CHRIST
(DEEMED TO BE UNIVERSITY)
BANGALORE | DELHI NCR | PUNE

Notice for the PhD Viva Voce Examination

Ms Teena Mary, Registration Number: 2170223, PhD Scholar at the Department of Statistics and Data Science, School of Sciences, CHRIST (Deemed to be University) will defend her PhD thesis at the public viva-voce examination on Monday, 29 June 2026 at 10.30 am in Room No. 05, Ground Floor, R&D Block, CHRIST (Deemed to be University), Bengaluru - 560029, Karnataka, India.

Title of the Thesis	:	**Securing File Fragment Classification Models Against Byte-Level Adversarial Attacks: A Detection-Based Defense Framework**
Discipline	:	**Data Science**
External Examiner - I	:	**Dr Lajish V L** Associate Professor and Head Department of Computer Science University of Calicut Thenhipalam - 673635 Kerala
External Examiner - II	:	**Dr John A** Associate Professor Department of Informatics Military College of Telecommunications (MCTE) Ministry of Defence, Government of India Dr Ambedkar Nagar - 453441 Madhya Pradesh
Supervisor	:	**Dr Sreeja C S** Assistant Professor Centre for Quantum Technology 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 (Academics)

Place: Bengaluru
Date: 22 June 2026

ABSTRACT

File fragment classification is essential in digital forensics and network security for identifying files when metadata is missing or corrupted. While recent deep learning-based classifiers achieve 65-79% accuracy on 512-byte clean fragments in the FFT-75 benchmark, their robustness under adversarial conditions has been underexplored. Empirical evaluation shows that simple byte-level attacks, such as padding and bit-flipping, cause accuracy to degrade sharply from 71.1% on clean fragments to an average of 15.8% under adversarial perturbations, exposing a limitation in existing methods. This research presents a two-stage detect-then-classify defense framework that addresses the accuracy-robustness trade-off inherent in traditional adversarial training. This research integrates three complementary components: (i) an attention-based adversarial detector achieving 95.46% specificity and 91.34% recall (91.44% overall accuracy) (ii) a baseline file fragment classifier (ByteRCNN) that preserves 71.1% accuracy on clean fragments through detection-guided routing; and (iii) a newly proposed Dual-Scale Attention-based Robust CNN (DSAR-CNN) designed specifically for adversarial fragment classification. DSAR-CNN achieves 68.4% accuracy on adversarially perturbed fragments evaluated over a final test set of 4.6 million samples. As adversarial attacks on file fragment classification remain under explored, the proposed approach is evaluated relative to the adversarially trained state-of-the-art baseline FFC model, highlighting significant gains in classification accuracy and robustness under adversarially manipulated fragments. The proposed framework is developed and evaluated on a large-scale corpus comprising 30.72 million fragments across 75 file types and 39 adversarial attack variants derived from the FFT-75 dataset. Experimental results demonstrate that the complete detect-then-classify approach achieves 70.91% accuracy on clean data with only a 0.19 percentage point penalty, 63.84% accuracy on adversarial data, and 70.20% accuracy in realistic mixed-threat scenarios comprising both clean and adversarial fragments. This outperforms the adversarial training approach by 12.04 percentage points. This proposed architecture offers a solution for strengthening file fragment classification systems against byte-level adversarial attacks such as padding and bit-flipping.

Keywords: *file fragment classification, digital forensics, adversarial robustness, detection- based defense, byte-level attacks, deep learning, attention mechanisms.*

Publications:

1. **T. Mary** and C. S. Sreeja, "Adversarial Shadows in Digital Forensics: New Insights Into File Fragment Classification Vulnerabilities and Defenses," in IEEE Access, vol. 14, pp. 11064-11083, 2026, doi: 10.1109/ACCESS.2026.3655822.
2. **T. Mary** and S. C. Sreeja, "Attention and representation learning in byte-level digital forensics: A survey of methods, challenges, and applications," International Journal of Advanced Computer Science and Applications, vol. 17, no. 2, 2026, doi: 10.14569/IJACSA.2026.0170213.
3. **T. Mary** and S. CS, "Attention-based CNN for Adversarial File Fragment Detection Against Padding and Bit-Flip Attacks," 2025 5th International Conference on Evolutionary Computing and Mobile Sustainable Networks (ICECMSN), Coimbatore, India, 2025, pp. 935-942, doi: 10.1109/ICECMSN68058.2025.11382778.
4. **T. Mary** and C. S. Sreeja, "File fragment classification," in Quantum Computing Models for Cybersecurity and Wireless Communications, John Wiley & Sons, Ltd., 2025, ch. 12, pp. 201-218, doi: 10.1002/9781394271429.ch12.
5. [PRE-ACCEPTED in Journal of Engineering and Technology for Industrial Applications] - Two-Stage Detect-Then-Classify Pipeline with DSAR-CNN for Robust Fragment Classification under Padding and Bit-Flip Attacks.