**Abstract**

SQL injection attacks remain one of the largest threats to web applications, because they allow the attacker to gain trusted access to data without authorization, which can lead to irreparable damage. As part of this project, we examined how deep learning and machine learning can aid in detecting these attacks automatically. In total, we built and evaluated six models: Logistic Regression, Support Vector Machine (SVM), Multilayer Perceptron (MLP), Recurrent Neural Network (RNN), Long Short-Term Memory (LSTM), and BERT (Bidirectional Encoder Representations from Transformers). Overall, BERT achieved the highest scores in accuracy, precision, recall, and F1-score. This demonstrates that transformer-based models such as BERT have a better understanding of SQL query structures, which makes them efficient in detecting complex attacks. This study shows how deep learning, especially BERT, can improve web application security.

**Keywords:** SQL Injection, Web Application Security, Deep Learning, Machine Learning, BERT, Transformer Models, Model Comparison, Threat Detection

**Résumé**

Les attaques par injection SQL restent l’une des plus grandes menaces pour les applications web, car elles permettent à un attaquant d’accéder de manière non autorisée aux données, ce qui peut entraîner des dommages irréparables. Dans le cadre de ce projet, nous avons étudié comment le deep learning et le machine learning peuvent aider à détecter automatiquement ces attaques. Au total, nous avons construit et évalué six modèles : la régression logistique, la machine à vecteurs de support (SVM), le perceptron multicouche (MLP), le réseau de neurones récurrent (RNN), la mémoire à long terme (LSTM) et BERT (Bidirectional Encoder Representations from Transformers). Dans l’ensemble, BERT a obtenu les meilleurs résultats en termes de précision, rappel, exactitude et score F1. Cela démontre que les modèles basés sur les transformers, comme BERT, ont une meilleure compréhension de la structure des requêtes SQL, ce qui les rend efficaces pour détecter des attaques complexes. Cette étude montre comment le deep learning, en particulier BERT, peut améliorer la sécurité des applications web.

**Mots-clés :** Injection SQL, Sécurité des applications web, Deep Learning, Machine Learning, BERT, Modèles Transformer, Comparaison de modèles, Détection de menaces

**ملخص**

تظل هجمات حقن من أخطر التهديدات التي تواجه تطبيقات الويب، حيث تتيحللمهاجم الوصول غير المصرح به إلى البيانات، مما قد يؤدي إلى أضرار جسيمة لا يمكن إصلاحها. في إطار هذا المشروع، قمنا بدراسة كيفية استخدام التعلم العميق والتعلم الآلي للمساعدة في الكشف التلقائي عن هذه الهجمات. طورنا وقمنا بتقييم ستة نماذج: الانحدار اللوجستي، آلة الدعم الناقل (SVM)، الشبكة العصبية متعددة الطبقات (MLP)، الشبكة العصبية التكرارية (RNN)، الذاكرة طويلة المدى (LSTM)، ونموذج BERT (تمثيلات المشفر ثنائية الاتجاه من المحولات). حقق نموذج BERT أفضل النتائج من حيث الدقة، الاستدعاء، الدقة النوعية، ومقياس F1. هذا يوضح أن النماذج المعتمدة على المحولات مثل BERT تمتلك فهماً أفضل لهياكل استعلامات SQL، مما يجعلها فعالة في اكتشاف الهجمات المعقدة. تبرز هذه الدراسة كيف يمكن للتعلم العميق، وخاصة BERT، تحسين أمان تطبيقات الويب.

**الكلمات المفتاحية:** حقن SQL، أمان تطبيقات الويب، التعلم العميق، التعلم الآلي، BERT، نماذج المحولات، مقارنة النماذج، اكتشاف التهديدات

[Chapter 1 SQL Injection 12](#_Toc200453537)

[1.1 Introduction 12](#_Toc200453539)

[1.2 SQL injection 12](#_Toc200453540)

[1.2.1 Definition 12](#_Toc200453541)

[1.2.2 How SQL Injection Works 13](#_Toc200453542)

[1.3 Techniques of SQL Injection 14](#_Toc200453543)

[1.3.1 Error-Based SQL Injection 14](#_Toc200453544)

[1.3.2 Blind SQL Injection 15](#_Toc200453545)

[1.3.2.1 Content-Based Blind SQL Injection 16](#_Toc200453546)

[1.3.2.2 Time-Based Blind SQL Injection 17](#_Toc200453547)

[1.3.3 Tautology-Based SQL Injection 18](#_Toc200453548)

[1.3.4 Union-Based SQL Injection 19](#_Toc200453549)

[1.4 Methods to prevent SQL Injection attacks. 22](#_Toc200453552)

[1.4.1 Prepared Statements (with Parameterized Queries) 23](#_Toc200453553)

[1.4.2 Stored Procedures 23](#_Toc200453554)

[1.4.3 Input Validation 24](#_Toc200453555)

[1.4.4 Escaping All User-Supplied Input 25](#_Toc200453556)

[1.5 Conclusion 25](#_Toc200453557)

[Chapter 2 Deep Learning 26](#_Toc200453558)

[2.1 Introduction 26](#_Toc200453560)

[2.2 Machine learning 27](#_Toc200453561)

[2.2.1 Machine Learning Types 27](#_Toc200453562)

[2.2.1.1 Supervised Learning (SL): 27](#_Toc200453563)

[2.2.1.2 Unsupervised Learning: 28](#_Toc200453564)

[2.2.1.3 Reinforcement Learning: 29](#_Toc200453565)

[2.2.2 Machine learning algorithms 29](#_Toc200453566)

[2.2.2.1 Logistic regression 29](#_Toc200453567)

[2.2.2.2 Support Vector Machine (SVM) 30](#_Toc200453568)

[2.3 Deep Learning 32](#_Toc200453569)

[2.3.1 Artificial Neural Networks (ANNs) 32](#_Toc200453570)

[2.3.2 Activation functions 35](#_Toc200453571)

[2.3.2.1 Non-Linear Activation Functions 35](#_Toc200453572)

[2.3.3 Deep learning architectures 37](#_Toc200453573)

[2.3.3.1 Recurrent Neural Networks 38](#_Toc200453574)

[2.3.3.2 Long Short-Term Memory Networks 41](#_Toc200453579)

[2.3.3.4 Transformers 43](#_Toc200453580)

[2.3.3.5 BERT 48](#_Toc200453581)

[2.4 Conclusion 51](#_Toc200453582)

[Chapter 3 Conception and Implementation 52](#_Toc200453583)

[3.1 Introduction 52](#_Toc200453585)

[3.2. Dataset 52](#_Toc200453586)

[3.3 Models Implemented 53](#_Toc200453587)

[3.3.1 Support Vector Machine (SVM) 54](#_Toc200453588)

[3.3.2 Logistic Regression (LR) 54](#_Toc200453589)

[3.3.3 Multilayer Perceptron (MLP) 54](#_Toc200453590)

[3.3.4 Recurrent Neural Network (RNN) 55](#_Toc200453591)

[3.3.5 Long Short-Term Memory (LSTM) 56](#_Toc200453592)

[3.3.6 BERT 57](#_Toc200453593)

[3.3.6.1 Reading and displaying the dataset 58](#_Toc200453594)

[3.3.6.2 Creating the training and test sets 58](#_Toc200453595)

[3.3.6.3 Building the model 59](#_Toc200453596)

[3.3.6.4 Fine-tuning the BERT model 59](#_Toc200453597)

[3.4 Conclusion 62](#_Toc200453598)

[Chapter 4 Performence Evaluation and Resaults 63](#_Toc200453599)

[4.1 Introduction 63](#_Toc200453601)

[4.2 Development Environment Overview 63](#_Toc200453602)

[4.2.1 Programming language 63](#_Toc200453603)

[4.2.2 Libraries 63](#_Toc200453604)

[4.2.3 Development setup 64](#_Toc200453605)

[4.2.3.1 Visual Studio Code 64](#_Toc200453606)

[4.2.3.2 Jupyter Notebook 64](#_Toc200453607)

[4.2.3.3 Google colab 64](#_Toc200453608)

[4.3 Performance Evaluation Metrics 65](#_Toc200453609)

[4.4 Evaluation on Test Set (20%) 66](#_Toc200453610)

[4.4.1 Results Presentation 66](#_Toc200453611)

[4.4.2 Visual Performance Analysis 68](#_Toc200453612)

[4.4.3 Performance Analysis of BERT 68](#_Toc200453613)

[4.4.3.1 Training Loss Curve 70](#_Toc200453614)

[4.4.3.2 Model Evaluation on New Unseen Data 70](#_Toc200453615)

[References 74](#_Toc200453616)

**List of figures**

**Figure 1.1** SQL Injection attack

**Figure 1.2** Prepared Statements example using php

**Figure 1.3** Stored Procedure example using PHP

**Figure 1.4** Input validation example using PHP

**List of tables**

**Table 1.1** Results of a SELECT query without UNION

**Table 1.2** Result of user query after a Union based SQL injection.

**General Introduction**

# Chapter 1

# SQL Injections

## 1.1 Introduction

With increasingly digital living, web applications are at the core of day-to-day life from managing finances and online purchasing to collaborating and communicating. This ease of the virtual world comes with inherent security challenges. Cyber attackers persistently evolve their methods to exploit weaknesses, thereby endangering unauthorized data access, downtime of services, and irreparable damage to reputation.

## 1.2 SQL injection

### 1.2.1 Definition

A SQL injection attack consists of insertion or “injection” of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system. SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to affect the execution of predefined SQL commands[[2].](#_[2]__)

**Figure 1.1** SQL Injection attack

### 1.2.2 How SQL Injection Works

It typically involves the following steps:

1. **Identification of vulnerable inputs:** Attackers first identify inputs within the web application that are vulnerable to SQL injection. These inputs could be text fields in a form, URL parameters, or any other input mechanisms.
2. **Crafting the malicious SQL query:** Once a vulnerable input is identified, attackers create a SQL statement intended to be inserted into the query executed by the application. This statement aims to alter the original SQL query to perform actions unintended by the application developers.
3. **Bypassing application security measures:** Attackers often have to bypass protections like input validation or escaping special characters. They achieve this through techniques like string concatenation or utilizing SQL syntax to comment out parts of the original query.
4. **Executing the malicious query:** When the application executes the SQL query, it includes the attacker’s malicious input. This modified query can perform actions such as unauthorized viewing of data, deletion of data, or even database schema alterations.
5. **Extracting or manipulating data:** Depending on the attack, the outcome might be the extraction of sensitive information (like user credentials), altering existing data, adding new data, or even deleting significant portions of the database.
6. **Exploiting database server vulnerabilities:** Advanced SQL injections may exploit vulnerabilities in the database server, extending the attack beyond the database to the server level. This can include executing commands on the operating system or accessing other parts of the server’s file system.

This process leverages the dynamic execution of SQL in applications where user inputs are directly included in SQL statements without proper validation or escaping. takes advantage of how SQL queries are built, often in a way that the developers did not anticipate[[3].](#_[3]_Bright_security)

##### Real-Life SQL Injection Attack Examples

Over the past 20 years, many SQL injection attacks have targeted large websites, business and social media platforms. Some of these attacks led to serious data breaches. A few notable examples are listed below[.](file:///C:\Users\ASUS%20ROG\AppData\Roaming\Microsoft\Word\SQL#_[3]_OWASP_)

###### **Breaches Enabled by SQL Injection**

* **GhostShell attack**—hackers from APT group Team GhostShell targeted 53 universities using SQL injection, stole and published 36,000 personal records belonging to students, faculty, and staff.
* **Turkish government**—another APT group, RedHack collective, used SQL injection to breach the Turkish government website and erase debt to government agencies.
* **7-Eleven breach**—a team of attackers used SQL injection to penetrate corporate systems at several companies, primarily the 7-Eleven retail chain, stealing 130 million credit card numbers.
* **HBGary breach**—hackers related to the Anonymous activist group used SQL Injection to take down the IT security company’s website. The attack was a response to HBGary CEO publicizing that he had names of Anonymous organization members.

## ****1.3 Techniques of SQL Injection****

### 1.3.1 Error-Based SQL Injection

**Error-based**[**SQL injection**](https://beaglesecurity.com/blog/vulnerability/sql-injection-vulnerability.html) is a type of security vulnerability and attack that occurs when an attacker injects malicious SQL statements into a web application’s input fields, causing the application to generate SQL errors.

These errors can reveal sensitive information about the application’s database structure, data, or configuration[[4]](#_[4]_Beagle_Security).

**How It Works:**

**Injection point:** An attacker identifies a vulnerable input field, such as a search box or login form, where user input is directly incorporated into SQL queries.

**Injecting malicious code:** The attacker inputs carefully crafted SQL code as part of their input. This code is designed to cause SQL syntax errors when the application processes it[[4].](file:///C:\Users\ASUS%20ROG\AppData\Roaming\Microsoft\Word\Blind#_[4]_OWASP,_)

**Example**[[5]](#_[5]_Dafydd_Stittard)**: Conditional Errors in Oracle/MS-SQL**



**Explanation**:

1. **Subquery**:
   * The subquery (SELECT username FROM all\_users WHERE username = 'DBSNMP') checks if a user named DBSNMP exists in the all\_users table.
2. **Condition**:
   * If the user DBSNMP exists, the condition (SELECT username FROM all\_users WHERE username = 'DBSNMP') = 'DBSNMP' evaluates to TRUE.
3. **Error Induction**:
   * When the condition is TRUE, the database evaluates the expression 1/0, which causes a **divide-by-zero error**.
   * If the condition is FALSE (i.e., the user does not exist), the expression 1/0 is **not evaluated**, and no error occurs.

**Detection**:

* If the application returns an **HTTP 500 error** or a database error message, the attacker can infer that the condition is TRUE (i.e., the user DBSNMP exists).
* If no error occurs, the condition is FALSE (i.e., the user does not exist).

**Advanced Use Case: Data Exfiltration**

**Scenario**:

* A web application allows users to sort search results using a sort parameter:



The backend SQL query:



**Malicious Injection**:

The attacker injects a payload into the sort parameter to test a condition:



**Explanation**:

1. **Subquery**:
   * The subquery (SELECT SUBSTR(MAX(object\_name),1,1) FROM user\_objects) extracts the **first character** of the largest object name in the user\_objects table.
2. **Condition**:
   * If the first character is 'Y', the condition evaluates to TRUE, and the database attempts to evaluate 1/0, causing a **divide-by-zero error**.
   * If the first character is not 'Y', no error occurs, and the query returns results normally.
3. **Inference**:
   * The attacker can use this technique to **brute-force** each character of the object name by testing different values (e.g., 'A', 'B', 'C', etc.).

### 1.3.2 Blind SQL Injection

Blind SQL (Structured Query Language) injection is a type of [SQL Injection](https://owasp.org/www-community/attacks/SQL_Injection) attack that asks the database true or false questions and determines the answer based on the applications response. This attack is often used when the web application is configured to show generic error messages, but has not mitigated the code that is vulnerable to SQL injection.

When an attacker exploits SQL injection, sometimes the web application displays error messages from the database complaining that the SQL Query’s syntax is incorrect. Blind SQL injection is nearly identical to normal [SQL Injection](https://owasp.org/www-community/attacks/SQL_Injection), the only difference being the way the data is retrieved from the database. When the database does not output data to the web page, an attacker is forced to steal data by asking the database a series of true or false questions. This makes exploiting the SQL Injection vulnerability more difficult, but not impossible [[6].](file:///C:\Users\ASUS%20ROG\AppData\Roaming\Microsoft\Word\Blind#_[6]_OWASP,_)

#### 1.3.2.1 Content-Based Blind SQL Injection

**How It Works:**  
 Unlike traditional SQL injection, where database error messages expose data directly, blind SQL injection does not return query results to the user. Attackers exploit this by providing conditional queries and observing the application's response to infer data from the database.

**Technical Explanation:**  
 Blind SQL injection relies on evaluating conditions based on the application's responses. Attackers inject SQL conditions and observe response differences (e.g., message change or page behavior) to deduce data.

**Example:**

vulnerable web application allows the attacker to inject SQL on a URL parameter that fetches data based on an id. The attacker confirms the vulnerability by injecting true/false statements in the id parameter to identify between valid and invalid SQL queries.

The attacker first sends a request like:



This executes:



Next, the attacker tests for SQL injection by adding a false condition:



The query becomes:



Since 1=2 is false, the page returns no content, confirming the injection.

Then, the attacker tests a true condition:



The query becomes:



This question retrieves the anticipated data, revealing the vulnerability.Contrasting the output of these two injections, the attacker can determine that the page is vulnerable to SQL injection and proceed to pull data from the database[[6]](file:///C:\Users\ASUS%20ROG\AppData\Roaming\Microsoft\Word\Blind#_[5]_OWASP,_).

**Explanation:**

Here, the attacker uses a spurious condition (and 1=2) to decide whether the page is vulnerable to SQL injection. Since no information is returned, the attacker confirms the vulnerability. A real condition (and 1=1) provides expected information, ascertaining that the injection has been successful. The attacker now iterates data, e.g., table names or other confidential data, using similar true/false conditions based on the database schema.

#### ****1.3.2.2 Time-Based Blind SQL Injection****

**How It Works:**  
 In time-based blind SQL injection, attackers use SQL functions like **SLEEP()** to introduce a delay in the server’s response. If the delay occurs, it indicates the injected SQL condition is true; if not, it is false. This helps attackers extract data even when no visible content is returned.

**Technical Explanation:**  
The attacker sends queries that include conditional delays, such as:  
xyz' AND IF(1=1, SLEEP(5), 0) – The server delays for 5 seconds, confirming the condition is true.  
xyz' AND IF(1=2, SLEEP(5), 0) – No delay occurs, confirming the condition is false.

**Example:**

Consider a web application that retrieves user information based on a user ID provided in the URL:



The corresponding SQL query might be:



If the application is vulnerable to Time-Based Blind SQL Injection, an attacker can manipulate the id parameter to include a time delay function.

**Malicious Injection:**

****

In this example, the injected SQL statement includes a conditional function that causes the database to pause for 5 seconds if the condition 1=1 is true.

**Explanation:**

Here, the attacker is inserting a conditional SQL function that will intentionally delay the database's response time. The inserted SQL query is:



The IF(1=1, SLEEP(5), 0) function will evaluate the condition 1=1, which is always fulfilled. So the SLEEP(5) function will be invoked, and the database will take 5 seconds to reply.

If the application responds in 5 seconds, the attacker confirms successful injection and exposure of the application to Time-Based Blind SQL Injection.

The attackers may use this technique to provide educated guesses on the structure and content of the database even when direct extraction is not possible.

### 1.3.3 Tautology-Based SQL Injection

The term ‘tautology’ originates from the field of logic, where it is used to describe a statement that is always true, regardless of the truth values of its components. In other words, a tautological statement is one that is true by virtue of its logical form alone [[7]](file:///C:\Users\ASUS%20ROG\AppData\Roaming\Microsoft\Word\SQL#_[7]_Moxso,_).

**How It Works:**

This attack exploits the use of tautological SQL statements.

Always result in true and thus bypasses authentication and other security measures.

**Technical Explanation:**  
 A tautology is a logical statement that remains true under any combination of values. Malicious users insert such statements into SQL queries, compelling the database to execute and authenticate unauthorized requests.



**OR '1'='1'** in this example guarantees the condition will always be true, giving access.  
Real-World Scenario: An attacker hacks a login form on a web page, bypassing user authentication and accessing an administrator account**.**

### 1.3.4 Union-Based SQL Injection

**How It Works:**

The UNION operator is used in SQL to combine the results of two or more SELECT statements into a single result set. When a web application contains a SQL injection vulnerability that occurs in a SELECT statement, attackers can utilize this operator to insert an additional query and merge its outcome with the outcome of the initial query[[5].](#_[5]_Dafydd_Stittard)

**Technical Explanation:**

Using this method, malicious users can retrieve unauthorized data from the database. UNION-based SQL injection is widely supported by all the major database management systems (DBMS) and is generally the best way to extract specific database contents when query results are directly presented on the application interface.

**Example 1**[**[8]**](#_[8]_Justin_Clarke,)**: Extracting the Current Database User**

**Scenario**

A web application shows product information based on a product ID passed in the URL. The application is susceptible to SQL injection since it puts user input directly into the SQL query without sanitizing. The attacker finds such vulnerability and chooses to exploit it in order to get the current database user, which can assist them in knowing the access level they have and strategize future attacks.  
  
The attacker knows that the application has a database backend (for example, Microsoft SQL Server, MySQL, or Oracle) and wishes to extract the username of the account which issued the queries.

**Malicious Injection:**

The attacker sends the following malicious URL to the application:



**Explanation:**

1. **Original Query:**  
   The application executes the following query to retrieve product details:



This query returns the details of the product with ID 12.

1. **Injected Query**  
   The attacker appends a UNION SELECT statement to the original query to retrieve the current database user:



* + The UNION operator combines the results of the original query with the results of the injected query.
  + The system\_user function (or equivalent, depending on the database) retrieves the username of the current database user.
  + The NULL values are used to match the number of columns in the original query (since the injected query only needs one column for the username, but the original query returns four columns).

1. **Combined Query:**  
   The database executes the following combined query:

****

**Result:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Id** | **Type** | **Description** | **Price** |
| 12 | Book | SQL Injection Attacks | 50 |
| NULL | db\_user | NULL | NULL |

**Table 1.1** Results of a SELECT query without UNION.

#### Example 2: Extracting Multiple Rows from the customers Table

**Scenario:**

A web application displays product details based on a product ID passed in the URL. The application is vulnerable to SQL injection because it directly incorporates user input into the SQL query without proper sanitization. The attacker discovers this vulnerability and decides to exploit it to extract sensitive customer data from the **customers** table in the database.

The attacker's goal is to retrieve the full list of customers (first and last names) from the database.

**Malicious Injection:**

The attacker sends the following malicious URL to the application:



***Explanation:***

1. **Original Query:**  
   The application executes the following query to retrieve product details:



This query returns the details of the product with ID 12.

1. **Injected Query:**  
   The attacker appends a UNION SELECT statement to the original query to retrieve data from the customers table:



* + The UNION operator combines the results of the original query with the results of the injected query.
  + The NULL value is used to match the number of columns in the original query (since the customers table has only three columns, but the original query returns four columns).

1. **Combined Query:**  
   The database executes the following combined query:



**Result:**

|  |  |  |  |
| --- | --- | --- | --- |
| id | **Type** | **Description** | **Price** |
| 12 | Book | SQL Injection Attacks | 50 |
| 1 | Charles | Smith | NULL |
| 2 | Lydia | Clayton | NULL |
| 3 | Bernard | Jones | NULL |

**Table 1.2** Result of user query after a Union based SQL injection.

**4 Explanation of the Result:**

* The first row represents the product details from the original query.
* The subsequent rows represent the data extracted from **the customers** table, including **userid, first\_name**, and **second\_name**.
* The **NULL** value in the **Price** column is used to align the injected data with the original query's column structure.

## 1.4 Methods to prevent SQL Injection attacks.

Attackers can use SQL injection on an application if it has dynamic database queries that use string concatenation and user supplied input. To avoid SQL injection flaws.

There are simple techniques for preventing SQL injection vulnerabilities and they can be used with practically any kind of programming language and any type of database [[9].](#_[7]_OWASP_Cheat)

### 1.4.1 Prepared Statements (with Parameterized Queries)

When developers are taught how to write database queries, they should be told to use prepared statements with variable binding (also known as parameterized queries). Prepared statements are simple to write and easier to understand than dynamic queries, and parameterized queries force the developer to define all SQL code first and pass in each parameter to the query later.

If database queries use this coding style, the database will always distinguish between code and data, regardless of what user input is supplied. Also, prepared statements ensure that an attacker cannot change the intent of a query, even if SQL commands are inserted by an attacker.

In PHP, PHP Data Objects (PDO) offer a more effective approach to database interactions. By providing methods that simplify parameterized queries, PDO ensures that user input is always treated as data rather than executable SQL code and enhances code readability and also ensures greater portability across multiple databases[.](#_[4]_OWASP_Cheat)



**Figure 1.2** Prepared Statements example using php[[10]](#_[4]_OWASP_Cheat)

### 1.4.2 Stored Procedures

Though stored procedures are not always safe from SQL injection, developers can use certain standard stored procedure programming constructs. This approach has the same effect as using parameterized queries, as long as the stored procedures are implemented safely (which is the norm for most stored procedure languages).

**Safe Approach to Stored Procedures :**

If stored procedures are needed, the safest approach to using them requires the developer to build SQL statements with parameters that are automatically parameterized, unless the developer does something largely out of the norm. The difference between prepared statements and stored procedures is that the SQL code for a stored procedure is defined and stored in the database itself, then called from the application.

Since prepared statements and safe stored procedures are equally effective in preventing SQL injection, your organization should choose the approach that makes the most sense for you.

The following code example call a stored procedure with an input/output parameter.



**Figure 1.3** Stored Procedure example using PHP[[11]](file:///C:\Users\ASUS%20ROG\AppData\Roaming\Microsoft\Word\Prepared_statements#_[11]PHP_)

### 1.4.3 Input Validation

Input validation is performed to ensure only properly formed data is entering the workflow in an information system, preventing malformed data from persisting in the database and triggering malfunction of various downstream components.

Input validation should happen as early as possible in the data flow, preferably as soon as the data is received from the external party.

Data from all potentially untrusted sources should be subject to input validation, including not only Internet-facing web clients but also backend feeds over extranets, from [suppliers, partners, vendors or regulators](https://badcyber.com/several-polish-banks-hacked-information-stolen-by-unknown-attackers/), each of which may be compromised on their own and start sending malformed data.

Example validating email addresses with [filter\_var()](https://www.php.net/manual/en/function.filter-var.php)



**Figure 1.4** Input validation example using PHP[[12]](file:///C:\Users\ASUS%20ROG\AppData\Roaming\Microsoft\Word\Validation#_[12]PHP_,_)

### ****1.4.4 Escaping All User-Supplied Input****

In this approach, the developer will escape all user input before putting it in a query. It is very database specific in its implementation. This methodology is frail compared to other defenses, and we CANNOT guarantee that this option will prevent all SQL injections in all situations.

If an application is built from scratch or requires low risk tolerance, it should be built or re-written using parameterized queries, stored procedures, or some kind of Object Relational Mapper (ORM) that builds your queries for you.

## 1.5 **Conclusion**

SQL injection remains a very important security threat to web applications. Some of the basic security measures that, if applied correctly, can protect against these attacks are input validation, prepared statements, and escaping user inputs. Other steps include restricting the functions that the user is allowed to perform. But no single method can fully guarantee protection from attacks of multitude types and changing SQL injection techniques. An attacker's primary goal is searching for a new way to bypass security, especially when not properly applied; this may result in a serious breach of sensitive data. For these reasons, these security steps must be followed consistently, regularly reviewed as part of a full security strategy, and supported by AI-based tools that help catch and block advanced and automated SQL injection attacks.  
  
To gain a better understanding of how AI-based tools operate, it is critical to explore the areas of machine learning and deep learning. These enable systems to learn from data, identify complex patterns, and upgrade themselves over time-a new dimension very much in favor of boosting cybersecurity. Hence, the following chapter will elucidate the background on machine learning, its different types and algorithms, and then proceed with deep learning architectures, which have shown great promise in detecting complex patterns and improving the accuracy of security systems.

# 

# Chapter 2

# Deep Learning

## 2.1 Introduction

The field of **AI**, using the strongest tools available in computer science, works toward imitating intelligence in a human being. These systems can perform a variety of tasks typically attributed to human cognitive abilities, such as decision-making, pattern recognition, and problem-solving. Artificial intelligence has come a long way over the years, fueling innovations such as self-driving cars, intelligent virtual assistants, and highly advanced recommendation systems, revolutionizing industries and everyday life.

In this part, basic machine-learning (ML) methodologies are looked into, a major subfield of AI. We will describe the three paradigms of learning: supervised learning, unsupervised learning, and reinforcement learning. Standard algorithms in machine learning will also be addressed followed by a transition into deep learning (DL), which is an enhanced version of ML that exploits multi-layer neural networks. The immediate goal in this instance is to firmly establish some of the fundamental concepts of these methods and their frameworks, in preparation for their application to real-world problems, including cybersecurity and SQL injection detection.

## 2.2 Machine learning

The field of machine learning is concerned with the question of how to construct computer programs that automatically improve with experience. In recent years many successful machine learning applications have been developed, ranging from data-mining programs that learn to detect fraudulent credit card transactions, to information-filtering systems that learn users' reading preferences, to autonomous vehicles that learn to drive on public highways. At the same time, there have been important advances in the theory and algorithms that form the foundations of this field.[[13]](#_[13]Mitchell,_T._M,)

### 2.2.1 Machine Learning Types

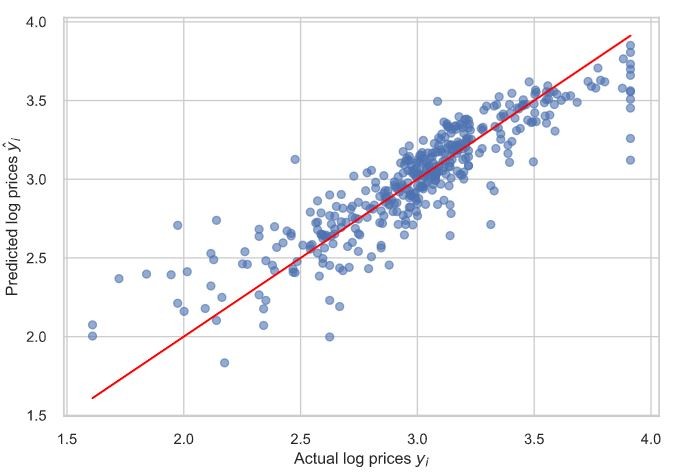
In machine learning, this kind of learning process is usually classed into three main parts which are supervised learning, unsupervised learning, and reinforcement learning. Each type serves a certain distinct purpose and is used with certain types of problems. Besides those three types, hybrid approaches such as commodity inclusion and special techniques have also emerged to maintain and solve more complex issues.

#### 2.2.1.1 Supervised Learning (SL):

**Supervised learning (SL)** is a machine learning approach that leverages labelled data to educate a system in forecasting outcomes based on its training. It closely mimics the process of human learning under the guidance of an instructor, employing specific instances to deduce overarching principles. SL is typically divided into two main categories.

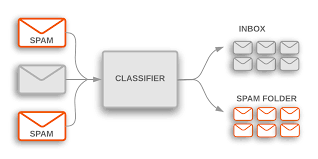
**Regression:** Regression is a term used in statistics, which is a type of statistical analysis that aims to understand the relationship between a dependent variable (response variable) and one or more independent variables (predictors) such as in market trends or weather forecasting. The most common type is linear regression

A typical example of regression is **house price prediction**, where features like house size, number of rooms, and location are used to estimate the price.



**Figure 2.1** Linear Regression Example – House Price Prediction

**Classification:** Classification is a SL technique that involves categorizing data into distinct classes. It is a recursive process that recognizes and groups data objects into pre-defined categories or labels. This technique is used to predict the outcome of a given problem based on input features. It can be applied to structured or unstructured data, and the classes are commonly known as target, label, or categories. The aim of classification is to assign an unknown pattern to a known class. For example, classifying emails as "spam" or "not spam" is a common application of classification.



**Figure 2.2** Classification Example – Spam vs Not Spam Emails

Both the Classification and Regression algorithms can be used for forecasting in machine learning and operate with the labelled datasets. But the distinction between classification vs regression is how they are used on particular machine learning problems. [[14]](#_[14]_Amer_F.A.H.)

#### 2.2.1.2 Unsupervised Learning:

[Unsupervised learning](https://www.ibm.com/think/topics/unsupervised-learning), also known as unsupervised machine learning, uses machine learning algorithms to analyze and cluster unlabeled datasets (subsets called clusters). These algorithms discover hidden patterns or data groupings without the need for human intervention.

Unsupervised learning’s ability to discover similarities and differences in information make it ideal for exploratory data analysis, cross-selling strategies, customer segmentation, and image and pattern recognition. It’s also used to reduce the number of features in a model through the process of dimensionality reduction. [Principal component analysis (PCA)](https://www.ibm.com/think/topics/principal-component-analysis) and singular value decomposition (SVD) are two common approaches for this. Other algorithms used in unsupervised learning include neural networks, [k-means clustering](https://www.ibm.com/think/topics/k-means-clustering), and probabilistic clustering methods.[[15]](file:///C:\Users\ASUS%20ROG\AppData\Roaming\Microsoft\Word\Machine#_[14]_IBM_,)

#### 2.2.1.3 Reinforcement Learning:

Reinforcement learning problems involve learning how to map situations to actions to maximize a numerical reward signal. These problems are inherently closed-loop, as the system’s actions influence its future inputs. Unlike other forms of machine learning, the learner is not explicitly told which actions to take but must discover the best ones through trial and error. In more complex scenarios, actions impact not only immediate rewards but also future states and long-term rewards, making decision-making more challenging.[[16]](#_[15]_Reinforcement_Learning:)

### 2.2.2 Machine learning algorithms

#### 2.2.2.1 Logistic regression

Logistic regression is a supervised machine learning algorithm used for classification tasks, predicting the probability that an instance belongs to a specific class. It is a statistical method that analyzes the relationship between independent variables and a categorical outcome.

Logistic regression applies the sigmoid function to map input values to a probability ranging between 0 and 1. Instead of fitting a regression line, it models an "S"-shaped curve to distinguish between classes.[[17]](file:///C:\Users\ASUS%20ROG\AppData\Roaming\Microsoft\Word\_Logistic#_[17]GeeksforGeeks_,)

**Key Points:**

* Logistic regression predicts the output of a categorical dependent variable.
* The outcome is discrete (e.g., Yes/No, 0/1, True/False) but represented as a probability between 0 and 1



**Figure 2.3** Example Curve: How Study Hours Affect Exam Success Rate

#### 2.2.2.2 ****Support Vector Machine (SVM)****

**A support vector machine (SVM) is a supervised learning algorithm used for many classification and regression problems, including signal processing, medical applications, natural language processing, and speech and image recognition.**

The objective of the SVM algorithm is to find a hyperplane that, to the best degree possible, separates data points of one class from those of another class. “Best” is defined as the hyperplane with the largest margin between the two classes, represented by plus versus minus in the figure below. Margin means the maximal width of the slab parallel to the hyperplane that has no interior data points. Only for linearly separable problems can the algorithm find such a hyperplane; for most practical problems, the algorithm maximizes the soft margin, allowing a small number of misclassifications.

**Support vectors** are a subset of the training observations that define the position of the separating hyperplane. These are the data points closest to the hyperplane and are crucial for determining the optimal margin. While SVMs are originally designed for binary classification, they can be extended to multiclass problems by combining multiple binary classifiers.



**Figure 2.4** SVM**:** Optimal Hyperplane and Support Vectors

To handle non-linearly separable data, SVMs use **kernel methods**. Kernel functions transform the data into a higher-dimensional space, where classes may become linearly separable. This transformation is implicit and computationally efficient, thanks to the **kernel trick**. Common kernel types include:

* **Linear**: Suitable for linearly separable data.
* **Polynomial**: Captures polynomial relationships between features.
* **Radial Basis Function (RBF)**: Effective for complex, non-linear boundaries.
* **Sigmoid**: A Mercer kernel under specific conditions.

Training an SVM involves solving a quadratic optimization problem to find the hyperplane that minimizes the soft margin. The number of transformed features depends on the number of support vectors, making the model compact and efficient once trained.

**Key advantages of SVMs** include their ability to handle high-dimensional data, robustness to outliers, and effectiveness in solving non-linear problems using kernels. Once trained, only the support vectors are needed to define the decision boundary, making SVMs suitable for automated code generation and real-world applications.[[18]](file:///C:\Users\ASUS%20ROG\AppData\Roaming\Microsoft\Word\Support#_[17]_GeeksforGeeks_,)

**Real-world machine learning use cases**

Here are just a few examples of machine learning you might encounter every day:

**Speech recognition :** It is also known as automatic speech recognition (ASR), computer speech recognition, or speech-to-text, and it is a capability which uses natural language processing (NLP) to translate human speech into a written format. Many mobile devices incorporate speech recognition into their systems to conduct voice search—e.g. Siri—or improve accessibility for texting.

**Customer service :** [Online chatbots](https://www.ibm.com/products/watsonx-orchestrate/customer-service) are replacing human agents along the customer journey, changing the way we think about customer engagement across websites and social media platforms. Chatbots answer frequently asked questions (FAQs) about topics such as shipping, or provide personalized advice, cross-selling products or suggesting sizes for users. Examples include [virtual agents](https://www.ibm.com/products/watsonx-assistant) on e-commerce sites, messaging bots, using Slack and Facebook Messenger, and tasks usually done by virtual assistants and voice assistants.

**Computer vision** : This [AI](https://www.ibm.com/consulting/artificial-intelligence) technology enables computers to derive meaningful information from digital images, videos, and other visual inputs, and then take the appropriate action. Powered by convolutional neural networks, computer vision has applications in photo tagging on social media, radiology imaging in healthcare, and self-driving cars in the automotive industry.

**Recommendation engines :** Using past consumption behavior data, AI algorithms can help to discover data trends that can be used to develop more effective cross-selling strategies. Recommendation engines are used by online retailers to make relevant product recommendations to customers during the checkout process.  
  
**Robotic process automation (RPA) :** Also known as software robotics, RPA uses intelligent automation technologies to perform repetitive manual tasks.

**Automated stock trading** : Designed to optimize stock portfolios, AI-driven high-frequency trading platforms make thousands or even millions of trades per day without human intervention.

**Fraud detection:** Banks and other financial institutions can use machine learning to spot suspicious transactions. Supervised learning can train a model using information about known fraudulent transactions. Anomaly detection can identify transactions that look atypical and deserve further investigation.[[19]](file:///C:\Users\ASUS%20ROG\AppData\Roaming\Microsoft\Word\Machine#_[18]_IBM_,)

## 2.3 Deep Learning

Deep learning is a subfield of machine learning that employs deep neural networks for analyzing and interpreting complex data. Such networks are modeled after the human brain and allow the computer to identify patterns and relationships without human intervention in large amounts of unstructured information. The deep learning model is continuously improving its accuracy by tuning internal parameters with training**.**

Deep learning models can be trained to perform classification tasks and recognize patterns in images, text, audio, and other types of data. This technology also enables automation of tasks that typically require human intelligence, such as image description and audio transcription. Where human brains have millions of interconnected neurons that work together to learn information, deep learning features neural networks constructed from multiple layers of software nodes that work together.

This technique has achieved astonishing outcomes in image recognition, understanding natural language, and processing speech, making it the foundation of contemporary artificial intelligence systems.[[20]](file:///C:\Users\ASUS%20ROG\AppData\Roaming\Microsoft\Word\What#_[19]_TeckTarget,_)

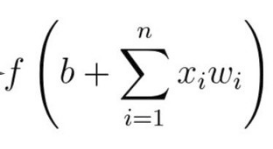
### 2.3.1 Artificial Neural Networks (ANNs)

Artificial Neural Networks (ANN) are inspired by the way biological neural system works, such as the brain process information. The information processing system is composed of a large number of highly interconnected processing elements (neurons) working together to solve specific problems. ANNs, just like people, learn by example. Similar to learning in biological systems, ANN learning involves adjustments to the synaptic connections that exist between the neurons.



**Figure 2.5** Neuron Computation in an Artificial Neural Network

Here [X1, X2, X3] are the input features to the neural networks represented as X. Whereas the superscript is used to denote the layer. The weights are denoted by [W1, W2, W3] associated with each connection to the neuron from the input of that particular layer. The bias is represented by b associated with the neuron. “z” is the weighted sum of inputs added with the bias which is linear in nature. “a” is the activation function that is applied to z to add non-linearity as complex models can't be represented as a line.



*n* = the number of inputs

from the incoming layer

The activation function is applied to the weighted sum of inputs to the neuron, including the bias term, and the resulting value becomes the neuron's output, which is then passed to the next layer. Its primary role is to introduce non-linearity into the model, allowing the network to learn complex patterns and approximate any arbitrary function. In this one-layer neural network architecture, the output of the activation function in layer serves as the final output, denoted as y’. This output is used to compute the loss function, L (a, y), which measures the deviation between the predicted and actual output. This deviation is crucial for backpropagation and optimization, which will be discussed in later sections[.[21]](file:///C:\Users\ASUS%20ROG\AppData\Roaming\Microsoft\Word\Basic#_[21]_Medium_)



**Figure 2.6** Basic Structure of an Artificial Neural Network

An artificial neural network is primarily composed of three layers: the input layer, one or more hidden layers, and the output layer. These layers collectively work to process the information and yield meaningful predictions.

**Input layers** serve as the entry point for data into the neural network. Each neuron in this layer corresponds to either a specific feature of the input dataset or an input vector. For instance, in an image classification problem, all input neurons may specify the intensity of each individual pixel. This layer exists purely for the purpose of passing on the raw input values to the next layer without change.

**Hidden layers** serve to process and transform information passed to them from the input layer. They are called hidden since nothing about their inner workings can be observed directly. In a typical hidden layer, a neuron takes in inputs from the preceding layer, applies a weighted summation, adds a bias, and applies an activation function on the result. Depending on the complexity of the task, a network can have varying numbers of hidden layers with varying numbers of neurons in each layer. DNNs having multiple hidden layers are quite popular in applications such as image recognition, speech processing, and natural language understanding since they can efficiently extract many complex patterns from the data.

**The output layer is** the final layer of the network that provides the prediction made by the model. The structure of this layer is based on the solved problem. In the case of classification networks, each output neuron corresponds to one class; in regression problems, usually only one output neuron provides a continuous value: an activation function is then used in the output layer according to the type of task, e.g., softmax for multi-class classification and any linear function for regression.

These layers are interconnected by **weighted links** that determine the importance of each input. The weights are adjusted during training.

### 2.3.4 Deep Learning Training Cycle

**1 Data input and preprocessing:** First, load and clean the data. This includes handling missing values or corrupted entries and removing outliers. Then transform the inputs to a consistent format – for example, normalize or scale numerical features (so they lie in a similar range) and apply any needed augmentation. Finally, split the dataset into training, validation, and test sets to ensure the model is evaluated on unseen data.

**2 Forward propagation :** Pass each training example through the network layer by layer to compute an output prediction. In each layer, inputs are combined with the layer’s weights and biases and sent through an activation function. This “forward pass” produces the network’s output given the current parameters.

**3 Loss function calculation:** Compare the network’s prediction to the true target using a loss (cost) function. The loss function quantifies the error – for example, mean squared error for regression or cross-entropy for classification. In other words, the loss measures the difference between the predicted output and the actual label, a larger difference leads to a larger loss value.

**4 Backpropagation:** Compute the gradient of the loss with respect to each weight by propagating the error backward through the network. During this backward pass, the chain rule is used to determine how much each weight contributed to the final error. In effect, backpropagation finds the error signal for each layer and weight so we know how to change the weights to reduce the loss

**5 Weight updates (optimization):** Use an optimization algorithm (like stochastic gradient descent or Adam) to adjust the network’s weights and biases using the gradients found by backpropagation. For example, stochastic gradient descent (SGD) subtracts a fraction (the learning rate) of the gradient from each weight, moving it in the direction that reduces loss. More advanced optimizers like Adam adapt the learning rate for each parameter and include momentum terms (combining ideas from momentum and RMSprop) to speed up convergence.

### 2.3.2 Activation functions

Activation functions play a fundamental role in neural networks by determining how neurons process input data and transfer information to subsequent layers. The choice of activation function significantly influences the network's performance and learning capability

#### 2.3.2.1 Non-Linear Activation Functions

A network using only a linear activation function is essentially equivalent to a simple linear regression model, limiting its ability to capture complex patterns in data. Non-linear activation functions enable deep networks to model intricate relationships between inputs and outputs.

They allow backpropagation by ensuring derivatives depend on input values, facilitating effective weight adjustments. They also enable the creation of deep networks, where transformed outputs from one layer pass non-linearly to the next, improving the model's ability to learn complex representations.

1. Sigmoid (Logistic) Activation Function

This function takes any real value as input and outputs values in the range of 0 to 1 making it useful for probabilistic models and binary classification tasks.

 The larger the input (more positive), the closer the output value will be to 1.0, whereas the smaller the input (more negative), the closer the output will be to 0.0, as shown below.

****

**Figure 2.7** Sigmoid Activation Function

It is ideal for probability-based applications due to its constrained output range and is differentiable, ensuring smooth gradient updates during optimization. However, it suffers from the vanishing gradient problem, as extreme values lead to near-zero derivatives, hindering learning. Additionally, it is not zero-centered, which can slow down the training process.

2.Tanh (Hyperbolic Tangent) Function

The Tanh function is similar to the sigmoid function but maps input values to a range between -1 and 1, providing stronger non-linearity.

****

**Figure 2.8** Tanh (Hyperbolic Tangent) Function

Its outputs are zero-centered, which improves convergence speed in deep networks, and it is often used in recurrent neural networks (RNNs) and convolutional neural networks (CNNs). However, it still suffers from the vanishing gradient problem, albeit less than the sigmoid function.

3. ReLU (Rectified Linear Unit) Function

ReLU is one of the most commonly used activation functions in deep learning. It introduces non-linearity by outputting zero for negative inputs while retaining positive values unchanged.



**Figure 2.9** ReLU (Rectified Linear Unit) Function

It is computationally efficient, as only a subset of neurons activates at a time, and helps accelerate gradient descent convergence due to its non-saturating nature. However, it suffers from the Dying ReLU problem, where neurons can become permanently inactive for negative inputs, preventing further updates.[[22]](#_[22]_V7_Labs,)

### 2.3.3 Deep learning architectures

Deep learning has enjoyed tremendous advancement in the last few years, serving as the major pillar for innovation in many different fields. Each architecture is designed for particular problems, with the performance in each case optimized for the specific needs of the task at hand.

Over the years, many deep learning models have been developed, often extending some fundamental designs. Among these, convolutional neural networks (CNNs), recurrent neural networks (RNNs), and long short-term memory networks (LSTMs) are the most commonly known. In their respective areas, these architectures have been very efficient, thereby enabling progress in image recognition, sequence modeling, and time series analysis.

#### 2.3.3.1 Recurrent Neural Networks

Recurrent Neural Networks (RNNs) are neural networks designed to recognize patterns in sequences of data. They’re used for identifying patterns such as text, genomes, handwriting, or numerical time series data from stock markets, sensors, and more.

Unlike traditional [feedforward neural networks](https://www.analyticsvidhya.com/blog/2022/03/basic-introduction-to-feed-forward-network-in-deep-learning/), where inputs are processed only once in a forward direction, RNNs possess a unique feature: They have loops in them, allowing information to persist.

This looping mechanism enables RNNs to remember previous information and use it to influence the processing of current inputs. This is like having a memory that captures information about what has been calculated so far, making RNNs particularly suited for tasks where the context or the sequence is crucial for making predictions or decisions[.[23]](file:///C:\Users\ASUS%20ROG\AppData\Roaming\Microsoft\Word\Why#_[23]_Shelf_)

**Structure of RNNs**

RNNs are made of neurons: data-processing nodes that work together to perform complex tasks. The neurons are organized as input, output, and hidden layers. The input layer receives the information to process, and the output layer provides the result. Data processing, analysis, and prediction take place in the hidden layer.



**Figure 2.10:** Recurrent Neural Network (RNN) Architecture

The diagram illustrates the unrolled RNN over time steps, showing:

**•** **Inputs (xₜ):** Sequential data (e.g., words in a sentence).

**• Hidden states (hₜ):** Memory units with recurrent weights (Wₕₕ).

**• Outputs (yₜ):** Predictions at each step.

**• Weight matrices (Wₓₕ, Wₕₕ, Wₕᵧ):** Shared across time steps for efficiency

**Hidden layer**

RNNs work by passing the sequential data that they receive to the hidden layers one step at a time. However, they also have a self-looping or recurrent workflow: the hidden layer can remember and use previous inputs for future predictions in a short-term memory component. It uses the current input and the stored memory to predict the next sequence.

For example, consider the sequence: Apple is red. You want the RNN to predict red when it receives the input sequence Apple is. When the hidden layer processes the word Apple, it stores a copy in its memory. Next, when it sees the word is, it recalls Apple from its memory and understands the full sequence: Apple is for context. It can then predict red for improved accuracy. This makes RNNs useful in speech recognition, machine translation, and other language modeling tasks.

**Training**

Machine learning (ML) engineers train deep neural networks like RNNs by feeding the model with training data and refining its performance. In ML, the neuron's weights are signals to determine how influential the information learned during training is when predicting the output. RNNs share the same weights across time steps.

ML engineers adjust weights to improve prediction accuracy. They use a technique called back propagation through time (BPTT) to calculate model error and adjust its weight accordingly. BPTT rolls back the output to the previous time step and recalculates the error rate. This way, it can identify which hidden state in the sequence is causing a significant error and readjust the weight to reduce the error margin.

**types of recurrent neural networks:**

RNNs are often characterized by one-to-one architecture: one input sequence is associated with one output. However, you can flexibly adjust them into various configurations for specific purposes. The following are several common RNN types.

**One-to-many**

This RNN type channels one input to several outputs. It enables linguistic applications like image captioning by generating a sentence from a single keyword.

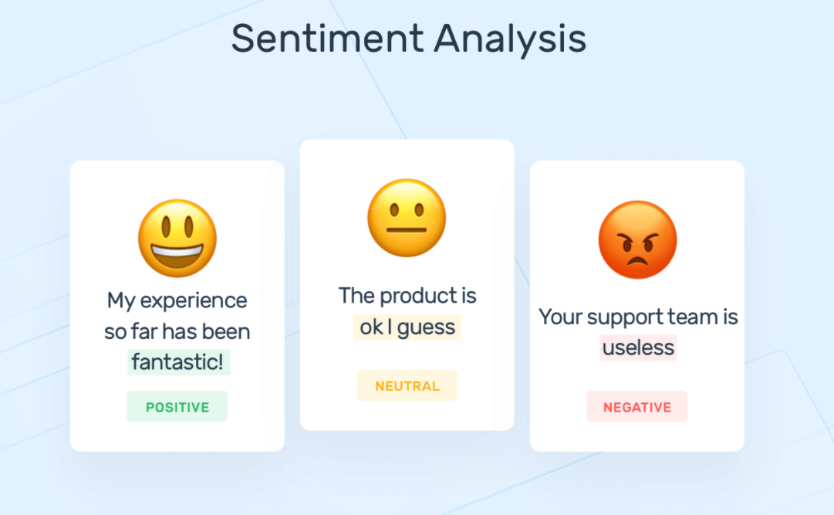


**Many-to-many**

The model uses multiple inputs to predict multiple outputs. For example, you can create a languagetranslator with an RNN, which analyzes a sentence and correctly structures the words in a different language.

**Many-to-one**

Several inputs are mapped to an output. This is helpful in applications like sentiment analysis, where the model predicts customers’ sentiments like positive, negative, and neutral from input testimonials[.[24]](#_[24]_Amazone_Web)



**Limitations of RNNs**

Despite their effectiveness, RNNs suffer from several limitations that impact their performance, especially when dealing with long sequences:

**Vanishing gradient problem**: One of the significant drawbacks of basic RNNs is the vanishing gradient problem. It occurs when gradients during training become extremely small as they are backpropagated through time. This limits the network's ability to capture long-range dependencies.

**Exploding gradient problem**: RNNs can also suffer from the exploding gradient problem, where gradients become exceptionally large during training, causing numerical instability. Exploding gradient is easier to detect and manage.

**Limited memory**: Traditional RNNs have a limited memory capacity, and they struggle to carry information across many time steps. This can be problematic when dealing with long sequences where the network may "forget" important information from earlier time steps[.[25]](What_are#_[25]AIML,_)

#### 2.3.3.2 Long Short-Term Memory Networks

Traditional RNNs struggle with long-term dependencies due to the vanishing and exploding gradient problem. To address this, **Long Short-Term Memory (LSTM) networks** were introduced.

A long short-term memory (LSTM) network is a type of recurrent neural network (RNN). LSTMs are predominantly used to learn, process, and classify sequential data because they can learn long-term dependencies between time steps of data.

**Architecture and Functioning:**

LSTM layers use additional gates to control what information in the hidden state is exported as output and to the next hidden state. These additional gates overcome the common issue with RNNs in learning long-term dependencies. In addition to the hidden state in traditional RNNs, the architecture for an LSTM block typically has a memory cell, input gate, output gate, and forget gate. The additional gates enable the network to learn long-term relationships in the data more effectively. Lower sensitivity to the time gap makes LSTM networks better for analyzing sequential data than simple RNNs. In the figure below, you can see the LSTM architecture and data flow at time step t.



**Figure 2.11:** LSTM Gate Mechanisms

Data flow at time step t for an LSTM unit. The forget gate and memory cell prevent the vanishing and exploding gradient problems.

These formulas define the internal mechanisms of the LSTM cell and correspond to the diagram above.

As illustrated in Figure 2.10, the diagram shows the equations used to compute the forget gate *fₜ*, input gate *iₜ*, candidate memory *Cₜ*, updated cell state *Cₜ*, output gate *oₜ*, and hidden state *hₜ*.

****

**Figure 2.12 –**Mathematical Formulation of LSTM Gates and States**.**

**Gate Mechanisms and Information Flow**

The weights and biases to the input gate control the extent to which a new value flows into the LSTM unit. Similarly, the weights and biases to the forget gate and output gate control the extent to which a value remains in the unit and the extent to which the value in the unit is used to compute the output activation of the LSTM block, respectively.

The following diagram illustrates the data flow through an LSTM layer with multiple time steps. The number of channels in the output matches the number of hidden units in the LSTM layer



**Figure2.13** LSTM Layer Architecture and Operations

Data flow for an LSTM with multiple time steps. Each LSTM operation receives the hidden state and cell state from the previous operation and passes an updated state and cell state to the next operation.

**Applications of LSTM Networks:**

LSTMs work well with sequence and time-series data for classification and regression tasks. LSTMs also work well on videos because videos are essentially a sequence of images. Similar to working with signals, it helps to perform feature extraction before feeding the sequence of images into the LSTM layer. Leverage convolutional neural networks (CNNs) (e.g., GoogLeNet) for feature extraction on each frame. The following figure shows how to design an LSTM network for different tasks[.[26]](Long#_[26]_MathsWorks,_)

#### 2.3.3.4 Transformers

Recurrent neural networks (RNNs), including LSTMs and GRUs, are state-of-the-art for sequence modeling and transduction tasks like machine translation. However, their sequential computation limits parallelization, especially for long sequences. Attention mechanisms improve dependency modeling but are typically used with RNNs.

The Transformer eliminates recurrence, relying entirely on attention for global dependencies, enabling greater parallelization and state-of-the-art results. Unlike convolutional models (e.g., ByteNet, ConvS2S), the Transformer reduces operations for distant dependencies to a constant. It is the first model to use only self-attention, avoiding RNNs or convolutions.



**Figure 2.14** Transformer Model Architecture with Multi-Head Attention

**1. Encoder and Decoder Stacks**

**Encoder**: The encoder is composed of a stack of N = 6 identical layers. Each layer has two sub-layers. The first is a multi-head self-attention mechanism, and the second is a simple, positionwise fully connected feed-forward network. We employ a residual connection around each of the two sub-layers, followed by layer normalization. That is, the output of each sub-layer is LayerNorm(x + Sublayer(x)), where Sublayer(x) is the function implemented by the sub-layer itself. To facilitate these residual connections, all sub-layers in the model, as well as the embedding layers, produce outputs of dimension dmodel= 512.

**Decoder**: The decoder is also composed of a stack of N = 6 identical layers. In addition to the two sub-layers in each encoder layer, the decoder inserts a third sub-layer, which performs multi-head attention over the output of the encoder stack. Similar to the encoder, we employ residual connections around each of the sub-layers, followed by layer normalization. We also modify the self-attention sub-layer in the decoder stack to prevent positions from attending to subsequent positions. This masking, combined with fact that the output embeddings are offset by one position, ensures that the predictions for position i can depend only on the known outputs at positions less than i.

**2. Embeddings and Softmax**

Similarly to other sequence transduction models, we use learned embeddings to convert the input tokens and output tokens to vectors of dimension dmodel. We also use the usual learned linear transformation and softmax function to convert the decoder output to predicted next-token probabilities. In our model, we share the same weight matrix between the two embedding layers and the pre-softmax linear transformation, similar to. In the embedding layers, we multiply those weights by √ dmodel.

**3. Attention**

An attention function can be described as mapping a query and a set of key-value pairs to an output, where the query, keys, values, and output are all vectors. The output is computed as a weighted sum of the values, where the weight assigned to each value is computed by a compatibility function of the query with the corresponding key.[[27]](#_[27]_Ashish_Vaswani,)



**Figure 2.15** Scaled Dot-Product Attention Mechanisms

3.1 Scaled Dot-Product Attention

The scaled dot-product attention mechanism is an important part of Transformer architecture and works with queries, keys, and values as the input. First, now, the model computes a dot product over the similarity of each query with all the keys. To avoid any training instability due to very large similarity scores, the values of these similarity scores are scaled down by dividing them by the square root of the key dimension.

Each word in a sequence is mapped to three vectors:

* Query (Q)
* Key (K)
* Value (V)



**Figure 2.14** Self-Attention Equation

These scaled scores are subsequently put through a softmax, which returns the normalized weights. The weights tell the model how much importance to attach to each value whilst combining them into a final output. This mechanism enables an efficient focus on only the relevant parts of the input. Scaled dot-product attention, being much faster and memory-efficient compared to additive attention that involves computing similarities with a small neural network, perfectly fits the bill in case of large-scale applications.



**Figure 2.16** Scaled Dot-Product Attention Mechanisms

3.2 Multi-Head Attention

Multi-head attention is extension of the basic attention mechanism in that it enables the model to jointly attend to different regions of the input simultaneously. Instead of computing one attention function, it computes multiple projections of the queries, keys, and values using different learned projections. They are computed in parallel and concatenated, projected one last time to produce the final output.



This enables the model to capture diverse information from different representation subspaces, thus it is better suited to handle complex patterns. For example, Transformers typically consist of eight attention heads that run on reduced dimensions in an attempt to provide computational efficiency.



**Figure 2.17** Multi-Head Attention Mechanisms

**4. Positional Encoding**

Transformers lack inherent information about the order of the input sequence due to their parallel processing nature. [Positional encoding](https://www.geeksforgeeks.org/positional-encoding-in-transformers/) is introduced to provide the model with information about the position of each token in the sequence.

Positional encodings are added to the input embeddings to give the model a sense of token order. These encodings can be either learned or fixed.[[28]](Architecture#_[28]_GeeksforGeeks,_)

In the original Transformer architecture, fixed sinusoidal functions are used for encoding positions.

5. Point-wise Feedforward Network

Point-wise feedforward networks are used extensively in transformer architectures. These networks consist of two linear transformations with a ReLU activation in between. The first linear transformation expands the dimensionality of each input position and the second reduces it back to the original dimension. This layer operates independently on each position within the input sequence, which allows it to efficiently process long sequences in parallel. Its significance lies in its ability to introduce non-linearity and increase the model's capacity to capture complex features, improving the performance of tasks like language modeling, translation, and more.

The mathematical formulation is:



where W1 expands dimensions (e.g., from dmodel​ to dff), and W2*W*2​ compresses back to dmodel.

The point-wise feedforward network concept gained prominence with the introduction of the Transformer model in the seminal paper "Attention Is All You Need" by Vaswani et al. in 2017. The model's innovative architecture, including this type of feedforward network, revolutionized the field of natural language processing (NLP).[[29]](Point-wise#_[29]_Envisioning,_)

#### 2.3.3.5 BERT

**1.Introduction to BERT**

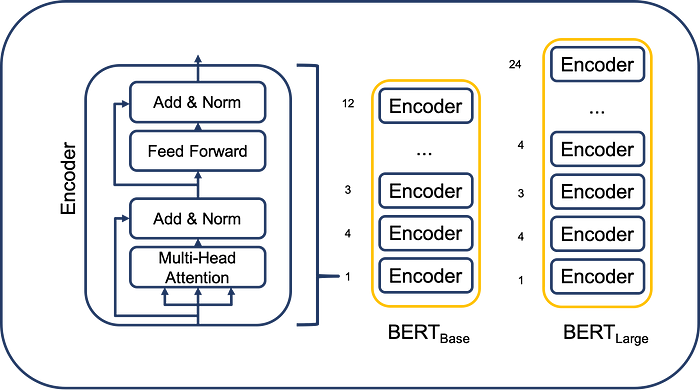
In recent years, deep learning has brought tremendous changes in natural language processing. Among such great innovations is BERT, by Google, that introduced this powerful bidirectional training mechanism within the Transformer construct. BERT’s construction is able to capture deeper contextual relationships in text and set new state-of-the-art benchmarks across the different NLP tasks. The general-purpose nature of BERT allows it to be easily fine-tuned, making it well-suited for SQL injection detection, where subtle semantic patterns are crucial.

**2.BERT Architecture** Overview

The BERT model architecture is a multilayer bidirectional Transformer encoder, based on the encoder component of the original Transformer model. While the original Transformer use an encoder-decoder structure where the encoder processes input sequences using self-attention mechanisms and the decoder combines self-attention with encoder-decoder attention, BERT focuses exclusively on the encoder to learn deep contextual representations.



The BERT architecture is available in two main configurations : BERTBASE and BERTLARGE. BERTBASE consists of 12 encoder layers, 768 hidden units per layer, and 12 attentions heads, resulting in approximately 110 million parameters. In contrast, BERTLARGE extends the architecture to 24 encoder layers, 1024 hidden units, and 16 attentions heads, totaling around 340 million parameters.



BERT-Base’s encoder uses the standard Transformer encoder design. It is a stack of 12 identical layers. Each layer contains two sub-layers, first a multi-head self-attention module and second a position-wise feed-forward network. In line with the original Transformer, each sub-layer is wrapped with a residual (add) connection and then followed by layer normalization. Precisely, the output of each sub-layer is computed as   
LayerNorm(x + SubLayer(x)), where SubLayer(x) is either the attention or feed-forward function. This architecture ensures that the output dimensionality in every layer matches the input dimensionality, so the representation size remains unchanged across all 12 layers.[[26]](#_[26]_Ashish_Vaswani,)

As a result, BERT models are capable of learning more complex contextual representations from input sequences.

**3. Pre-training BERT**

In the pre-training stage, BERT is trained on a gigantic corpus of unlabelled text with two unsupervised tasks:

**Masked Language Modeling (MLM):**

Instead of predicting the next word in a sequence (as with typical language models), BERT sifts through and randomly masks some of the input tokens and subsequently learns to predict the masked tokens from the context in which they appear. For example, given the sentence "The SQL [MASK] is malicious," the model will learn the missing word is likely "query."

**Next Sentence Prediction (NSP):**

This task is forecasting whether a specific sentence B has a tendency to follow sentence A naturally in the original text. This helps in providing the model with an appreciation of correspondence between sets of sentences, and this is useful for question answering and sentence classification.

By learning from these two tasks, BERT learns a rich bidirectional language understanding, which allows it to learn nuanced semantic and syntactic relationships between words in text.

**4. Fine-tuning**

After the pre-training was accomplished, BERT-instance could be fine-tuned to perform specific downstream tasks, such as text classification, sentiment analysis, named entity recognition, or in this piece of work, SQL injection detection.

During fine-tuning:

**.** BERT with weights from pre-training is loaded.

**.** Then, a simple classification layer is added on top of the output of BERT (e.g., a single dense layer followed by a softmax or sigmoid activation).

**.** The entire network, including the pre-trained layers, is then trained on the target dataset with labeled examples.

This step requires far less time and fewer labeled examples than would normally be required to train a deep model from scratch, because BERT provides a strong linguistic knowledge base to begin with.

**4. 4 Advantages and Limitations of BERT**

BERT has revolutionized natural language understanding by enabling deep bidirectional context learning. It has set state-of-the-art performance on a wide range of tasks. However, it is computationally expensive, and fine-tuning may require careful hyperparameter tuning and preprocessing strategies. Furthermore, its effectiveness may decrease on tasks involving very short texts or domain-specific language if not properly adapted.

## 2.4 Conclusion

This chapter explored the fundamentals of machine learning and deep learning, examining their core concepts, key algorithms, and architectural models. These technologies are the cornerstone of modern-day artificial intelligence, in the sense that AI systems learn from data and take decisions based on need. An understanding of these frameworks will thus allow a reader to understand how advanced models such as BERT are operationalized for complex tasks such as SQL injection detection. We shall now use this understanding to study deep learning model implementation in practical cybersecurity scenarios.

# 

# Chapter 3

# Conception and Implementation

## 3.1 Introduction

The chapter describes the models' design and implementation for SQL injection detection. Different architectures evaluated in our work include the traditional machine learning and deep learning approaches. The rationale behind this approach is to assess and compare the models' performances on the same dataset in order to find the one most suitable for accurately detecting SQL injection attempts. The next sections describe the dataset employed, as well as the preprocessing done on it, followed by the design for each of the models and the evaluation strategy considered for training and testing.

## 3.2. Dataset

To train an effective deep learning model successfuly, we need to make sure the dataset is properly chosen. For our project, we needed a dataset that includes samples classified into two categories: queries containing SQL injection and those that do not.Using this dataset, the trained model will be able to detect whether a query is a SQL injection or a normal query.

 We found a collection of "SQL Injection Datasets" on Kaggle. Among these datasets, we discovered a collection of datasets that put togetherby a person named " Syed Saqlain Hussain Shah" and it contain three (3) datasets.

**SQLi.csv** contains 3951 samples with 78% classified as normal queries and 28% as malicious queries.

**SQLiV2.csv** contains 33726 samples with 66% classified as normal queries and 34% as malicious queries.

**SQLiV3.csv** contains 30873 samples with 62% classified as normal queries and 37% as malicious queries and 1% as other.

After training and testing multiple machine learning and deep learning models on the three datasets, we found SQLIV3.CSV to be the most suitable dataset for our project. Models trained on this dataset were better able to detect SQL injection attacks and benign queries compared to other datasets, SQLIV3.csv consisyently led to a higher accuracy and better generalization across different models, making it the optimal choice for our final implementation.

**DATA preprocessing**

Before training the models, the SQLIV3.csv dataset needs to be preprocessed as follows:

-We found two trailing commas (,,) at the end of all the lines in the CSV file and removed these unnecessary characters using a Python script.

- Filters the rows to keep only those that contain exactly 2 columns and removes empty rows.

By applying the above preprocessing steps, we ultimately created a partitioned dataset containing:

* **30,614 SQL queries**.
* Each entry consists of a **Sentence** (the SQL query) and a **Label** (0 for benign, 1 for SQL Injection).

**Label distribution**:

* **Normal (Label = 0)**: 19,268 queries
* **Malicious (Label = 1)**: 11,346 queries



## 3.3 Models Implemented

This section on models presents the various models that have been developed for detecting SQL injections. A number of machine learning models and deep learning models were trained and evaluated with varying architecture and hyperparameters. The aim is to see how traditional techniques and modern, state-of-the-art techniques differ in input to achieve results on the same dataset.

For each model, we describe the structure, the main hyperparameters used during training, and the results obtained. These models are as follows:

Support Vector Machine (SVM)

Logistic Regression (LR)

Multilayer Perceptron (MLP)

Simple Neural Network (SN)

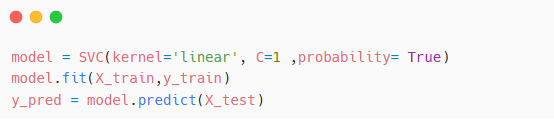
Recurrent Neural Network (RNN)

Long Short-Term Memory (LSTM)

Bidirectional Encoder Representations from Transformers (BERT)

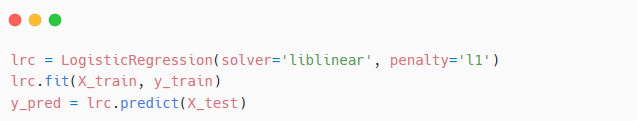
### 3.3.1 Support Vector Machine (SVM)

We used a Support Vector Machine with a linear kernel (`kernel='linear'`) and regularization parameter C = 0.1. The input queries were transformed into vectors by applying TF-IDF with 3000 features as the maximum. We dropped duplicates and split the dataset into 80% training and 20% testing sets prior to model training.



### 3.3.2 Logistic Regression (LR)

We trained a Logistic Regression classifier to detect SQL injection payloads using TF-IDF features (maximum of 3000 features). The classifier was initialized with solver='liblinear' and penalty='l1'. After removing duplicate queries, the dataset was divided into 80% for training and 20% for testing.



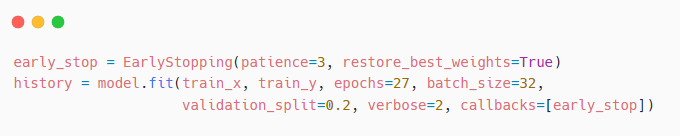
### 3.3.3 Multilayer Perceptron (MLP)

We trained a Multi-Layer Perceptron (MLP) neural network Using ReLU activation functions with three hidden layers comprising 512, 256, and 128 units respectively. For binary classification, the output layer employed a sigmoid activation function. Using TF-IDF with a maximum of 3000 characteristics, input queries were vectorized.  
  
Using the binary cross-entropy loss function and the SGD optimizer with a learning rate of 0.01, the model was compiled. Using 20% of the training set for validation, it was trained for 27 epochs on 80% of the data with early stopping activated (patience = 3). To guarantee clean input data, duplicates were deleted from the test set prior to evaluation.

**Build and Compile the Model**

****

**Train with Early Stopping**

****

### 3.3.4 Recurrent Neural Network (RNN)

We trained a Recurrent Neural Network to detect sequential patterns in SQL injection attempts by feeding in tokenized and padded input queries. Character filters were disabled, and case sensitivity was preserved during preprocessing to maintain the SQL syntax and structure.   
  
The first layer of the model architecture was an Embedding layer of 128 dimensions, followed by a SimpleRNN layer of 128 units. To avoid overfitting, we put in a Dropout layer at 0.5. Then a Dense layer of 64 units was added with ReLU activation and L2 regularization (λ = 0.01). The output layer has a sigmoid activation for binary classification.  
  
The model was compiled using binary crossentropy as the loss function and the Adam optimizer with a learning rate of 0.0001. The model was trained for 20 epochs with early stopping at 3 epochs' patience, and the best weights from validation were restored.

**Build and Compile the Model**



**Train with Early Stopping**

****

### 3.3.5 Long Short-Term Memory (LSTM)

We have trained an LSTM network to recognize sequential patterns in SQL injection attempts by feeding in tokenized and padded sequences. Character filters were disabled and case sensitivity was preserved during preprocessing to preserve the integrity of the SQL syntax.

The model architecture consisted of a 256-dimensional embedding layer, followed by two stacked LSTM layers with 256 and 128 units respectively. This was followed by a fully connected Dense layer of 64 units with ReLU activation, and a sigmoid-activated output layer for binary classification.

Training was carried out for 30 epochs using the Adam optimizer, a learning rate of 0.001, and the binary cross-entropy loss function to minimize. Early stopping with patience of 3 epochs was employed to prevent overfitting, and the best model weights were restored based on validation performance.

**Build and Compile the Model**

****

**Train with Early Stopping**

****

While several classical and deep learning models were implemented (see Sections 3.3.1 to 3.3.5), particular emphasis is placed on the BERT model due to its recent state-of-the-art performance and its central role in our contribution. Therefore, Section 3.3.6 provides a more detailed explanation of its implementation.

### 3.3.6 BERT

**Why BERT for SQL Injection Detection**

We selected BERT as our SQL injection detection model due to its high capacity to comprehend both meaning and context of textual information, particularly in structured input such as SQL queries. What makes BERT distinctively effective is the fact that it processes the whole input bidirectionally which helps it pick up on subtle patterns that might indicate an attack. Unlike older models that generally rely on basic keyword matching or predefined rules, BERT learns from the actual composition and intent of the query. After fine-tuning on a database consisting of normal and malicious SQL queries, the model was able to accurately identify suspicious inputs that could potentially represent injection attempts. Thus, BERT proves to be a reliable and effective tool for web application security improvement.

We decided to use the BERTBASE model for our implementation mainly because our dataset contains 30,614 labeled queries. Since BERTBASE is less complex than BERTLARGE, it trains faster and uses fewer resources, while still performing well for classification tasks like detecting SQL injection attacks.

**BERT Code and Implimentation**

In this section, we present the code and detailed implementation of our SQL injection detection model, which is based on the BERT architecture.

#### 3.3.6.1 Reading and displaying the dataset

****

This code detects the character encoding of the CSV file SQLiV3\_cleaned2.csv using the chardet library and then reads the file into a pandas DataFrame(df) with the correct encoding. This ensures the file is read without encoding errors, especially if it's not in UTF-8 format.

#### 3.3.6.2 Creating the training and test sets

****

In this code, the text data (Sentence column) and the corresponding label data (Label column) are extracted from the DataFrame and converted to lists. Afterward, the texts\_from\_array function of ktrain is used to do the preprocessing of these texts so that they can be used for fine-tuning the model. With preprocess\_mode='bert', the word text is passed through a BERT tokenizer that lowercases, tokenizes into word pieces, pads, and then sequences exceeding 100 tokens are automatically shortened. It is intentionally split into training and validation (with 20% of samples used for validation) sets (val\_pct=0.2), the class\_names parameter specifies the two label classes allowing the function to handle the binary classification task of SQL injection detection Then, the function returns the preprocessed train and validation sets (x\_train, y\_train, x\_test, y\_test), while the preproc object contains the tokenizer and configurations used during the preprocessing stage.

#### 3.3.6.3 Building the model

****

This code initializes a text classification model using the BERT architecture with the preprocessed training data (x\_train, y\_train) and the associated preprocessing configuration preproc. It sets up the model ready for fine-tuning on our dataset.

#### 3.3.6.4 Fine-tuning the BERT model

****

The ktrain.get\_learner function creates a learner object that combine the model and training procedure. The model argument takes the pre-trained BERT model that we want to fine-tune. The training data (train\_data) is passed as a tuple containing the input features (x\_train) and their corresponding labels(y\_train). Validation data (val\_data), given as a tuple, then get their inputs and labels (x\_test and y\_test) used to measure performance of the model during training.   
  
The batch\_size=32 means that the training data will be divided into mini-batches of 32 samples, which helps with efficient gradient updates and memory usage. Returned as the learner object, it can now hold the model and data so it is ready to be fine-tuned and validated and later used for prediction purposes.



This method of fit\_onecycle is used to fine-tune the pretrained model. The learning rate (lr=2e-5) control the update of the model weights and has been made very low for stable fine-tuning. The number of epochs is 4, meaning that the training dataset is passed through the model four times.   
 The One Cycle learning rate policy applied by this method slowly increases the learning rate from a very low value to max value and then brings it down to its lowest rate, helping to improve training speed and overall model performance.

To summarize the architecture and training settings of all implemented models, including BERT, we present in the following tables a comparative overview of the key hyperparameters and configurations. This serves as a reference before evaluating their performance in the next chapter.

| **Model** | **Preprocessing** | **Architecture** | **Hyperparameters** |
| --- | --- | --- | --- |
| **SVM** | - TF-IDF (max 3000 features) - Deduplication | -Linear kernel | **-**C=0.1 |
| **LR** | - TF-IDF (max 3000 features) - Deduplication | **-**Linear kernel | -penalty='l1'  -solver='liblinear' |
| **MLP** | - TF-IDF (max 3000 features) - Deduplication | -512-256-128 (ReLU/Sigmoid) | **-**learning\_rate=0.01 (SGD) |
| **RNN** | -  Tokenization + padding - Case-sensitive | - SimpleRNN(128) + Embedding(128) | -learning\_rate=0.0001 (Adam) |
| **LSTM** | Tokenization + padding - Case-sensitive | - Embedding(256) + LSTM(256 → 128) | -learning\_rate=0.001 (Adam) |
| **BERT** | - BERT tokenizer - Lowercasing | - BERTBASE (12 layers) | -lr=2e-5 (OneCycle) |

**Table 3.1:** Overview of Fundamental Parameters and Architectures Used in Model Implementation

As shown in Table 3.1, traditional models like SVM and Logistic Regression were paired with TF-IDF vectorization and simple linear kernels, allowing for efficient training and interpretability. The regularization parameters (C for SVM, L1 penalty for LR) were chosen to balance generalization and sparsity.

For neural networks, the MLP was designed with three dense layers that progressively shrink to capture nonlinear patterns in TF-IDF features, whereas RNN and LSTM models processed tokenized input sequences that preserve the syntactic structure of queries. RNN architecture remains relatively shallow so as to prevent overfitting, whereas LSTM is stacked with memory units that capture long-term dependencies.

BERT, on the other hand, is the language model under the transformers trained on big corpora. Fine-tuning with a small learning rate of 2e-5 and an OneCycleLR scheduler guarantees the achievement of stable convergence. The preprocessing step⎯truncation and lowercasing⎯keeps in line with the pretraining settings of BERTBASE.

The niceties on architecture and preprocessing were made so that a fair comparison can be effected across the various learning paradigms, adapting each model to its strong points in text classification.

| **Model** | **Optimization** | **Regularization** | **Epochs** |
| --- | --- | --- | --- |
| **SVM** | - N/A (solver) | - Implicit L2 | **-**N/A |
| **LR** | -N/A (solver) | **-**L1 penalty | - N/A |
| **MLP** | - SGD + BCE | -Early Stopping (patience=3) | 27 |
| **RNN** | -  Adam + BCE | -Dropout(0.5) + L2(λ=0.01) | 20 |
| **LSTM** | -Adam + BCE | -Early Stopping (patience=3 | 30 |
| **BERT** | - AdamW + BCE | - Built-in dropout | 4 |

1. **Table 3.2:** Optimization Techniques, Regularization Methods, and Training Epochs Used per Model

Each model was configured and hyperparametrized by several configurations and hyperparameters to ensure they reached their maximal performance. The general settings outlined in the above table are essentially the best combinations available for the experiments carried out. Different learning rates, optimizers, regularizers, and epochs were observed with respect to their behavior during training. For example, with recurrent models like RNN and LSTM, there were issues with vanishing gradient; hence, hidden units were tuned, dropout layers employed, and early stopping used. Also, the epochs needed control not to lead to overfitting, which was more critical for deeper architectures. This final configuration, including using AdamW for BERT, dropout for RNNs, and early stopping for MLP and LSTM, consistently showed better performance than alternatives. They provide a compromise between the model's complexity, its rate of training, and its capacity to generalize, thus standing as the best of all configurations we tried.

## 3.4 Conclusion

In this chapter, we described the building and preparing processes for the various SQL injection detection models. We gave the dataset, how it was cleaned and processed, the model structure, and the parameters used in training. The work also offered some code examples and comparison tables to keep things clear.

Testing of the models and analyzing results follow in this; therefore, this work was laying the foundation for the next step. In Chapter 4, we will assess the performance of these models with test data and on fresh unseen data as well: normal and attack. We will compare the results to know which one is the best..

# 

# Chapter 4

# Performance Evaluation and Results

## 4.1 Introduction

In this chapter, we present the evaluation of our SQL injection detection models. After building, training and fine-tuning the models in the previous chapter, we now assess their performance using different metrics. The evaluation is done on both the test dataset and unseen data to check how well each model generalizes. We also compare our results with other existing works and provide explanations for the performance differences.

## 4.2 Development Environment Overview

### 4.2.1 Programming language

**Python**

Python is widely used in machine learning and deep learning, and for good reason. Its clean and simple syntax makes it easy to learn and work with, which is especially helpful when building and testing complex models.  A key strong point of Python is its huge selection of libraries, which include TensorFlow, PyTorch, Scikit-learn, and Keras. These libraries offer pre-written code and functionsthat save time and make the development process easier. Python also has a huge community of developers and researchers, which means there’s plenty of documentation, tutorials, and support available online. Python offers simplicity, flexibility, and strong tools, all of which render it an optimal language for machine learning and deep learning projects.

### 4.2.2 Libraries

**Numpy :** The fundamental library for numerical computation in Python, NumPy, handles arrays, mathematical operations, and prediction outputs such as probability arrays and class labels.  
  
**Pandas :** The pandas library is efficient for data manipulation and data analysis. we used it in this study to import the CSV dataset, remove duplicate rows, handle missing data, and cast data into appropriate formats for training models  
Chardet: Chardet library is a character encoding detection library, and we have used it in order to detect an appropriate encoding for our CSV file which could be read by pandas successfully.  
  
**Ktrain :** A high-level TensorFlow/Keras library that facilitates easy training, testing, and interpretation of deep learning models. Consistent with this, we used it to transform data into BERT-compatible format, train a text classification model, and evaluate the performance of the model.

**Matplotlib :** matplotlib is a graph and chart creation library. We leveraged it to plot class distributions, training loss and validation loss, training accuracy and validation accuracy, and the confusion matrix.

### 4.2.3 Development setup

#### 4.2.3.1 Visual Studio Code

Visual Studio Code (VS Code) is free, open-source software meant for coding, developed by Microsoft. Its support many programming languages such as Python, C++, JavaScript, etc. Equipped with syntax highlighting, code completion (IntelliSense), a debugging tools, and a customizable user interface, and an integrated terminal.

VS Code is very extensible and its capability can, therefore, be enhanced by any user with thousands of extensions that support frameworks, debugger.

It has support for Markdown to style text, allowing users to document alongside their code. With its lightweight might combined with powerful development features, Visual Studio Code is among the most popular editors for web developers, data scientists, DevOps engineers, and others.

#### 4.2.3.2 Jupyter Notebook

The Jupyter Notebook is an open-source, browser-based interactive environment that offers users the ability to create and share documents that contain live code, equations, visualizations, and narrative text. Data scientists, machine learning specialists and scientific researchers are massive user bases of Jupyter Notebooks. They are used for easy experimentation, reproducibility, and collaborative purposes. A notebook is divided into cells, cells can be individually run. Having such a structure makes the Jupyter Notebook very handy for stepwise analysis, prototyping, and reporting. The format enhances understanding by combining code with explanations and visual output.

#### 4.2.3.3 Google colab

Google Colaboratory (or Colab) is a free cloud service that allows users to write and execute Python in Jupyter Notebook environment without the necessity of local setup. Supporting machine learning, deep learning, data analysis, and research workflows. Colab offers access to computing resources , i.e., CPUs, GPUs, and TPUs, right within the browser. It is majorly used for prototyping, or collaborative development, built-in support for Google Drive and support for major Python libraries such as TensorFlow, PyTorch, and Pandas.

For our work, we used The NVIDIA Tesla T4. It is a powerful energy-efficient GPU designed for a wide range of AI workloads. It was built over the Turing architecture and includes Tensor Cores to accelerate deep learning compute and RT Cores for ray tracing. The T4 GPU comes with 16 GB of GDDR6 memory and supports mixed precision computing. It also delivers up to 260 TOPS (Tera Operations per Second) for INT8 inference. It is mostly used in cloud environments (like Google Colab) for efficiently accelerated machine learning workflows.

## 4.3 Performance Evaluation Metrics

The classification performance of the fine-tuned BERT model in detecting SQL injection attacks was evaluated with the help of multiple performance evaluation metrics. They include accuracy, precision, recall, and F1-score, which help to analyze the effectiveness of the model detecting malicious and benign SQL queries.

**Confusion Marix**

A confusion matrix is a table that summarizes the performance of a classification model by comparing its predicted labels to the true labels. It displays the number of true positives (TP), true negatives (TN), false positives (FP), and false negatives (FN) of the model's predictions[.[30]](#_[30]_EVIDENTLY_AI,)



True Positive (TP) : It shows the number of correctly identified positive cases.

True Negative (TN) : It shows the number of correctly identified negative cases.

False Positive (FP) :  It shows the number of incorrectly predicted positive cases.

False Negative (FN) : It shows the number of incorrectly predicted negative cases.

**1 Accuracy :**

Accuracy is a fundamental metric for evaluating the performance of a classification model, providing a quick snapshot of how well the model is performing in terms of correct predictions.



**2 Precision :**

Precision is a measure of a model’s performance that tells you how many of the positive predictions made by the model are actually correct. This metric reflects the model’s ability to avoid false positives, high precision means that when the model predicts “positive,” it is usually correct.



**3 Recall :**

It measures how well the model captures all relevant positive cases. This measures the model’s ability to capture positive instances, high recall means most true positives are detected by the classifier.



**4 F1-score :**

The F1-score is metric that balances both precision and recall**.** This metric usually tells us how precise (correctly classifies true positives) and robust (minimizes false negatives) our classifier is**.** The more the F1 score better will be performance.

****

## 4.4 Evaluation on Test Set (20%)

### 4.4.1 Results Presentation

In this section, we present the performance results of the proposed models evaluated on the test dataset, which represents 20% of the original data. We report common classification metrics such as Accuracy, Precision, Recall, and F1-score to assess each model's ability to correctly detect SQL injection attempts**.**

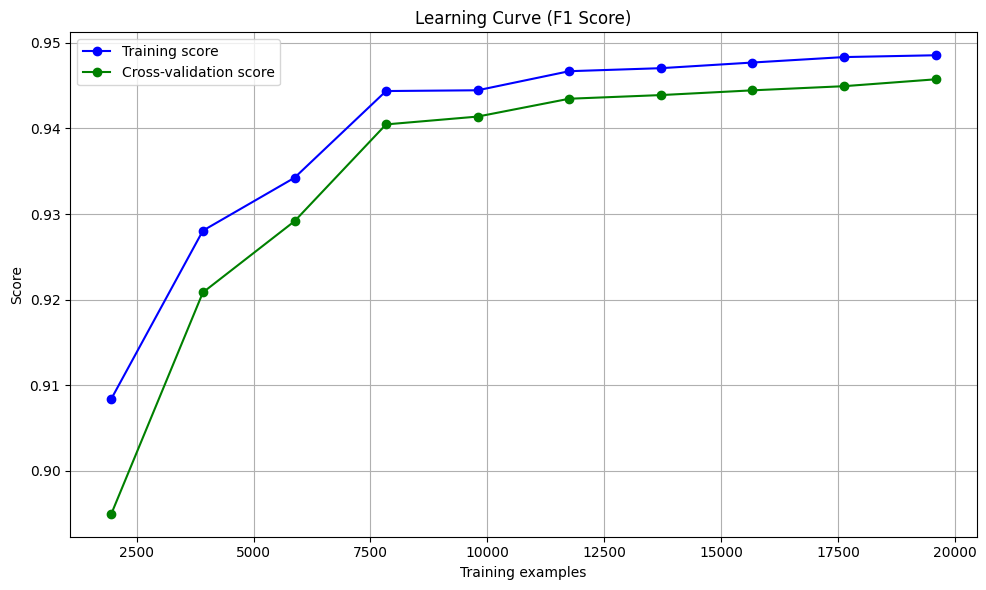
|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Model** | **Accuracy** | **Precision** | **Recall** |  | **F1 Score** | **Precision** |
| **SVM** | 98.56% | 99.86 % | 96.25% |  | 99.02% | N/A |
| **LR** | 98.12% | 99.72% | 95.25% |  | 97.44% | 99.74 |
| **MLP** | 99.44% | 99.51% | 98.98% |  | 99.25% |  |
| **RNN** | 99.06% | 100% | 97.51% |  | 98.74% |  |
| **LSTM** | 99.62% | 99.73% | 99.25% |  | 99.49% |  |
| **BERT** | **99.92%** | **99.87%** | **100%** |  | **99.93%** | 98.05% |

**Table 4.1** Performance Comparison of Models on SQL Injection Dataset

The experimental results demonstrate outstanding performance across all evaluation metrics. Traditional machine learning models such as Support Vector Machine (SVM) and Logistic Regression are strong contenders; for instance, the SVM model got an accuracy of 98.56% and an F1-score of 99.02%. Contrary to popular belief, which states that SVM accuracy tends to saturate on complex tasks, our model indeed showed fine generalization ability along with confirmation of training and validation curves.   
  
The deep learning models; the MLP and RNN also enhanced the system. LSTM had slightly higher performance: 99.62% accuracy and 99.49% F1-score. But BERT was the strongest performer, with 99.92% accuracy and 100% recall-an indication that it is unbeatable when it comes to detecting SQL injections from very complex types of input patterns.  
  
Beyond the ability of any model, the dataset was a big factor for such astounding performances, having been cleaned and preprocessed to minimize noise and ensure higher consistency of training data. Extensive hyperparameter tuning was done for every model to extract the maximum out of the training, including trying out numerous configurations before finally settling on the best.

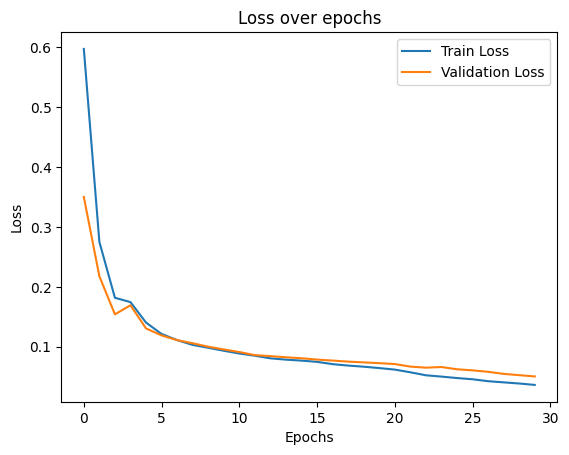
These results demonstrate the effectiveness of using deep learning, especially Transformer-based models, for SQL injection detection. The next section provides additional visualizations (learning curves and confusion matrices) to support these findings and illustrate the training behavior of selected models.

### 4.4.2 Visual Performance Analysis

****

**Figure 4.2** F1-Score Across Cross-Validation Folds for the SVM Model

For the SVM model, additional cross-validation was performed. The F1-score remained consistently high across folds, and the training/cross-validation curve shows a stable gap, confirming that the model does not overfit and generalizes well.

****

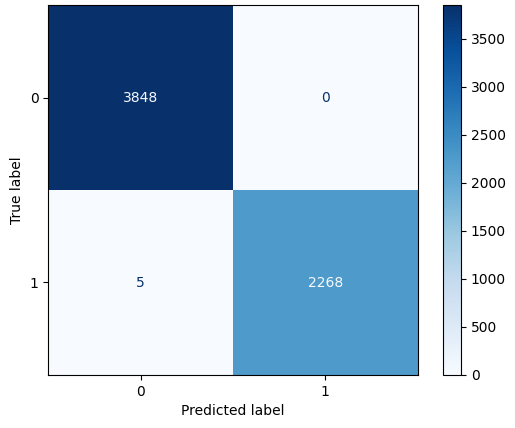
**Figure 4.3** LSTM Training and Validation Loss over Epochs

This figure illustrates the training and validation loss progression for the LSTM model. The close alignment of both curves and the continuous decrease in loss demonstrate stable learning and the absence of overfitting**.**

### 4.4.3 Performance Analysis of BERT

The results obtained reflect the model’s ability to correctly classify instances and demonstrate its effectiveness in detecting SQL injection queries benign queries.

**Confusion matrix :**

****

**Class 0** = Negative class (Benign queries)

**Class 1** = Positive class (SQL injection queries)

**TN (True Negative :** benign queries predicted as benign queries **)** = 3848

**FP (False Positive :** benign queries predicted as SQL injection**)** = 0

**FN (False Negative :** SQL injection predicted as benging queries **)** = 5

**TP (True Positive :** SQL injection predicted as SQL injection**)** = 2268

**Accuracy :**

The model achieves an accuracy of approximately **99.92%**, meaning that nearly all predictions both positive and negative are correct. This metric shows the overall effectiveness of the classifier across both classes, indicating very strong general performance.

**Precision :**

With a precision of **100%**, the model demonstrates perfect reliability in its positive predictions. It means that every instance labeled as positive by the model is indeed a true positive, with no false positives recorded, showing that the model achieves high reliability in classifying SQL injection instances.

**Recall :**

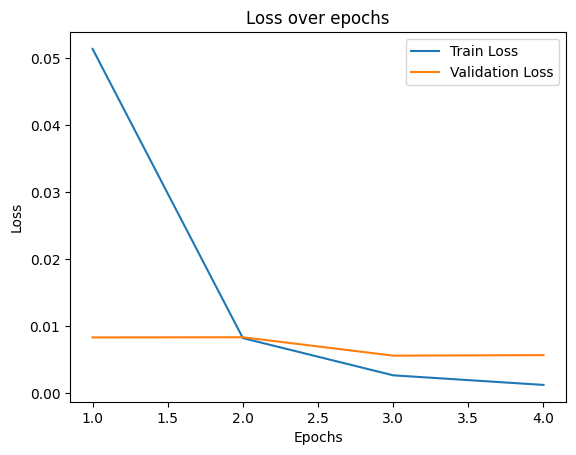
The recall is approximately **99.78%**, indicating that the model successfully captures almost all actual positive instances. Only 5 positive cases were missed (false negatives), showing that the model has high sensitivity and is effective at detecting relevant cases.

**F1-Score :**

The F1-score, calculated at **99.89%**, balances precision and recall into a single metric. It confirms that the model maintains both high correctness in its predictions and thoroughness in identifying positive instances. This makes it highly dependable in scenarios requiring both precision and sensitivity.

#### 4.4.3.1 Training Loss Curve

We show the training loss curve to better understand how the BERT model learned during training. The loss keeps going down steadily, which means the model is learning well without problems like overfitting. This shows that the training went smoothly and the model works well.



**Figure 4.** Training Loss Curve for the Fine-Tuned BERT Model

#### 4.4.3.2 Model Evaluation on New Unseen Data

First, we created a predictor object that use the fine-tuned model and preprocessing pipeline to make predictions on new data:

We then took a test dataset named sqliv2\_utf8.csv. From this dataset, 500 examples were sampled for each class (label 0, label 1), a total of 1000 examples. The prediction results are summarized below:

**For Label = 1:**

The model correctly predicted all **500 samples as SQL injections**, reaching an **accuracy of 100%** for this class. This means that no positive instances were missed by the model.

**For Label = 0:**

Of the 500 Label 0 samples, the model predicted **499 were predicted correctly as benign queries,** and 1 was predicted incorrectly as a SQL injection. An accuracy of **99.8%** for the benign queries.

**Overall Performance :**

Below is the confusion matrix showing these results:



The confusion matrix offers a comprehensive overview of the model's ability to correctly classify each category on unseen data, demonstrating its ability to accurately distinguish between Class 0 (benign queries) and Class 1 (SQL injection**)** instances. The analysis shows exceptional performance across all standard evaluation metrics:

1. **Accuracy (99.9%) :**

With almost perfect accuracy, the model made 999 out of 1000 correct predictions. This exceptional performance suggests that the model has learned the underlying patterns in the data extremely well. That one misclassification accounts for just 0.1% error rate.

1. **Precision (99.8%)**

With a single false positive, this implies the precision value of 99.8%, which means that whenever the model predicted Class 1, it was almost surely correct. High precision is particularly valuable in scenarios where false positives carry significant costs.

1. **Recall (100%)**

The perfect recall score indicates the model successfully identifies all actual positive cases without any false negatives. This is crucial for applications where missing positive cases (Type II errors) could have serious consequences, such as detecting SQL injection attacks.

1. **F1-Score (99.9%)**

Almost perfectly balanced between precision and recall, the F1 indicates that there is a clear balance of these metrics with no trade-offs. This means that in terms of the model, one metric is not sacrificed for the other: achieving high precision and perfect recall at the same time.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Model** | **Accuracy** | **Precision** | **Recall** |  | **F1 Score** |
| **SVM** | 99,08% | 100% | 99,08% |  | 99.02% |
| **LR** | 97,44% | 100% | 97,44% |  | 98,70% |
| **MLP** | 98,99% | 100% | 98,99% |  | 99,49% |
| **RNN** | 98,85% | 100% | 98,85% |  | 99,42% |
| **LSTM** | 98,35% | 100% | 97.85% |  | 99,17% |
| **BERT** | **99.90%** | **99.98%** | **100%** |  | **99.99%** |

**Table 4.2** Performance Comparison of Models on Unseen SQL Injection Dataset

The five traditional and deep learning models were subjected to evaluation on the full sqliv2\_utf8 dataset consisting of 11,424 SQL injection samples and 22,302 benign queries: SVM, Logistic Regression, MLP, RNN, and LSTM. BERT, however, was tested only on a balanced subset of this dataset: 1,000 samples, with 500 SQL injection cases and 500 benign queries. Being tested on a smaller test bed, BERT still generated the best performance metrics, when compared to the other models.

# ****References****

##### [1]

##### [2] OWASP “SQL Injection (SQLI)”:

<https://owasp.org/www-community/attacks/SQL_Injection>

##### [3] Bright security “SQL Injection Attack”:

<https://brightsec.com/blog/sql-injection-attack/>

##### [4] Beagle Security “Error based SQL Injection”

<https://beaglesecurity.com/blog/vulnerability/error-based-sqli.html>

##### [5] Dafydd Stittard and Marcos Pinto,The web Application Hacker’s Handbook: Finding and Exploiting Security Flaws, 2nd Edition, Wiley Publishing Inc, 2011.

##### [6] OWASP, “Blind SQL injection”:

<https://owasp.org/www-community/attacks/Blind_SQL_Injection>

##### [7] Moxso, “SQL Tautology” :

<https://moxso.com/blog/glossary/tautology>

##### [8] Justin Clarke, SQL Injection Attackes and Deffense

##### [9] OWASP Cheat Sheet Series, “SQL Injection Prevention”:

<https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html>

##### [10] OWASP Cheat Sheet Series, “Query Parameterization”:

<https://cheatsheetseries.owasp.org/cheatsheets/Query_Parameterization_Cheat_Sheet.html>

##### [11] PHP “Prepared statements and stored procedures”:

[https://www.php.net/manual/en/pdo.prepared-statements.php](https://www.php.net/manual/en/pdo.prepared-statements.php )

##### [12] PHP , “Validation”:

<https://www.php.net/manual/fr/filter.examples.validation.php>

##### [13] Mitchell, T. M, Machine Learning. McGraw-Hill, 1997.

##### [14] Amer F.A.H. ALNUAIMI and Tasnim H.K. ALBALDAWI, An overview of machine learning classification techniques.

##### [15] IBM ,“Machine Learning”

<https://www.ibm.com/think/topics/machine-learning>

##### [16] Reinforcement Learning: An Introduction Second edition, in progress Richard S. Sutton and Andrew G. Barto c 2014, 2015

##### [17] GeeksforGeeks ,“ Logistic Regression in Machine Learning”

<https://www.geeksforgeeks.org/understanding-logistic-regression/>

##### [18] MathsWorks, “Support Vector Machine”

<https://www.mathworks.com/discovery/support-vector-machine.html>

##### [19] IBM ,“Machine Learning”

<https://www.ibm.com/think/topics/machine-learning>

##### [20] TeckTarget, “What is deep learning and how does it work?”

<https://www.techtarget.com/searchenterpriseai/definition/deep-learning-deep-neural-network>

##### [21] Medium “Basic Notations and Representation: Neural Networks”

<https://medium.com/@anushruthikae/basic-notations-and-representation-neural-networks-d46a1be97471>

##### [22] V7 Labs, “Activation Functions in Neural Networks [12 Types & Use Cases]”

<https://www.v7labs.com/blog/neural-networks-activation-functions#3-types-of-neural-networks-activation-functions>

##### [23] Shelf, “Why Recurrent Neural Networks (RNNs) Dominate Sequential Data Analysis”

<https://shelf.io/blog/recurrent-neural-networks/>

##### [24] Amazone Web Services, “What is RNN (Recurrent Neural Network)?”

<https://aws.amazon.com/what-is/recurrent-neural-network/?nc1=h_ls>

##### [25]AIML, “What are the advantages and disadvantages of a Recurrent Neural Network (RNN)? ”

<https://aiml.com/what-are-the-advantages-and-disadvantages-of-a-recurrent-neural-network-rnn/>

##### [26] MathsWorks, “Long Short-Term Memory (LSTM)”

<https://www.mathworks.com/discovery/lstm.html>

##### [27] Ashish Vaswani, Noam Shazeer, Niki Parmar, Jakob Uszkoreit, Llion Jones, Aidan N. Gomez, Lukasz Kaiser, Illia Polosukhin, Attention is all you need, version 5, 2017.

##### [28] GeeksforGeeks, “Architecture and Working of Transformers in Deep Learning”

<https://www.geeksforgeeks.org/architecture-and-working-of-transformers-in-deep-learning/>

##### [29] Envisioning, “Point-wise Feedforward Network”

<https://www.envisioning.io/vocab/point-wise-feedforward-network>

##### [30] EVIDENTLY AI, “How to interpret a confusion matrix for a machine learning model”

<https://www.evidentlyai.com/classification-metrics/confusion-matrix>