UNIVERSITY LƯƠNG THẾ VINH

e-ISSN: 3093 – 3145

Tạp chí Khoa học và Công nghệ Y khoa, 2025, 02, 028-032

ĐÁNH GIÁ LỖ HỔNG VÀ ĐỀ XUẤT GIẢI PHÁP TĂNG CƯỜNG BẢO MẬT CƠ SỞ DỮ LIỆU TRONG SQL SERVER

Trần Thái Sơn[1], Trần Bình Thành[2*]

[1] Trường Trung học Cơ sở Hạ Hoà, 114 Đường Hùng Vương, Khu 7, Xã Hạ Hoà, tỉnh Phú Thọ

*[2]*Trường Đại học Lương Thế Vinh, Đường Cầu Đông, Phường Nam Định, Tỉnh Ninh Bình, Việt Nam*

Tác giả liên hệ: *tranbinhthanh@ltvu.edu.vn*

THÔNG TIN BÀI BÁO

Ngày nhận: 03/11/2025

Ngày hoàn thiện: 20/11/2025

Ngày chấp nhận: 29/11/2025

Ngày đăng: 06/12/2025

TỪ KHÓA

Bảo mật SQL Server;
Mã hóa dữ liệu;
SQL Injection;
Kiểm toán cơ sở dữ liệu;
Quản lý truy cập.

TÓM TẮT

Bảo mật cơ sở dữ liệu đóng vai trò then chốt trong việc duy trì tính toàn vẹn và bảo vệ thông tin nhạy cảm của các tổ chức. Nghiên cứu này tập trung đánh giá các lỗ hổng bảo mật phổ biến trong môi trường SQL Server, bao gồm các vấn đề về xác thực, phân quyền, mã hóa dữ liệu, kiểm toán và che giấu dữ liệu động. Trên cơ sở đó, bài báo đề xuất một số giải pháp kỹ thuật và thực hành tốt nhất nhằm tăng cường khả năng phòng vệ trước các mối đe dọa tấn công. Kết quả nghiên cứu góp phần cung cấp cơ sở khoa học và định hướng ứng dụng cho việc xây dựng hệ thống cơ sở dữ liệu SQL Server an toàn và tin cậy hơn.

ASSESSMENT OF VULNERABILITIES AND PROPOSED SOLUTIONS TO ENHANCE DATABASE SECURITY IN SQL SERVER

Son Thai Tran[1], Thanh Tran Binh[2*]

Ha Hoa Lower Secondary School, 114 Hung Vuong Street, Area 7, Ha Hoa Commune, Phu Tho Province, Viet Nam

Luong The Vinh University, Cau Dong Street, Nam Dinh Ward, Ninh Binh Province, Viet Nam

*Corresponding Author: *tranbinhthanh@ltvu.edu.vn*

ARTICLE INFO

Received: Nov 03nd, 2025

Revised: Nov 20th, 2025

Accepted: Nov 29th, 2025

Published: Dec 06th, 2025

KEYWORDS

SQL Server security;
data encryption;
SQL Injection;
database auditing;
access management.

ABSTRACT

Database security plays a crucial role in maintaining data integrity and protecting sensitive information within organizations. This study evaluates common security vulnerabilities in SQL Server environments, focusing on issues such as authentication, authorization, data encryption, auditing, and dynamic data masking. Based on the analysis, the paper proposes several technical measures and best practices to enhance defensive capabilities against potential attacks. The findings provide scientific insights and practical guidance for developing more secure and reliable SQL Server database systems.

1. Giới Thiệu

Trong bối cảnh chuyển đổi số diễn ra mạnh mẽ, cơ sở dữ liệu giữ vai trò trọng tâm trong hầu hết các hệ thống thông tin hiện đại, đảm nhận chức năng lưu trữ, xử lý và truy xuất dữ liệu phục vụ cho hoạt động của tổ chức. Trong số các hệ quản trị cơ sở dữ liệu quan hệ (RDBMS), Microsoft SQL Server là một trong những nền tảng được ứng dụng rộng rãi nhờ khả năng tích hợp, hiệu năng cao và hỗ trợ toàn diện cho doanh nghiệp ở nhiều quy mô khác nhau.

Tuy nhiên, cùng với sự gia tăng về khối lượng và mức độ phức tạp của dữ liệu, các mối đe dọa bảo mật đối với hệ thống cơ sở dữ liệu cũng ngày càng đa dạng và tinh vi hơn. Các hình thức tấn công như SQL Injection, truy cập trái phép, khai thác lỗ hổng trong cấu hình hoặc truyền tải dữ liệu không an toàn có thể gây hậu quả nghiêm trọng, dẫn đến rò rỉ thông tin, thiệt hại tài chính và suy giảm uy tín tổ chức.

Bảo mật cơ sở dữ liệu không chỉ là vấn đề kỹ thuật thuần túy mà còn là một yếu tố chiến lược trong quản trị rủi ro và tuân thủ quy định về an toàn thông tin. Đặc biệt, đối với các tổ chức phụ thuộc nhiều vào SQL Server trong vận hành và quản lý dữ liệu, việc thiếu cơ chế bảo mật phù hợp có thể khiến hệ thống dễ bị tổn thương trước các cuộc tấn công mạng ngày càng tinh vi.

Trước thực tế đó, bài báo này hướng đến đánh giá các lỗ hổng bảo mật phổ biến trong môi trường SQL Server, đồng thời đề xuất các giải pháp kỹ thuật và thực hành tốt nhất nhằm tăng cường mức độ an toàn và bảo vệ toàn diện dữ liệu. Nghiên cứu kỳ vọng mang lại cái nhìn hệ thống, giúp các tổ chức nâng cao năng lực phòng thủ và quản trị an ninh thông tin trong hệ quản trị SQL Server.

2. Các lỗ hổng bảo mật thường gặp trong SQL Server

Bất chấp các tính năng bảo mật được tích hợp sẵn, SQL Server vẫn chịu rủi ro từ nhiều lỗ hổng do cấu hình kém, sai sót trong thiết kế ứng dụng, hoặc do thiếu quy trình quản trị phù hợp. Phần này trình bày các nhóm lỗ hổng thường gặp, kèm ví dụ minh họa và hệ quả thực tế.

2.1 Xác thực và phân quyền yếu kém

Hệ thống xác thực và phân quyền là lớp bảo vệ cơ bản nhằm đảm bảo chỉ những chủ thể được ủy quyền mới có khả năng truy cập và thao tác trên dữ liệu. Tuy nhiên, các thực tiễn kém như sử dụng mật khẩu yếu, chia sẻ tài khoản, không áp dụng nguyên tắc quyền tối thiểu (least privilege) hoặc không thu hồi quyền khi nhân sự thay đổi, đều tạo điều kiện cho kẻ tấn công khai thác và leo thang đặc quyền. Một tài khoản có quyền cao (ví dụ: sysadmin) bị xâm nhập có thể dẫn tới việc toàn bộ cơ sở dữ liệu bị chiếm quyền hoặc dữ liệu bị xóa/đổi. Những rủi ro này thường xuất phát từ thiếu chính sách quản lý mật khẩu, không triển khai xác thực tích hợp (Windows/AD) hoặc thiếu cơ chế xác thực đa yếu tố cho các tài khoản quan trọng.

2.2 Tấn công SQL Injection

SQL Injection (SQLi) là một trong các mối đe dọa phổ biến và có tính tàn phá cao đối với các hệ quản trị cơ sở dữ liệu. Kẻ tấn công lợi dụng việc xử lý đầu vào không an toàn tại lớp ứng dụng để chèn hoặc thay đổi câu lệnh SQL, từ đó truy xuất, chỉnh sửa hoặc xóa dữ liệu trái phép, thậm chí thực thi lệnh hệ thống thông qua các hàm mở rộng. Nguyên nhân chính thường là do xây dựng truy vấn động nối chuỗi (string concatenation) thay vì sử dụng truy vấn tham số hoá (parameterized queries) hoặc stored procedures an toàn.

Truy vấn trên — khi nhận đầu vào không kiểm soát — có thể trả về kết quả hợp lệ mà không cần mật khẩu, dẫn tới đăng nhập trái phép.

2.3 Lỗ hổng trong truyền tải dữ liệu

Dữ liệu truyền qua mạng giữa máy chủ SQL và ứng dụng khách có thể bị chặn bắt (sniffing) hoặc thay đổi nếu không được bảo vệ bằng kênh an toàn. Việc không sử dụng SSL/TLS hoặc cấu hình sai các chứng chỉ, kết nối không riêng tư (unencrypted) sẽ mở ra khả năng tấn công MITM (man-in-the-middle), đặc biệt nguy hiểm khi dữ liệu truyền tải chứa thông tin nhạy cảm như số tài khoản, mã số định danh hoặc thông tin cá nhân.

2.4 Thiếu kiểm toán và giám sát

Kiểm toán và giám sát là thành phần thiết yếu để phát hiện, phân tích và phản ứng kịp thời với các sự kiện bảo mật. Nhiều tổ chức tắt hoặc không cấu hình đầy đủ các tính năng audit/logging trong SQL Server, khiến việc phát hiện các hoạt động bất thường (ví dụ: truy vấn dữ liệu nhạy cảm ngoài giờ, đăng nhập thất bại lặp lại, thay đổi quyền) trở nên khó khăn. Thiếu lịch sử hoạt động còn cản trở quá trình điều tra sự cố và tuân thủ các yêu cầu pháp lý.

2.5 Cấu hình sai các thiết lập bảo mật

Cấu hình mặc định hoặc việc bật các tính năng không cần thiết (ví dụ xp_cmdshell, dịch vụ SQL Server Browser mở cổng UDP, quyền quá rộng cho tài khoản dịch vụ) tạo ra bề mặt tấn công lớn hơn. Các sai sót trong cấu hình mạng, firewall, hoặc quyền hệ thống tập tin cũng góp phần làm tăng khả năng bị xâm nhập. Một số tính năng, nếu được kích hoạt không thận trọng, cho phép kẻ tấn công thực thi lệnh hệ thống hoặc leo thang quyền từ SQL Server lên hệ điều hành.

2.6 Tổng kết ngắn về các lỗ hổng

Những nhóm lỗ hổng nêu trên thường xuyên xuất hiện đồng thời trong cùng một hệ thống, khiến rủi ro tăng lên theo cấp số nhân. Việc chỉ khắc phục một điểm yếu đơn lẻ thường không đủ — cần tiếp cận toàn diện, kết hợp kỹ

thuật (mã hóa, kiểm soát truy cập, audit) và quản trị (chính sách mật khẩu, quản lý tài khoản, cập nhật bản vá). Phần tiếp theo sẽ trình bày các thực hành tốt nhất và kỹ thuật bảo mật tiên tiến nhằm giảm thiểu các lỗ hổng này.

3. Thực hành bảo mật SQL Server

Bảo mật trong SQL Server cần được tiếp cận theo nguyên tắc "phòng ngừa nhiều lớp" (defense in depth), trong đó mỗi lớp bảo vệ độc lập hỗ trợ và củng cố lẫn nhau. Các biện pháp kỹ thuật dưới đây được xem là thực hành tốt nhất (best practices) nhằm giảm thiểu rủi ro từ các lỗ hổng đã nêu, đồng thời đảm bảo tính toàn vẹn, bảo mật và khả dụng của hệ thống cơ sở dữ liệu.

3.1. Xác thực và phân quyền chặt chẽ

Cơ chế xác thực là tuyến phòng thủ đầu tiên quyết định quyền truy cập hệ thống. SQL Server hỗ trợ hai phương thức: Windows Authentication và SQL Server Authentication, trong đó nên ưu tiên Windows Authentication hoặc Active Directory (AD) để tận dụng chính sách mật khẩu mạnh, xác thực đa yếu tố (MFA) và quản lý tập trung. Thực hành tốt gồm: bật MFA cho tài khoản quản trị, áp dụng nguyên tắc phân quyền tối thiểu, rà soát và thu hồi quyền định kỳ, tránh dùng tài khoản SA trong vận hành.

3.2. Mã hóa dữ liệu ở mọi cấp độ

Mã hóa (Encryption) là cơ chế bảo vệ dữ liệu ngay cả khi bị truy cập trái phép. SQL Server hỗ trợ nhiều lớp mã hóa như Transparent Data Encryption (TDE) để mã hóa toàn bộ cơ sở dữ liệu, Always Encrypted để mã hóa dữ liệu ở cấp cột ngay từ phía ứng dụng khách, và Connection Encryption (SSL/TLS) để bảo vệ dữ liệu khi truyền tải. Thực hành tốt gồm: bật TDE cho cơ sở dữ liệu nhạy cảm, dùng Always Encrypted cho thông tin cá nhân hoặc tài chính, bắt buộc kết nối dùng TLS 1.2 trở lên, và lưu khóa mã hóa trong Azure Key Vault hoặc HSM.

3.3. Cập nhật và vá lỗ hổng định kỳ

Cập nhật và vá lỗi (Patch Management) là yếu tố quan trọng giúp duy trì hiệu suất và bảo mật hệ thống. Các bản cập nhật từ Microsoft không chỉ cải thiện hiệu năng mà còn khắc phục lỗ hổng nghiêm trọng — nhiều cuộc tấn công xảy ra do hệ thống chưa được vá kịp thời. Thực hành tốt gồm: thiết lập lịch cập nhật định kỳ, kiểm tra tương thích trước khi triển khai, dùng SQL Server Update Management hoặc WSUS để tự động quản lý bản vá, theo dõi cảnh báo từ Microsoft Security Response Center (MSRC) và đảm bảo bản vá Windows đồng bộ với SQL Server.

3.4. Củng cố và tăng cường bảo mật màng và firewall

Bảo mật mạng (Network Security) là lớp phòng thủ quan trọng cho SQL Server trong môi trường mạng phức tạp, nơi kẻ tấn công có thể quét cổng hoặc khai thác dịch vụ từ xa. Thực hành tốt gồm: giới hạn truy cập chỉ từ IP/subnet đáng tin cậy, tắt dịch vụ không cần thiết như SQL Browser, dùng VPN hoặc Azure Private Link cho truy cập từ xa, bật Windows Firewall và chỉ mở port cần thiết (mặc định 1433/TCP), đồng thời áp dụng Network Security Groups (NSG) trong môi trường đám mây.

3.5. Kiểm toán và giám sát an ninh

Kiểm toán (Auditing) giúp ghi nhận mọi hoạt động truy cập và thay đổi trong cơ sở dữ liệu, hỗ trợ phát hiện và ngăn chặn hành vi bất thường. SQL Server cung cấp các công cụ như SQL Server Audit, Extended Events, và Policy-Based Management. Thực hành tốt gồm: bật SQL Server Audit để theo dõi đăng nhập và thay đổi dữ liệu, tích hợp log với hệ thống SIEM (như Microsoft Sentinel hoặc Splunk), thiết lập cảnh báo cho hành vi đáng ngờ (đăng nhập thất bại, truy cập ngoài giờ, thay đổi quyền), và định kỳ phân tích nhật ký để phát hiện xu hướng tấn công.

4. Các kỹ thuật bảo mật

4.1. Bảo mật cấp hàng (Row-Level Security - RLS)

RLS cho phép áp dụng các chính sách truy cập tùy chỉnh cho từng hàng dữ liệu, giúp kiểm soát chi tiết hơn và giảm thiểu nguy cơ truy cập trái phép.

Ví dụ: Trong một hệ thống quản lý nhân sự, nhân viên chỉ có thể xem dữ liệu cá nhân của họ, trong khi quản lý có thể xem thông tin của toàn bộ nhân viên. Cách triển khai Row-Level Security trong SQL Server như sau:

Bước 1: Tạo bảng dữ liệu

```
CREATE TABLE EmployeeData (
    EmployeeID INT PRIMARY KEY,
    EmployeeName NVARCHAR(100),
    Department NVARCHAR(50),
    ManagerID INT
);
```

Bước 2: Tạo hàm bảo mật

```
CREATE FUNCTION
dbo.fn_RLS_EmployeeSecurity(@ManagerID INT)
RETURNS TABLE
WITH SCHEMABINDING
AS
RETURN
(
    SELECT 1 AS AccessResult
    WHERE @ManagerID = USER_ID()
      OR USER_ID() IN (SELECT ManagerID FROM
EmployeeData)
);
```

Bước 3: Tạo chính sách bảo mật.

```
CREATE SECURITY POLICY
```

EmployeeSecurityPolicy
ADD FILTER PREDICATE
dbo.fn_RLS_EmployeeSecurity(ManagerID)
ON dbo.EmployeeData
WITH (STATE = ON);

Bước 4: Kiểm tra hoạt động

Khi nhân viên đăng nhập và truy vấn bảng EmployeeData, SQL Server chỉ trả về dữ liệu tương ứng với tài khoản của họ.

Người quản lý có thể truy cập toàn bộ dữ liệu của nhân viên dưới quyền mà không cần quyền truy vấn bổ sung.

4.2. Always Encrypted trong SQL Server

Always Encrypted là cơ chế mã hóa cấp cột được Microsoft giới thiệu từ SQL Server 2016, cho phép dữ liệu được mã hóa và giải mã ngay tại ứng dụng khách (client) thay vì tại máy chủ. Cách tiếp cận này giúp đảm bảo dữ liệu luôn ở trạng thái mã hóa trong quá trình lưu trữ, xử lý và truyền tải, kể cả khi cơ sở dữ liệu bị truy cập trái phép.

Nguyên lý hoạt động

Always Encrypted sử dụng hai loại khóa:

Column Master Key (CMK): lưu trữ an toàn trong kho khóa ngoài (như Windows Certificate Store hoặc Azure Key Vault).

Column Encryption Key (CEK): được SQL Server quản lý và mã hóa bằng CMK.

Ứng dụng khách sử dụng trình điều khiển (driver) hỗ trợ Always Encrypted để mã hóa dữ liệu trước khi gửi đến SQL Server và tự động giải mã khi nhận lại kết quả, giúp DBA hoặc tin tặc không thể đọc dữ liệu ở dạng rõ (plaintext).

4.3. Phát hiện và ngăn chặn tấn công tự động trong SQL Server

Trong môi trường vận hành hiện đại, SQL Server thường là mục tiêu của nhiều dạng tấn công tự động như SQL Injection, Brute Force Login, hay DoS/DDoS, gây tổn thất nghiêm trọng về dữ liệu và hiệu suất hệ thống. Để giảm thiểu rủi ro, SQL Server được trang bị các cơ chế phát hiện và phòng vệ chủ động, cho phép giám sát, cảnh báo và ngăn chặn hành vi tấn công theo thời gian thực.

4.3.1. Microsoft Defender for SQL

Là giải pháp bảo mật tích hợp của Microsoft Azure, Defender for SQL sử dụng công nghệ phân tích hành vi và học máy để:

- Phát hiện hoạt động bất thường, chẳng hạn như truy vấn độc hại hoặc SQL Injection.
- Tự động gửi cảnh báo và đề xuất biện pháp khắc phục.
- Phân tích log để xác định mẫu tấn công và đề xuất cải thiện cấu hình bảo mật.

Nhờ khả năng hoạt động thời gian thực, công cụ này giúp tổ chức phát hiện sớm mối đe dọa và giảm đáng kể thiệt hại tiềm tàng.

4.3.2. Kiểm soát truy cập mạng (Firewall và Network Security)

SQL Server có thể bị khai thác nếu mở truy cập từ địa chỉ IP không tin cậy. Cần áp dụng cơ chế lọc mạng, VPN hoặc Azure Private Link để bảo vệ kết nối.

Ví dụ: Giới hạn truy cập SQL Server chỉ từ mạng nội bộ bằng cách cấu hình tường lửa:

```
EXEC sp_set_firewall_rule
  @name = 'Allow_Only_Office_IP',
  @start_ip_address = '203.0.113.10',
  @end_ip_address = '203.0.113.10';
```

Cấu hình này giúp ngăn chặn truy cập trái phép từ bên ngoài tổ chức.

4.3.3. Phòng chống SQL Injection

Một trong những phương pháp hiệu quả nhất là tham số hóa truy vấn thay vì nối chuỗi động.

Không an toàn:

```
EXEC('SELECT * FROM Users WHERE Username = ''' + @username + ''' AND Password = ''' + @password + '''');
```

An toàn hơn:

```
CREATE PROCEDURE ValidateUser
  @username NVARCHAR(50),
  @password NVARCHAR(50)
AS
BEGIN
  SELECT * FROM Users
  WHERE Username = @username AND Password = @password;
END;
```

Ngoài ra, bật SQL Server Audit để ghi nhận các truy vấn nghi ngờ:

```
CREATE SERVER AUDIT SQLInjectionAudit
TO FILE (FILEPATH = 'C:\AuditLogs\');
ENABLE SERVER AUDIT SQLInjectionAudit;
```

4.3.4. Phát hiện truy cập bất thường và tấn công Brute Force

Cấu hình Audit giúp phát hiện hành vi đăng nhập thất bại lặp lại hoặc thay đổi quyền trái phép.

```
CREATE SERVER AUDIT FailedLoginAudit
TO FILE
(FILEPATH = 'C:\AuditLogs\FailedLogins\');
CREATE SERVER AUDIT SPECIFICATION FailedLoginsSpec
FOR SERVER AUDIT FailedLoginAudit
ADD (FAILED_LOGIN_GROUP);
ALTER SERVER AUDIT SPECIFICATION FailedLoginsSpec WITH (STATE = ON);
```

Khi có nhiều lần đăng nhập thất bại từ một IP lạ, hệ thống có thể tự động khóa tài khoản hoặc gửi cảnh báo cho quản trị viên.

4.3.5. Giám sát nhật ký bằng hệ thống SIEM

Tích hợp SQL Server với SIEM (Security Information and Event Management) như Microsoft Sentinel, Splunk hoặc QRadar cho phép:

- Thu thập và phân tích log tập trung.
- Phát hiện tấn công phối hợp hoặc có tính chuỗi.
- Tự động tạo cảnh báo và thực thi phản ứng.

Ví dụ: EXEC xp_readerrorlog 0, 1, 'Login failed';

Dữ liệu này có thể được gửi đến SIEM để xác định các IP hoặc tài khoản nghi vấn.

5. Kết luận

Bảo mật cơ sở dữ liệu là một thành phần trọng yếu trong việc đảm bảo an toàn thông tin và duy trì tính toàn vẹn của hệ thống dữ liệu doanh nghiệp. Thông qua quá trình phân tích các lỗ hổng phổ biến trong SQL Server – bao gồm xác thực yếu, tấn công SQL Injection, cấu hình sai, và thiếu cơ chế kiểm toán – nghiên cứu này cho thấy rủi ro bảo mật chủ yếu không chỉ đến từ công nghệ, mà còn từ quy trình quản trị và ý thức vận hành của con người.

Bài báo đã trình bày một hệ thống các giải pháp kỹ thuật và thực hành tốt nhất nhằm tăng cường bảo vệ dữ liệu trong SQL Server, như xác thực đa yếu tố, mã hóa dữ liệu đa lớp, kiểm toán và giám sát an ninh, cùng các kỹ thuật tiên tiến như Row-Level Security (RLS) và Always Encrypted. Ngoài ra, việc tích hợp Microsoft Defender for SQL và hệ thống SIEM giúp nâng cao khả năng phát hiện, ngăn chặn tấn công tự động và giảm thiểu rủi ro tiềm ẩn.

Từ góc độ ứng dụng, nghiên cứu nhấn mạnh rằng bảo mật cơ sở dữ liệu cần được triển khai theo mô hình phòng thủ nhiều lớp (Defense in Depth), kết hợp giữa công nghệ, quy trình quản lý và đào tạo con người. Trong tương lai, các hướng nghiên cứu tiếp theo có thể tập trung vào ứng dụng trí tuệ nhân tạo (AI) và học máy (Machine Learning) trong giám sát hành vi truy cập, phát hiện bất thường và tự động hóa phản ứng bảo mật trong môi trường SQL Server.

Tài liệu tham khảo

[1] Sun, B., Zhao, S., & Tian, G. (2024). SQL queries over encrypted databases: a survey. Connection Science, 36(1), 2323059.

[2] Pan, X., Obahiaghon, A., Makar, B., Wilson, S., & Beard, C. (2024). Analysis of database security. Open Access Library Journal, 11(4), 1-19.

[3] Ajasa, A. D., Chizari, H., & Alam, A. (2025). Database Security and Performance: A Case of SQL Injection Attacks Using Docker-Based Virtualisation and Its Effect on Performance. Future Internet, 17(4), 156.

[4] Dasari, N. S., Badii, A., Moin, A., & Ashlam, A. (2025). Enhancing SQL Injection Detection and Prevention Using Generative Models. arXiv preprint arXiv:2502.04786.

[5] Microsoft. (2024, February 29). SQL Server security best practices. Microsoft Docs.

[6] Bhupathiraju, S. K. R. (2025). Key Features and Innovations in SQL Server 2025: Advancing Performance, Security, and AI Integration. IJSAT-International Journal on Science and Technology, 16(1).