CHRIST
(DEEMED TO BE UNIVERSITY)
BANGALORE · INDIA

Notice for the PhD Viva Voce Examination

Mr Raghavendra Rao A (Registration Number: 2071906), PhD scholar at the School of Sciences, CHRIST (Deemed to be University), Bangalore will defend his PhD thesis at the public viva-voce examination on Tuesday, 19 September 2023 at 11.00 am in Room No. 044, Ground Floor, R & D Block, CHRIST (Deemed to be University), Bengaluru - 560029.

Title of the Thesis	:	**Design and Development of Artificial Intelligence Based Knowledge Management System for Managing Software Security Vulnerabilities**
Discipline	:	**Data Science**
External Examiner (Outside Karnataka)	:	**Dr Soumyadev Maity** Associate Professor Department of Information Technology Indian Institute of Information Technology, Allahabad Prayagraj, Uttar Pradesh - 211012
External Examiner (Within Karnataka)	:	**Dr R Muthukumar** Director Centre For Reliability Electronics Test and Development Ministry of Electronics and Information Technology Government of India, Thiruvanmiyur Chennai – 600041 Tamil Nadu
Supervisor	:	**Dr Debabrata Samanta** Associate Professor Department of Computer Science School of Sciences CHRIST (Deemed to be University) Bengaluru - 560029 Karnataka

The members of the Research Advisory Committee of the Scholar, the faculty members of the Department and the School, interested experts and research scholars of all the branches of research are cordially invited to attend this open viva-voce examination.

Registrar

Place: Bengaluru
Date: 06 September 2023

ABSTRACT

Software development practices play a significant role in building the world's future. It is the place where exciting technological evolution begins in the world. Exploration of critical challenges in the area of software development plays a significant role in fueling the pace of technological progression in the industry. This work focuses on exploring important areas of software development practices and problems faced by the industry. Understanding the critical parts of the software system development eco-system and the stakeholders associated with those will be important.

Customers of software development teams, the software development industry and knowledge sources, and the software development internal eco-system are the broad focus areas of study. Leveraging the data already spread across the eco-system and facilitating easy access to practitioners as and when there is a need will be one of the primary focuses. The software development landscape module, customer landscape module, and industry landscape module are the key modules that will be explored in this work. The core aspiration of the work will be to integrate all the possible data across the industry and process the same and make it easily accessible to the practitioners as and when they are needed. The process also makes the data smarter and more insightful over time.

***Keywords**: Software security vulnerabilities, Software development, Data science, Deep learning for software development, the Knowledge management system in software development*

Publications:

1. **Althar, R.R.**, Samanta, D. The realist approach for evaluation of computational intelligence in software engineering. Innovations Syst Softw Eng 17, 17–27 (2021). https://doi.org/10.1007/s11334-020-00383-2 Mathematical Foundations based Statistical Modeling of Software Source Code for Software System Evolution
2. **Althar, R. R.**, Samanta, D., Kaur, M., Alnuaim, A. A., Aljaffan, N., Aman Ullah, M. (2021). Software Systems Security Vulnerabilities Management by Exploring the Capabilities of Language Models Using NLP. Computational Intelligence and Neuroscience, 2021.
3. **Althar, R. R.**, Alahmadi, A., Samanta, D., Khan, M. Z., Alahmadi, A. H. (2022). Mathematical foundations based statistical modeling of software source code for software system evolution. Mathematical Biosciences and Engineering, 19(4), 3701-3719.
4. **R. R. Althar**, D. Samanta, M. Kaur, D. Singh and H. -N. Lee, "Automated Risk Management based Software Security Vulnerabilities Management," in IEEE Access, 2022, doi: 10.1109/ACCESS.2022.3185069.