Báo cáo đánh giá về các mối đe dọa bảo mật trên cơ sở dữ liệu

Shivnandan Singh Rakesh Kumar Rai

*PG Scholar, Đại học Galgotias Asstt. Giáo sư, ITS Engg College*

*Greater Noida, UP, Ấn Độ Đại Noida, UP, Ấn Độ*

**Tóm tắt: Dữ liệu là một trong những yếu tố quan trọng đối với bất kỳ tổ chức nào. Như chúng ta biết rằng cơ sở dữ liệu là tập hợp dữ liệu và chương trình để thực hiện các hoạt động trên dữ liệu đó. Vì vậy, để chạy thành công cho bất kỳ tổ chức nào, chúng tôi phải bảo mật dữ liệu của mình. Vì vậy, trong bài viết này, chúng tôi phải tập trung vào các mối đe dọa liên quan đến cơ sở dữ liệu cũng như một số thuật toán liên quan đến bảo mật cơ sở dữ liệu. Cơ sở dữ liệu có tỷ lệ vi phạm cao nhất trong số tất cả các tài sản kinh doanh, theo Báo cáo vi phạm dữ liệu năm 2012 của Verizon. Verizon báo cáo rằng 96% hồ sơ bị vi phạm là từ cơ sở dữ liệu và Open Security Foundation tiết lộ rằng 242,6 triệu hồ sơ có khả năng bị xâm phạm trong năm 2012.**

1. **CÁC MỐI ĐE DỌA BẢO MẬT CƠ SỞ DỮ LIỆU:**

Có nhiều cách để bảo mật cơ sở dữ liệu. Những cách này dựa trên các khía cạnh khác nhau của việc bảo mật cơ sở dữ liệu. Các khía cạnh khác nhau với các phương pháp truyền thống được tóm tắt dưới đây.

* 1. **- Lạm dụng đặc quyền quá** mức: Khi người dùng cuối hoặc ứng dụng được cấp cơ sở dữ liệu, các đặc quyền này có thể bị lạm dụng cho các đặc quyền truy cập mục đích độc hại vượt quá yêu cầu của chức năng công việc của họ. Ví dụ: quản trị viên trường đại học có công việc chỉ yêu cầu khả năng thay đổi thông tin liên hệ của sinh viên có thể tận dụng các đặc quyền cập nhật cơ sở dữ liệu quá mức để thay đổi điểm. Một người dùng cơ sở dữ liệu nhất định kết thúc với các đặc quyền quá mức vì lý do đơn giản là quản trị viên cơ sở dữ liệu không có thời gian để xác định và cập nhật các cơ chế kiểm soát đặc quyền truy cập chi tiết cho mỗi người dùng. Do đó, tất cả người dùng hoặc nhóm lớn người dùng đều được cấp đặc quyền truy cập mặc định chung vượt xa các yêu cầu công việc cụ thể.
  2. -Ngăn chặn lạm dụng đặc quyền quá mức - Kiểm soát truy cập cấp truy vấn Giải pháp cho các đặc quyền quá mức là kiểm soát truy cập cấp truy vấn.

Mức độ chi tiết của kiểm soát truy cập dữ liệu phải mở rộng ra ngoài bảng đến các hàng và cột cụ thể trong bảng. Kiểm soát truy cập cấp truy vấn đề cập đến một cơ chế hạn chế các đặc quyền cơ sở dữ liệu đối với các hoạt động SQL bắt buộc tối thiểu (SELECT, UPDATE, v.v.) và dữ liệu. Một cơ chế kiểm soát truy cập cấp truy vấn đủ chi tiết sẽ cho phép quản trị viên trường đại học giả mạo được mô tả trước đây cập nhật thông tin liên lạc, nhưng đưa ra cảnh báo nếu anh ta cố gắng thay đổi điểm. Kiểm soát truy cập cấp truy vấn không chỉ hữu ích để phát hiện lạm dụng đặc quyền quá mức của các nhân viên độc hại.

* 1. - Lạm dụng đặc quyền hợp pháp: Người dùng cũng có thể lạm dụng các đặc quyền cơ sở dữ liệu hợp pháp cho các mục đích trái phép. Hãy xem xét một nhân viên chăm sóc sức khỏe giả mạo giả mạo với các đặc quyền để xem hồ sơ bệnh nhân cá nhân thông qua một ứng dụng Web tùy chỉnh. Cấu trúc của ứng dụng Web thường giới hạn người dùng xem lịch sử chăm sóc sức khỏe của từng bệnh nhân - nhiều hồ sơ không thể được xem đồng thời và các bản sao điện tử không được phép. Tuy nhiên, nhân viên giả mạo có thể phá vỡ những hạn chế này bằng cách kết nối với cơ sở dữ liệu bằng cách sử dụng một máy khách thay thế như MS-Excel. Sử dụng MS-Excel và thông tin đăng nhập hợp pháp của mình, nhân viên có thể truy xuất và lưu tất cả hồ sơ bệnh nhân.

Không chắc rằng các bản sao cá nhân của cơ sở dữ liệu hồ sơ bệnh nhân như vậy tuân thủ bất kỳ chính sách bảo vệ dữ liệu bệnh nhân nào của tổ chức chăm sóc sức khỏe. Có hai rủi ro cần xem xét. Đầu tiên là nhân viên lừa đảo sẵn sàng đánh đổi hồ sơ bệnh nhân để lấy tiền. Thứ hai (và có lẽ phổ biến hơn) là nhân viên cẩu thả truy xuất và lưu trữ một lượng lớn thông tin vào máy khách của họ cho các mục đích công việc hợp pháp.

Khi dữ liệu tồn tại trên máy điểm cuối, nó sẽ dễ bị tấn công, Trojan, trộm cắp máy tính xách tay, v.v.

* 1. Những kẻ tấn công nâng cao đặc quyền có thể lợi dụng các lỗ hổng phần mềm nền tảng cơ sở dữ liệu để chuyển đổi đặc quyền truy cập từ đặc quyền của người dùng thông thường sang đặc quyền của quản trị viên. Các lỗ hổng có thể được tìm thấy trong, các chức năng tích hợp, các thủ tục được lưu trữ, triển khai giao thức và thậm chí cả các câu lệnh SQL. Ví dụ: một nhà phát triển phần mềm tại một tổ chức tài chính có thể lợi dụng chức năng dễ bị tổn thương để có được đặc quyền quản trị cơ sở dữ liệu. Với đặc quyền quản trị, nhà phát triển giả mạo có thể tắt các cơ chế kiểm toán, chuyển tiền, tạo tài khoản không có thật, v.v.

Ngăn chặn nâng cao đặc quyền - IPS và kiểm soát truy cập cấp truy vấn Khai thác độ cao đặc quyền có thể được ngăn chặn bằng sự kết hợp của các hệ thống ngăn chặn xâm nhập truyền thống (IPS) và kiểm soát truy cập cấp truy vấn (xem Đặc quyền quá mức ở trên). IPS kiểm tra lưu lượng cơ sở dữ liệu để xác định các mẫu tương ứng với các lỗ hổng đã biết. Ví dụ: nếu một chức năng nhất định được biết là dễ bị tấn công, thì IPS có thể chặn tất cả quyền truy cập vào quy trình dễ bị tổn thương hoặc (nếu có thể) chỉ chặn các quy trình đó bằng các cuộc tấn công nhúng.

**1.5**: Các lỗ hổng nền tảng trong các hệ điều hành cơ bản (Windows 2000, UNIX, v.v.) và các dịch vụ bổ sung được cài đặt trên máy chủ cơ sở dữ liệu có thể dẫn đến truy cập trái phép, hỏng dữ liệu hoặc từ chối dịch vụ. Ví dụ, Blaster Worm đã lợi dụng lỗ hổng Windows 2000 để tạo ra các điều kiện từ chối dịch vụ.

Ngăn chặn các cuộc tấn công nền tảng - Cập nhật phần mềm và phòng chống xâm nhập Bảo vệ tài sản cơ sở dữ liệu khỏi các cuộc tấn công nền tảng đòi hỏi sự kết hợp giữa cập nhật phần mềm thường xuyên (bản vá) và Hệ thống ngăn chặn xâm nhập (IPS).

Nhà cung cấp cung cấp các bản cập nhật loại bỏ các lỗ hổng được tìm thấy trong nền tảng cơ sở dữ liệu theo thời gian. Thật không may, các bản cập nhật phần mềm được cung cấp và thực hiện bởi các doanh nghiệp theo chu kỳ định kỳ. Giữa các chu kỳ cập nhật, cơ sở dữ liệu không được bảo vệ. Ngoài ra, các vấn đề tương thích đôi khi ngăn cản cập nhật phần mềm hoàn toàn. Để giải quyết những vấn đề này, IPS nên được thực hiện. Như đã mô tả trước đây, IPS kiểm tra lưu lượng cơ sở dữ liệu và xác định các cuộc tấn công nhắm vào các lỗ hổng đã biết.

**1.6** - SQL Injection Trong một cuộc tấn công SQL injection, thủ phạm thường chèn (hoặc "tiêm") các câu lệnh cơ sở dữ liệu trái phép vào một kênh dữ liệu SQL dễ bị tấn công. Thông thường, các kênh dữ liệu được nhắm mục tiêu bao gồm các thủ tục được lưu trữ và các tham số đầu vào của ứng dụng Web. Các câu lệnh được tiêm này sau đó được chuyển đến cơ sở dữ liệu nơi chúng được thực thi. Sử dụng SQL injection, kẻ tấn công có thể truy cập không hạn chế vào toàn bộ cơ sở dữ liệu.

Ngăn chặn SQL Injection Ba kỹ thuật có thể được kết hợp để chống lại SQL injection một cách hiệu quả: ngăn chặn xâm nhập (IPS), kiểm soát truy cập cấp truy vấn (xem Lạm dụng đặc quyền quá mức) và tương quan sự kiện. Tuy nhiên, IPS một mình là không đáng tin cậy vì các chuỗi SQL injection dễ bị dương tính giả. Các nhà quản lý bảo mật chỉ dựa vào IPS sẽ bị bắn phá với các cảnh báo SQL injection "có thể". IPS có thể xác định các thủ tục được lưu trữ dễ bị tổn thương hoặc chuỗi SQL injection. Tuy nhiên, bằng cách tương quan chữ ký SQL injection với một vi phạm khác như vi phạm kiểm soát truy cập cấp truy vấn, một cuộc tấn công thực sự có thể được xác định với độ chính xác cực cao. Không có khả năng chữ ký SQL injection và một vi phạm khác sẽ xuất hiện trong cùng một yêu cầu trong hoạt động kinh doanh bình thường.

**1.7** - Biên bản kiểm toán yếu Ghi lại tự động tất cả các giao dịch cơ sở dữ liệu nhạy cảm và / hoặc bất thường phải là một phần của nền tảng

Cơ sở cho bất kỳ triển khai cơ sở dữ liệu nào. Chính sách kiểm toán cơ sở dữ liệu yếu kém thể hiện rủi ro tổ chức nghiêm trọng ở nhiều cấp độ.

* Rủi ro pháp lý - Các tổ chức có cơ chế kiểm toán cơ sở dữ liệu yếu (hoặc đôi khi không tồn tại) sẽ ngày càng thấy rằng họ mâu thuẫn với các yêu cầu quy định của chính phủ. Sarbanes-Oxley (SOX) trong lĩnh vực dịch vụ tài chính và Trách nhiệm giải trình và cung cấp thông tin chăm sóc sức khỏe

Đạo luật (HIPAA) trong lĩnh vực chăm sóc sức khỏe chỉ là hai ví dụ về quy định của chính phủ với các yêu cầu kiểm toán cơ sở dữ liệu rõ ràng.

* Răn đe – Giống như máy quay video ghi lại khuôn mặt của các cá nhân vào ngân hàng, cơ chế kiểm toán cơ sở dữ liệu phục vụ để ngăn chặn những kẻ tấn công biết rằng theo dõi kiểm toán cơ sở dữ liệu cung cấp cho các nhà điều tra pháp y liên kết những kẻ xâm nhập với tội phạm.
* Phát hiện và phục hồi - Các cơ chế kiểm toán đại diện cho tuyến bảo vệ cơ sở dữ liệu cuối cùng. Nếu kẻ tấn công tìm cách phá vỡ các biện pháp phòng thủ khác, dữ liệu kiểm toán có thể xác định sự tồn tại của vi phạm sau khi thực tế. Dữ liệu kiểm toán sau đó có thể được sử dụng để liên kết vi phạm với một người dùng cụ thể và / hoặc sửa chữa hệ thống.
  1. - Từ chối dịch vụ Từ chối dịch vụ (DOS) là một loại tấn công chung, trong đó quyền truy cập vào các ứng dụng mạng hoặc dữ liệu bị từ chối cho người dùng dự định. Các điều kiện từ chối dịch vụ (DOS) có thể được tạo ra thông qua nhiều kỹ thuật - nhiều trong số đó có liên quan đến các lỗ hổng đã đề cập trước đó. Ví dụ, DOS có thể đạt được bằng cách tận dụng lỗ hổng nền tảng cơ sở dữ liệu để làm sập máy chủ. Các kỹ thuật DOS phổ biến khác bao gồm hỏng dữ liệu, ngập mạng và quá tải tài nguyên máy chủ (bộ nhớ, CPU, v.v.). Quá tải tài nguyên đặc biệt phổ biến trong môi trường cơ sở dữ liệu. Các động lực đằng sau DOS cũng đa dạng tương tự. Các cuộc tấn công DOS thường liên quan đến lừa đảo tống tiền, trong đó kẻ tấn công từ xa sẽ liên tục làm sập máy chủ cho đến khi nạn nhân gửi tiền vào tài khoản ngân hàng quốc tế. Ngoài ra, DOS có thể được bắt nguồn từ nhiễm giun. Dù nguồn là gì, DOS đại diện cho một mối đe dọa nghiêm trọng đối với nhiều tổ chức.

* 1. Các lỗ hổng giao thức truyền thông cơ sở dữ liệu Ngày càng có nhiều lỗ hổng bảo mật được xác định trong các giao thức truyền thông cơ sở dữ liệu của tất cả các nhà cung cấp cơ sở dữ liệu. Bốn trong số bảy bản sửa lỗi bảo mật trong hai IBM DB2 FixPacks gần đây nhất giải quyết các lỗ hổng giao thức1. Tương tự, 11 trong số 23 lỗ hổng cơ sở dữ liệu được sửa trong bản vá hàng quý gần đây nhất của Oracle liên quan đến các giao thức. Hoạt động gian lận nhắm vào các lỗ hổng này có thể bao gồm từ truy cập dữ liệu trái phép, tham nhũng dữ liệu, từ chối dịch vụ. Ví dụ, sâu SQL Slammer2 đã lợi dụng một lỗ hổng trong giao thức Microsoft SQL Server để buộc từ chối dịch vụ. Để làm cho vấn đề tồi tệ hơn, không có hồ sơ nào về các vectơ gian lận này sẽ tồn tại trong dấu vết kiểm toán gốc vì các hoạt động giao thức không được bao phủ bởi các cơ chế kiểm tra cơ sở dữ liệu gốc.

Ngăn chặn các cuộc tấn công giao thức truyền thông cơ sở dữ liệu Các cuộc tấn công giao thức truyền thông cơ sở dữ liệu có thể bị đánh bại bằng công nghệ thường được gọi là Xác thực giao thức. Công nghệ xác thực giao thức về cơ bản phân tích cú pháp (tháo rời) lưu lượng cơ sở dữ liệu và so sánh nó với mong đợi. Trong trường hợp lưu lượng truy cập trực tiếp không phù hợp với mong đợi, các hành động cảnh báo hoặc chặn có thể được thực hiện. Xác thực giao thức truyền thông cơ sở dữ liệu của Secure Sphere kiểm tra và bảo vệ chống lại các mối đe dọa giao thức bằng cách so sánh các giao thức truyền thông cơ sở dữ liệu trực tiếp với các cấu trúc giao thức dự kiến. Không có giải pháp kiểm toán hoặc bảo mật cơ sở dữ liệu nào khác cung cấp khả năng này. Nó có nguồn gốc thông qua Imperva Application Defense

**1.10**: Các chương trình xác thực yếu cho phép kẻ tấn công giả định danh tính của người dùng cơ sở dữ liệu hợp pháp bằng cách đánh cắp hoặc lấy thông tin đăng nhập. Kẻ tấn công có thể sử dụng bất kỳ số lượng chiến lược nào để có được thông tin đăng nhập.

* Brute Force - Kẻ tấn công liên tục nhập các kết hợp tên người dùng / mật khẩu cho đến khi anh ta tìm thấy một kết hợp hoạt động. Quá trình vũ phu có thể liên quan đến phỏng đoán đơn giản hoặc liệt kê có hệ thống tất cả các kết hợp tên người dùng / mật khẩu có thể. Thường thì kẻ tấn công sẽ sử dụng các chương trình tự động để đẩy nhanh quá trình vũ phu.
* Kỹ thuật xã hội – Một kế hoạch trong đó kẻ tấn công lợi dụng xu hướng tự nhiên của con người để tin tưởng để thuyết phục người khác cung cấp thông tin đăng nhập của họ. Ví dụ: kẻ tấn công có thể tự giới thiệu qua điện thoại với tư cách là người quản lý CNTT và yêu cầu thông tin đăng nhập cho mục đích "bảo trì hệ thống".
* Đánh cắp thông tin xác thực trực tiếp – Kẻ tấn công có thể đánh cắp thông tin đăng nhập bằng cách sao chép ghi chú sau đó, tệp mật khẩu, nghiên cứu đang diễn ra của etcCenter (ADC) về các giao thức truyền thông cơ sở dữ liệu độc quyền và các lỗ hổng. Các nhà cung cấp cơ sở dữ liệu và ứng dụng bao gồm Oracle, Microsoft và IBM đã ghi nhận ADC với việc phát hiện ra các lỗ hổng nghiêm trọng và các kỹ thuật giảm thiểu đã dẫn đến tăng cường bảo mật trong các sản phẩm của họ. Dựa trên nghiên cứu này, Imperva có thể kết hợp kiến thức giao thức chưa từng có vào Secure Sphere.

**1.11:** Phương tiện lưu trữ cơ sở dữ liệu sao lưu thường hoàn toàn không được bảo vệ khỏi bị tấn công. Kết quả là, một số vi phạm bảo mật cao cấp đã liên quan đến hành vi trộm cắp băng sao lưu cơ sở dữ liệu và đĩa cứng. Tất cả các bản sao lưu cơ sở dữ liệu phải được mã hóa. Trên thực tế, một số nhà cung cấp đã gợi ý rằng các sản phẩm DBMS trong tương lai có thể không hỗ trợ tạo các bản sao lưu không được mã hóa. Mã hóa thông tin cơ sở dữ liệu sản xuất trực tuyến thường được đề xuất, nhưng những hạn chế về hiệu suất và quản lý khóa mật mã thường làm cho điều này không thực tế và thường được thừa nhận là một sự thay thế kém cho các kiểm soát đặc quyền chi tiết được mô tả ở trên.

# 2. KỸ THUẬT BẢO MẬT CƠ SỞ DỮ LIỆU

Để thực hiện bất kỳ giải pháp bảo mật nào cho một hệ thống máy tính, tổ chức phải đảm bảo ba khía cạnh là chính sách, cơ chế và đảm bảo. Các yêu cầu phải được thực hiện trong phần cứng, phần mềm và bên ngoài hệ thống máy tính được xác định theo chính sách. Cơ chế phù hợp để thực hiện các yêu cầu được thảo luận trong chính sách là điều không thể thiếu để một tổ chức có giải pháp bảo mật tính toán tốt. Đảm bảo là để đảm bảo rằng cơ chế đáp ứng các yêu cầu chính sách của tổ chức [1].

Những người dùng khác nhau có quyền truy cập khác nhau trên các đối tượng cơ sở dữ liệu khác nhau. Cơ chế kiểm soát truy cập liên quan đến việc quản lý quyền truy cập. Đây là kỹ thuật cơ bản để bảo vệ các đối tượng dữ liệu trong cơ sở dữ liệu và được hỗ trợ bởi hầu hết các DBMS [2]. Sau đó, một số kỹ thuật để chiến đấu với SQLIA được thảo luận trong bài báo.

## A. Cơ chế kiểm soát truy cập

Cơ chế kiểm soát truy cập là một kỹ thuật để duy trì tính bảo mật dữ liệu. Khi ai đó cố gắng truy cập đối tượng dữ liệu, Cơ chế kiểm soát truy cập sẽ kiểm tra quyền của người dùng đối với bộ ủy quyền. Chúng thường được chỉ định bởi quản trị viên bảo mật hoặc nhân viên an ninh. Ủy quyền được đưa ra theo chính sách bảo mật của tổ chức.

Cùng với cơ chế kiểm soát ra vào, một mạnh mẽ

Cơ chế xác thực cũng được yêu cầu để xác thực người dùng hợp lệ của hệ thống cơ sở dữ liệu. Sau đó, kiểm soát truy cập sẽ giúp xác định các quyền truy cập khác nhau trên các đối tượng dữ liệu khác nhau của cơ sở dữ liệu [2].

Có một số mô hình được đề xuất để kiểm soát truy cập trong các hệ thống cơ sở dữ liệu quan hệ. Các mô hình này đưa ra các cách tiếp cận để thực hiện kiểm soát truy cập trong cơ sở dữ liệu.

**1) Mô hình kiểm soát truy cập tùy ý:** Theo cách tiếp cận này, tùy thuộc vào quy tắc nhận dạng và ủy quyền của người dùng, quyền truy cập được cấp cho các đối tượng dữ liệu theo một số chính sách tùy ý. Ưu điểm chính ở đây là người dùng có thể cấp ủy quyền trên các đối tượng dữ liệu cho người dùng khác. Vì tính linh hoạt như vậy, đây là kỹ thuật được sử dụng rộng rãi trong nhiều tổ chức. Các thực thể hoạt động như người dùng trong hệ thống bảo mật cũng được gọi là chủ thể.

Quản lý ủy quyền là chức năng cấp và thu hồi ủy quyền. Vì vậy, bằng cách quản lý ủy quyền, ủy quyền được nhập vào hoặc loại bỏ khỏi cơ chế kiểm soát truy cập. Có hai loại chính quyền như vậy: Quản trị tập trung là loại hình quản trị trong đó một số đối tượng hoặc người dùng đặc quyền có thể cấp hoặc thu hồi ủy quyền. Quản trị quyền sở hữu là quyền quản lý trong đó người tạo đối tượng cấp và thu hồi quyền truy cập vào đối tượng. Chủ sở hữu có thể cấp cho người dùng khác quyền cấp hoặc thu hồi một số hoặc tất cả quyền truy cập vào đối tượng trong quản lý quyền sở hữu.

**2. Kiểm soát truy cập dựa trên nội dung:** Trong mô hình này, các quyết định kiểm soát truy cập phải dựa trên nội dung của dữ liệu [6]. Ví dụ: Bảng khách hàng có thông tin của tất cả các khách hàng của công ty. Vì vậy, chỉ những nhân viên, những người có liên quan đến các dự án về những khách hàng đó, mới có quyền truy cập vào những khách hàng đó. Cách tiếp cận này thường được thực hiện bằng cách sử dụng các chế độ xem. Chế độ xem bảo vệ được sử dụng để hỗ trợ kiểm soát truy cập dựa trên nội dung. Chế độ xem tốc ký được sử dụng để đơn giản hóa việc viết truy vấn. Chính sách truy cập ở đây có thể được thể hiện bằng ngôn ngữ cấp cao. Các sửa đổi được thực hiện trong dữ liệu không yêu cầu thay đổi chính sách kiểm soát truy cập. Nếu dữ liệu mới được chèn đáp ứng một số chính sách, thì nó sẽ tự động được trả về như một phần của dữ liệu được trả về bởi chế độ xem tương ứng [2].

**3. Kiểm soát truy cập hạt mịn:** Cơ chế này hỗ trợ kiểm soát truy cập ở cấp độ tuple [2]. Do đó, tên là Kiểm soát truy cập hạt mịn. Nó cho phép mức độ kiểm soát truy cập chi tiết. Để thực hiện một sơ đồ như vậy, nó đòi hỏi phải chuyên môn hóa các quan điểm. Cơ sở dữ liệu riêng ảo Oracle và mô hình Truman là những ví dụ thực hiện cơ chế truy cập như vậy [2].

**4) Mô hình kiểm soát truy cập bắt buộc:**  Kiểm soát truy cập bắt buộc dựa trên việc phân loại các đối tượng dữ liệu và người dùng [5][6]. Phân loại dựa trên tập hợp các lớp được sắp xếp theo thứ tự một phần được gọi là các lớp truy cập.

Lớp Access chứa Security level và tập hợp các category. Mức độ bảo mật thể hiện độ nhạy cảm của thông tin [5][6]. Kiểm soát truy cập trong mô hình truy cập này dựa trên hai nguyên tắc sau. Không đọc lên: Người dùng chỉ có thể đọc những đối tượng dữ liệu có lớp truy cập bị chi phối bởi lớp truy cập của người dùng. Không ghi xuống: Người dùng chỉ có thể viết những đối tượng dữ liệu có lớp truy cập thống trị các lớp truy cập của người dùng.

Các nguyên tắc này hạn chế luồng dữ liệu nhạy cảm vào các đối tượng dữ liệu ở các lớp truy cập thấp hơn hoặc không thể so sánh được [6]. Có các khái niệm cơ sở dữ liệu nâng cao như cơ sở dữ liệu quan hệ đối tượng và cơ sở dữ liệu dựa trên đối tượng. Các cơ chế kiểm soát truy cập này được sửa đổi để phù hợp với các cơ sở dữ liệu này. Thậm chí một số mô hình được đề xuất cho dữ liệu XML [5][6]. **B. Kỹ thuật chiến đấu với SQLIA**

Như đã thảo luận trước đó, SQLIA là cuộc tấn công nguy hiểm nhất vào cơ sở dữ liệu. Phần này thảo luận về một số kỹ thuật để phát hiện và ngăn chặn SQLIA. Các phương pháp phát hiện cho SQLIA có thể được phân loại rộng rãi thành các phương pháp tiếp cận được tạo trước và sau khi tạo. Các phương pháp tiếp cận sau tạo thường hữu ích trong khi phân tích SQL động được tạo bởi ứng dụng web. Các phương pháp được tạo sẵn thường được sử dụng trong giai đoạn thử nghiệm của ứng dụng web. Một số cách tiếp cận được tạo bài đăng là [3]**: Đánh giá nhận biết cú pháp tích cực:** Ở đây, các chuỗi đầu vào hợp lệ ban đầu được cung cấp cho hệ thống để phát hiện SQLIA. Nó phân loại các chuỗi đầu vào và truyền các chuỗi không đáng tin cậy một cách nhanh chóng. Đánh giá nhận biết cú pháp được thực hiện trên các chuỗi được lan truyền để quyết định các chuỗi không đáng tin cậy. Đánh giá cú pháp được thực hiện tại điểm tương tác cơ sở dữ liệu. Có một số vấn đề với phương pháp này. Việc khởi tạo các chuỗi tin cậy phụ thuộc vào nhà phát triển và việc lưu trữ các chuỗi đáng tin cậy có thể dẫn đến một cuộc tấn công khác.

**Đánh giá chuỗi nhạy cảm với ngữ cảnh:** Ở đây bất kỳ dữ liệu nào do người dùng cung cấp đều được coi là không đáng tin cậy và dữ liệu do ứng dụng cung cấp được coi là đáng tin cậy. Siêu dữ liệu không đáng tin cậy được sử dụng để phân tích cú pháp. Phân tích cú pháp này phân biệt hằng số chuỗi và số. Sau đó, tất cả các ký tự không an toàn sẽ bị xóa khỏi số nhận dạng chữ và số. Một số vấn đề trong cách tiếp cận này là khởi tạo các ký tự không an toàn phụ thuộc vào nhà phát triển và việc loại bỏ các ký tự không an toàn hạn chế chức năng ứng dụng.

**Đánh giá cây phân tích cú pháp dựa trên ngữ pháp:** Trong phương pháp này, các truy vấn SQL được tạo từ đầu vào của người dùng được phân tích cú pháp bằng ngữ pháp được xác định trước.

## C. Mã hóa dữ liệu

Đây là kỹ thuật cơ bản được sử dụng để bảo mật bất kỳ loại thông tin hoặc dữ liệu nào. Vì vậy, kỹ thuật này thậm chí có thể được áp dụng cho cơ sở dữ liệu.



**Hình: 1**

Trong khi thực hiện mã hóa cơ sở dữ liệu, phải đưa ra quyết định về việc thực hiện mã hóa bên trong hay bên ngoài cơ sở dữ liệu. Một số vấn đề liên quan đến kỹ thuật này là: Làm thế nào để bảo mật khóa khỏi kẻ tấn công hệ thống? Làm thế nào để cấp quyền quản trị thao tác dữ liệu bằng khóa? Và Làm thế nào để cung cấp quyền truy cập hạn chế cho các khóa?

Các khía cạnh quan trọng cần được xem xét trong khi mã hóa cơ sở dữ liệu là làm thế nào để quản lý các khóa mã hóa. Một số khía cạnh liên quan đến vấn đề này là Số lượng khóa mã hóa cần thiết, lưu trữ khóa, bảo vệ quyền truy cập khóa và tần suất thay đổi khóa Cách tiếp cận được đề xuất để lưu trữ khóa là, tách khóa và dữ liệu nằm trong cơ sở dữ liệu. Nói chung, các khóa được lưu trữ trong phần cứng như các tệp bị hạn chế truy cập hoặc mô-đun lưu trữ phần cứng. Quá trình mã hóa có thể được thực hiện trong cơ sở dữ liệu hoặc bên ngoài cơ sở dữ liệu. Nhưng có những đánh đổi về hiệu suất và bảo mật cần được xem xét khi thực hiện chính sách này. Nếu mã hóa được thực hiện trong cơ sở dữ liệu, thì sẽ có ít tác động hơn đến môi trường ứng dụng. Hiểu thuật toán mã hóa được hỗ trợ bởi DBMS cũng đóng vai trò quan trọng trong khi đưa ra chiến lược để thực hiện kỹ thuật này. Hạn chế của phương pháp này là các khóa mã hóa cũng được lưu trữ trong cùng một cơ sở dữ liệu.

Một cách khác để thực hiện mã hóa trong cơ sở dữ liệu là thực hiện nó trên các máy chủ mã hóa riêng biệt. Tính toán mã hóa và giải mã được thực hiện máy chủ mã hóa. Vì vậy, ở đây chi phí mã hóa được loại bỏ khỏi DBMS và chuyển sang các máy chủ mã hóa riêng biệt để duy trì hiệu suất của DBMS. Khóa mã hóa và dữ liệu cũng có thể được tách ra. Cách tiếp cận này thường được tuân theo trong khi mã hóa cơ sở dữ liệu [4]. Các thuật toán thường được sử dụng để mã hóa cơ sở dữ liệu và thường được DBMS hỗ trợ là DES, Triple DES, RC2, RC4, DESX và AES.

Có nhiều cấu hình khác nhau có sẵn để mã hóa và giải mã cơ sở dữ liệu. Một số trong số chúng được liệt kê dưới đây

[2].

**Mã hóa hệ thống tệp:** Ở đây đĩa vật lý nơi cơ sở dữ liệu cư trú được mã hóa. Toàn bộ cơ sở dữ liệu được mã hóa bằng khóa mã hóa duy nhất nên không thể thực hiện kiểm soát truy cập tùy ý.

**Mã hóa cấp độ DBMS:** Có nhiều sơ đồ cho loại mã hóa này. Một lược đồ dựa trên định lý Phần dư Trung Quốc, trong đó mỗi hàng được mã hóa bằng các khóa con khác nhau cho các ô khác nhau. Vì vậy, mã hóa ở cấp độ hàng và giải mã ở cấp độ tế bào hoặc trường là có thể bằng sơ đồ này.

Có một số sơ đồ dựa trên đa thức nội suy của Newton được sử dụng để mã hóa cơ sở dữ liệu.

Có một lược đồ SPDE mã hóa từng ô I cơ sở dữ liệu với tọa độ ô của nó như tên bảng, tên cột và id hàng, v.v. Vì vậy, trong sơ đồ này, các cuộc tấn công rò rỉ tĩnh và các cuộc tấn công nối được ngăn chặn.

**Mã hóa cấp ứng dụng:** Trong kỹ thuật này, một phần mềm trung gian được đề xuất để dịch các truy vấn do người dùng kích hoạt thành một loạt các truy vấn mới sẽ thực thi trên cơ sở dữ liệu được mã hóa. Kỹ thuật này đã được thực hiện trong Hệ thống bảo vệ dữ liệu. **Mã hóa phía máy khách***:* Kỹ thuật này thường được sử dụng trong trường hợp ―Cơ sở dữ liệu như một kịch bản dịch vụǁ trong đó toàn bộ cơ sở dữ liệu được tổ chức thuê ngoài để giảm chi phí bảo trì. Vì vậy, ở đây quyền riêng tư dữ liệu là mối quan tâm lớn. Mã hóa là giải pháp cơ bản trong trường hợp này.  **Lập chỉ mục dữ liệu được mã hóa***:* Có nhiều cơ chế lập chỉ mục được đề xuất. Cấu trúc chỉ mục cây B được chuẩn bị trên các giá trị văn bản thuần túy trong bảng và sau đó mã hóa bảng được thực hiện ở cấp độ hàng. Mã hóa Btree được thực hiện ở cấp nút.

## D. Xáo trộn dữ liệu

Xáo trộn dữ liệu là một quá trình làm cho thông tin nhạy cảm trong cơ sở dữ liệu phi sản xuất an toàn để có khả năng hiển thị rộng hơn [5][6]. Xáo trộn dữ liệu còn được gọi là vệ sinh dữ liệu, che giấu dữ liệu và xáo trộn dữ liệu.

Xáo trộn dữ liệu thường được sử dụng khi người dùng có quyền truy cập thích hợp vào dữ liệu trong cơ sở dữ liệu nhưng vẫn cần phải bảo mật thông tin nhạy cảm khỏi họ. Ví dụ về những người dùng như vậy có thể là nhà phát triển hoặc người thử nghiệm bên thứ ba làm việc trên dữ liệu trong cơ sở dữ liệu. Vì vậy, các giá trị của dữ liệu nhạy cảm được thay đổi nhưng các giá trị vẫn thực tế về bản chất.

## E. Các kỹ thuật khác để bảo mật cơ sở dữ liệu

Để tránh các vấn đề suy luận trong cơ sở dữ liệu, kỹ thuật khởi tạo poly có thể được sử dụng. Trong phương pháp này, nhiều trường hợp của cùng một dữ liệu được cho phép nhưng việc phân loại dữ liệu đó phải khác nhau. Nó có ảnh hưởng đến các mối quan hệ, bộ dữ liệu và các yếu tố dữ liệu. Các mối quan hệ với poly instantiation là quan hệ với các lớp truy cập khác nhau. Có hai loại khởi tạo poly là khởi tạo poly hữu hình và vô hình. Khi người dùng cao hơn chèn dữ liệu vào trường có dữ liệu thấp, dữ liệu cao được nhập dưới dạng bộ dữ liệu mới trong quá trình khởi tạo poly có thể nhìn thấy. Khi người dùng thấp chèn dữ liệu vào trường đã có dữ liệu cao, dữ liệu thấp sẽ được nhập dưới dạng bộ dữ liệu mới. Điều này được gọi là khởi tạo poly vô hình [7].

Kiểm toán là một kỹ thuật khác có thể được sử dụng để chống lại cuộc tấn công suy luận vào cơ sở dữ liệu. Lịch sử của tất cả các truy vấn do người dùng kích hoạt được duy trì theo phương pháp này. Phân tích các truy vấn như vậy có thể giúp tìm kiếm cuộc tấn công suy luận và có thể tránh được trong giai đoạn sau. Nhưng cách tiếp cận này phát hiện các trường hợp tấn công suy luận rất hạn chế và khó thực hiện trên thực tế [7].

# KẾT THÚC

Cơ sở dữ liệu tạo thành xương sống của nhiều ứng dụng ngày nay. Chúng là hình thức lưu trữ chính cho nhiều tổ chức. Vì vậy, các cuộc tấn công vào cơ sở dữ liệu cũng đang gia tăng vì chúng là hình thức tấn công rất nguy hiểm. Chúng tiết lộ dữ liệu quan trọng hoặc quan trọng cho kẻ tấn công. Các cuộc tấn công khác nhau vào cơ sở dữ liệu được thảo luận trong bài báo này. Xem xét một số kỹ thuật bảo mật cơ sở dữ liệu quan trọng như kiểm soát truy cập, kỹ thuật chống lại SQLIA, mã hóa và xáo trộn dữ liệu được thảo luận. Ngay cả một số lĩnh vực nghiên cứu trong tương lai trong lĩnh vực bảo mật cơ sở dữ liệu cũng được thảo luận trong bài báo này. Nghiên cứu này sẽ dẫn đến giải pháp cụ thể hơn cho vấn đề bảo mật cơ sở dữ liệu.

# THAM KHẢO

[1] SushilJajodia, ―Database security and Privacyǁ, ACM Computing Surveys, Vol. 28, No.1, March 1996

[2] Elisa Bertino, Ravi sandhu, ―Database Security- Concepts, Approach and Challenges, IEEE Transactions on Dependable and Secure Computing, Vol 2, No 1, January-March 2005

1. Debasish Das, Utpal Sharma, D.K. Bhattacharyya, ―An Approach to detection of SQL Injection Attack Based on Dynamic Query Matching, International Journal of Computer Applications (09758887), vol 1 –No 25, page no 28-34.
2. RSA Security Inc., **"**Securing Data at Rest: Developing a Database Encryption Strategy, A White Paper for developers, e-business managers and ITǁ, Website, September 7 2012,

http://www.rsa.com/products/bsafe/whitepapers/DDES\_WP\_0702.p DF

1. A NET 2000 Ltd., **"**Vấn đề xáo trộn dữ liệuǁ, Sách trắng (2010),

Trang mạng, Tháng 10 10 2012,

http://www.datamasker.com/datascramblingissues.pdf

1. Huw Price, **"**Hướng dẫn ngắn về xáo trộn, che giấu và làm xáo trộn dữ liệu sản xuất, Công cụ lướiǁ Sách trắng, Trang web,

Tháng 10 15 2012, http://www.grid-

tools.com/download/Data\_Masking.pdf

1. Ravi S Sandhu, SushilJajodia, ―Bảo mật và kiểm soát dữ liệu và cơ sở dữ liệuǁ, Sổ tay quản lý bảo mật, Nhà xuất bản Auerbach,

1993, trang 481-499