AL AMIN, Ph.D.

Assistant Professor of Computer Science | AI/ML • Cybersecurity • Trustworthy & Distributed Intelligent Systems

U.S. PERMANENT RESIDENT

Huston-Tillotson University, Austin, TX 78702 | alamin.aston.ml@gmail.com | +1 (615) 975-6993 |
IEEE Member
Google Scholar| LinkedIn

RESEARCH PROFILE

Research-active computer scientist and engineer working at the intersection of artificial intelligence, machine learning, cybersecurity, privacy-preserving distributed intelligence, and scientific computing. Research integrates federated learning, Vision Transformers, learnable encryption, differential privacy, lightweight homomorphic encryption, explainable AI, large language models, multimodal/agentic AI, and physics-informed learning. Prior telecommunications engineering experience spans wireless networks, radio-access infrastructure, IP/VLAN networking, system integration, and multi-generation mobile systems. Applications include cybersecurity, healthcare/medical imaging, edge and distributed computing, scientific discovery, and cyber-physical systems.

RESEARCH AREAS

Artificial Intelligence & Machine Learning • Cybersecurity & Digital Forensics • Trustworthy & Privacy-Preserving AI • Federated & Distributed Learning • Efficient/Edge Intelligence • Large Language Models & Agentic AI • Vision Transformers • Explainable AI • Medical/Biomedical AI • Scientific Machine Learning • Wireless & Networked Systems

ACADEMIC APPOINTMENT

Assistant Professor, Department of Computer Science — Huston-Tillotson University (HBCU), Austin, TX **Jan 2026–Present**

- Teach Digital Forensics and Cyber Crime; Artificial Intelligence & Robotics; Introduction to Data Science; Data Structures and Programming; and Programming Foundations II.
- Lead curriculum redesign and syllabus development aligned with ABET student outcomes; serve on the Departmental ABET Accreditation Committee supporting assessment, curriculum mapping, and continuous improvement.
- Design outcome-based assessments, laboratory activities, and project-based learning; mentor undergraduate research in cybersecurity, AI, medical AI, data science, and software engineering.
- Develop research initiatives in cybersecurity, privacy-preserving machine learning, trustworthy AI, and scientific data analytics; contribute to externally oriented proposal development involving NSF, DOE, national laboratories, and industry.

EDUCATION

Ph.D., Engineering and Computational Science — Tennessee State University, Nashville, TN **2025**

- Department of Electrical and Computer Engineering.

M.Sc., Electrical and Electronic Engineering (with Professional Experience) — University of Portsmouth, United Kingdom **2022**

SELECTED RESEARCH APPOINTMENTS

Selected Visiting Faculty, U.S. DOE Visiting Faculty Program — Ames National Laboratory, Ames, IA **Summer 2027**

- Selected for a 10-week collaborative research appointment focused on AI for Scientific Discovery using multimodal LLMs, Retrieval-Augmented Generation (RAG), and physics-grounded AI for magnetic materials discovery.
- Planned collaboration on MAGNUS, integrating scientific literature, materials databases, crystal structures, and DFT-based verification for trustworthy materials discovery.

AI Researcher (Doctoral) Tennessee State University, Nashville, TN **Jan 2023–2025**

- Developed privacy-preserving AI frameworks integrating Vision Transformers, federated learning, learnable encryption, differential privacy, and lightweight homomorphic encryption for secure medical image analysis.
- Designed communication-efficient federated learning architectures using compact encrypted feature representations rather than conventional full-gradient sharing.
- Integrated Grad-CAM, LIME, and SHAP for explainability; studied membership inference, model inversion, secure data sharing, and heterogeneous federated-learning risks.

INDUSTRY & POSTDOCTORAL RESEARCH

Postdoctoral Researcher — Centific Global Solutions, Inc., San Antonio, TX **Dec 2024–Jan 2025**

- Developed and evaluated Agentic AI workflows integrating LLMs, vision-language models, RAG, and autonomous reasoning for enterprise AI applications.

Ph.D. Technical Intern — Centific Global Solutions, Inc., San Antonio, TX **Jun 2025–Aug 2025**

- Improved reproducibility in human evaluation of LLM-generated code using rubric-guided AI-assisted feedback; developed a multilingual LLM-as-a-Judge framework accepted to AI-SQE at ICSE 2026.

ENGINEERING & TELECOMMUNICATIONS EXPERIENCE

Field Services Engineer — Nokia, Bangladesh **Jul 2018–Jun 2020**

- Engineered and supported multi-vendor telecommunications infrastructure across 2G/3G/LTE environments, including Nokia FSMF, Alcatel-Lucent BTS/NodeB, transmission systems, VLAN/IP networking, site integration, commissioning, KPI validation, acceptance testing, and network troubleshooting.

Site Engineer — ZTE Corporation, Dhaka, Bangladesh **Nov 2016–Jun 2018**

- Supported deployment and integration of 2G/3G/4G telecommunications infrastructure through technical site surveys, equipment commissioning, VLAN configuration, NOC-coordinated troubleshooting, KPI analysis, acceptance testing, and field-engineering support.

Field Services Engineer — Ericsson, Bangladesh **Jan 2016–Sep 2016**

- Installed, commissioned, integrated, and troubleshot GSM/WCDMA/LTE radio-access infrastructure, including Ericsson RBS systems, transport connectivity, hardware/software diagnostics, antenna systems, VLAN configuration, KPI monitoring, and customer technical support.

RESEARCH HIGHLIGHTS & CONTRIBUTIONS

- **Federated Learning Forensics:** Developed FedTrace for forensic client attribution and attack-onset localization in heterogeneous federated learning; submitted to NDSS 2027.
- **AI-Enabled Cyber Defense:** Co-authored SENTINEL, a multi-pathway architecture for Living-off-the-Land APT detection from Windows command lines; accepted at IEEE MILCOM 2026.
- **Privacy-Preserving Distributed AI:** Designed encrypted-feature and differential-privacy federated-learning approaches to reduce inference exposure while preserving collaborative model utility.
- **Communication-Efficient AI:** Developed Vision Transformer-based federated architectures using compact encrypted feature representations to reduce communication overhead without exposing raw data.
- **Explainable & Trustworthy AI:** Integrated Grad-CAM, SHAP, and LIME into privacy-sensitive AI systems to improve interpretability and transparency.
- **LLM & Agentic AI:** Developed LLM-as-a-Judge methodologies and conduct research on RAG, multimodal foundation models, Agentic AI, and autonomous intelligent systems.
- **Scientific & Medical AI:** Developed physics-informed and privacy-preserving learning approaches for medical imaging and emerging AI-for-scientific-discovery applications.

GRANT ACTIVITY

- Lead PI: NSF 26-512, Unlocking Dataset Value for AI-Enabled Scientific Discovery (AI Datasets), in collaboration with Dr. Prashant Singh, Ames National Laboratory. [In Preparation, 2026]
- Lead PI: Security, Privacy, and Trust in Cyberspace (SaTC 2.0), NSF 25-515. [In Preparation, 2026]

PEER-REVIEWED PUBLICATIONS

1. SENTINEL: A Multi-Pathway Architecture for Detecting Living-off-the-Land APT Attacks on Windows Command Lines. IEEE Military Communications Conference (MILCOM), 2026.
2. Al Amin et al. Privacy-Preserving Federated Vision Transformer Learning Leveraging Lightweight Homomorphic Encryption in Medical AI. IEEE ICNC, 2026.
3. Al Amin et al. Lightweight Privacy-First Federated Learning for Medical AI. EAI SecureComm, 2026.
4. Al Amin et al. AI-Driven Secure Data Sharing: A Trustworthy and Privacy-Preserving Approach. IEEE CCNC, 2025.
5. Al Amin et al. ViT Enhanced Privacy-Preserving Secure Medical Data Sharing and Classification. IEEE CCNC, 2025.
6. Al Amin et al. XAI-Empowered MRI Analysis for Consumer Electronic Health. IEEE Transactions on Consumer Electronics, 71(1), 2025.
7. Al Amin et al. Multilingual Code Evaluation with LLM-as-a-Judge: AI-Assisted Feedback for Human-Centric Understanding. AI-SQE at ICSE, 2026.
8. Al Amin et al. Physics-Embedded Feature Learning for AI in Medical Imaging. IEEE SoutheastCon, 2026.

9. Al Amin et al. Advancing Healthcare: Innovative ML Approaches for Improved Medical Imaging in Data-Constrained Environments. IEEE GLOBECOM, 2025.
10. Al Amin et al. An Explainable AI Framework for Artificial Intelligence of Medical Things. IEEE GLOBECOM, 2023.
11. Al Amin et al. Multi Hospital MRI Analysis with Privacy-Preserving Ensemble Enhanced Federated Learning. IEEE SoutheastCon, 2024.
12. Al Amin et al. Integrating AI and Edge Computing for Advanced Safety at Railroad Grade Crossings. Journal of Rail Transportation Planning and Management, 2024.
13. Al Amin et al. Intelligent Railroad Grade Crossing: Semantic Segmentation and Object Detection for Enhanced Safety. IRF Global R2T Conference, 2023.
14. Al Amin et al. Industrial Product Defect Detection Using Custom U-Net. IEEE ICCIT, 2022.
15. Al Amin et al. Analysing and Detecting Extreme-Selfie Images Using Ensemble Technique. IEEE ICCIT, 2022.
16. Al Amin et al. ADPT: An Automated Disease Prognosis Tool Using Hybrid Deep Learning Architecture. IEEE ICCT, 2022.
17. Grid-Wise Physics-Informed Federated Learning with Spatially-Localized Feature Regularization for Heterogeneous Medical Image Classification. IEEE Access, 2026.

SUBMITTED MANUSCRIPTS

- FedTrace: Forensic Client Attribution and Attack-Onset Localization in Heterogeneous Federated Learning. Submitted to NDSS 2027.

TEACHING & UNDERGRADUATE MENTORSHIP

- Current teaching portfolio: Digital Forensics and Cyber Crime; Artificial Intelligence & Robotics; Introduction to Data Science; Data Structures and Programming; Programming Foundations II.
- Develop project-based and laboratory-centered learning experiences spanning Python programming, algorithms, AI/ML, data analysis, cybersecurity, and digital forensics.
- Mentor undergraduate students in artificial intelligence, cybersecurity, medical AI, data science, and software engineering research, including implementation, dataset preparation, experimentation, visualization, and research communication.
- Spring 2026 Artificial Intelligence and Robotics teaching evaluations: 4.7/5.0 for instructor preparation and clarity; 75% of respondents rated overall instructor performance Excellent.

PROFESSIONAL & SCHOLARLY SERVICE

- Peer Reviewer: IEEE GLOBECOM (2023, 2024).
- Peer Reviewer: IEEE SoutheastCon (2024, 2025).
- Peer Reviewer: IEEE International Conference on Computing, Networking and Communications (ICNC).
- Peer Reviewer: Transportation Research Board (TRB).

TECHNICAL EXPERTISE

AI & Machine Learning: Vision Transformers, deep learning, foundation models, LLMs, Agentic AI, RAG, multimodal AI, federated learning, transfer learning, physics-informed AI.

Cybersecurity & Digital Forensics: APT/LOTL detection, digital forensics, federated-learning security, membership inference, model inversion, secure data sharing, privacy attacks and defenses.

Privacy-Preserving & Trustworthy AI: Learnable encryption, differential privacy, lightweight homomorphic encryption, secure multi-party learning, privacy-preserving medical AI, communication-efficient federated learning.

Distributed, Edge & Networked Systems: Federated/distributed learning, communication-efficient AI, wireless networks, GSM/WCDMA/LTE, radio-access networks, IP/VLAN networking, transmission systems, system integration and troubleshooting.

Medical/Biomedical & Explainable AI: Medical image analysis, MRI classification, Grad-CAM, SHAP, LIME, clinical decision support.

Programming & Platforms: Python, Java, MATLAB; PyTorch, TensorFlow, Hugging Face Transformers, scikit-learn, OpenCV, Keras, LangChain; NVIDIA CUDA, GPU computing, distributed deep learning, Microsoft Azure, Docker, Linux, Git/GitHub.