Pradip Kunwar

pkunwar42@tntech.edu | linkedIn/pradip-kunwar-72b00165 | +1-931-284-8749

SUMMARY

- Ph.D. Researcher specializing in the intersection of Large Language Models (LLMs), Privacy and Security.
- Expertise in Parameter-Efficient Fine-Tuning (PEFT), Sparse Mixture-of-Experts (MoE), and Differential Privacy (DP).
- 8+ years of cross-functional leadership experience in the AI industry, bridging the gap between research-grade algorithms and production-ready AI products.
- **Research Interests:** Privacy-preserving ML, Adversarial Robustness, PEFT methods, Tensor-Train Decompostion.

EDUCATION

Ph.D., AI and Security — Tennessee, USA | Aug 23 - Ongoing
Tennessee Technological University

B.Tech in Electronics and Communication — INDIA | Jul 12 - Jul16
National Institute of Technology (NIT), Rourkela

PUBLICATIONS

- **Privacy Enhanced PEFT: Tensor Train Decomposition Improves Privacy Utility Tradeoffs under DP-SGD**, *(Under peer review)*, Jan 2026
- **TT-LoRA MoE: Unifying Parameter-Efficient Fine-Tuning and Sparse Mixture-of-Experts**, *Accepted on Supercomputing 2025*, Apr 2025
- **SoK: Leveraging Transformers in Malware Analysis**, *Accepted on IEEE Transactions on Dependable and Secure Computing*, June 2025
- **MalFormer001- Multimodal Transformer Fused Attention based Malware Detector**, *Accepted on IEEE SmartComp*, June 2024
- **A Survey on Adversarial Attacks for Malware Analysis**, *Accepted on IEEE Access*, July 2024

SKILLS

Core Research: LLMs, PEFT (LoRA, TT-LoRA), Mixture-of-Experts, Differential Privacy, Adversarial ML.
ML Frameworks: PyTorch, Opacus, TensorFlow, Keras, HuggingFace Transformers, Scikit-learn.
Data & Analytics: NumPy, Pandas, SciPy, NLTK, Spacy, Matplotlib, SQL.
Engineering: Python, C++, React, Git, Linux/Bash, LaTeX.
Soft Skills: Leadership, Problem Solving, Teamwork, Work Ethics.

PROJECTS

Privacy Analysis of TTLoRA — May 25 - Jan 26

- Conducted the first formal privacy audit of Tensor Trained LoRA (TTLoRA) vs. standard LoRA, demonstrating that tensor-based weight compression provides an inherent regularization effect against attacks.
- Designed and implemented a custom Differentially Private (DP) training framework using private-transformers and PyTorch, achieving a superior privacy-utility trade-off compared to Full Fine-Tuning and standard LoRA.
- Proved that TTLoRA maintains higher model utility under strict privacy budgets ($\epsilon < 1.0$) by reducing the parameter space and implementing more structurally constrained architecture.

TTLoRA based MoE for Multi-task Learning — Dec 24 - Apr 25

- Developed a novel Sparse Mixture-of-Experts (MoE) architecture using Tensor-Train LoRA (TTLoRA) to enable efficient multi-task fine-tuning without catastrophic forgetting.
- Designed a low-parameter routing mechanism that utilizes only 2% of standard LoRA parameters while maintaining competitive performance on SQuAD and GLUE benchmarks.

- Successfully mitigated knowledge interference in multi-task scenarios by isolating task-specific knowledge within sparse tensor-compressed experts.

Multimodal Transformer Fused Attention for Malware Detection — Dec 24 - Ongoing

- Proposed a novel multimodal architecture (MalFormer001) that leverages fused attention across four feature domains—image, graph, text, and audio—to identify sophisticated malware.
- Developing the feature extraction pipeline and transformer encoder modules to validate the effectiveness of cross-modal attention mechanism.

Nepali News classifier and summarizer — Apr 22 - Jul 22

- Developed an LSTM-based NLP pipeline to perform multi-class classification and extractive summarization on Nepali news articles dataset.

Classified Market Information Platform — Feb 17 - Nov 19

- Designed and deployed a digital marketing search engine designed to index and retrieve local vendor data for real-time user queries.
- Led the backend development of the platform's core matching algorithm, and data retrieval for a growing database of local service providers.

Hand Gesture Recognition System — Aug 15 - Jul 16

- Designed a real-time gesture recognition system using LabVIEW to capture and process hand movements via camera inputs.
- Developed a classification logic to accurately distinguish between "Rock, Paper, Scissors" gestures.

WORK EXPERIENCE

LOS ALAMOS NATIONAL LABORATORY Graduate Research Intern — NM, USA Jan 25 – Ongoing

- Conducting research on **Trustworthy AI** and robustness.

TENNESSEE TECH UNIVERSITY Graduate Research Assistant — TN, USA Aug 23 – Ongoing

- Leading research on **Security and Privacy of LLMs**, specifically evaluating membership inference attacks and developing DP-aware training loops for compressed architectures.

FUSEMACHINES — Nepal/US Dec 19 – Aug 23

Senior AI Product Manager | May 22 – Aug 23

- **Fuse Extract:** Led the development of an OCR/NER pipeline using Handwriting Recognition for banking documents; optimized accuracy for dual-language (Nepali/English) contexts.
- **Squadery ML:** Led the development of automated CV parsing and semantic scoring models, leveraging NLP to automate candidate-job matching.
- **Squadery Connect Application:** Led the development of a centralized consultant lifecycle platform, automating hiring workflows and resource management to streamline global staffing operations.

Senior AI Solutions Lead (Sales/APAC) | May 20 – Apr 22

- Directed the technical pre-sales and implementation of Fuse Classroom, an AI-integrated LMS, for 50+ educational institutions with over 15,000+ users.

Management Analyst | Dec 19 – Apr 20

- Standardized technical recruitment and onboarding workflows for AI engineering teams to reduce scaling friction.

KHOZINFO.COM Founder — Nepal Aug 16 – Nov 19

- Built and scaled a digital marketing search engine; designed the initial backend architecture to handle 1,500+ client data pipelines and localized search indexing.

HOSTELCART.COM Co-Founder — India Apr 15 - Jul 16

- Launched an e-commerce platform incubated at NIT Rourkela Incubation Center, scaling to process 1,000+ orders in 30 days.

AWARDS AND RECOGNITION

- Selected as **RSA Scholar** to attend **RSAC 2026**, San Francisco.
- Awarded **ACM SIGHPC Rusty Lusk Student Scholarship** to attend **SC25**; recognized for contributions to high-performance computing and LLM efficiency.
- Awarded **NSF Student Travel Grant** for PhD Forum presentation at **SMARTCOMP** 2024, Osaka, Japan.
- Awarded **NSF Student Travel Grant** for attending **FLAIRS AI** Conference 2024 at Florida, USA.
- Awarded scholarship for **highest SAT II score** for the undergraduate program.
- Awarded **'National School of Sciences Merit Scholarship'** full tuition waiver to study +2 Science degree.
- **Top 10** student from the school in S.L.C (School Leaving Certificate).

ACTIVITIES

- Co-Leader of **CCT - Creative Communication Team** to establish team spirit and bolster engagement culture at Fusemachines Nepal office, 2021-23.
- Initiated open air musical events **MAKTUB,** 2016 and **ACOUSTICA** in college during Fests 2014 & 15.
- Central coordinator of **Multi Ethnic Festival 2014 & 15, International Students Meet 2013 & 14** in college.
- First prize winner of **Hindi band competition** in Cultural Fest 2015, BIT Meshra, India
- First prize winner of **Hindi band competition** in Spring Fest 2014, **IIT Kharagpur**, India.
- First prize winner of **Texas Instruments Innovation Challenge 2014** held at college.