Abdullah Khan

MS Computer Science Graduate (Gold Medalist), University of Wah, Pakistan

+92-303-2228717 | Abdullah Khan | Portfolio | abdullahkhanswati@outlook.com (Personal)

Summary

Motivated and research-focused Gold Medalist in MS Computer Science with 6 years of full-stack development experience and a strong foundation in AI, machine learning, and cybersecurity. Skilled in transformer architectures, large language models, and deep learning for both audio and medical image analysis. Completed a thesis on zero-shot deepfake voice cloning detection using transformer-based and rule-driven methods, while also exploring quantum computing for secure and robust AI systems. Research interests include AI security, explainable and trustworthy models, intrusion detection for autonomous vehicles, and multimodal deep learning. Seeking a PhD opportunity to advance secure, reliable, and high-impact AI technologies.

Research Interests: Information Security, Speech Processing, Deep Learning & AI, Quantum Computing, Medical Imaging

Education

•**Master of Science in Computer Science (Gold Medalist)** *2023 – 2025*
University of Wah, Wah Cantt, Pakistan CGPA: 3.81/4.0

- **Thesis:** Transformer and Rule-Based Zero-Shot Voice Cloning Detection
- **Supervisor:** Professor Dr. Wazir Zada Khan
- **Coursework:** Advanced Machine Learning, Advanced Network Security, Advanced Analysis of Algorithms, Research Methodologies, Advanced Operating Systems, Web Mining, Quantum Computing, Image Processing

•**Bachelor of Science in Software Engineering** *2018 - 2022*
COMSATS University Islamabad, Wah Campus, Pakistan CGPA: 3.37/4.0

- **FYP:** Restaurant QR System *(Ranked 1st among final-year projects)*
- **Supervisor:** Mr. Waheed Ahmed Khan

Publications

Published

[1] **Abdullah Khan**, Arooj Fatima, Ridda Jamil, Hassan Ahmed, Aini Saba. **Enhancing Social Media Bot Detection with Cross-Feature Gating and Residual Learning**. In *ICCK Transactions on Emerging Topics in Artificial Intelligence*, vol. 3, no. 1, pp. 20–32, 2026. Institute of Central Computation and Knowledge. DOI: 10.62762/TETAI.2025.791029.

[2] **Abdullah Khan**, Sherif Tawfik Amin, Hareem Kibriya, Wazir Zada Khan, Ayesha Siddiqa, Ali Tahir. **A Dynamic Approach for Detecting Attacks in Controller Area Networks**. In *Proceedings of the 2025 International Conference on Emerging Technologies in Electronics, Computing, and Communication (ICETECC)*, Jamshoro, Pakistan, 23–25 April 2025, IEEE, DOI: 10.1109/ICETECC65365.2025.11070255.

[3] M. Bibi, S. Mehmood, **Abdullah Khan**, Faseeh-Ur-Rehman and M. Danish. **Leveraging Blockchain for Transparent and Trustworthy E-Certificate Verification System**. In *Proceedings of the 2025 International Conference on Frontiers of Information Technology (FIT)*, Islamabad, Pakistan, 2025, pp. 1-6, IEEE, DOI: 10.1109/FIT67061.2025.11333746.

Submitted

[S.1] **Abdullah Khan**, Wazir Zada Khan, Ayesha Siddiqa, Faisal Alanazi, Muhammad Khurram. **Efficient Quantum Neural Networks for Synthetic Voice Identification in IoT-Enabled Holographic Counterparts**. Manuscript submitted to *Transactions on Consumer Electronics*, IEEE, 2025.

[S.2] **Abdullah Khan**, Sherif Tawfik, Hareem Kibriya, Wazir Zada Khan, Aeysha Siddiqa. **CANShield-X: An Explainable DL-heuristic Framework for the Detection of Automotive Attacks in Controller Area Network**. Manuscript submitted to *Mehran University Research Journal of Engineering and Technology*, MURJET, 2026.

[S.3] **Abdullah Khan**, Hassan Ahmed, Maryam Javaid, Hassan Khan. **Bi-GRU–Based Intrusion Detection for UAV Controller Area Networks**. Manuscript submitted to *2026 International Conference on IT and Industrial Technologies (ICIT)*, IEEE-indexed.

[S.4] Hassan Ahmed, **Abdullah Khan**, Azhar Mahmood, Jibran Mir, Sohaib Ahmed. **CAN You Need More Attention? CANformer-XL: Long-Context Intrusion Detection in Controller Area Networks Using Transformer-XL**. Manuscript submitted to *Statistical Analysis and Data Mining*, Wiley, 2025.

[S.5] Raja Muhammad Bilal Arshad, Hassan Ahmed, **Abdullah Khan**. **ARTP: An Autonomous Red-Team Planner for Pentesting**. Manuscript submitted to the *2026 International Conference on IT and Industrial Technologies (ICIT)*, IEEE-indexed.

In Progress

[IP.1] **Abdullah Khan**, Wazir Zada Khan. **A Survey on Voice Cloning Detection: State-of-the-art Challenges and Future Directions**, 2026.

[IP.2] **Abdullah Khan**, Wazir Zada Khan. **Quantum Neural-Convolutional Model for Brain Tumor Classification & Segmentation**, 2026.

[IP.3] **Abdullah Khan**, Wazir Zada Khan. **Development of a Large-Scale Fake News Dataset and Transformer-Based Detection Models**, 2026.

[IP.4] **Abdullah Khan**, Hassan Ahmed. **From Analysis To Defense: Benchmarking LLM Jailbreak Vulnerability and Introducing A Novel Jailbreak Detection Model**, 2026.

[IP.5] Zeeshan Ali, Hassan Ahmed, **Abdullah Khan**. **Optimizing Click Through Rate Prediction using Ensemble Deep Learning and XAI-based SHAP Approaches**, 2026.

Experience

•**Lead Developer** *June 2022 - Present*
gamersandgeek Gamers and Geek - Tech and Gaming Blog
Responsibilities

- Led the design and development of the blog's front-end and back-end architecture, ensuring performance, scalability, and security
- Managed content integration, SEO optimization, and analytics tracking to improve site visibility and user engagement

•**Full Stack Developer** *Jan 2018 - 2022*
etechpk Eteckpk - IT Solutions and Services
Responsibilities

- Developed and maintained client-facing service modules, including booking systems, CRM integrations, and automated inquiry handling
- Built scalable APIs and dashboards to support operations, analytics, and customer support workflows
- Collaborated with stakeholders to design user-centric features, ensuring seamless performance across devices and platforms

For more development projects and professional details, visit my LinkedIn: Abdullah-projects

Technical Skills

Languages: PHP, Python, SQL, Solidity, JavaScript, React, Node.js, C++, Java
Libraries: NumPy, Pandas, TensorFlow, PyTorch, Scikit-learn, Keras, Matplotlib, Seaborn, Plotly, XGBoost, Qiskit, PennyLane, Cirq
Developer Tools: Github, Visual Studio, Google Colab, Anaconda
Databases: Relational Database (MySQL)
Research: LaTeX, Endnote, Edraw Max
Tools: Kaggle, Jupyter Notebook, Google Colab, Canva, MS Office, MS Access, MS Visio, CISCO Packet Tracer, Wireshark
Operating Systems: Windows, Linux

Soft Skills

Communication: Strong written and verbal skills, public speaking, active listening, and concise articulation
Collaboration: Team coordination, relationship building, cross-functional cooperation, and empathy
Analytical Thinking: Creative problem-solving, logical reasoning, and adaptability in dynamic environments
Leadership: Strategic decision-making, task delegation, team motivation, and conflict resolution
Time Management: Effective prioritization, deadline management, goal orientation, and multitasking capabilities

Projects

•**An Explainable DL-Heuristic Framework for Automotive Attack Detection in Controller Area Networks**
Tools, Programming Languages & Libraries: *Python, TensorFlow, Keras, Pandas, NumPy, Scikit-learn, SHAP*

- Developed a lightweight intrusion detection framework combining Multi-Layer Perceptron and Gated Recurrent Unit models with domain-driven heuristic rules to detect sophisticated threats, including replay and flooding attacks, in Controller Area Networks.
- Integrated SHAP to provide interpretability for model predictions, enhancing transparency in automotive cybersecurity.
- Achieved 99.73% accuracy, with precision, recall, and F1-score above 99.7%, and reduced attack detection time to 54 microseconds per sample, enabling real-time deployment in resource-constrained vehicular environments.

•**Analyzing the Impact of Quantum Gates**
Tools, Programming Languages & Libraries: *Qiskit, Python, NumPy, Matplotlib, Scikit-learn, Keras, PyTorch, PennyLane*

- Investigated the effect of various quantum gates on the classification accuracy of quantum neural networks for audio deepfake detection using the DEEP-VOICE dataset.
- Analyzed combinations of PhaseShift, SWAP, and other gates to identify optimal configurations for efficient detection.
- Performed comparative evaluations against classical counterparts, highlighting benefits in performance and resource efficiency.

•**A Survey on Voice Cloning Detection: State-of-the-art Challenges and Future Directions**
Tools, Programming Languages & Libraries: *LaTeX, Python, Google Scholar, IEEE Xplore, Scopus*

- Conducted an extensive literature review on deep learning and signal processing methods used in voice cloning detection.
- Identified current limitations and gaps in consumer device adaptation, dataset diversity, and robustness to adversarial attacks.
- Proposed future research directions including explainability, privacy-preserving techniques, and quantum-enhanced detection.

•**Quantum Gate Optimization for Audio Deepfake Detection in Holographic IoT**

Tools, Programming Languages & Libraries: *Qiskit, Python, Matplotlib, NumPy, PennyLane, Scikit-learn, Keras*

- Developed a hybrid quantum-classical system against deepfake audio threats through optimized gate-level circuit design, evaluating 28 quantum gate configurations on periodic audio data.
- Identified the CNOT+S gate combination as optimal by leveraging entanglement-driven correlation and phase-sensitive feature extraction for synthetic voice detection.
- Demonstrated enhanced detection performance with reduced computational load in resource-constrained holographic environments.

•**Quantum Neural-Convolutional Model for Brain Tumor Classification**

Tools, Programming Languages & Libraries: *Qiskit, Keras, TensorFlow, Python, NumPy, Scikit-learn, OpenCV*

- Developed a hybrid quantum-classical convolutional neural network (QNN-CNN) for brain tumor classification from MRI scans.
- Integrated quantum layers to reduce model complexity while preserving classification performance.
- Achieved high accuracy on the BraTS dataset and demonstrated the potential of quantum computing in medical imaging.

•**A Dynamic Approach for Detecting Attacks in Controller Area Networks**

Tools, Programming Languages & Libraries: *Python, TensorFlow, Keras, Pandas, NumPy, Scikit-learn*

- Designed a hybrid detection framework combining rule-based logic with deep learning models (GRU, RNN, and LSTM) to identify anomalies in Controller Area Networks (CAN) used in autonomous vehicles.
- Implemented time-series-based sequence modeling to detect various attack types such as spoofing, fuzzing, and DoS.
- Demonstrated improved detection accuracy and adaptability by dynamically adjusting thresholds based on learned traffic behavior.

•**Development of a Large-Scale Fake News Dataset and Transformer-Based Detection Models**

Tools, Programming Languages & Libraries: *Hugging Face Transformers, PyTorch, BERT, LLaMA, Pandas, Scikit-learn, Python*

- Collected, cleaned, and compiled a large-scale fake news dataset of over 50,000 articles from diverse open-source platforms for misinformation research.
- Designed and executed experiments using multiple transformer-based language models (BERT, LLaMA, RoBERTa) for binary classification of real vs. fake news.
- Evaluated model performance across architectures and conducted interpretability analysis using attention mechanisms to explore how models detect misinformation.

Courses and Trainings

–**Introduction to Blockchain** *2023*
Udemy

–**Introduction to Cybersecurity** *2023*
Udemy

–**Web Development** *2022*
Udemy

–**Mobile Development** *2022*
Udemy

–**Logo Designing Workshop** *2022*
COMSATS University Islamabad, Wah Campus

–**Kali Linux - Hacking Challenges** *2022*
Udemy

Referees

Professor Dr. Wazir Zada Khan
Dean, Faculty of Computer Sciences, University of Wah, Wah Cantt, Pakistan
Email: wazirzadakhan@yahoo.com
Scholar Profiles: University of Wah - Personal Page | Google Scholar | LinkedIn

Dr. Ayesha Siddiqa
Assistant Professor & Chairperson, Department of Computer Science, University of Wah, Wah Cantt, Pakistan
Email: ayesha.siddiqa@yahoo.com
Scholar Profiles: University of Wah - Personal Page | Google Scholar