TrustedDB: A Trusted Hardware based Database with Privacy and Data Confidentiality

ABSTRACT:

Traditionally, as soon as confidentiality becomes a concern, data is encrypted before outsourcing to a service provider. Any software-based cryptographic constructs then deployed, for server-side query processing on the encrypted data, inherently limit query expressiveness. Here, we introduce TrustedDB, an outsourced database prototype that allows clients to execute SQL queries with privacy and under regulatory compliance constraints by leveraging server-hosted, tamper-proof trusted hardware in critical query processing stages, thereby removing any limitations on the type of supported queries. Despite the cost overhead and performance limitations of trusted hardware, we show that the costs per query are orders of magnitude lower than any (existing or) potential future software-only mechanisms. TrustedDB is built and runs on actual hardware and its performance and costs are evaluated here.

EXISTING SYSTEM:

Existing research addresses several such security aspects, including access privacy and searches on encrypted data. In most of these efforts data is encrypted before outsourcing. Once encrypted however, inherent limitations in the types of primitive operations that can be performed on encrypted data lead to fundamental expressiveness and practicality constraints. Recent theoretical cryptography results provide hope by proving the existence of universal homeomorphisms, i.e.,...
encryption mechanisms that allow computation of arbitrary functions without decrypting the inputs. Unfortunately actual instances of such mechanisms seem to be decades away from being practical

PROBLEM DEFINITION:

- Trusted hardware is generally impractical due to its performance limitations and higher acquisition costs. As a result, with very few exceptions, these efforts have stopped short of proposing or building full-fledged database processing engines.
- Computation inside secure processors is orders of magnitude cheaper than any equivalent cryptographic operation performed on the provider's unsecured server hardware, despite the overall greater acquisition cost of secure hardware.

PROPOSED SYSTEM:

we posit that a full-fledged, privacy enabling secure database leveraging server-side trusted hardware can be built and run at a fraction of the cost of any (existing or future) cryptography-enabled private data processing on common server hardware. We validate this by designing and building TrustedDB, a SQL database processing engine that makes use of tamperproof cryptographic coprocessors such as the IBM 4764 in close proximity to the outsourced data. Tamper resistant designs however are significantly constrained in both computational ability and memory capacity which makes implementing fully featured database solutions using secure coprocessors (SCPs) very challenging. TrustedDB achieves this by utilizing common unsecured server resources to the
maximum extent possible. E.g., TrustedDB enables the SCPU to transparently access external storage while preserving data confidentiality with on-the-fly encryption. This eliminates the limitations on the size of databases that can be supported. Moreover, client queries are pre-processed to identify sensitive components to be run inside the SCPU. Non-sensitive operations are off-loaded to the untrusted host server. This greatly improves performance and reduces the cost of transactions.

ADVANTAGES OF PROPOSED SYSTEM:

i. The introduction of new cost models and insights that explain and quantify the advantages of deploying trusted hardware for data processing,

ii. the design, development, and evaluation of TrustedDB, a trusted hardware based relational database with full data confidentiality, and

iii. Detailed query optimization techniques in a trusted hardware-based query execution model.
IEEE Projects 100% WORKING CODE + DOCUMENTATION+ EXPLANATION – BEST PRICE
LOW PRICE GUARANTEED

SYSTEM ARCHITECTURE:

HARDWARE REQUIREMENTS:

- System: Pentium IV 2.4 GHz.
- Hard Disk: 40 GB.
- Monitor: 15 inch VGA Colour.
- Mouse: Logitech Mouse.
- Ram: 512 MB
- Keyboard: Standard Keyboard
SOFTWARE REQUIREMENTS:

- Operating System : Windows XP.
- Coding Language : ASP.NET, C#.Net.
- Database : SQL Server 2005