ABDULLAH MELHEM

Ph.D. in Computer and Cyber Sciences
Department of Information Systems & Analytics, McCoy College of Business
Texas State University, 601 University Drive, San Marcos, TX 78666-4616
Phone: +1 (706) 750-6860 - **Email:** melhem@txstate.edu

Google Scholar | ORCID | Web of Science

EDUCATION

Augusta University (AU), USA *August 2026*
Ph.D. in Computer and Cyber Sciences

Jordan University of Science and Technology (JUST), Jordan *Sep 2021*
M.S. in Computer Science

Yarmouk University (YU), Jordan *Sep 2017*
B.S. in Computer Science

RESEARCH INTERESTS

High-performance and scalable AI systems; distributed and federated learning; privacy-preserving machine learning; secure and resilient model aggregation; machine learning for cybersecurity; adversarial robustness; large-scale NLP and LLM evaluation; blockchain-assisted distributed AI; data-intensive social-media and healthcare analytics.

WORK EXPERIENCE

Assistant Professor of Instruction August 2026 - Present
Department of Information Systems & Analytics Texas State University

Graduate Research Assistant Jan 2023 - August 2026
Advisor: Dr. Ahmed AlEroud Augusta University

- Designed secure and resilient federated learning frameworks for distributed healthcare analytics, including clustered model training, adaptive model selection, lightweight blockchain coordination, and functional-encryption-based aggregation.
- Developed reproducible machine learning pipelines in Python/PyTorch/TensorFlow for large-scale experimental evaluation across heterogeneous data settings.
- Evaluated adversarial robustness, model resilience, and privacy-preserving aggregation strategies for distributed AI systems.
- Published first-author work in IEEE Internet of Things Journal, ACM Transactions on the Web, IWCMC, HICSS, and ASONAM on secure federated learning, adversarial NLP, and AI-driven analytics.

Artificial Intelligence Developer (Full time) - Industrial Experience July 2020 - Jan 2023
Supervisor: Prof. Ashraf M. A. Ahmad Jordan Design & Development Bureau (JODDB)

- Developed AI-based computer vision solutions for defense and security applications, including face search, license-plate recognition, vehicle/driver verification, and automated gate-access systems.
- Implemented, optimized, and productionized machine-learning algorithms for real-world deployment, with emphasis on inference efficiency, latency reduction, memory usage, and reliability in operational environments.

- Built OSINT data-processing and analytics pipelines for social-media data collection, normalization, account-level analysis, regional trend detection, and structured reporting.
- Designed backend services, APIs, and user-facing dashboards to support time-sensitive decision-making and intelligence analysis.
- Developed scalable multilingual data-processing and model-evaluation pipelines for large social-media datasets across low-resource languages and multiple platforms.

PUBLICATIONS

1. Abdullah Melhem, Ahmed Aleroud, Abdullah Al-Mamun, and Mohamed I. Ibrahem. "Clustered Federated Learning for Healthcare Analytics: A Dual Blockchain-Functional Encryption Method for Fortified Aggregation". In: *IEEE Internet of Things Journal* (2026), pp. 1–1. DOI: 10.1109/JIOT.2026.3658441
2. Abdullah Melhem, Ahmed Aleroud, Abdullah Al-Mamun, Mohamed I. Ibrahem, and Nidal Nasser. "Secure and Resilient Clustered Federated Learning for Web-Enabled Healthcare Analytics Using Lightweight Blockchain and Adaptive Model Selection". In: *ACM Trans. Web* (Mar. 2026). ISSN: 1559-1131. DOI: 10.1145/3801730. URL: https://doi.org/10.1145/3801730
3. Nour Alhussien, Ahmed Aleroud, Abdullah Melhem, and Samer Y Khamaiseh. "Constraining adversarial attacks on network intrusion detection systems: transferability and defense analysis". In: *IEEE Transactions on Network and Service Management* 21.3 (2024), pp. 2751–2772
4. Abdullah Melhem, Ahmed Aleroud, Abdullah Al-mamun, George Karabatis, and Mohamed I Ibrahem. "Adversary-Resilient Clustered Federated Learning for Secure AI-Driven Healthcare Data Analytics". In: *2025 International Wireless Communications and Mobile Computing (IWCMC)*. IEEE. 2025, pp. 630–636
5. Abdullah Melhem, Ahmed Aleroud, and Albert Craig Douglas. "Evading Detection or Triggering False Alarms? A Character-Level Adversarial Attack on LLM Detection of Arabic Social Media Bots". In: *59th Hawaii International Conference on System Sciences (HICSS)*. 2026
6. Abdullah Melhem, Ahmed Aleroud, and Albert Craig Douglas. "GraphRAG-based NLP at Risk: Graphemic Dot-Level Adversarial Attack on Arabic Sentiment and LLM Retrieval-Augmented Models". In: *The 17th International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2025)*. Springer Nature. 2025
7. Christopher Mason, Ahmed Aleroud, Abdullah Melhem, Zain Halloush, and Jason A Williams. "Generative AI vs. Human Deception: A Comparative Analysis of ChatGPT, Gemini, and Human-Generated Disinformation". In: *Proceedings of the 2025 ACM International Workshop on Security and Privacy Analytics*. 2025, pp. 13–22
8. Abbas Al-Refaie, Majd Al-Atrash, Abdullah Melhem, and Natalija Lepkova. "Web-based maintenance prediction of machine conditions and failure modes using machine learning". In: *Journal of Advanced Manufacturing Systems* 24.02 (2025), pp. 359–383
9. Abdullah Melhem, Zain Halloush, and Ahmed Aleroud. "Dynamic Network Analysis of Cognitive Attacks Using Meta-Network Modeling and Community Detection Algorithms". In: *2024 IEEE 6th International Conference on Cognitive Machine Intelligence (CogMI)*. IEEE. 2024, pp. 240–246
10. Abdullah Melhem, Ahmed Aleroud, and Zain Halloush. "Ai-based multimodal to identify state-linked social media accounts in the middle east: A study on twitter". In: *2023 IEEE International Conference on Intelligence and Security Informatics (ISI)*. IEEE. 2023, pp. 1–6
11. Ahmed Aleroud, Abdullah Bani Melhem, Nour Alhussien, and Craig Douglas Albert. "sPAN-pROP: Combatting Contextualized Social Media State-Linked Propaganda in the Middle East". In: (2023).

DOI: 10.25785/amcis2023/10

12. Craig Douglas Albert, Ahmed Aleroud, Yufan Yang, Abdullah Melhem, and Josh Rutland. "Twitter propaganda operations: analyzing sociopolitical issues in Saudi Arabia". In: *Social Media+ Society* 9.4 (2023), p. 20563051231216964
13. Rehab Duwairi and Abdullah Melhem. "A deep learning-based framework for automatic detection of drug resistance in tuberculosis patients". In: *Egyptian Informatics Journal (Q1)* 24.1 (2023), pp. 139–148
14. Abdullah Melhem, Omar AlZoubi, Wail Mardini, and Muneer Bani Yassein. "Applications of blockchain in smart cities". In: *Proceedings of the second international conference on data science, E-learning and information systems*. 2019, pp. 1–7

POSTERS AND PRESENTATIONS

Poster

- AU-UGA Cyber-Physical Systems Innovation Symposium *Fall 2025*
- AU Computer & Cyber Graduate Student Orientation Fall Fest *Fall 2024*

Presentation

- The Hawaii International Conference on System Sciences (HICSS-59) *Spring 2026*
- 2025 Information Advantage Conference *Fall 2025*
- International Wireless Communications & Mobile Computing Conference (IWCMC) *Spring 2025*
- 2024 IEEE 6th International Conference on Cognitive Machine Intelligence (CogMI) *Spring 2024*
- 2024 Augusta University Information Warfare Conference (IW) *Spring 2024*
- 2023 IEEE International Conference on Intelligence and Security Informatics (ISI) *Spring 2023*

FELLOWSHIPS & AWARDS

- Earning The Runner-up Poster Award
  AU Computer & Cyber Graduate Student Orientation Fall Fest *Fall 2024*
- $1,000 Travel Award
  The Graduate School at Augusta University *Fall 2024*
- Graduate research assistant scholarship of ONR-DoD, A Socio-political Analysis of Arabic Social Media Attacks Using Computational Modeling. PI Dr. Ahmed Aleroud, $500,622 *2023 - 2025*

ACADEMIC SERVICE

- Journal Reviewing: IEEE Internet of Things Journal, IEEE Transactions on Network and Service Management
- Conference Reviewing: 17th EAI International Conference on Digital Forensics & Cyber Crime

CERTIFICATES

- United States Army Cyber School, Certificate of Appreciation 2026. Commended by the Commandant for contributions to cyber leader development through instructional sessions for Cyber Captains.
- United States Army Cyber School, Certificate of Appreciation 2025. Commended by the Commandant for contributions to cyber leader development through instructional sessions for Cyber Captains.

- CASOS Summer Institute, Carnegie Mellon University - Completed curriculum in Computational Analysis of Social and Organizational Systems (CASOS)
- Heal+ Student training, University of Amsterdam - Data Driven Decision Making and Evaluation in Medicine
- Introduction to TensorFlow for Artificial Intelligence, Machine Learning, and Deep Learning, Online course at Coursera.

PROFESSIONAL PRACTICE AND RESEARCH LEADERSHIP

Professional Appointments and Role Functions

2020–2023

Artificial Intelligence Developer - Industrial Experience
Jordan Design & Development Bureau (JODDB) - Company
Full-time employment: 48 hours/week
Professional Responsibilities and Leadership:

- **Machine Learning Development:** Developed, optimized, and deployed AI and machine-learning solutions for operational defense and security environments.
- **Web Development and Engineering:** Built data-processing pipelines, back-end services, APIs, dashboards, technical documentation, and structured reports. Improved inference efficiency, latency, memory use, and operational reliability.
- **Industrial Mentorship:** Led and mentored university students completing graduation-required industrial training.

2023–2026

Graduate Research Assistant - Academic Research Appointment
Augusta University
Part-time appointment: 20 hours/week; Full-time doctoral enrollment
Professional Responsibilities and Leadership:

- **Research Development:** Designed and evaluated secure, resilient, and privacy-preserving machine-learning methods.
- **Experimental Research:** Developed reproducible research pipelines and conducted evaluations of adversarial robustness, model resilience, and secure aggregation.
- **Scholarly Activity:** Prepared research manuscripts, technical reports, presentations, and supporting research documentation.

Graduate Research Leadership and Mentorship

• **Network intrusion detection research (6 months):** Led technical research on adversarial transferability, machine-learning experiments, domain constraints, defense evaluation, and interpretation of results.

Scholarly outcome: "Constraining Adversarial Attacks on Network Intrusion Detection Systems: Transferability and Defense Analysis," *IEEE Transactions on Network and Service Management*, vol. 21, no. 3, pp. 2751–2772, 2024.

• **Generative AI and disinformation research:** Technical mentorship in dataset development, experimental design, feature analysis, machine-learning model evaluation, and interpretation of results comparing human-, ChatGPT-, and Gemini-generated health disinformation.

Scholarly outcome: "Generative AI vs. Human Deception: A Comparative Analysis of ChatGPT, Gemini, and Human-Generated Disinformation," *Proceedings of the 2025 ACM International Workshop on Security and Privacy Analytics*, pp. 13–22, 2025.

- **Predictive maintenance research (4 months):** Technical leadership and mentorship in data preprocessing, machine-learning model development, performance evaluation, interpretation of results, and web-based deployment.

  Scholarly outcome: "Web-Based Maintenance Prediction of Machine Conditions and Failure Modes Using Machine Learning," *Journal of Advanced Manufacturing Systems*, vol. 24, no. 2, pp. 359–383, 2025.

COURSES TAUGHT

Texas State University *Fall 2026*
Department of Information Systems & Analytics

- **ISAN 3350 – Information Systems Security**
- **ISAN 3380 – Enterprise Information Technology and Business Intelligence**

SKILLS

Programming Languages	Python, C++
Machine Learning Tools	Pytorch, Tensorflow, Sklearn, Pandas, Numpy
Web Development	DJANGO web framework, backend APIs
Databases	MongoDB, MySQL
Distributed-Scalable AI	Federated learning, secure aggregation, blockchain-assisted coordination
High-Performance Computing	Running and managing experiments on HPC environments
Data Engineering	Data collection, preprocessing, pipeline development, data quality control