CVR COLLEGE OF ENGINEERING

(An UGC Autonomous Institute, Accredited by NAAC with 'A' Grade)

Department of Computer Science and Engineering

List of Journals Referred Relevant to Seminar Topic

Name of the Student	:R.Vishnuvardhan	Section: CSE-B
Roll Number	: 20B81A05B9	Date:31-07-2023
Area of Seminar Topic	:AIML & CS	

S. No	Journal Details	
1	Title of Journal	The Influence of Artificial Intelligence on E-Governance and Cybersecurity in Smart Cities: A Stakeholder's Perspective
	Publisher	IEEE
	Web Site	https://ieeexplore.ieee.org/document/10177170
	ISSN Number	2169-3536
	Indexed In	Google Scholar, Cross ref , Scopus, Web of Science
2	Title of Journal	Detection Of Phishing Using Machine Learning
	Publisher	IJERT
	Web Site	https://www.ijert.org/detection-of-phishing-using-machine-learning
	ISSN Number	2278-0181
	Indexed In	Scopus, Google Scholar, Web Of Science
3	Title of Journal	Intersection Between Machine Learning And Security & Privacy
	Publisher	IJERT
	Web Site	https://www.ijert.org/intersection-between-machine-learning-and-security-privacy
	ISSN Number	2278-0181
	Indexed In	Google Scholar

Signature of the Student

Area: AI & CS

Abstract -1

Title: The Influence of Artificial Intelligence on E-Governance and Cybersecurity in Smart Cities: A Stakeholder's Perspective

Artificial intelligence (AI) has been identified as a critical technology of Fourth Industrial Revolution (Industry 4.0) for protecting computer network systems against cyber-attacks, malware, phishing, damage, or illicit access. AI has potential in strengthening the cyber capabilities and safety of nation-states, local governments, and non-state entities through e-Governance. Existing research provides a mixed association between AI, e-Governance, and cybersecurity; however, this relationship is believed to be context-specific. AI, e-Governance, and cybersecurity influence and are affected by various stakeholders possessing a variety of knowledge and expertise in respective areas. To fill this context specific gap, this study investigates the direct relationship between AI, e-Governance, and cybersecurity. Furthermore, this study examines the mediating role of e-Governance between AI and cybersecurity and moderating effect of stakeholders involvement on the relationship between AI, e-Governance, and cybersecurity. The results of PLS-SEM path modeling analysis revealed a partial mediating impact of e-Governance between AI and cybersecurity. Likewise, moderating influence of stakeholders involvement was discovered on the relationship between AI and e-Governance, as well as between e-Governance and cybersecurity. It implies that stakeholders involvement has vital significance in AI and e-Governance because all stakeholders have interest in vibrant, transparent, and secured cyberspace while using e-services. This study provides practical implications for governmental bodies of smart cities for strengthening their cybersecurity measures..

Name: R.Vishnuvardhan

Section: CSE-B

Roll No: 20B81A05B9

Area:ML &CS

Abstract -2

Title: Detection Of Phishing Using Machine Learning

Phishing is known as social engineering crime/attack, a hacker or attacker tries to obtain important information from users and influence them by creating a harmful false link that perfectly resembles a real one. A person who clicks on the link is sent to the hacker's website rather than the legal one. User's data is compromised when they provide them sensitive information under the impression that it is authentic. As a result, there is a significant loss of personal information, and when an employee of the firm is compromised, there may also be a loss of corporate information. Due to this, there is a significant loss of one's personal data, and when an employee of the organization is compromised, there may also be a loss of the company's data. The traditional method of phishing detection involved creating a database containing a list of websites that should not be visited as well as the phishing links that were connected with it. This database was then compared to the entered URL to determine if it was or was not in the phishing database. However, there is a drawback to heuristic comprehensive search: if the phishing link is not in the database, there will be an issue and the user may still access the website. By using the website's link and validating them based on the URL characteristics, we may apply a machine learning method to get around the issue of exhaustive search and determine if a link is real or phished. We experimented with a number of methods before deciding to use the Random Forest algorithm on our dataset and developing a Chrome plugin. The random forest gives a accuracy of 89.60% and 0.59 seconds.

Name: R.Vishnuvardhan

Section: CSE-B

Roll No:20B81A05B9

Area:ML & CS

Abstract -3

Title: Intersection Between Machine Learning And Security & Privacy

Digital dangers are developing quickly, bringing about the deficiency of current security and protection measures accordingly, everybody on the Internet is a programmer's item. Machine language calculations and block chain approaches are being utilized to address security and protection concerns. Machine language calculations and block chain approaches have both been the subject of a few examinations. At last, we use Machine language calculations and block chain procedures to address security and protection issues in the area, and we feature and enlighten different snags and future examination subjects. The protection and security of the clients have become critical worries because of the association of the gadgets in various applications. To address security and protection challenges, blockchain approaches are turning out to be progressively pervasive in current IOT applications. Nonetheless, these investigations use Machine language calculations or block chain ways to deal with address either security or protection issues, requiring a consolidated appraisal of current endeavors to address both security and protection issues utilizing Machine language calculations and block chain methods. Accordingly, Machine Learning procedures are utilized to create exact results from enormous convoluted data sets, which can be used to figure and find weaknesses.

Name: R.Vishnuvardhan

Section: CSE-B

Roll No:20B81A05B9