Trust in an Untrusted World: Private Access over Public Infrastructures

Divyakant Agrawal
Leadership Endowed Chair in Computer Science
Distinguished Professor & Chair of Computer Science
University of California at Santa Barbara

Abstract. We live in an era where our digital lives are increasingly interdependent and deeply interconnected. These connections rely on a vast, layered ecosystem of actors—many of whose trustworthiness is uncertain or outright suspect. Over the past three decades, rapid advances in computing and communication technologies have brought unprecedented access and connectivity to billions of users. Yet this digitization comes at a cost: our interactions, queries, and data are increasingly vulnerable to privacy violations. Today, threats to privacy come not just from malicious individuals, but also from powerful institutions—ranging from service providers to nation-states. In this reality of an untrusted world, we pose several foundational research questions: (i) Can we design a **scalable voice communication system** that ensures absolute privacy? (ii) Can we build an **oblivious search engine** over public document repositories? (iii) Can we develop **scalable private query processing** over shared or public databases? (iv) And in the age of large language models, can we enable **private inference** for user queries? These are not just open problems — they are essential challenges if we are to build trusted services over untrusted infrastructures. In this talk, I will present recent work that leverages Homomorphic Encryption to address some of these questions. We explore the inherent **performance and scalability trade-offs** in enabling private access, search, and inference. If nothing else, our results underscore a critical insight: **ensuring privacy at scale is not impossible, but it comes at a high computational cost.**

Biography. **Divy Agrawal** is a Distinguished Professor and Chair of Computer Science at the University of California, Santa Barbara (UCSB), where he also holds the Leadership Endowed Chair in the Department of Computer Science. He received his B.E. (Hons.) in Electrical Engineering from BITS Pilani, followed by M.S. and Ph.D. degrees in Computer Science from the State University of New York at Stony Brook. Since joining UCSB, Professor Agrawal has established himself as a leading researcher in databases, distributed systems, cloud computing, and large-scale data infrastructures and analytics. Over the course of his career, he has published more than 400 research articles and mentored approximately 50 Ph.D. students. He currently serves as Editor-in-Chief of both the *Proceedings of the ACM on Modeling of Data* and the Springer journal *Distributed and Parallel Databases*. He has served on several editorial boards, including *ACM Transactions on Database Systems*, *IEEE Transactions on Knowledge and Data Engineering*, *ACM Transactions on Spatial Algorithms and Systems*, *ACM Books*, and the *VLDB Journal*. Professor Agrawal is a former Trustee of the VLDB Endowment and recently served as Chair of the ACM Special Interest Group on Management of Data (SIGMOD). His recognitions include the Gold Medal from BITS Pilani, the UCSB Academic Senate Award for Outstanding Graduate Mentoring, and multiple paper honors: Best Paper Awards (ICDE 2002, MDM 2011), an Influential Paper Award (NDSS 2024), and Test-of-Time Awards (ICDT, MDM). He is a Fellow of the ACM, IEEE, and AAAS.

Speaker Introduction. **Divy Agrawal** is a Distinguished Professor and Chair of Computer Science at the University of California, Santa Barbara, where he also holds the Leadership Endowed Chair. His research spans databases, distributed systems, cloud computing, and large-scale data analytics. He has published over 400 papers and mentored nearly 50 Ph.D. students. He serves as Editor-in-Chief of *PACMMOD* and *Distributed and Parallel Databases*, and chairs ACM SIGMOD. His recognitions include multiple best paper and test-of-time awards, the UCSB Graduate Mentoring Award, and a Gold Medal from BITS Pilani. He is a Fellow of the ACM, IEEE, and AAAS.