5 ЛР. ШИФРОВАНИЕ И ЗАЩИТА ДАННЫХ

# Особенности криптографической защиты в СУБД. Перечислите основные подходы к шифрованию в распределенных СУБД.

Các tính năng bảo vệ bằng mật mã trong DBMS. Liệt kê các phương pháp chính để mã hóa trong các DBMS phân tán.

Особенности криптографической защиты в СУБД

Các tính năng bảo vệ bằng mật mã trong DBMS

* Достаточная производительность процесса шифрования
* Hiệu suất đầy đủ của quá trình mã hóa
* Прозрачность реализации шифрования данных
* Tính minh bạch của việc thực hiện mã hóa dữ liệu
* Управление ключами шифрования
* Quản lý khóa mã hóa
* Строгое разделение ключей и зашифрованных данных
* Tách biệt nghiêm ngặt các khóa và dữ liệu được mã hóa
* Различные наборы данных для разных объектов СУБД
* Các bộ dữ liệu khác nhau cho các đối tượng DBMS khác nhau

**Основные подходы к шифрованию в распределенных СУБД**

Các phương pháp cơ bản để mã hóa trong DBMS phân tán

* Подход с внутренней к распределенной базе данных: пользовательские приложения шифруют данные и затем сохраняют зашифрованные данные в базе данных. Для использования сохраненных данных приложения извлекают зашифрованные данные из базы данных и затем дешифруют их.
* Phương pháp tiếp cận cơ sở dữ liệu phân tán từ phía sau: Ứng dụng của người dùng mã hóa dữ liệu và sau đó lưu trữ dữ liệu được mã hóa trong cơ sở dữ liệu. Để sử dụng dữ liệu được lưu trữ, các ứng dụng sẽ truy xuất dữ liệu được mã hóa từ cơ sở dữ liệu và sau đó giải mã nó.
* Внешняя по отношению к распределенной базе данных. Система распределенных баз данных имеет свои собственные возможности шифрования. Пользовательские приложения хранят данные и извлекают их, не осознавая, что данные хранятся в зашифрованном виде в базе данных.
* Bên ngoài cơ sở dữ liệu phân tán. Hệ thống cơ sở dữ liệu phân tán có khả năng mã hóa riêng. Ứng dụng người dùng lưu trữ và truy xuất dữ liệu mà không nhận ra rằng dữ liệu được lưu trữ được mã hóa trong cơ sở dữ liệu.

# Шифрование на уровне устройств хранения информации.

Mã hóa ở cấp độ thiết bị lưu trữ.

Шифрование на уровне хранилища означает шифрование данных в подсистеме хранения и защищает данные в состоянии покоя. Он хорошо подходит для шифрования файлов или целых каталогов в контексте операционной системы.

Mã hóa cấp độ lưu trữ có nghĩa là mã hóa dữ liệu trong hệ thống con lưu trữ và bảo vệ dữ liệu ở phần còn lại. Nó rất phù hợp để mã hóa các tập tin hoặc toàn bộ thư mục trong bối cảnh của hệ điều hành.

Преимущества

Thuận lợi

* позволяет избежать каких-либо изменений в существующих приложениях.
* tránh mọi thay đổi đối với các ứng dụng hiện có.
* поскольку подсистема хранения ничего не знает об объектах и структуре базы данных, стратегия шифрования не может быть связана ни с привилегиями пользователя, ни с конфиденциальностью данных. Шифрование только частей базы данных для уменьшения накладных расходов на шифрование, ограничено степенью детализации файлов.
* Bởi vì hệ thống con lưu trữ không biết gì về các đối tượng và cấu trúc của cơ sở dữ liệu nên chiến lược mã hóa không thể liên quan đến đặc quyền của người dùng hoặc tính bảo mật dữ liệu. Việc chỉ mã hóa các phần của cơ sở dữ liệu để giảm chi phí mã hóa bị giới hạn bởi mức độ chi tiết của tệp.

# Шифрование на уровне СУБД

Mã hóa ở cấp DBMS

Шифрование на уровне базы данных позволяет защитить данные, когда они вставляются в базу данных или извлекаются из нее.

Mã hóa cấp cơ sở dữ liệu giúp bảo vệ dữ liệu khi dữ liệu được chèn vào hoặc truy xuất từ ​​cơ sở dữ liệu.

Шифрования может быть

* частью структуры базы данных
* một phần của cấu trúc cơ sở dữ liệu
* связана с конфиденциальностью данных и/или привилегиями пользователя.
* liên quan đến quyền riêng tư dữ liệu và/hoặc đặc quyền của người dùng.
* выполняться с различной степенью детализации, например для таблиц, столбцов и строк, логических условий.
* được thực hiện với mức độ chi tiết khác nhau, ví dụ như đối với bảng, cột và hàng cũng như các điều kiện logic.

Процесс шифрования может привести к

Quá trình mã hóa có thể dẫn đến

* некоторым изменениям в приложениях;
* một số thay đổi trong ứng dụng;
* снижению производительности СУБД, поскольку шифрование обычно запрещает использование индексов для зашифрованных данных.
* Giảm hiệu suất DBMS do mã hóa thường cấm sử dụng các chỉ mục trên dữ liệu được mã hóa.

Ключи шифрования должны передаваться или храниться вместе с зашифрованными данными на стороне сервера.

Khóa mã hóa phải được truyền hoặc lưu trữ cùng với dữ liệu được mã hóa ở phía máy chủ.

# Шифрование на уровне приложения.

Mã hóa cấp ứng dụng.

Шифрование на уровне приложений перемещает процесс шифрования/дешифрования в приложения, которые генерируют данные.

Mã hóa cấp ứng dụng chuyển quá trình mã hóa/giải mã sang các ứng dụng tạo ra dữ liệu.

Шифрование выполняется в приложении, которое вводит данные в систему, данные отправляются в зашифрованном виде, поэтому сохраняются и извлекаются в зашифрованном виде, чтобы окончательно расшифроваться в приложении.

Quá trình mã hóa được thực hiện trong ứng dụng nhập dữ liệu vào hệ thống, dữ liệu được gửi được mã hóa nên được lưu trữ và truy xuất được mã hóa để cuối cùng được giải mã trong ứng dụng.

Преимущество: он отделяет ключи шифрования от зашифрованных данных, хранящихся в базе данных. Однако приложения должны быть изменены, чтобы принять это решение.

Ưu điểm: Nó tách các khóa mã hóa khỏi dữ liệu được mã hóa được lưu trữ trong cơ sở dữ liệu. Tuy nhiên, các ứng dụng phải được sửa đổi để đưa ra quyết định này.

В зависимости от степени детализации шифрования приложению может потребоваться получить больший набор данных . Пользователь (или любой злоумышленник, получивший доступ к машине, на которой запущено приложение) может взломать приложение, чтобы получить доступ к несанкционированным данным.

Tùy thuộc vào mức độ chi tiết của mã hóa, ứng dụng có thể cần truy xuất một tập dữ liệu lớn hơn. Người dùng (hoặc bất kỳ kẻ tấn công nào có được quyền truy cập vào máy chạy ứng dụng) có thể hack ứng dụng để có quyền truy cập vào dữ liệu trái phép.

Это приводит к снижению производительности и запрещает использование некоторых расширенных функций базы данных для зашифрованных данных, таких как хранимые процедуры и триггеры

Điều này dẫn đến hiệu suất kém và ngăn cản việc sử dụng một số tính năng cơ sở dữ liệu nâng cao trên dữ liệu được mã hóa, chẳng hạn như các thủ tục được lưu trữ và trình kích hoạt

С точки зрения детализации и управления ключами шифрование на уровне приложений обеспечивает максимальную гибкость, поскольку степень детализации шифрования и ключи шифрования можно выбирать в зависимости от логики приложения.

Về mặt chi tiết và quản lý khóa, mã hóa cấp ứng dụng mang lại tính linh hoạt cao nhất vì mức độ chi tiết mã hóa và khóa mã hóa có thể được chọn dựa trên logic ứng dụng.

# Роль аппаратных модулей безопасности (HS модулей) в структуре криптографической защиты современных СУБД.

Vai trò của mô-đun bảo mật phần cứng (mô-đun HS) trong cấu trúc bảo vệ mật mã của DBMS hiện đại.

Аппаратные модули безопасности (HS-модули) являются важным элементом криптографической защиты современных систем управления базами данных (СУБД). Они обеспечивают ускоренное и безопасное выполнение криптографических операций, таких как шифрование, хэширование и цифровая подпись.

Mô-đun bảo mật phần cứng (mô-đun HS) là một thành phần quan trọng trong bảo vệ mật mã của hệ thống quản lý cơ sở dữ liệu hiện đại (DBMS). Chúng cung cấp hiệu suất nhanh hơn và an toàn hơn cho các hoạt động mã hóa như mã hóa, băm và ký kỹ thuật số.

HS-модули обычно размещаются на отдельном физическом устройстве, называемом Hardware Security Module (HSM). HSM представляет собой высокопроизводительный криптографический ускоритель, который может обрабатывать большие объемы данных с высокой скоростью.

Các mô-đun HS thường được đặt trên một thiết bị vật lý riêng biệt được gọi là Mô-đun bảo mật phần cứng (HSM). HSM là một công cụ tăng tốc mật mã hiệu suất cao, có thể xử lý lượng lớn dữ liệu ở tốc độ cao.

В структуре криптографической защиты СУБД, HS-модули выполняют следующие задачи:

Trong cấu trúc bảo vệ mật mã của DBMS, các mô-đun HS thực hiện các nhiệm vụ sau:

* Шифрование данных - HS-модули обеспечивают безопасное шифрование данных на уровне СУБД. Это позволяет защитить конфиденциальные данные, такие как пароли, персональные данные и финансовые данные.
* Mã hóa dữ liệu - Mô-đun HS cung cấp mã hóa dữ liệu an toàn ở cấp DBMS. Điều này cho phép bạn bảo vệ dữ liệu nhạy cảm như mật khẩu, dữ liệu cá nhân và dữ liệu tài chính.
* Хранение ключей - HS-модули могут использоваться для хранения ключей шифрования и цифровой подписи. Это обеспечивает безопасное хранение ключей и защищает их от несанкционированного доступа.
* Lưu trữ khóa - Mô-đun HS có thể được sử dụng để lưu trữ khóa mã hóa và chữ ký số. Điều này cung cấp khả năng lưu trữ khóa an toàn và bảo vệ chúng khỏi bị truy cập trái phép.
* Аутентификация - HS-модули могут использоваться для выполнения аутентификации пользователей и устройств. Это обеспечивает защиту от атак типа Man-in-the-Middle и других видов атак на процесс аутентификации.
* Xác thực - Mô-đun HS có thể được sử dụng để thực hiện xác thực người dùng và thiết bị. Điều này cung cấp khả năng bảo vệ chống lại các cuộc tấn công Man-in-the-Middle và các loại tấn công khác vào quá trình xác thực.
* Аудит - HS-модули могут использоваться для регистрации криптографических операций. Это позволяет обеспечить контроль над использованием криптографических ключей и защитить систему от несанкционированного доступа.
* Kiểm tra - Mô-đun HS có thể được sử dụng để ghi nhật ký các giao dịch mật mã. Điều này cho phép bạn kiểm soát việc sử dụng khóa mật mã và bảo vệ hệ thống khỏi bị truy cập trái phép.

В целом, HS-модули являются важным компонентом криптографической защиты современных СУБД, обеспечивая безопасность и скорость выполнения криптографических операций. Они позволяют защитить данные от несанкционированного доступа и обеспечить безопасную работу системы управления базами данных.

Nhìn chung, các mô-đun HS là một thành phần quan trọng trong việc bảo vệ mật mã của các DBMS hiện đại, đảm bảo tính bảo mật và tốc độ của các hoạt động mật mã. Chúng cho phép bạn bảo vệ dữ liệu khỏi bị truy cập trái phép và đảm bảo hoạt động an toàn của hệ thống quản lý cơ sở dữ liệu.

# Роль гомоморфных криптосистем для облачных сервисов и систем хранения. Существующие решения и перспективы развития.

Vai trò của hệ thống mật mã đồng hình đối với các dịch vụ đám mây và hệ thống lưu trữ. Các giải pháp hiện có và triển vọng phát triển.

Гомоморфные криптосистемы - это тип технологии шифрования, которая позволяет выполнять вычисления на зашифрованные данные без необходимости расшифровать их. Это делает гомоморфные криптосистемы привлекательным решением для облачных служб и систем хранения, где необходимо безопасно хранить и обработать конфиденциальные данные.

Hệ thống mật mã đồng cấu là một loại công nghệ mã hóa cho phép thực hiện các phép tính trên dữ liệu được mã hóa mà không cần phải giải mã nó. Điều này làm cho hệ thống mật mã đồng cấu trở thành một giải pháp hấp dẫn cho các dịch vụ đám mây và hệ thống lưu trữ, nơi dữ liệu nhạy cảm cần được lưu trữ và xử lý một cách an toàn.

Одним из основных преимуществ гомоморфных криптосистем является то, что они позволяют пользователям выполнять вычисления по зашифрованным данным без необходимости подвергать данные открытого текста поставщику облачных услуг. Это может помочь предотвратить ущерб данных и несанкционированный доступ к конфиденциальной информации. Кроме того, гомоморфные криптосистемы также могут помочь снизить стоимость и сложность управления данными, поскольку они устраняют необходимость перемещения данных между поставщиком облачных услуг и клиентом.

Một trong những ưu điểm chính của hệ thống mật mã đồng cấu là chúng cho phép người dùng thực hiện tính toán trên dữ liệu được mã hóa mà không cần phải cung cấp dữ liệu văn bản gốc cho nhà cung cấp dịch vụ đám mây. Điều này có thể giúp ngăn ngừa hư hỏng dữ liệu và truy cập trái phép vào thông tin nhạy cảm. Ngoài ra, hệ thống mật mã đồng cấu cũng có thể giúp giảm chi phí và độ phức tạp của việc quản lý dữ liệu vì chúng loại bỏ nhu cầu di chuyển dữ liệu giữa nhà cung cấp dịch vụ đám mây và khách hàng.

В настоящее время существует несколько существующих гомоморфных криптосистем, которые используются в облачных службах и системах хранения. К ним относятся криптосистема Paillier, криптосистема RSA и джентри -криптосистему. Каждая из этих криптосистем имеет свои преимущества и недостатки, в зависимости от конкретного варианта использования.

Hiện tại, có một số hệ thống mật mã đồng cấu hiện có được sử dụng trong các dịch vụ đám mây và hệ thống lưu trữ. Chúng bao gồm hệ thống mật mã Paillier, hệ thống mật mã RSA và hệ thống mật mã gentry. Mỗi hệ thống mật mã này đều có những ưu điểm và nhược điểm riêng, tùy thuộc vào trường hợp sử dụng cụ thể.

В то время как гомоморфные криптосистемы уже используются в некоторых облачных службах и системах хранения, все еще существует много работ по разработке для повышения их эффективности и масштабируемости. Одной из областей исследований является разработка полностью гомоморфных криптосистем, которые позволяют выполнять произвольные вычисления на зашифрованных данных. Другая область исследований - разработка аппаратных ускорителей для гомоморфных криптосистем, которые могут помочь улучшить их производительность и снизить их вычислительную сложность.

Mặc dù các hệ thống mật mã đồng cấu đã được sử dụng trong một số dịch vụ đám mây và hệ thống lưu trữ nhưng vẫn còn rất nhiều công việc phát triển để cải thiện hiệu quả và khả năng mở rộng của chúng. Một lĩnh vực nghiên cứu là phát triển các hệ thống mật mã đồng hình hoàn toàn cho phép thực hiện các phép tính tùy ý trên dữ liệu được mã hóa. Một lĩnh vực nghiên cứu khác là phát triển bộ tăng tốc phần cứng cho các hệ thống mật mã đồng hình, có thể giúp cải thiện hiệu suất và giảm độ phức tạp tính toán của chúng.

В заключение, гомоморфные криптосистемы являются важной технологией для облачных сервисов и систем хранения, поскольку они обеспечивают безопасную обработку конфиденциальных данных без необходимости обнародовать данные общетекстого поставщика поставщику облачных услуг. Хотя уже существует несколько существующих гомоморфных криптосистем, которые используются на практике, все еще существует значительная работа по развитию для повышения их эффективности, масштабируемости и функциональности.

Tóm lại, hệ thống mật mã đồng hình là một công nghệ quan trọng đối với các dịch vụ đám mây và hệ thống lưu trữ vì chúng cho phép xử lý an toàn dữ liệu nhạy cảm mà không cần phải tiết lộ dữ liệu văn bản chung cho nhà cung cấp dịch vụ đám mây. Mặc dù đã có một số hệ thống mật mã đồng hình hiện có được sử dụng trong thực tế nhưng vẫn cần phải phát triển đáng kể để cải thiện hiệu quả, khả năng mở rộng và chức năng của chúng.

( https://medium.com/privacy-preserving-natural-language-processing/homomorphic-encryption-for-beginners-a-practical-guide-part-1-b8f26d03a98a )

# Перспективные направления исследований в области КМЗИ в БД.

Những hướng nghiên cứu đầy hứa hẹn trong lĩnh vực CMMI trong cơ sở dữ liệu.

* Гомоморфизм и его использование в облачных сервисах;
* Đồng hình và việc sử dụng nó trong các dịch vụ đám mây;
* Защита HSM модулей;
* Bảo vệ các mô-đun HSM;
* Большие данные (запросы, перешифровка);
* Dữ liệu lớn (truy vấn, mã hóa lại);
* защита data-in-rest при появлении квантовых алгоритмов (Шора и Гровера)
* bảo vệ dữ liệu trong phần còn lại với sự ra đời của thuật toán lượng tử (Shor và Grover)
* обезличивание данных
* ẩn danh dữ liệu