Efficient Hardware-Aware and Hardware-Enabled Algorithms for Secure In-Memory Databases

UTAH ARCH

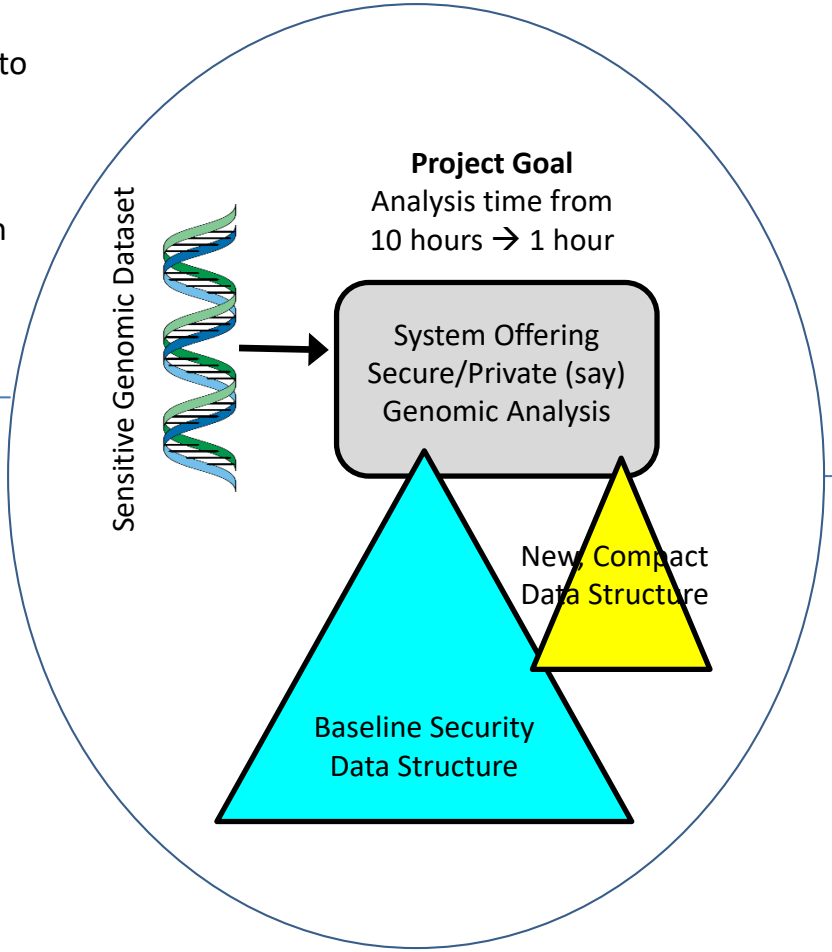
Challenge:

Memory systems are vulnerable to several attacks; commercial systems like SGX include some defenses. These and future defenses incur significant overheads in terms of bandwidth and memory capacity, reducing performance by an order of magnitude.

Solution:

Creation of smaller footprint data structures that are accessed in the common case.

- HPCA 2018: Distributed protocol to reduce data movement.
- ASPLOS 2018: Managing counter overflows and compressed hashes.
- ASPLOS 2019: Compact two-level security data structures.



Scientific Impact:

Integrity verification is a defense, already included in commercial processors like Intel SGX, that causes average slowdowns of 5.5x. The project defines practical ideas that bring this slowdown to 1.5x [ASPLOS 2018].

Modern system attacks have exploited side channels, that can cause slowdowns of nearly 10x. The project introduces new hardware and new protocols that bring the slowdown to 5x [HPCA 2018, ASPLOS 2019].

Broader Impact:

Secure systems will be vital for domains involving sensitive data, e.g., healthcare, finance, government. The project uses Intel SGX as a baseline and defines practical solutions, improving both performance and security, that are worthy of inclusion in next-generation commercial systems. In particular, the project improves the performance of Intel SGX by 3.7x.

The PI is involved in several efforts to grow a diverse pipeline of computer science majors, including programs targeted at Title I Elementary schools.

CNS-1718834, University of Utah,
PI: Rajeev Balasubramonian.