McKelvey School of Engineering
Department of Computer Science & Engineering
Washington University in St. Louis
St. Louis, MO, USA
+1 (319) 800 1834
umar.iqbal@wustl.edu
www.umariqbal.com
umaarr6

Umar Iqbal

Research Interests

Security and privacy researcher focused on AI agents, including execution isolation, permission management, and provenance-based runtime monitoring. My work combines systems design, empirical measurement, and user studies to develop practical safeguards. Systems engineering experience includes WebKit and Chromium instrumentation for privacy and security analysis.

Academic Appointments

2023– **Washington University in St. Louis**, *Assistant Professor*

2021–23 **University of Washington**, *Postdoctoral Scholar*
Advisor: Prof. Franziska Roesner

2020–21 **University of California-Davis**, *Visiting Student*
Advisor: Prof. Zubair Shafiq

2016 **Lahore University of Management Sciences**, *Research Assistant*
Advisor: Prof. Fareed Zaffar

Industry Experience

2020 **Apple Inc.**, *WebKit Intern*

2019 **Mozilla Corporation**, *Privacy, Networking & Security Intern*

2018 **Brave Software, Inc.**, *Ph.D. intern*

2017 **Microsoft Corporation**, *Program Manager Intern*

2013–16 **LMKT, Pakistan**, *Solution Analyst*

Technical Expertise

Systems Browser instrumentation; WebKit/JavaScriptCore; Chromium/Blink/V8; execution tracing; information-flow analysis.

Security & Privacy Agent execution isolation; permission management; provenance-based monitoring; browser fingerprinting; privacy measurement.

Education

2016–21 **University of Iowa**, *Ph.D. in Computer Science*
Advisor: Prof. Zubair Shafiq
Dissertation title: Towards a Privacy-Respecting Web
Graduate Research Excellence Award
Ada Louise Ballard and Seashore Dissertation Fellowship
Graduate College Post-Comprehensive Research Fellowship

2009–13 **National University of Computer & Emerging Sciences**
B.S. in Computer Science
Dean's list of honor 2012-13

Honors & Awards

2026 **NSF CAREER Award**, *Foundations for a Secure Agentic Web*

2024 **Caspar Bowden Runner-up Award for Outstanding Research in PET**

2023 **Best Paper Award**, *ACM Internet Measurement Conference*

2023 **Spotlight Paper (best paper award candidate)**, *The Web Conference (WWW)*

2021 **Computing Innovation Fellowship**, *Computing Research Association (CRA)*

2021 **Graduate Research Excellence Award**, *University of Iowa*

2020 **Best Applied Research Paper (AdGraph), 3rd place**, *CSAW Symposium NYU*

2020 **Ada Louise Ballard and Seashore Dissertation Fellowship**, *University of Iowa*

2019 **Graduate College Post-Comprehensive Research Fellowship**, *University of Iowa*

2016 **Winner PeaceTech Exchange**, *LUMS University, Pakistan*

2012–13 **Dean's List of Honor**, *FAST/NUCES University, Pakistan*

2016–21 **Travel Grants**, *IEEE S&P (2020, 21), NDSS (2020), ACM IMC (2017), IEEE CNS (2016), USENIX Security (2016)*

Publications

arXiv 2026 **What It Is, Not What It Says: Securing Agentic Browsing Interactions with Web Semantics**
Umar Iqbal
arXiv preprint arXiv:2610.22697, 2026

arXiv 2026 **PromptPET: Privacy-Utility Optimized Prompt Obfuscation**
Ke Yang, Olivia Figueira, **Umar Iqbal**, Athina Markopoulou
arXiv preprint arXiv:2607.02932, 2026

arXiv 2026 **Agent-Sentry: Bounding LLM Agents via Execution Provenance**
Rohan Sequeira, Stavros Damianakis, **Umar Iqbal**, Konstantinos Psounis
arXiv preprint, 2026

IMC 2026 **Measuring Google AI Overviews: Activation, Source Quality, Claim Fidelity, and Publisher Impact**
Haofei Xu, **Umar Iqbal**, Jacob M. Montgomery
ACM Internet Measurement Conference, Germany, 2026

S&P 2026 **Towards Automating Data Access Permissions in AI Agents**
Yuhao Wu, Ke Yang, Franziska Roesner, Tadayoshi Kohno, Ning Zhang, **Umar Iqbal**
IEEE Symposium on Security & Privacy, San Francisco, 2026

arXiv 2025 **SoK: Advances and Open Problems in Web Tracking**
Yash Vekaria, Yohan Beugin, Shaoor Munir, Gunes Acar, Nataliia Bielova, Steven Englehardt, **Umar Iqbal**, Alexandros Kapravelos, Pierre Laperdrix, Nick Nikiforakis, Jason Polakis, Franziska Roesner, Zubair Shafiq, Sebastian Zimmeck
arXiv preprint, 2025

IMC 2025 **An In-Depth Investigation of Data Collection in LLM App Ecosystems**
Yuhao Wu, Evin Jaff, Ke Yang, Ning Zhang, **Umar Iqbal**
ACM Internet Measurement Conference, Madison, 2025

NDSS 2025 **IsolateGPT: An Execution Isolation Architecture for LLM-Based Agentic Systems**
Yuhao Wu, Franziska Roesner, Tadayoshi Kohno, Ning Zhang, **Umar Iqbal**
Network and Distributed System Security Symposium, San Diego, 2025

USENIX 2024 **PURL: Safe and Effective Sanitization of Link Decoration**
Shaoor Munir, Patrick Lee, **Umar Iqbal**, Sandra Siby, Zubair Shafiq
USENIX Security Symposium, Philadelphia, 2024
Acceptance rate: 417/2276 = 18.32%

AIES 2024 **LLM Platform Security: Applying a Systematic Evaluation Framework to OpenAI's ChatGPT Plugins**
Umar Iqbal, Tadayoshi Kohno, Franziska Roesner
AAAI Conference on AI, Ethics, and Society, San Jose, 2024
Acceptance rate: 31.8%
Appeared at FTC PrivacyCon 2024

PETS 2024 **Opted Out, Yet Tracked: Are Regulations Enough to Protect Your Privacy?**
Zengrui Liu, **Umar Iqbal**, Nitesh Saxena
Proceedings on Privacy Enhancing Technologies, Bristol, 2024
Acceptance rate: 148 / 708 = 20.90%

IMC 2023 **Tracking, Profiling, and Ad Targeting in the Alexa Echo Smart Speaker Ecosystem**
Umar Iqbal, Pouneh N. Bahrami, Rahmadi Trimananda, Hao Cui, Alex Gamero-Garrido, Daniel Dubois, David Choffnes, Athina Markopoulou, Franziska Roesner, Zubair Shafiq
ACM Internet Measurement Conference, Montreal, 2023
Acceptance rate: 52/201 = 25.87%
Caspar Bowden Runner-up Award for Outstanding Research in Privacy Enhancing Technologies
ACM IMC Best Paper Award
Appeared at FTC PrivacyCon 2022

EAAMO 2023 **Gender Biases in Tone Analysis: A Case Study of a Commercial Wearable Device**
Christina Yeung, **Umar Iqbal**, Tadayoshi Kohno, Franziska Roesner
Equity and Access in Algorithms, Mechanisms, and Optimization, Boston, 2023

CCS 2023 **CookieGraph: Measuring and Countering First-Party Tracking Cookies**
Shaoor Munir, Sandra Siby, **Umar Iqbal**, Steven Englehardt, Zubair Shafiq,Carmela Troncoso
ACM Conference on Computer and Communications Security, Copenhagen 2023
Acceptance rate: 158/795 = 19.87%

WWW 2023 **Online Advertising in Ukraine and Russia During the 2022 Russian Invasion**
Christina Yeung, **Umar Iqbal**, Yekaterina O'Neil, Tadayoshi Kohno, Franziska Roesner
The Web Conference, Austin, 2023
Acceptance rate: 256/1492 = 17.2%
Spotlight paper (candidate for the best paper award)

USENIX 2022 **Khaleesi: Breaker of Advertising and Tracking Request Chains**
Umar Iqbal, Charlie Wolfe, Charles Nguyen, Steven Englehardt, Zubair Shafiq
USENIX Security Symposium, Boston, 2022
Acceptance rate: 256/1492 = 17.1%

USENIX 2022 **WebGraph: Capturing Advertising and Tracking Information Flows for Robust Blocking**
Sandra Siby, **Umar Iqbal**, Steven Englehardt, Zubair Shafiq, Carmela Troncoso
USENIX Security Symposium, Boston, 2022
Acceptance rate: 256/1492 = 17.1%

PETS 2022 **FP-Radar: Longitudinal Measurement and Early Detection of Browser Fingerprinting**
Pouneh Nikkhah Bahrami, **Umar Iqbal**, Zubair Shafiq
Privacy Enhancing Technologies Symposium, Sydney, 2022
Acceptance rate: 128/534=23.9%

ACSAC 2021 **Eluding ML-based Adblockers With Actionable Adversarial Examples**
Shitong Zhu, Zhongjie Wang, Xun Chen, Shasha Li, Keyu Man, **Umar Iqbal**, Zhiyun Qian, Kevin S Chan, Srikanth V Krishnamurthy, Zubair Shafiq, Yu Hao, Guoren Li, Zheng Zhang, Xiaochen Zou
Annual Computer Security Applications Conference, Online, 2021
Acceptance rate: 80/326=24.5%

S&P 2021 **Fingerprinting the Fingerprinters: Learning to Detect Browser Fingerprinting Behaviors**
Umar Iqbal, Steven Englehardt, Zubair Shafiq
IEEE Symposium on Security and Privacy, San Francisco, 2021
Acceptance rate: 77/643=11.9%

S&P 2020 **AdGraph: A Graph-Based Approach to Ad and Tracker Blocking**
Umar Iqbal, Peter Snyder, Shitong Zhu, Benjamin Livshits, Zhiyun Qian, Zubair Shafiq
IEEE Symposium on Security and Privacy, San Francisco, 2020
Acceptance rate: 104/841=12.3%
Best applied research paper, 3rd place, CSAW, NYU Tandon

WWW 2019 **ShadowBlock: A Lightweight and Stealthy Adblocking Browser**
Shitong Zhu, **Umar Iqbal**, Zhongjie Wang, Zhiyun Qian, Zubair Shafiq, Weiteng Cheng
The Web Conference, San Francisco, 2019
Acceptance rate: 225/1247=18%

IMC 2017 **The Ad Wars: Retrospective Measurement and Analysis of Anti-Adblock Filter Lists**
Umar Iqbal, Zubair Shafiq, Zhiyun Qian
ACM Internet Measurement Conference, London, 2017
Acceptance rate: 42/179=23.5%

DSN 2016 **Malware Slums: Measurement and Analysis of Malware on Traffic Exchanges**
Salman Yousaf, **Umar Iqbal**, Shehroze Farooqi, Raza Ahmad, Zubair Shafiq, Fareed Zaffar
IEEE/IFIP International Conference on Dependable Systems and Networks, France, 2016
Acceptance rate: 58/259 =22.4%

Open Source & Industry Impact

Intact & GenTree **Framework and representation for secure agentic web interactions**
GenTree represents webpages with element-level provenance, web semantics, and capabilities. Intact uses GenTree to isolate an agent's reasoning about individual elements, restrict actions to their capabilities, and require user consent for actions on third-party content. The release includes source code and a benchmark of 1,091 real webpages with injected prompt-injection attacks. [Source Code] [Data]

SecGPT **Execution architecture for LLM-based systems**
SecGPT is an architecture for secure execution of apps in LLM-based systems. The key idea behind SecGPT is to isolate the execution of apps and to allow interaction between apps and the system only through well-defined interfaces with user permission. [Source Code] [LlamaIndex Integration]

Brave Browser **AdGraph/PageGraph in Brave Browser**
AdGraph instrumented Chromium (Blink and V8) to capture detailed execution of web pages, including document modifications, network requests, and script execution. AdGraph is implemented in Brave (as PageGraph) [Official Announcement] [Brave's Integration] [Source Code]

Safari WebKit **WebKit's Intelligent Tracking Protection (ITP)**
I instrumented Intelligent Tracking Protection in WebKit (Safari) to capture JavaScript API execution. The instrumentation is useful in detecting the abuse of JavaScript APIs for fingerprinting. [Code Patch] [Code Patch]

Mozilla Firefox **JavaScript API Fingerprint-ability Reduction**
Firefox is re-evaluating the fingerprint-ability of JavaScript APIs detected by my research. [Bug reports to Mozilla Firefox]

Microsoft Edge **Adblock Landscape**
I wrote a technical report that evaluated the feasibility of ad and tracker blocking in Microsoft Edge. In light of my evaluation, Microsoft joined Coalition for Better Ads (CBA) to develop better ads standards for desktop and mobile web.

Ad/Tracker Blocking Filter Lists **Contribution to Filter Lists**
I have shared my research findings to improve ad/tracker detection block lists. My findings are incorporated by popular block lists, such as Disconnect (used by Firefox and Edge) and Easylist/EasyPrivacy (used by uBlock Origin and dozens of other anti-tracking tools).[Bug reports to filter lists]

Grants & Fellowships

NSF **CAREER: Foundations for a Secure Agentic Web**
2026, Total amount: $\$587,043$

CRA CI Fellowship — **Computing Innovation Fellowship**, *Computing Research Association (CRA)*
2021-23, Total amount: $254,934

Dissertation Fellowship — **Ada Louise Ballard and Seashore Dissertation Fellowship**, *University of Iowa*
2020, Total amount: $10,000

Post-comp Fellowship — **Graduate College Post-Comprehensive Research Fellowship**, *University of Iowa*
2019, Total amount: $10,000

Teaching

CSE 413A/ 4103 — **Web Privacy & Security**
Fall 2024, 2026
Washington University in St. Louis

CSE 527S — **Data-driven Privacy & Security**
Fall 2023, Spring 2024, Spring 2025
Washington University in St. Louis

Workshop Course — **ProperData IoT Privacy Workshop**
Summer 2023
University of California-Irvine

CS 1210 — **Fundamentals of Computing**
Summer 2021
University of Iowa

CS 4980 — **Online Advertising & Tracking**
Fall 2019
University of Iowa

Mentoring

Ph.D.

2025- **Chen Yang**, Washington University in St. Louis

2025- **Abylay Aitkazy**, Washington University in St. Louis

2023-25 **Yuhao Wu**, Washington University in St. Louis, *Post-grad: Sr. Staff AI Security Researcher, Palo Alto Networks*

2020-24 **Shaoor Munir**, University of California-Davis

2021-23 **Tina Yeung**, University of Washington

2020-23 **Pouneh Nikah Bahrami**, University of California-Davis

Master's

2024-25 **Ke Yang**, Washington University in St. Louis, *Post-grad: PhD Student at UC Irvine*

Undergraduate

2024 **Adejola Ogunsan**, Washington University in St. Louis

2021-23 **Maia Xiao**, University of Washington

2021-23 **Manasi Shah**, University of Washington

2019-21 **Charlie Wolfe**, University of Iowa, *Post-grad: Software Engineer at Apple*

2020-21 **Charles Nguyen**, University of California-Davis, *Post-grad: Software Engineer at Apple*

Professional Service

2027 **Program Committee Member**
USENIX Security Symposium (USENIX)

2027 **Program Committee Co-chair**
Workshop on Measurements, Attacks, and Defenses for the Web (MADWeb)

2026 **NSF Panelist (3×)**

2026 **Travel Grants Committee Chair**
ACM Internet Measurement Conference (IMC)

2026 **Program Committee Co-chair**
Workshop on Measurements, Attacks, and Defenses for the Web (MADWeb)
Policy-Relevant Privacy Research (PR2) Workshop

2026 **Program Committee Member**
USENIX Security Symposium (USENIX)

2025 **Program Committee Member**
USENIX Security Symposium (USENIX)
ACM Internet Measurement Conference (IMC)

2024 **Program Committee Member**
ACM Conference on Computer and Communications Security (CCS)
Workshop on Technology and Consumer Protection (ConPro)
Workshop on Designing Security for the Web (SecWeb)
Network and Distributed System Security (NDSS) Symposium Poster Program

2023 **Program Committee Member**
IEEE Symposium on Security and Privacy (Oakland)
USENIX Security Symposium (USENIX)

2022 **Workshop Organizer**
ProperData IoT Privacy Workshop
University of California-Irvine

2022 **Program Committee Member**
ACM Internet Measurement Conference (IMC)
Privacy Enhancing Technologies Symposium (PETS)
Workshop on Measurements, Attacks, and Defenses for the Web (MADWeb)

2021 **Program Committee Member**
ACM Conference on Computer and Communications Security (CCS)

2017-24 **Invited Reviewer**
IEEE Symposium on Security and Privacy (Oakland)
ACM Conference on Human Factors in Computing Systems (CHI)
The Web Conference (WWW)
Privacy Enhancing Technologies Symposium (PETS)
International Symposium on Research in Attacks, Intrusions and Defenses (RAID)
IEEE Transactions on Dependable and Secure Computing (TDSC)
ACM Transactions on the Web (TWEB)
Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)

UIowa **Student Travel Grant Review Committee Member**
2018-19 Graduate & Professional Student Government, The University of Iowa

IMC 2017 **Shadow Program Committee Member**
ACM Internet Measurement Conference

Invited Talks

2026 **Building Reliable Systems from Unreliable Models**
University of Illinois Urbana-Champaign, Security and Privacy Seminar Series

2026 **Building Reliable Systems from Unreliable Models**
University of Maryland, Baltimore County, Lab talk

2026 **Tremendously capable, Trivially Exploitable: Securing Systems Built on Unreliable AI**
Stanford Security Lunch

2026 **Tremendously capable, Trivially Exploitable: Securing Systems Built on Unreliable AI**
DuckDuckGo

2025 **Measurement-driven Privacy Audits**
ACM SIGMETRICS

2025 **Security and Privacy Issues in Agentic Web (Lightning Talk)**
Mozilla Security Research Summit

2025 **Systems Security Foundations for Secure AI Agents (Lightning Talk)**
Agentic AI Summit, UC Berkeley

2025 **Independent Auditing of Smart Speaker Data Usage Practices**
Comcast

2024 **LLM Platform Security: Systematic Evaluation of OpenAI's ChatGPT Plugins**
FTC PrivacyCon

2022 **The State of Web Privacy: Threats & Defenses**
Guest lecture CS484, University of Washington

2022 **Towards a Privacy-Respecting Web**
University of Iowa
University of New Orleans

2022 **Tracking, Profiling, & Ad-Targeting in Smart Speakers**
FTC PrivacyCon
ProperData IoT Privacy Workshop

2022 **Breaking Advertising & Tracking Request Chains**
Ad-filtering Developer Summit

2020 **Fingerprinting the Fingerprinters**
Brave Software

2019 **Machine Learning for Ad and Tracker Blocking**
Adblock Developer Summit
UIowa Graduate Research Symposium

2019 **Machine Learning for Fingerprinting Detection**
Mozilla Corporation

2019 **An Overview of Ad and Tracker Blocking**
Mozilla Security Research Summit

Select Media Coverage

NPR 2026 **We tested how AI chatbots would handle foreign propaganda. They did surprisingly well**, *Huo Jingnan*, [Link]

TheRegister 2024 **GPT apps fail to disclose data collection, study finds**, *Thomas Claburn*, [Link]

KPLR Ch. 11 2023 **Privacy Concerns Over Amazon's Growing Footprint**, *Kathleen Berger*, [Link]

Fox News 2022 **Privacy Concerns Over Amazon's Growing Footprint**, *Bret Baier*, [Link]

TheVerge 2022 **Researchers find Amazon uses Alexa voice data to target you with ads**, *Jennifer Pattison Tuohy*, [Link]

ZDNet 2020 **A quarter of the Alexa Top 10K websites are using browser fingerprinting scripts**, *Catalin Cimpanu*, [Link]

CNET 2018 **Brave's AI blocks ads better than today's browser plug-ins, company says**, *Stephen Shankland*, [Link]