CHRIST
(DEEMED TO BE UNIVERSITY)
BANGALORE · INDIA

Notice for the PhD Viva Voce Examination

Mr Kapil Tiwari (Registration Number: 2090207), PhD scholar at the School of Sciences, CHRIST (Deemed to be University), Pune Lavasa Off Campus will defend his PhD thesis at the public viva-voce examination on Saturday, 16 December 2023 at 10.30 am in the Discussion Room (Room No. A213), CHRIST (Deemed to be University), Delhi NCR Off Campus, Ghaziabad, Uttar Pradesh-201003.

Title of the Thesis	:	**Development of Privacy Preserving Machine Learning Techniques Using Secure Multi-Party Computation**
Discipline	:	**Computer Science**
External Examiner (Outside Maharashtra)	:	**Dr Thippeswamy G** Professor and Dean Department of CSE BMS Institute of Technology and Management Avalahalli, Yelahanka Bengaluru-560064 Karnataka
External Examiner (Within Maharashtra)	:	**Dr Vivek Deshpande** Professor Vishwakarma Institute of Information Technology Survey No. 3/4, Kondhwa (Budruk) Pune – 411048, Maharashtra
Supervisor	:	**Dr Jossy P George** Professor Department of Computer Science CHRIST (Deemed to be University) Delhi NCR Off Campus, Ghaziabad Uttar Pradesh – 201003

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: Delhi

Date: 11 December 2023

ABSTRACT

Machine learning (ML) has brought about a paradigm shift in insight generation across various domains, including healthcare, finance, and pharma, by leveraging historical data. However, the effectiveness of ML solutions hinges on the seamless collaboration between data owners, model owners, and ML clients while ensuring that privacy concerns are meticulously addressed. Unfortunately, existing privacy-preserving solutions have not been able to offer efficient and confidential ML training and inference. This has led to an increased focus on Privacy-Preserving Machine Learning (PPML), which has become a flourishing area of research aimed at safeguarding the privacy of machine learning stakeholders. In this regard, the present research introduces novel techniques for private ML inference and training of models using Secure Multi-Party Computation (SMPC) and Differential Privacy (DP) methods on horizontally and vertically partitioned datasets. The proposed techniques are implemented using Python with open-source libraries such as SyMPC and PyDP to ensure confidential inference and model protection. The findings across various parameters illustrate the effectiveness of the suggested techniques in addressing the privacy concerns of model owners and inference clients, with no significant impact on accuracy and a linear influence on performance as the privacy parameters, such as secure nodes count within the SMPC cluster. are increased. Furthermore, the privacy gain is substantiated by information privacy measures such as Mutual Information and KL-Divergence across different privacy budgets, which demonstrate empirically that privacy can be preserved with high ML accuracy and minimal performance cost.

Keywords: *Privacy-Preserving Machine Learning (PPML), Secure Multi-Party Computation (SMPC), Privacy, Machine Learning (ML), Confidential Inference and Model Protection.*

Publications:

1. **Kapil Tiwari,** Samiksha Shukla & Jossy P. George (2021), A Systematic Review of Challenges and Techniques of Privacy-Preserving Machine Learning. Lecture Notes in Networks and Systems book series (LNNS, volume 290) with SPRINGER NATURE on 27th August 2021. https://doi.org/10.1007/978 -981-16-4486-3_3
2. **Kapil Tiwari,** Kritica Bisht & Jossy P. George (2022), CoInMPro: Confidential Inference and Model Protection Using Secure Multi-Party Computation. Lecture Notes in Networks and Systems book series (LNNS, volume 290) with SPRINGER NATURE on 4th February 2022. https://doi.org/10.1007/978 -981-19-2211-4_1
3. **Kapil Tiwari,** Jossy P. George (2022), A SYSTEM FOR CONFIDENTIAL INFERENCE AND MODEL PROTECTION USING SECURE MULTI-PARTY COMPUTATION. Patent. Published Awaiting Examination: Dated 4th February 2022 with application number 202241004611.
4. **Kapil Tiwari,** Jossy P. George (2022), CoinMPro DP. India Copyright. Granted: diary number 13926/2022-CO/L and request number 56673 dated 26th June 2022 and Granted on 28th November 2022.
5. **Kapil Tiwari,** Jossy P. George(2022), A System for Confidential Training Inference for Vertically Partitioned Datasets using Secure Multi-Party Computation. Patent. Published Awaiting Examination: Dated 14th October 2022 with application number 202241057386.
6. **Kapil Tiwari,** Nirmalya Sarkar, Jossy P. George(2022), Confidential Training and Inference using Secure Multi-Party Computation on Vertically Partitioned Dataset. Scalable Computing: Practice and Experience ISSN: 18951767.