**Computing Division**

**ESOFT Metro Campus**

**Kurunegala**

**Planning a computing project Semester - 2**

**Activity – Week 1**

**Objective:** To develop research skills of students and help the students learn how to locate, evaluate and use scholarly sources effectively

**Task1**: In order to understand what is happening in your selected area of research, please find out literature relevant to that area.Review recent academic papers, articles, websites and case studies on ‘**’Artificial intelligence in detecting and preventing cyberattacks**’’ and fill the following table. List down at least 10 .

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Source** |  | **Title** | **Author Name** | **Date** | **Key points taken** |
| 1. | Example:  Journal  Article | Cyber security meets artificial intelligence: a survey | Jian-hua LI | September 16, 2018, | The paper reviews how artificial intelligence (AI), particularly machine learning (ML) and deep learning (DL), are applied to detect and counteract cyberattacks, enhancing cybersecurity measures    The study analyzes the vulnerabilities AI systems themselves face in adversarial environments.    The paper explores how to construct secure AI systems in distributed environments, emphasizing privacy-preserving approaches like federated learning and encrypted neural networks to protect data during training processes |
| 2. | |  | | --- | |  | | |  | | --- | | Deep Learning in Neural Networks: An Overview | | * Jürgen Schmidhuber | 2015 | * Comprehensive overview of deep learning architectures, algorithms, and applications in computer vision and NLP. |
| 3 |  | Green Cloud Computing: Balancing energy in data centres | * Anton Beloglazov, Rajkumar Buyya | 2012 | * Discusses energy-efficient resource allocation in cloud data centers to minimize power consumption. |
| 4 |  | Computer Security: Principles and Practice | * William Stallings | 2018 | * Focuses on modern cybersecurity threats, encryption methods, access control, and system protection strategies. |
| 5 |  | Evolution and impact of E-Learning technologies | * Curtis J. Bonk, Charles R. Graham | 2013 | * Analyses the role of e-learning platforms, virtual classrooms, and blended learning in modern education. |
| 6 |  | |  | | --- | | Wireless Sensor Networks |  |  | | --- | |  | | * Ian F. Akyildiz, Weilian Su | 2002 | * Explains WSN architecture, protocols, applications in environmental monitoring, and scalability challenges. |
| 7 |  | DevOps: A systematic literature review | * Len Bass, Ingo Weber, Liming Zhu | 2015 | * Covers DevOps principles, automation, CI/CD pipelines, and its role in bridging development and operations. |
| 8 |  | Cloud Security and Privacy | * Tim Mather, Subra Kumaraswamy | 2011 | * Investigates data privacy, compliance issues, and secure cloud adoption strategies. |
| 9 |  | Machine Learning for Predictive Data Analytics | * John D. Kelleher, Brian Mac Namee, Aoife D’Arcy | 2015 | * Introduces supervised and unsupervised learning methods for predictive modelling and analytics. |
| 10 |  | |  | | --- | | Smart Cities and IoT: Opportunities and challenges |  |  | | --- | |  | | * Andrea Zanella, Nicola Bui | 2014 | * Highlights IoT applications in smart cities, urban planning, traffic management, and energy efficiency. |

1

# HND COM - SE