

Yasir Siddiq

Barcelona, Spain | +34 667603209 | [yasir.siddiq@gmail.com] |

[<https://www.linkedin.com/in/yasir-siddiq-8a80b722/>] | <https://github.com/yasirsiddiq01> |

<https://orcid.org/0009-0005-3074-4275> | <https://huggingface.co/yasirsiddiq>

RESEARCH PROFILE

Software Engineering and AI assurance research with a background in telecommunication systems, university teaching and reproducible ML evaluation. Current work focus on trustworthy agentic and multiagent AI, Observable workflows, bounded operational authority, runtime assurance, policy as code, failure containment, and evidence-based escalation. Recent outputs apply these ideas to DevSecOps and 5G/6G automation. Research goal is to advance from implementation-oriented assurance prototypes toward rigorous specification and verification of agent interactions, permissions, commitments, and operational decisions.

RESEARCH INTERESTS

Multiagent systems, agent interaction and coordination, formal specification and verification, trust and security in agent systems, runtime assurance, policy gated authority, software dependability, agentic DevSecOps, human oversight, auditable autonomous systems, uncertainty aware evaluation and failure containment.

SCHOLARY AND RESEARCH OUTPUTS

Before AI Can Merge or Deploy: Minimum Governance Controls for Autonomous Agents in DevSecOps Pipelines | PUBLIC POLICY MEMO — 2026

Yasir Siddiq and Sadaf Anwar. Version 1.0, 11 August 2026. Defines bounded authority for AI agents through explicit capability levels and policy outcomes such as ALLOW, REQUIRE_HUMAN_APPROVAL, ABSTAIN and BLOCK. Public technical-governance output; not presented as peer-reviewed validation.

<https://doi.org/10.5281/zenodo.21888494>

GATE-5G: From Prediction to Permission in AI-Assisted 5G Networks | PUBLIC POLICY MEMO — 2026

Yasir Siddiq and Sadaf Anwar. Version 1.0, August 2026. Proposes an evidence-conditioned boundary between AI inference and operational authority in increasingly autonomous network systems.

<https://doi.org/10.5281/zenodo.21855481>

Large Language Models in AI-Augmented DevSecOps Pipelines: Exploring Secure Software Engineering Practices and Architectural Challenges | PUBLISHED JOURNAL ARTICLE — 2026

Co-author. International Journal of Advanced Research, Vol. 3, Issue 3, published 31 July 2026. Examines secure software-engineering practices, architectural challenges, human oversight, governance, explainability and continuous validation in LLM-assisted DevSecOps.

A Leakage-Safe Study of Trust-Aware Fault Classification in ns-3/5G-LENA Using QoS-Derived Features | ACCEPTED — WECE 2026; PUBLICATION PENDING

First author, with Sadaf Anwar. Controlled 5G simulation and grouped ML evaluation study; results highlight strong overload separability but persistent ambiguity for subtle radio degradation, motivating assurance-aware use of classifier outputs.

User-Centered Design Practices in Scrum Development Process: A Distinctive Advantage? | IEEE INMIC — 2014

Co-author. 17th IEEE International Multi-Topic Conference (INMIC), pp. 161–166

EDUCATION

- MS Software Engineering | NUST-CEME, Pakistan | 2010–2014
- BS Software Engineering | University of Engineering & Technology (UET) Taxila, Pakistan | 2003–2006

RESEARCH AND TECHNICAL GOVERNANCE WORK

Policy-Gated Authority for AI Agents in DevSecOps | IMPLEMENTED TECHNICAL-GOVERNANCE PROTOTYPE — 2026

Python policy-as-code implementation accompanying the published policy memo.

<https://github.com/yasirsiddiq01/gov-devsecops>

- Models bounded authority levels from A0 — OBSERVE through A3 — CONTROLLED_CHANGE, with explicit ALLOW, REQUIRE_HUMAN_APPROVAL, ABSTAIN and BLOCK decisions.
- Includes scenario-based evaluation, audit-oriented controls and regression tests; explicitly blocks production-secret access, disabling security checks and unauthorized governance-policy modification.

Intentional Agent Monitoring Lab / Multi-Agent Trust Safety Lab | REPRODUCIBLE DEMONSTRATORS — 2026

Lightweight demonstrators modelling agent roles, goals, tasks, inputs/outputs, risk signals, verification states and goal-satisfaction status to study observable and safer multi-agent workflows.

<https://github.com/yasirsiddiq01>

Agentic AI Resilience Lab | ACTIVE PORTFOLIO RESEARCH PROJECT — 2026

Modular environment for agent tracing, cascade/failure scenarios, runtime risk signals, verification states, failure containment and human-supervised recovery concepts.

GATE-5G Reference Implementation | IMPLEMENTED RESEARCH PROTOTYPE — 2026

Functional Python implementation separating AI inference from operational authority through policy/audit logic, study-specific adapters, CLI demonstration and regression tests.

<https://github.com/yasirsiddiq01/trust-aware-fault-classification-5g>

PROFESSIONAL EXPERIENCE

Wireless Engineer – 2G/3G/LTE Back Office | Huawei | Riyadh, Saudi Arabia | 2015

- Integrated and supported BTS3900/BTS3900L, DBS3900 and LampSite deployments; prepared offline/online configuration scripts and coordinated field integration teams.

- Configured LTE X2-related elements, endpoint groups, SCTP links and peers; supported site acceptance and resolved RAN/configuration issues.
- Worked with carrier aggregation, IPsec-enabled sites, small cells, penta-band configurations, VSWR/sector-swap troubleshooting and RAN inventory/report extraction.

RAN/BSS Consultant & Project Coordination | SOMTEL International | Hargeisa, Somaliland | 2013–2014

- Resolved operational issues including configuration mismatch, zero-call conditions, delta path loss, sector swap and outages caused by transmission, hardware or power failures.
- Prepared rollout plans and coordinated civil, power, transmission, RAN, NOC, OMCR, logistics and contractor teams; contributed to bringing 55 sites from zero to on-air within three months.
- Supported scopes of work, subcontractor planning, partner shortlisting, negotiations, BOQs, customer presentations and backbone-link activities.

RAN/BSS Team Lead & BSS Engineer | Alcatel-Lucent | Pakistan | 2007–2013

- Standardized KPI monitoring and coordinated fault recovery with minimum service downtime; planned BSC rehomings, site cutovers, link upgrades, transmission rerouting and live-network expansions.
- Commissioned and troubleshot A9130 BSC/MFS, A9125 TC, Evolium 9100/9110 BTS and AWY9400 PDH microwave systems, including OMCR monitoring, TRX work, VSWR/sweep testing and transmission cutovers.
- Prepared project plans, scopes of work, resource/timeline plans, contractor assignments, technical sessions and customer presentations.

UNIVERSITY TEACHING

Computer Science / Software Engineering Lecturer | NUML; Higher Education Department; PMAS Arid Agriculture University | Pakistan | 2017–2023

- Taught Artificial Intelligence, Computer Communications and Networks, Operating Systems, Database Management Systems, Computer Graphics and introductory Computer Science.
- Prepared laboratories and assessments and contributed to academic/administrative committees.

ADDITIONAL RESEARCH & TECHNICAL WORK

Systematic Mapping and Evidence Review — AI Governance and Assurance in Telecommunications | ONGOING — 2026

Independent evidence review examining runtime assurance, human oversight, evaluation evidence and operational authority for AI/ML and increasingly autonomous telecom systems.

Requirements Traceability and LLM Evaluation | RESEARCH DATA / EVALUATION WORK — 2026

Worked with requirements-traceability candidate pairs, controlled train/validation/test splits, augmentation and LLM-oriented experiments, with attention to project/domain overlap, negative-pair construction and leakage risks.

Linux Server Operations & Monitoring Lab | TECHNICAL LAB — 2026

Hands-on observability and troubleshooting work covering processes, memory, storage, services and logs; relevant to runtime evidence, incident diagnosis and system-state interpretation.

RESEARCH METHOD & TECHNICAL SKILLS

Research / evaluation	Experimental design; grouped validation; leakage control; model comparison; class-level failure analysis; confidence/uncertainty analysis; systematic/evidence review; reproducibility documentation.
Agentic / multi-agent AI	Agent roles/goals/tasks; workflow tracing; trust/risk signals; verification states; goal-satisfaction status; cascade/failure scenarios; human-supervised recovery; LLM/agentic-AI evaluation.
Governance / assurance	Runtime assurance; evidence-conditioned authority; policy-as-code; provenance/auditability; bounded autonomy; escalation/abstention; human oversight; failure containment.
Software / systems	Python; FastAPI; Streamlit; SQLite/SQLAlchemy; pytest; Git/GitHub; GitHub Actions; Docker; Linux/Ubuntu/CentOS; C/C++; Java.
AI / data	pandas; scikit-learn; NumPy; SciPy; Jupyter; Matplotlib; feature engineering; classification pipelines; structured datasets; data-quality checks.
Networks / cloud	ns-3/5G-LENA; 2G/3G/4G/LTE; RAN/BSS O&M; KPIs/QoS; incident and fault diagnosis; Microsoft Azure administration; GCP foundational knowledge.

CERTIFICATION & TRAINING

- Microsoft Certified: Azure Administrator Associate (AZ-104), 2024; Azure Fundamentals (AZ-900), 2023.
- Project Management: Introduction to Project Management and PMP Certification Course (40 PDU); Professional Diploma in Project Management with MS Project.
- International technical training in China on MCRRH; Alcatel-Lucent on-the-job training in BSC, MFS, transcoder, BTS and microwave-link commissioning/troubleshooting.

LANGUAGES

English — Fluent | Urdu — Native | Punjabi — Conversational | Catalan — Basic