Защищённая база данных. Архитектура.

В. А. Бойко, *ФИТ НГУ*

Научный руководитель:

С. Ф. Кренделев, *к.ф.-м.н., зав. лаб. НИЧ НГУ*

Работа выполняется при финансовой поддержке Минобрнауки РФ (договор № 02.G25.31.0054

План

1. Обзор
2. Новизна
3. Пакетная архитектура

1. Обзор

- Для обеспечения конфиденциальности данных в удалённой БД, их можно шифровать.

1. Обзор

- Для обеспечения конфиденциальности данных, их можно шифровать.

  Проблема: трудно оперировать зашифрованными данными

1. Обзор

Чтобы проводить операции, надо шифровать особым способом:

1. Гомоморфные алгоритмы
2. OPE алгоритмы

1. Обзор

Использование особых алгоритмов шифрования позволяет:

1. Проводить операции в БД
2. Дешифровать данные только на клиенте

1. Обзор

При шифровании данных, изменяется не только представление данных, но и то, как над ними надо проводить операции.

$A > B \Rightarrow A' < B'$

2. Новизна

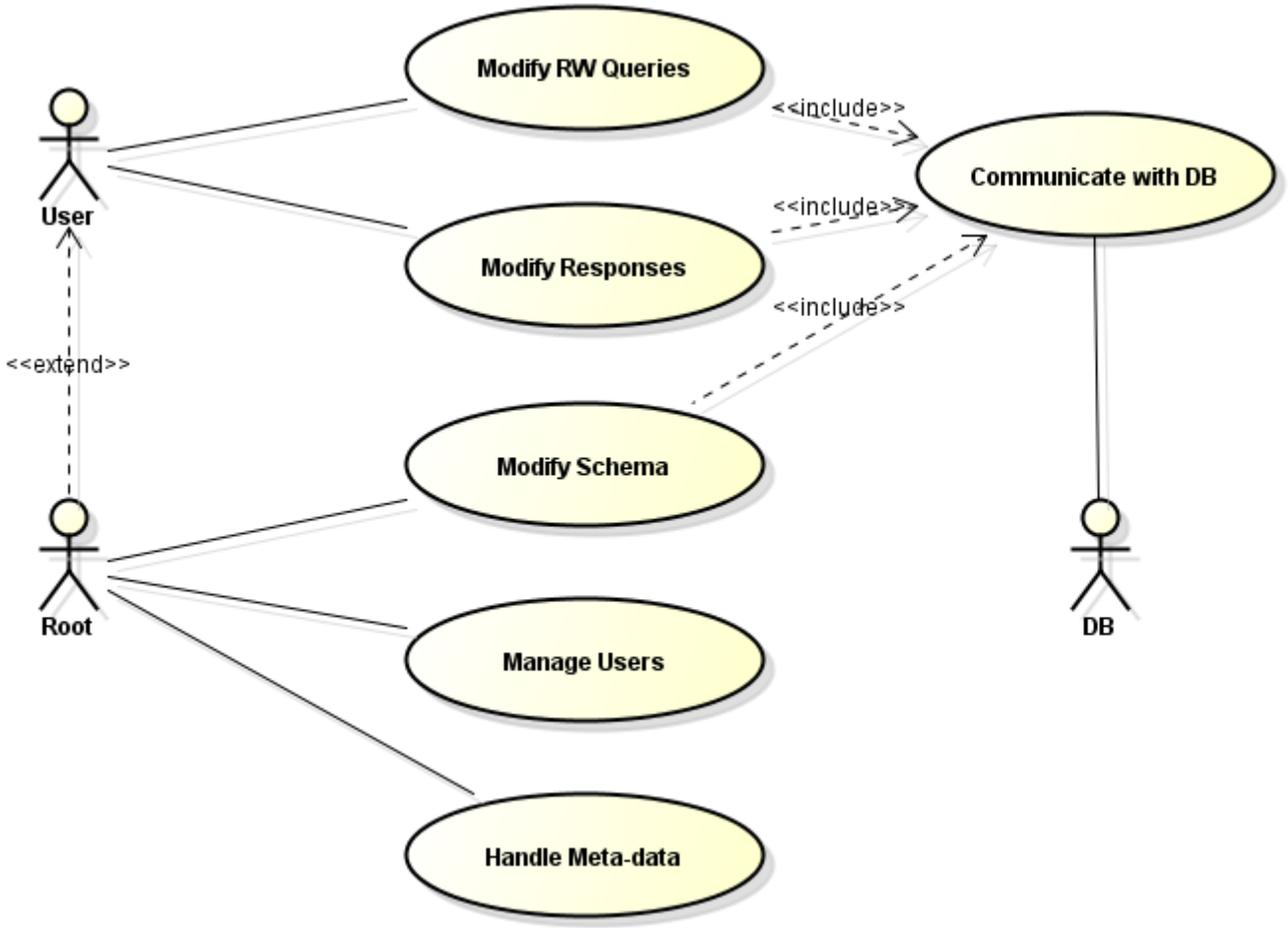
В нашей системе используются разработанные в лаборатории алгоритмы шифрования, ранее нигде не использовавшиеся.

2. Новизна

От того, как изменяются данные, и как изменяются запросы к данным, зависит устройство системы.

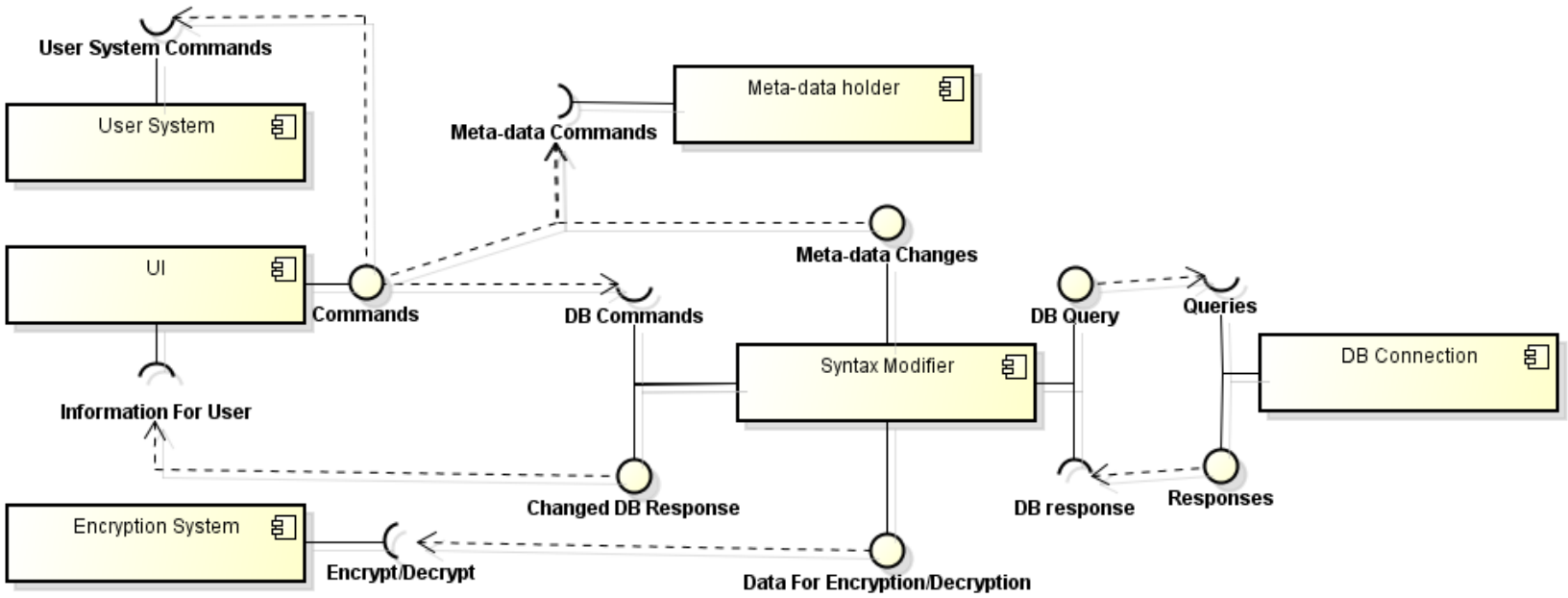
3. Пакетная архитектура

Верхнеуровневая use-case модель прототипа



3. Пакетная архитектура

Основные пакеты



4. Результаты

1. Была построена архитектура системы
2. Построен прототип
3. Протестирован прототип
4. Результаты представлены на МНСК 2014, Россия
5. Доклад о работе принят как один из ключевых докладов на конференцию РИТ++ 2014, Россия
6. Результаты в соавторстве приняты к публикации на конференции FedCSIS (EAIS'14), Польша
7. Результаты работы отправлены на конференцию NSS 2014, Китай

Дальнейшее развитие

- Работа с удалённой БД
- Кэширование
- Вся арифметика
- Оптимизации
- Интеграция с уже существующими продуктами
- Поддержка MySQL