Proposal Defense

Doctor of Philosophy in Information Science

“Securing Blockchain-based Timed Data Release: Theory and Applications” by Jingzhe Wang

Date: August 7, 2024
Time: 9:30 a.m. – 11:30 a.m.
Place: Room 828, Information Sciences Building, 135 N Bellefield Ave, Pittsburgh PA 15260

Committee:
- Dr. Balaji Palanisamy, Advisor, Associate Professor and Associate Chair, Department of Informatics and Networked Systems, School of Computing and Information
- Dr. James Joshi, Professor, Department of Informatics and Networked Systems, School of Computing and Information
- Dr. Stephen Lee, Assistant Professor, Department of Computer Science, School of Computing and Information
- Dr. Prashant Krishnamurthy, Professor, Department of Informatics and Networked Systems, School of Computing and Information

Abstract:
Timed Data Release (TDR) is a practical security mechanism that safeguards data until a specified time has elapsed. With recent advancements in blockchain technology, practical solutions to support decentralized timed data release using blockchains are gaining importance. This dissertation aims to build the theoretical foundations for securing Blockchain-based Timed Data Release (B-TDR) while shedding light on its applicability to real-world applications. The first part of this dissertation offers an attack-resilient design for B-TDR by carefully incorporating an uncertainty aware reputation measure with algorithmic frameworks, including temporal graphs and approximation algorithms. The second part safeguards and enhances B-TDR through cryptographic approaches consisting of the following novel designs: (1) A controllable B-TDR design that protects data before the release time while offering fine-grained data control, (2) A privacy-preserving and reliable B-TDR design that ensures data availability and fault tolerance while maintaining privacy, (3) A privacy-preserving event-driven data release protocol that enables data release upon the occurrence of a prescribed event, generalizing the concept of timed data release to support event-based release, and (4) A novel variant B-TDR with time-varying privacy levels that supports gradually relaxing data privacy over time. The third part of this dissertation expands the reach of B-TDR to support a set of representative applications by designing (1) a novel secure voting and auction applications based on B-TDR, (2) an engineered B-TDR design that enables scheduled microblog publication, and (3) a single-round secure multiparty computation supported by B-TDR.