Dr. Ahsan Wajahat, Ph.D.

ahsan.sunny56@nwpu.edu.cn
Website
Google Scholar
+86 13031065449
+92 3003223612
WeChat: ahsanmaymar



Employment History

2026/07– Present — **Chairman of the Department.** Department of Computer Science, Lasbela University of Agriculture, Water and Marine Sciences, Uthal, Balochistan.

2024/12– Present — **Postdoctoral Research Fellow.** School of Software, Northwestern Polytechnical University, Xi'an, China.

- Conducted research and mentored graduate students in their research projects.
- Collaborated with research team on ongoing academic projects.

2021/03 – Present — **Lecturer of Computer Science.** Lasbela University of Agriculture, Water and Marine Sciences, Pakistan.

- **Taught undergraduate courses:** Fundamentals of Computer Science, Introduction to Programming, Object-Oriented Programming, Data Structures, Human-Computer Interaction, and Artificial Intelligence.

2013-02 – 2014-05 — **Network Administrator,** Netkom Communications Technology LLC, Dubai and Islamabad.

- **Key responsibilities:** Network infrastructure management, system configuration and maintenance, troubleshooting network issues, implementing security protocols, and providing technical support to clients.

Education

2024–12– Present — **Postdoctoral Researcher, Northwestern Polytechnical University, Xi'an, China**.
Research in Federated Learning and Privacy-Preserving AI for Malware Detection.

2018-09 – 2024-07 — **Ph.D., Software Engineering, Beijing University of Technology**
Thesis title: *Intelligent Android Mobile Malware Detection Using Permission Requests and API Calls*

2013-08 – 2016-12 — **M.S. Information Technology, Sindh Agriculture University, Pakistan**.
Optional: Thesis title: *A Lightweight Approach for User Space Keylogger Detection*

2007-08 – 2012-09 — **B.S. Information Technology, Sindh Agriculture University, Pakistan**.

Research Publications

Journal Articles

1. A. Nazir, J. He, N. Zhu, A. Wajahat, F. Ullah, and S. Qureshi, "And pathan, ms 2024. collaborative threat intelligence: Enhancing iot security through blockchain and machine learning integration," *Journal of King Saud University-Computer and Information Sciences*, vol. 101939,
2. A. Hussain, W. Jungshen, A. Turab, Y. Gilani, K. I. Ahmed, and A. Wajahat, "Cmhf-3dnet: A transformer-based framework for improved brain tumor segmentation across modalities," *Academic Radiology*, 2026.
3. J. Latif, S. Zhang, S. ur Rehman, A. Wajahat, A. Nazir, and A. Imran, "Enhancing surveillance and early warning of infections and antimicrobial resistance using machine learning and deep learning: A systematic review," *Neurocomputing*, p. 133 502, 2026.
4. A. Wajahat, K. Zhang, A. Hussain, M. Elloumi, M. Hamdi, and T. M. Alam, "Lamdex: An explainable lightweight android malware detection system for enhancing iot app security," *Scientific Reports*, 2026.
5. A. Wajahat, K. Zhang, J. Latif, and A. Ahad, "Systematic analysis of machine learning, deep learning, and hybrid models for android and iot ecosystems: A review," *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, vol. 16, no. 3, e70119, 2026.
6. I. Ahmad, F. Shang, M. S. Pathan, A. Wajahat, and Y.-S. Kim, "Dual-stream hybrid architecture with adaptive multi-scale boundary-aware mechanisms for robust urban change detection in smart cities," *Scientific Reports*, vol. 15, no. 1, p. 30 729, 2025.
7. J. Latif, A. Wajahat, A. Tahir, A. Bilal, M. Zakariah, and A. Alnuaim, "A nature-inspired ai framework for accurate glaucoma diagnosis," *Comput Model Eng Sci*, vol. 143, no. 1, 2025.
8. A. Nazir et al., "Empirical evaluation of ensemble learning and hybrid cnn-lstm for iot threat detection on heterogeneous datasets," *The Journal of Supercomputing*, vol. 81, no. 6, p. 775, 2025.
9. S. S. Qureshi et al., "Advanced ai-driven intrusion detection for securing cloud-based industrial iot," *Egyptian Informatics Journal*, vol. 30, p. 100 644, 2025.
10. S. S. Qureshi et al., "Enhancing iot security and healthcare data protection in the metaverse: A dynamic adaptive security mechanism," *Egyptian Informatics Journal*, vol. 30, p. 100 670, 2025.
11. F. Ullah et al., "Ehr management evolution through purpose-based access control and blockchain smart contracts," *International Journal of Information Security*, vol. 24, no. 1, p. 63, 2025.
12. Z. Ahmad, A. Wajahat, and M. S. Pathan, "A comprehensive study for malware detection through machine learning in executable files," *International Journal for Electronic Crime Investigation*, vol. 8, no. 1, pp. 3–48, 2024.
13. X. Ma et al., "Detecting iot botnet attacks through ensemble and meta ensemble approaches," *International Journal of Network Security*, vol. 26, no. 5, pp. 885–900, 2024.
14. A. Nazir et al., "A deep learning-based novel hybrid cnn-lstm architecture for efficient detection of threats in the iot ecosystem," *Ain Shams Engineering Journal*, vol. 15, no. 7, p. 102 777, 2024.
15. A. Nazir et al., "Collaborative threat intelligence: Enhancing iot security through blockchain and machine learning integration," *Journal of King Saud University-Computer and Information Sciences*, vol. 36, no. 2, p. 101 939, 2024.
16. S. S. Qureshi et al., "A new deep learning paradigm for iot security: Expanding beyond traditional ddos detection," *International Journal of Network Security*, vol. 26, no. 3, pp. 349–360, 2024.
17. S. U. Qureshi et al., "Systematic review of deep learning solutions for malware detection and forensic analysis in iot," *Journal of King Saud University-Computer and Information Sciences*, vol. 36, no. 8, p. 102 164, 2024.

18 F. Ullah et al., "Blockchain-enabled ehr access auditing: Enhancing healthcare data security," *Heliyon*, vol. 10, no. 16, 2024.

19 F. Ullah et al., "Cost-effective ehr management: Image compression and blockchain," *International Journal of Network Security*, vol. 26, no. 5, pp. 874–884, 2024.

20 A. Wajahat et al., "An effective deep learning scheme for android malware detection leveraging performance metrics and computational resources," *Intelligent Decision Technologies*, vol. 18, no. 1, pp. 33–55, 2024.

21 A. Wajahat et al., "Outsmarting android malware with cutting-edge feature engineering and machine learning techniques.," *Computers, Materials & Continua*, vol. 79, no. 1, 2024.

22 A. Wajahat et al., "Securing android iot devices with guarddroid transparent and lightweight malware detection," *Ain Shams Engineering Journal*, vol. 15, no. 5, p. 102 642, 2024.

23 Z. Ahmad, M. S. Pathan, and A. Wajahat, "A comparative analysis of malware detection methods traditional vs. machine learning," *International Journal for Electronic Crime Investigation*, vol. 7, no. 4, pp. 3–18, 2023.

24 A. Nazir et al., "Advancing iot security: A systematic review of machine learning approaches for the detection of iot botnets," *Journal of King Saud University-Computer and Information Sciences*, vol. 35, no. 10, p. 101 820, 2023.

25 S. Qureshi et al., "Analysis distributed denial-of-service attack deploy deep learning techniques," *International Journal of Network Security*, vol. 25, no. 5, pp. 745–757, 2023.

26 A. Wajahat, K. Zhang, J. Latif, X. Ma, A. Ahad, and K. I. Ahmed, "Dynamic weighted federated learning: A scalable and privacy-centric approach to android iot malware detection," *Concurrency and Computation: Practice and Experience*, 2023. DOI: 10.1002/cpe.70441

27 A. Wajahat et al., "An adaptive semi-supervised deep learning-based framework for the detection of android malware," *Journal of Intelligent & Fuzzy Systems*, vol. 45, no. 3, pp. 5141–5157, 2023.

28 S. Qureshi et al., "An adaptive multi-layer architecture for iot based idps for attacks using deep learning method," *International Journal of Network Security*, vol. 24, no. 5, pp. 815–827, 2022.

29 S. Qureshi et al., "Browser forensics: Extracting evidence from browser using kali linux and parrot os forensics tools," *International Journal of Network Security*, vol. 24, no. 3, pp. 557–572, 2022.

30 S. Qureshi, J. Li, F. Akhtar, S. Tunio, Z. H. Khand, and A. Wajahat, "Analysis of challenges in modern network forensic framework," *Security and Communication Networks*, vol. 2021, no. 1, p. 8 871 230, 2021.

31 S. Qureshi, S. Tunio, F. Akhtar, A. Wajahat, A. Nazir, and F. Ullah, "Network forensics: A comprehensive review of tools and techniques," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 5, 2021.

32 S. Qureshi et al., "A hybrid dl-based detection mechanism for cyber threats in secure networks," *Ieee Access*, vol. 9, pp. 73 938–73 947, 2021.

33 S. Qureshi, G. Das, S. Tunio, F. Ullah, A. Nazir, and A. Wajahat, "Performance analysis of open source solution" ntop" for active and passive packet analysis relating to application and transport layer," *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 3, 2019.

Conference Proceedings

1 A. Nazir et al., "Ensemble learning techniques for the detection of iot botnets," in *Proceedings of the 2024 3rd International Conference on Cyber Security, Artificial Intelligence and Digital Economy*, 2024, pp. 80–85.

2. S. S. Qureshi et al., "A method for examining and reducing malicious url connections by machine learning," in *2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC)*, IEEE, 2024, pp. 1–6.
3. X. Ma, Y. Yi, Y. Luo, A. Wajahat, and A. Nazir, "Hacker community detection in online social network: A case study," in *Third International Conference on Green Communication, Network, and Internet of Things (CNIoT 2023)*, SPIE, vol. 12814, 2023, pp. 277–283.
4. F. Akhtar, A. Shakeel, A. Nazir, A. Wajahat, F. Ullah, and S. Qureshi, "A study and application development on monitoring cardio-vascular attack using internet of thing (iot)," in *2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*, IEEE, 2020, pp. 1–5.
5. M. Z. Azeem, A. Imran, F. Akhtar, A. Wajahat, J. Latif, and S. A. Memon, "Effects of code cloning in mobile applications," in *2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*, IEEE, 2020, pp. 1–6.
6. S. A. Memon et al., "Discretization of the crime rate from numerical into categorical," in *2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*, IEEE, 2020, pp. 1–7.
7. A. Nazir et al., "Evaluating energy efficiency of buildings using artificial neural networks and k-means clustering techniques," in *2020 3rd international conference on computing, mathematics and engineering technologies (iCoMET)*, IEEE, 2020, pp. 1–7.
8. A. Wajahat, A. Nazir, F. Akhtar, S. Qureshi, F. Razaque, A. Shakeel, et al., "Interactively visualize and analyze social network gephi," in *2020 3rd international conference on computing, mathematics and engineering technologies (iCoMET)*, IEEE, 2020, pp. 1–9.
9. A. Wajahat, A. Imran, J. Latif, A. Nazir, and A. Bilal, "A novel approach of unprivileged keylogger detection," in *2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*, IEEE, 2019, pp. 1–6.

Books and Chapters

1. M. U. Akhtar et al., "Computational modeling and analysis of behavioral patterns for infectious disease networks dismantling," in *Computational and Deep Learning Models for Advanced Behavioral Analysis*, IGI Global Scientific Publishing, 2026, pp. 365–390.
2. A. Ahad, J. Zheng, A. Wajahat, S. U. Khan, M. Tahir, and M. A. Sheikh, "Cybersecurity for internet of things: Big data optimization for iot-based real-time network traffic analysis," in *Cybersecurity and Privacy in Smart Health*, Y.-D. Zhang, S. Wang, and C. Li, Eds., Cham: Springer International Publishing, 2020, pp. 45–68. DOI: 10.1007/978-3-030-47913-5_3

Skills

Languages	Fluent in English and Urdu; basic proficiency in Mandarin Chinese.
Programming	Python, PyTorch, TensorFlow, Scikit-learn, Java, MATLAB, LaTeX.
Machine Learning	Federated Learning, Deep Learning, Explainable AI, Privacy-Preserving AI, Data Preprocessing and Augmentation.
Data Science	Data analysis and visualization using Python (Pandas, Matplotlib, Seaborn).
Tools	Git, Jupyter, Overleaf, VS Code, Linux environments, Google Colab.
Academic	Research writing, academic reviewing, teaching, and technical training.

Memberships

IEEE Member	IEEE Member- 97051959
IEEE Technical Committee	IEEE Member of Technical Committee on Computer Architecture (TCCA)
IEEE Councils	Member of IEEE Council on Superconductivity
IEEE Sensors Council	Member of IEEE Sensors Council

Miscellaneous Experience

Awards and Achievements

2018 **Chinese Government Scholarship**, awarded by the China Scholarship Council (CSC).

2023 **Special Contribution Award**, awarded by Beijing Municipal Government.

2024 **Science and Technology Award**, awarded by Beijing University of Technology.

2025 **Science and Technology Award**, awarded by Beijing University of Technology.

Reviewer Recognition

2025-06-03 Reviewed for **IEEE Access** on the manuscript titled *FE-BiONet: A Deep Learning Model with Interpretable Feature Embedding for Mental Health Recognition and Grading Based on Structured Data*.

2025-05-24 Reviewed for **IEEE Access** on the manuscript titled *Towards Modeling Malicious Behavior Detection Using Audit Logs Based on a Hierarchical Process Structure*.

2025-04-16 Reviewed for **Systems** on the manuscript titled *Effective Context-Aware File Path Embeddings for Anomaly Detection*.

2025-04-05 Reviewed for **Sensors** on the manuscript titled *ML-Based Security Solutions for IoT Networks: A Comprehensive Survey*.

2025-03-21 Reviewed for **Electronics** on the manuscript titled *An Evaluation Framework for Cybersecurity Maturity Aligned with the NIST CSF*.

2025-01-30 Reviewed for **IEEE Access** on the manuscript titled *Cost-Efficient Secure Hybrid RAG Assessment*.

2025-01-29 Reviewed for **Sensors** on the manuscript titled *HiViT-IDS: An Efficient Network Intrusion Detection Method Based on Vision Transformer*.

2024-05-05 Reviewed for **IEEE Internet of Things Journal** on the manuscript titled *Quantum-Inspired Synergies: Advancing Information Security through Quantum Cryptography, AI/ML, IoT, and Cybersecurity Integration*.

2023-09-25 Reviewed for **IEEE Internet of Things Journal** on the manuscript titled *Secure Quantum Communication: Functionalities, Applications, Challenges, and Future Directions*.

Conference Participation

2025 **Technical Program Committee Member**, 2025 8th International Conference on Data Science and Information Technology DSIT 2025.
Beijing, China, November 14, 2025 - November 16, 2025.

2024 **Session Chair**, 9th International Conference on Large-scale Industrial Software, Embedded Software, and Artificial Intelligence, Northwestem Polytechnical University
Xian, China, October 17th-18th, 2024.

Conference Participation (continued)

2019 **Invited Speaker**, 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)
Sukkur, Pakistan, January 30th-31st, 2019.
Talk Title: Advancing AI-Driven Cybersecurity For Mobile And IoT Ecosystem.

References

Prof. Dr. Chuangbai Xiao
Professor
Beijing University of Technology, Beijing, China
cbxiao@bjut.edu.cn TEL: +86-13901006025

Prof. Dr. He Jingsha
Professor
Beijing University of Technology, Beijing, China
jhe@bjut.edu.cn TEL: +86-1067391762

Prof. Dr. Sun Guangmin
Professor
Beijing University of Technology, Beijing, China
Gmsun@bjut.edu.cn TEL: +86-1067391526