Prisma/DB

Data breaches due to targeted hacker attacks are no longer a sci-fi scenario and are constantly seen on the news. Just this year, top 4 data breaches that happened to Anthem insurance company, MySpace, Turkish citizenship database, and Philippines' Commission of Elections, have exposed detailed personal data of about 350m people, leave alone uncountable cases of smaller incidents.

Cryptography is a go-to technology for protecting data. However, the established cryptographic tools are unable to provide end-to-end protection, leaving large parts of data lifecycle completely unprotected. Operators of data have to use multiple layers of much weaker protection methods to cover up the intervals, where cryptography can't help. As we can see from the news, it doesn't always help.

In recent years, there have been many ground-breaking research results in cryptography, including so-called homomorphic cryptography, which makes it possible to perform complex processing of encrypted data without decrypting it.

In order to help companies protect their data, we propose a technology called Prisma/DB. Prisma/DB relies on many of the recent research results and combines them together into a transparent, "plug-and-play" layer of data protection for database systems. Exposing identical to the original interface of communication with the database, Prisma/DB becomes a transparent middle-man in communication between the user and the database. It takes the data queries from the user and transforms them into equivalent encrypted queries, which are then sent to the encrypted database; the database in its turn responds with encrypted result, which is decrypted by Prisma/DB and given back to the user, who may not even be aware that the database is fully encrypted.
Homomorphic cryptography, which is one of the corner stones of the proposed project, has been called the "Holy Grail of Cryptography" that will revolutionize public clouds. Even though, there has been an increase in research activity in this area in recent years, there are no products available in the market that provide implementations of homomorphic cryptosystems in conjunction with database systems.
In the world, where data is the new oil, this projects aims to fulfil the need in data security by providing a comprehensive data security solution with currently unmatched capabilities based on latest achievements in cryptography.

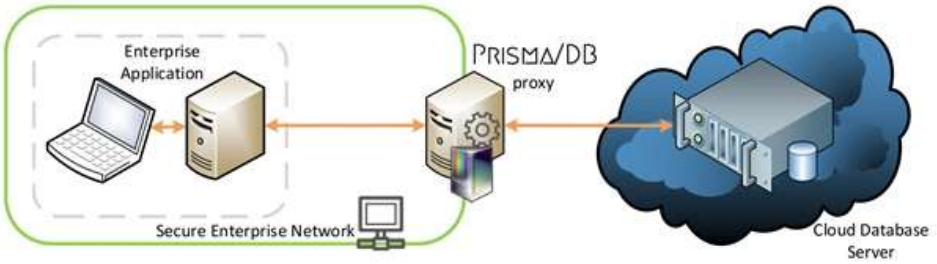

Figure 1. Topology of Use Case #1

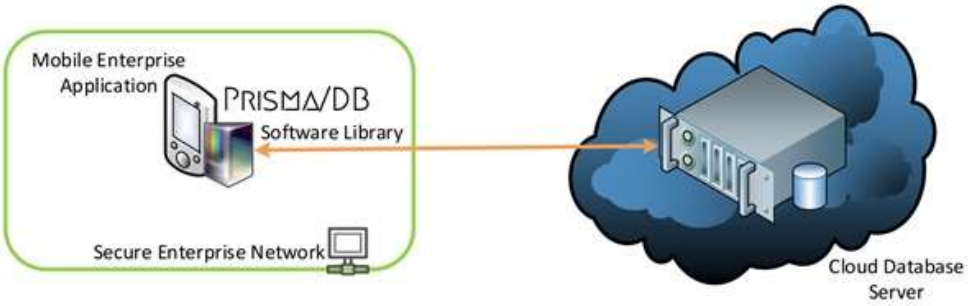

Figure 2. Topology of Use Case #2.
Mobile Enterprise Application is not necessarily physically located on premises, it may be connected in via VPN or other similar technologies.

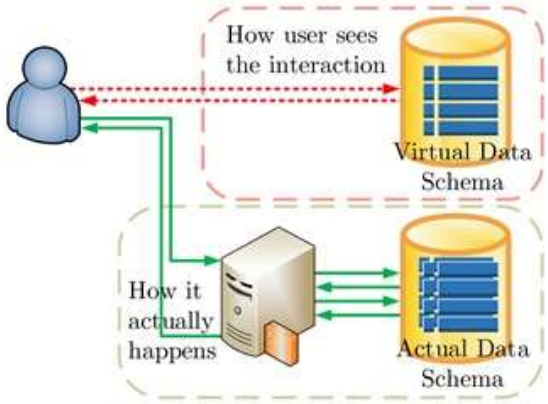

Figure 3. Actual and virtual data schemas.

Figure 4. Examples of how queries are transformed into their encrypted versions.

Principal Investigator	Assoc. Prof. Ng Wee Keong *(SCSE)*
Researcher	Dr. Vasily Sidorov
School / Department	School of Computer Science and Engineering
Source of Funding	Ministry of Education, Singapore