC, Bokaro

ATAL

Our Prominent Speakers

Days ⇨	1	2	3	4	5	6
Session I	Prof.(Dr.) A.P. Burnwal GGSESTC, Bokaro	Mr. Balaji Venketeshwar Cyber Vidyapeeth Foundation, *Faridabad, Haryana*	Prof. (Dr.) S.C. Dutta BIT Sindri	Prof. A.G.P Kujur JUT, Ranchi	Industrial visit	Prof .(Dr.) Chandrashekhar Azad NIT, Jamshedpur
Session II	Prof. Bhaskra Nand GEC Jehanabad, Bihar.	Mr. Shashank Shekhar Garuryar Cyber Vidyapeeth Foundation, Faridabad, Haryana	Prof. (Dr.) Shubhash Chandra Yadav Central University of Jharkhand, Ranchi	Dr. Deepak Kumar Wipenex IT Private Limited, Bokaro	Dr. S.K Jha Sityog Institute of Technology, Aurangabad, Bihar	MCQ & Reflection Journal

ORGANIZED BY
Department of
Bachelor of Computer Application
GGSESTC
Kandra(v), Chas, Bokaro, Jharkhand – 827013

ATAL FDPs

The field of higher education is currently undergoing a transformative phase in order to adapt to global trends. The National Education Policy (NEP) of 2020 serves as a guiding light for this transformative journey. The community of quality teachers holds great potential in driving these changes and plays a crucial role in the development, sharing, and dissemination of knowledge. In the present scenario, with disruptive technological advancements, the role of higher education teachers has become more important than ever before. NEP-2020 aims to empower these teachers by providing them with capacity building training and workshops, enabling them to identify, define, and implement the necessary changes. Without the active involvement of a competent body of quality higher education teachers, the vision of achieving the status of a global knowledge leader, known as Vishwa Guru, cannot be realized. In a world characterized by rapid change, complexity, and uncertainty, the skills of the past are no longer sufficient for today or tomorrow. Technological advancements have multiplied since the time of the Industrial Revolution, and social change along with demographic diversity has given rise to a multitude of innovative thinkers. Each new generation faces a world that is changing faster than ever before. In addition to digitalization, other significant megatrends such as globalization, sustainability, and automation are shaping our society. The COVID-19 pandemic has further accelerated change in all aspects of work and life. In light of these developments, the skills required for Education 4.0 go beyond mere digital proficiency. They encompass complex problem-solving, critical thinking, creativity, people management, teamwork and collaboration, emotional intelligence, judgment and decision making, service orientation, negotiation, project management, cognitive flexibility, and motivation. It is through a faculty that possesses these diverse and energized skills that the foundation for Education 4.0 is built.

FACULTY DEVELOPMENT PROGRAMMES (FDPs)

The objective of AICTE's Training and Learning (ATAL) is to impart quality training through Faculty Development Programmes (FDPs) for Faculty Members, Postgraduate students, Research scholars and Industry Professionals so that the participants:

1. will acquire a sound domain knowledge and associated skills set to apply in real life with industry connect.
2. are equipped with Institutional Leadership skills for academic leadership.
3. are understanding their roles in community wellbeing, national building and also their own career development.
4. can effectively communicate knowledge and skill sets to the students in an efficient manner and their teaching-learning effectiveness is assessed.

2.1(ii) What will be taught

1. Emerging/Core subject area domain knowledge/content 2. Applied knowledge/Lab practical related to the content. 3. Research Avenues/Industrial emerging trends. 4. Analysis & reflection of 2 quality research journal articles on the topic 5. Related Pedagogical approaches including technology integration. 6. Comprehensive assessment/evaluation designing (theory & practical) 7. One of the sessions should be on any of the four categories: a. National Education Policy (NEP) 2020 Implementation b. Indian values & ethos, Classroom conduct & behavior (teaching learning

psychology)

c. Life Skills such as time and stress management (more may be added)

d. Research Methodology

2.1(iii) FDP Flow

Mode: - In house (offline)for theory and practical/labs/ experiential learning.

At least 1 industrial visit to nearby Institute of National Importance/ IoE/prominent multidisciplinary university/CSIR or DST labs/Training Institute/Incubation centers/MSME centers/ Studios etc.

1. Explain the importance of the topic, suggest study, review of 2 research journal articles on the topic.

2. Deliver Concepts of applications/emerging trends
3. Share real-world applications of the topic
4. Ask topical questions at the beginning of the session (rotate)
5. Ask key takeaways at the end of session for understanding.
6. Form small groups to discuss and report back to the class.
7. Invite guest speakers from the industry/corporate/research labs to share their broader perspectives.

Session 1

Name of the Expert: **Prof. (Dr.) A.P.Burnwal**

Designation: **Associate Professor, Department of BSH (Mathematics)**

Organization: **CGSESTC, Bokaro**

Topic: The Evolving Cyber Threat Landscape: Understanding the motivations, tactics, and tools used by attackers

The cyber threat landscape is constantly evolving as attackers refine their strategies, tools, and objectives. This dynamic environment poses significant challenges for organizations, governments, and individuals seeking to protect their digital assets. The motivations behind cyber-attacks range from financial gain and espionage to political ideologies and personal grievances. Cybercriminals employ a variety of tactics, including phishing, malware, exploitation of vulnerabilities, and Distributed Denial-of-Service (DDoS) attacks, among others. To carry out these attacks, they leverage an array of tools such as remote access tools (RATs), ransomware, exploitation frameworks, and botnets. As attackers grow more sophisticated, so too must cyber security defences, emphasizing the importance of proactive threat detection, timely vulnerability

patching, user awareness, and robust incident response planning. This topic explores the evolving nature of cyber threats, examining the underlying motivations, common attack techniques, and the tools employed by cybercriminals to help organizations better understand and defend against these increasingly complex risks.

Session 2

Name of the Expert: Prof. Bhaskra Nand

Designation: Assistant Professor, Department of Computer Science & Engineering (Cyber Security)

Organization: GEC Jehanabad, Bihar

Topic: Cyber security Fundamentals: CIA triad (Confidentiality, Integrity, Availability), Risk management, Security policies and frameworks

Cyber security is a critical aspect of modern digital infrastructures, focusing on safeguarding sensitive information and maintaining the functionality of systems and networks. The core principles of cyber security often referred to as the CIA triad—Confidentiality, Integrity, and Availability—serve as the foundation for designing and implementing effective security measures. Confidentiality ensures that data is accessible only to authorized individuals, integrity maintains the accuracy and trustworthiness of data, and availability guarantees that systems and data are accessible when needed. Risk management plays a key role in identifying, assessing, and mitigating potential threats to reduce vulnerabilities and safeguard assets. Additionally, robust security policies and frameworks guide organizations in structuring their cybersecurity efforts, ensuring compliance with best practices, regulatory requirements, and evolving threat landscapes. This topic explores these fundamental concepts—CIA triad, risk management, and security policies—providing a comprehensive understanding of how they work together to establish a secure and resilient digital environment for organizations and individuals alike.

Session 3

Name of the ExpertMr. Balaji Venketeshwar

DesignationCyber Défense Researcher

OrganizationCyber Vidyapeeth Foundation, Faridabad, Haryana

Topic: Network Security: Firewalls, Intrusion Detection Systems (IDS), secure network architecture design.

Network security is a critical aspect of modern information systems, aiming to protect data integrity, confidentiality, and availability against malicious threats. The implementation of robust security measures is essential to mitigate the risks posed by cyber-attacks. This topic explores three key components of network security: Firewalls, Intrusion Detection Systems (IDS), and Secure Network Architecture Design. Firewalls serve as the first line of defence, controlling incoming and outgoing network traffic based on predetermined security rules. Intrusion Detection Systems (IDS) monitor network traffic to detect and respond to potential threats, identifying unauthorized access or malicious activity. Lastly, secure network architecture design focuses on structuring networks in a way that minimizes vulnerabilities and enhances security, incorporating principles like segmentation, redundancy, and access control. Together, these elements form a

multi-layered defence strategy, providing organizations with the necessary tools to safeguard their networks against evolving cyber threats. The topic highlights best practices and emerging trends in these areas, offering insights into building a resilient network security framework.

Session 4

Name of the Expert: **Mr. Shashank Shekhar Garuryar**

Designation:**Chairman**

Organization:**Cyber Vidyapeeth Foundation, Faridabad, Haryana**

Topic: Cryptography & Data Security: Encryption algorithms, digital signatures, key management practices

Cryptography and data security are essential components of modern information protection, ensuring the confidentiality, integrity, and authenticity of sensitive data. This topic examines three fundamental aspects of cryptography and data security: encryption algorithms, digital signatures, and key management practices. Encryption algorithms, such as symmetric and asymmetric cryptography, are employed to encode data, ensuring that only authorized parties can decrypt and access it. Digital signatures provide a mechanism for verifying the authenticity and integrity of messages, offering assurance that the data has not been tampered with and confirming the identity of the sender. Effective key management practices are crucial for maintaining the security of cryptographic systems, as they govern the generation, distribution, storage, and lifecycle of encryption keys. The topic discusses the challenges and best practices in the implementation of

these cryptographic techniques, highlighting their role in protecting data against unauthorized access and tampering. Additionally, it explores the emerging trends in cryptography, such as quantum-resistant algorithms, and their potential impact on future data security strategies.

Session 5

Name of the Expert Prof. (Dr.) S.C. Dutta

Designation: Associate Professor & Head, Department of CSE, CSE (DS), IT

Organization BIT Sindri

Topic: Cloud Security: Threats and challenges in cloud environments, securing cloudbased data and applications

Cloud security has become a paramount concern as organizations increasingly migrate their data and applications to cloud environments. This topic addresses the key threats and challenges faced in securing cloud-based systems and services, focusing on the protection of data and applications within cloud infrastructures. The dynamic nature of cloud environments introduces several vulnerabilities, including data breaches, unauthorized access, and service disruptions, which require robust security strategies to mitigate. Securing cloud- based data involves the use of encryption, access control, and identity management to ensure that sensitive information remains protected both in transit and at rest. Additionally, securing cloud-based applications requires the integration of security practices throughout the software development lifecycle,

including vulnerability assessments and continuous monitoring. The topic examines the shared responsibility model in cloud security, where both cloud service providers and users must collaborate to maintain security standards. It also explores emerging threats, such as attacks targeting multi-cloud environments and supply chain vulnerabilities, and presents strategies for strengthening cloud security frameworks to address these evolving risks. The topic concludes with an exploration of best practices and tools for securing cloud environments, offering insights into how organizations can confidently leverage the cloud while maintaining a high level of security.

Session 6

Name of the Expert: **Prof. (Dr.) Shubhash Chandra Yadav**

Designation: **Professor & Head, Department of Computer Science and Technology**

Organization: **Central University of Jharkhand, Ranchi**

Topic: Application Security: OWASP Top 10, secure coding practices, vulnerability scanning for web applications

Application security is a critical aspect of safeguarding modern software applications from potential threats and vulnerabilities. This topic explores key principles of application security, focusing on the OWASP Top 10, secure coding practices, and vulnerability scanning for web applications. The OWASP Top 10 identifies the most prevalent security risks in web applications, such as injection attacks, broken authentication, and cross-site scripting (XSS), providing a foundational framework for developers to address common vulnerabilities. Secure coding practices, including input validation, proper error handling, and the principle of least privilege, are vital in reducing the attack surface and ensuring that applications are resilient against exploitation. Additionally, vulnerability scanning tools play a crucial role in identifying weaknesses in web applications, allowing developers to proactively address security flaws before they can be exploited by attackers. The topic highlights best practices for integrating security into the software development lifecycle (SDLC) and discusses the importance of continuous monitoring and regular testing to keep applications secure. By emphasizing the need for a comprehensive, proactive approach to application security, this topic provides valuable insights into how developers and organizations can reduce risk and build secure, robust applications.

Session 7

Name of the Expert: Prof. A.G.P Kujur

Designation: Assistant Controller of Exams and Assistant Professor, Department of CSE

Organization: JUT, Ranchi and BIT Sindri

Topic: Emerging Threats: Social Engineering, Ransom ware, Block chain security, Internet of Things (IoT) security challenges

The landscape of cyber security is constantly evolving, with new and emerging threats posing significant risks to individuals and organizations. This topic examines four key emerging threats: social engineering, ransomware, blockchain security, and Internet of Things (IoT) security challenges. Social engineering attacks exploit human psychology to gain unauthorized access to sensitive information or systems, making awareness and training crucial in mitigating this threat. Ransomware continues to be a pervasive and destructive form of cyber attack, encrypting victim data and demanding payment for its release, highlighting the need for robust backup strategies and incident response plans. Blockchain technology, while offering enhanced security features, introduces new vulnerabilities, particularly in smart contracts and decentralized applications,

which require novel security approaches. Lastly, IoT security challenges are growing as the number of interconnected devices increases, with vulnerabilities in IoT devices providing entry points for cybercriminals to exploit. This topic explores the risks associated with each of these emerging threats, discusses current defence strategies, and outlines best practices for mitigating these risks. It also emphasizes the need for continuous innovation in cyber security tools and practices to stay ahead of increasingly sophisticated attacks, offering insights into how organizations can better protect themselves in a rapidly evolving threat landscape.

Session 8

Name of the Expert: Dr. Deepak KUmar

Designation: Managing Director

Organization: WIPNEX IT PVT. LTD., Bokaro

Topic: Cyber security in AI/ML: Security risks in Machine Learning models, adversarial attacks. Cyber security in Critical Infrastructure: Protecting power grids, transportation systems, and other critical assets.

As artificial intelligence (AI) and machine learning (ML) technologies become increasingly integrated into various sectors, cyber security concerns surrounding these innovations are also on the rise. This topic explores two critical areas: cyber security in AI/ML systems and cyber security in critical infrastructure. In the realm of AI/ML, the topic discusses the security risks inherent in machine learning models, such as data poisoning, model inversion, and adversarial attacks, where malicious actors manipulate input data to mislead or deceive the model. These vulnerabilities threaten the integrity and reliability of AI systems, requiring novel defence mechanisms and ethical considerations to mitigate potential exploitation. Additionally, the topic highlights the cyber security challenges faced by critical infrastructures, including power grids, transportation systems, and other vital assets. These systems are increasingly interconnected and dependent on digital technologies, making them prime targets for cyber attacks that could disrupt operations, cause widespread damage, or jeopardize public safety. The topic examines existing security measures, such as robust access control, real-time monitoring, and incident response protocols, while emphasizing the need for resilient, multi-layered defence strategies to safeguard critical infrastructure. The discussion underscores the importance of evolving cyber security approaches to address the unique risks posed by both AI/ML systems and critical infrastructure in an increasingly digital and interconnected world.

Session 9

Name of the Expert: **Dr. S.K. Jha**

Designation: **Director and Professor, Department of CSE**

Organization: **Sityog Institute of Technology, Aurangabad, Bihar**

Topic: Cyber security Law and Policy: Legal aspects of data breaches, cybercrime investigations, international frameworks.

As cyber threats become more sophisticated, the legal and policy frameworks governing cyber security are critical in ensuring accountability and protecting digital assets. This topic explores the legal aspects of cyber security, focusing on data breaches, cybercrime investigations, and international cyber security frameworks. Data breaches have become a major concern for organizations, raising questions regarding liability, data protection laws, and the legal responsibilities of companies in safeguarding personal and sensitive information. The topic examines key regulations such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), addressing how these laws shape organizational practices and impose legal obligations in the event of a breach. Cybercrime investigations, including digital forensics, chain of custody, and evidence preservation, are also discussed,

highlighting the challenges law enforcement faces in investigating cybercrime across jurisdictional boundaries. Furthermore, the topic delves into the international frameworks that govern cyber security, such as the Budapest Convention on Cybercrime, and the need for global cooperation to address cross-border cyber threats. The topic concludes by exploring emerging legal and policy trends, including the evolving role of artificial intelligence in cyber security governance and the increasing importance of compliance with global standards. By analyzing the intersection of law, policy, and cyber security, this topic provides insight into the complex legal landscape and offers recommendations for organizations and governments in navigating these challenges.

Session 10

Name of the Expert: Dr. Chandrashekhar Azad

Designation: Assistant Professor, Department of Computer Science & Engineering

Organization: NIT Jamshedpur

Topic: The Future of Cyber security: Emerging trends, technologies like block chain/machine learning, and their impact on security. Career Opportunities in Cyber security: Different career paths, skills required and ongoing professional development.

The future of cyber security is shaped by rapid advancements in technology and the increasing complexity of cyber threats. This topic explores emerging trends in cyber security, focusing on technologies like blockchain and machine learning, and their transformative impact on security practices. Blockchain offers potential in enhancing data integrity and secure transactions, while machine learning provides advanced capabilities for threat detection, anomaly identification, and predictive security models. However, these technologies also introduce new challenges, such as securing decentralized systems and addressing the vulnerabilities of AI-powered security tools. Additionally, the topic highlights the growing demand for skilled cyber security professionals and explores various career opportunities within the field. It discusses different career paths, including roles in security analysis, penetration testing, incident response, and cyber security architecture, and outlines the technical and soft skills required to succeed, such as expertise in cryptography, network security, programming, and problem-solving. The importance of ongoing professional development through certifications, continuous learning, and staying up to date with emerging threats is also emphasized. The topic concludes by emphasizing the need for a holistic approach to cyber security, where technological advancements are complemented by a skilled workforce equipped to address the evolving security landscape.