Vol. 3 No. 2 (2025)

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138

Print ISSN
3007-312X

An Innovative Machine Learning based end-to-end Data Security Framework in Emerging Cloud Computing Databases and Integrated Paradigms: Analysis on Taxonomy, challenges, and Opportunities

Muhammad Shaharyar Ramzan[1]
Department of Computer Science, Faculty of Computer Science & IT Superior, University Lahore, 54000, Pakistan.
shaharyarramzan56@gmail.com
Fawad Nasim[2]
Department of Computer Science, Faculty of Computer Science & IT Superior, University Lahore, 54000, Pakistan
fawad.nasim@superior.edu.pk
Hafiz Nabeel Ahmed[3]
University of Hertfordshire, nabeelahmedbulc@gmail.com
Umar Farooq[4]
University of Northumbria. Umarnorthumbria@gmail.com
Muhammad Sheraz Nawaz[5]
University of Management and Technology (UMT), Lahore, 54000, Pakistan. msheraz135@outlook.com
Syed Krar Haider Bukhari[6]
Department of Computer Science, Faculty of Computer Science & IT Superior, University Lahore, 54000, Pakistan
karar.haider@superior.edu.pk
Hamayun Khan[7]
Department of Computer Science, Faculty of Computer Science & IT Superior, University Lahore, 54000, Pakistan
hamayun.khan@superior.edu.pk

Vol. 3 No. 2 (2025)

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138

Print ISSN
3007-312X

Abstract

Database systems have been prime targets for cyber-attacks and threats due to the critical nature of the data they store. SQL injection is the most persistent and critical threat to database security, which enables attackers to manipulate queries and access, unauthorized data to steal sensitive information. Now-a-day the rising complexity of cyberattacks, traditional-based detection systems often fall due to short in accurately identifying the vulnerabilities. In the last few years, machine learning algorithms have played an important role in detecting SQL injection attacks due to their ability to analyze threats. This paper aims to provide a comprehensive comparative analysis of machine learning algorithms employed in SQL injection detection. In this paper we evaluate the performance across diverse datasets, and metrics to show the accuracy, precision, recall and computational efficiency are examined to detect their strengths and limitations. Additionally, this paper discusses the feature selection, model interpretability, real-time application and challenges in threat detection. These findings provide a clear understanding of the most effective machine learning approaches for enhancing database security, which provide comprehensive guidelines for future research and development. The paper analyzes recent Machine learning studies and explores advanced strategies for mitigating these threats, such as AI-driven anomaly detection, blockchain-based security models, and Zero Trust architectures. The objective is to provide a clear understanding of the risks and actionable insights into building robust, secure database systems. This study offers a comprehensive

Spectrum of Engineering Sciences
Online ISSN
3007-3138
Print ISSN
3007-312X

analysis aimed at helping researchers and practitioners develop effective data security measures, ensuring both resilience and adaptability in an increasingly hostile cyber environment.

Keywords: Database, Security, SQL Injection, Machine learning, Cyber risk, Open data, Systematic review, DBMS, database security threat mitigation, Data protection strategies for DBMS, Cyber threats in database management

Introduction

SQL injection is one of the most dangerous and persistent attacks for the security of vulnerability targeting the database to manipulate queries and access the unauthorized to steal the sensitive information. Increasing the reliance on the database application across industries, therefore, needs to develop advanced methods for SQL injection detection [1]. Traditional techniques like input validation, parameterized queries and web application firewalls, while effective to the extent, struggle to adapt to complex systems to detect the threats. Machine learning provides a comprehensive approach to detect the mitigate SQL injection attacks through pattern recognition, anomaly detection and real-time analysis [2]. This paper provides a comprehensive review of various machine learning algorithms used for SQL injection detection, evaluating their performance, computational efficiency and real-world scenarios, which provide database security and guide future research in this domain. Despite advancements in cybersecurity technologies, significant gaps remain in fully addressing the risks associated with DBMS. Current research often focuses on isolated threats or specific technologies, resulting in

Spectrum of Engineering Sciences
Online ISSN
3007-3138
Print ISSN
3007-312X

fragmented strategies [3]. Moreover, the dynamic nature of cyber threats and the lack of integrated solutions highlight the need for a holistic approach to database security. This review consolidates findings from multiple studies to bridge these gaps, providing a comprehensive understanding of the challenges and potential solutions [4]. The database server is used for storing and managing the data in the finance, healthcare, e-commerce and government sectors. Now I need to ensure the security of the database which protects the stolen sensitive data [5, 6]. Pervasive threats are the most dangerous for database security SQL injection, a type of cyberattack where malicious SQL statements are inserted into fields to manipulate database queries. These types of attacks can bypass authentication, sensitive data even destroy databases which poses a severe challenge to cybersecurity professionals [7, 8].

Vol. 3 No. 2 (2025)

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138

Print ISSN
3007-312X

Table 1: Non-technical threats in DBMS [9]

Technical threats	Description of threats	Impact and example of threats
Human error	Human mistakes such as accidental disclosures of sensitive information, misdirected emails, and unintentional disclosure of login credentials.	Disclosures of sensitive information, misdirected emails, unintentional disclosure of login credentials
Insider threats	People who have access to sensitive data can intentionally misuse this data for malicious reasons. They are considered as threatening as the outsider threats. Insiders may be disgruntled employees, contractors and business partners. Some tactics that malicious users may use are copying files onto a Universal Serial Bus (USB) drive, emailing sensitive information to a personal account, sharing access credentials with unauthorized individuals, or even planting malware or other hacking tools to facilitate their activities. Insider threats can also be inadvertent negligence by individuals.	Internal threats from employees, lack of awareness and employee negligence
Third-party risks	Some organizations rely on third-party systems or services to manage their data, security vulnerabilities in these third-party systems, or services put enterprise data at risk.	Third-party risks

The Prevalence of SQL injection attacks is a necessity for robust detection to prevention mechanisms. The traditional approaches such as input validation and parameterized queries provide some defense, they adapt to novel and sophisticated attack patterns. These limitations for researchers and practitioners to explore advanced techniques, including the application of machine learning to detect and mitigate SQL injection attacks [10, 11].

Vol. 3 No. 2 (2025)

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138

Print ISSN
3007-312X

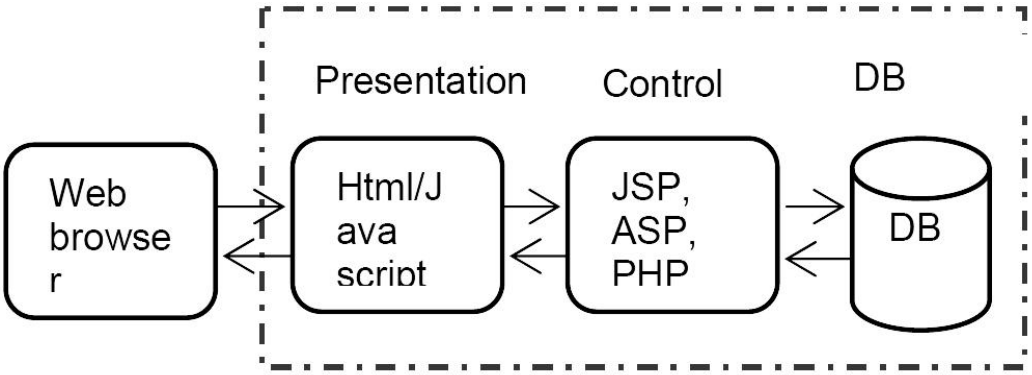

Figure 1: Web & Cloud Database Architecture [12]

SQL injection is a highly effective and dangerous cyberattack that targets web applications and database systems by exploiting vulnerabilities in user input. This type of attack injects malicious SQL code into input fields, like login forms or search boxes, which are executed by the database server. The attacker manipulates the query, which was not intended by the original developers, which provides authorization access to sensitive data like usernames, passwords, financial records and confidential information [13].

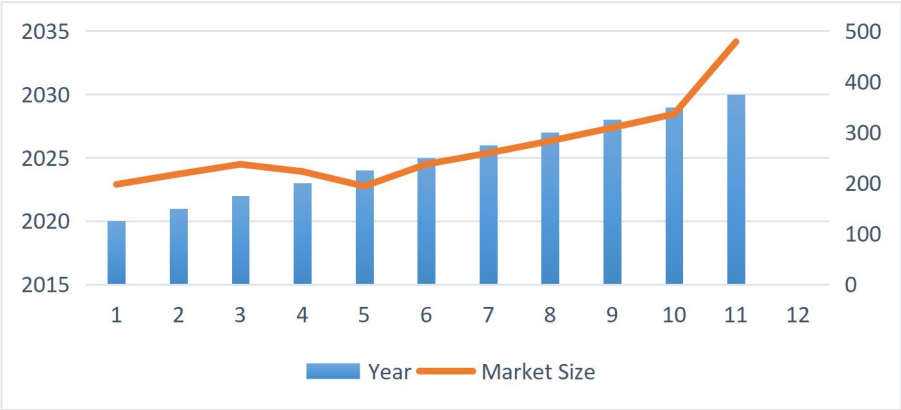

Figure 2: Show the Market Size of Cybersecurity for DB

Vol. 3 No. 2 (2025)

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138

Print ISSN
3007-312X

Significance and Taxonomy of SQL Injection

SQL (Structured Query Language) is a database language that is used to add, delete, modify, and query data in a relational database. As long as the system uses the database, most of it interacts with the database through SQL statements. The SQL injection attacks can bypass authentication mechanisms, which allows attackers to access the system without privileges of proper authorization. The attackers can use SQL injection to delete and modify data causing severe operational disruptions or financial damage. One of the main reasons SQL injection persists is the threat, which allows attackers with limited technical expertise to exploit poorly secured applications. In advanced security methods, SQL injection plays an important role in exploiting vulnerabilities in web applications, particularly those that do not follow the best practices for input validation and query handling [14]. This makes SQL injection a concern for cybersecurity professionals tasked with protecting sensitive data and ensuring the integrity of database applications [15].

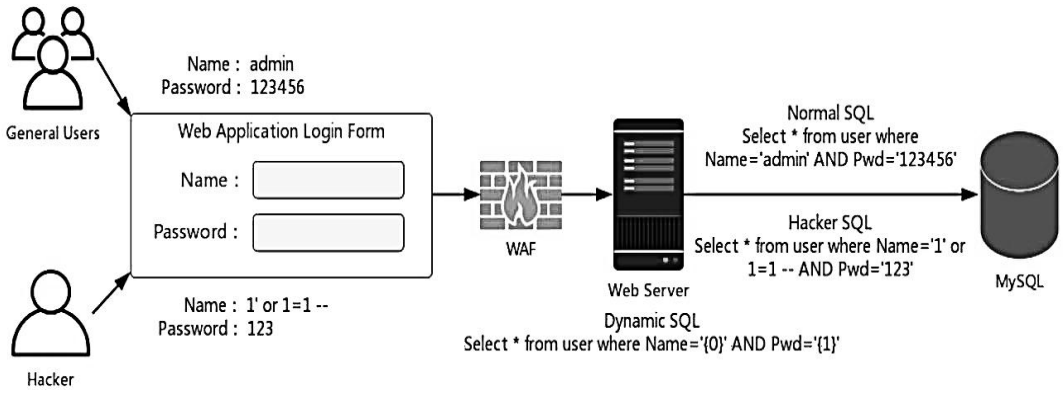

Figure 3: Attack Process of SQL Injection [16]

The application of databases across a wide range of industries has made secure by management practices more critical than ever. The

Vol. 3 No. 2 (2025)
Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

rapidly increasing digital platforms in the finance, healthcare, e-commerce and government sectors rely on sophisticated database systems to store and manage the vast amount of sensitive data [17, 18]. The sophistication of attacks increases and their impact on these industries has become more severe. In the financial sector, a successful SQL injection attack can lead to the unauthorized extraction of customer data like account numbers, credit card details and translation histories and other personal information. This data can be stolen on the black market, which is used for identity theft and fraud.

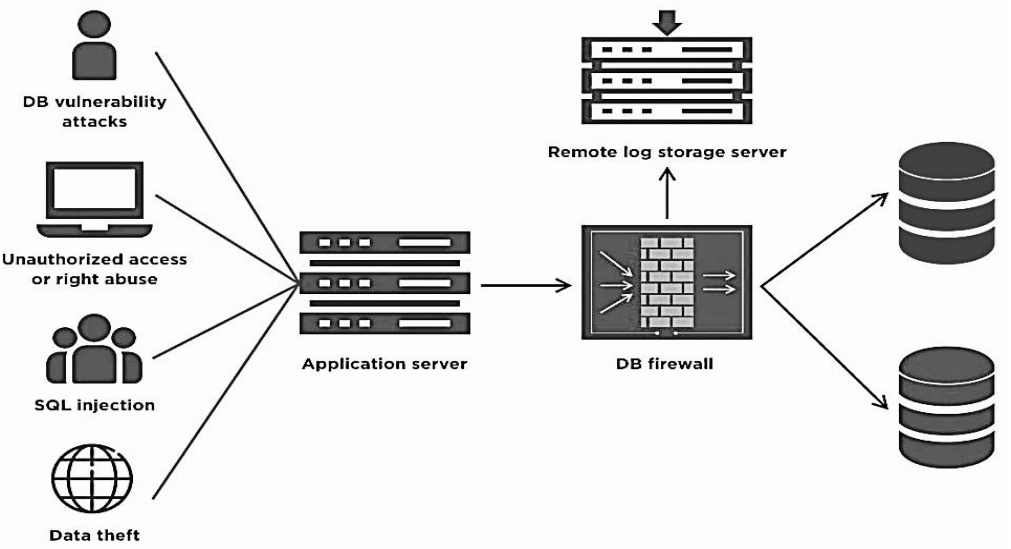

Figure 4: Database with Firewall Security system [19]

The financial losses from breaches of data can be substantial, especially if the attacker disrupts the banking operations or online payment system. In the healthcare sector, databases contain sensitive patient information like medical histories, test results and personal identification. In SQL, the UNION operator is used to join two SQL statements or queries [20].

Vol. 3 No. 2 (2025)

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138

Print ISSN
3007-312X

Union Based SQL Injection

Union SQL Injection takes advantage of this feature to make the database return desired results in addition to the intended results.

Error Based SQL Injection

Error-Based SQL Injection Error error-based SQL Injection approach works by passing an invalid input in the query and thereby triggering an error in the database.

Blind SQL Injection

Blind SQL Injection attack is a technique where the malicious user asks questions to the database and decides on further course of action based on the returned answers.

Boolean-Based SQL Injection

Boolean-Based SQL Injection Boolean-based SQL Injection is an inferential SQL Injection technique that relies on sending an SQL query to the database which forces the application to return a different result depending on whether the query returns a TRUE or

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

FALSE result.

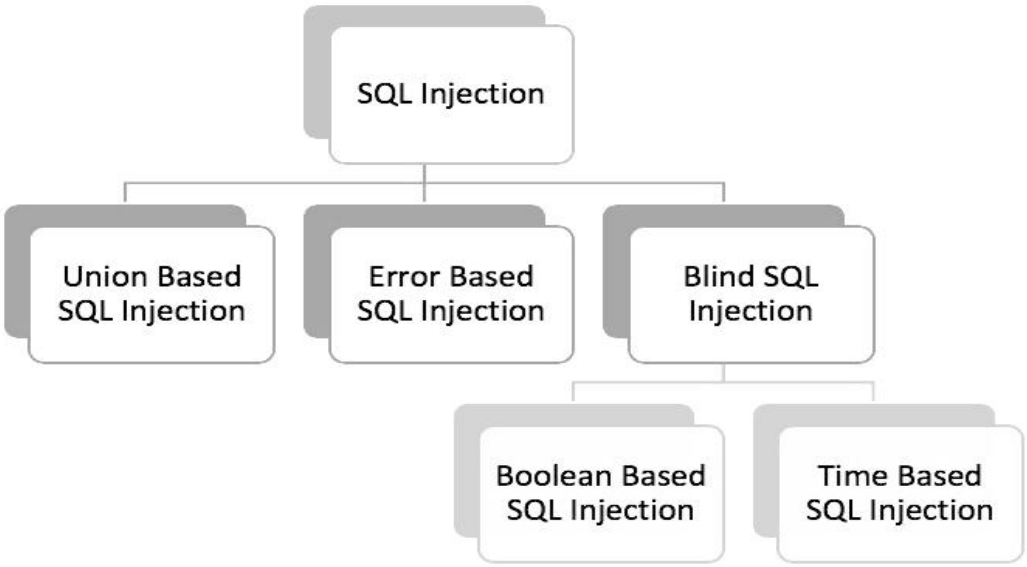

Figure 5: Various Types of SQL Injection [21]

The SQL injection attack on the healthcare system exposes private data, which violates patient privacy laws. This is a risk for patients, which leads to costly legal penalties, lawsuits and regulatory sanctions. The e-commerce business faces the challenges of securing customer data and also the transactional information [22]. SQL injection can allow attackers to access the customer profiles, order histories and payment details, leading to direct financial theft. The SQL injection attacks can damage the integrity of product inventories and order systems, including halting sales and delivery issues. When a customer feels that their data is not secure they abandon online platforms which causes the loss. The e-commerce platforms also face the risk of negative publicity and loss as a result of security breaches. In the government sector, SQL injection attacks can steal public service databases like citizens' personal information, tax records, voting data

Vol. 3 No. 2 (2025)

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138

Print ISSN
3007-312X

and national security data. The attackers in the government sector, lose trust in government services, which is a risk to national security and even interference with election processes [23].

Table 2: Non-technical threats in Databases [24]

Countermeasures	Description
Data encryption	Encryption is the process of transforming data into a coded format to make it unreadable by intruders and difficult to decipher, whether it is during transmission or at rest. It can be applied to many data types, such as emails, files, databases, and other communication channels. Encryption can also prevent insider threats, as insiders who have access to the data will not be able to read it unless they have the required authorization. In addition, it helps organizations to ensure their confidentiality, integrity, and availability by adhering to several data protection regulations, such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA). Ensures the security of users by converting the data with the AES algorithm to the database management system, Message Digest (MD5), and Secure Hash Algorithm (SHA-256) to protect network data transmission. It is cost-effective; investing in the implementation of encryption technology is cheaper than dealing with the consequences of data breaches.
Access control	All DBMS use access control to create user accounts and passwords to prevent unauthorized people from entering the database system and obtaining confidential information. Granting and revoking privileges are methods of enforcing access control. The organization must set policies defined by access control that all contact with the databases must adhere to. It is suggested that web tripwire and login rituals be integrated using Multi-Factor Authentication (MFA). Access control allows organizations to do the following: - Access control allows organizations to implement a layered defense approach to security. - Helps organizations follow protection data regulations. - Prevents insider threats. - Allows organizations to detect and respond to security incidents. Access control systems consist of: - File permissions to create, read, edit, or delete files on the server. - Program permissions are the rights of executing an application program on the server. - Data rights, the rights of retrieving, or updating data in a database. Access control mechanisms: 1. Discretionary Access Control (DAC) 2. Mandatory Access Control (MAC) 3. Role-Based Access Control (RBAC)

Spectrum of Engineering Sciences
Online ISSN
3007-3138
Print ISSN
3007-312X

Governments provide high-profile targets for cyber criminals and adopt advanced defense mechanisms to protect their databases. The objective of the study is analysis of the comprehensive review and comparison of machine learning algorithms for detecting SQL injection attacks. The main objective of this focuses on evaluating the performance of each algorithm. The study aims to assess the computational efficiency and their practical applicability in real-world scenarios, like handling large-scale data and providing real-time threat detection [25]. We analyze the strengths and limitations of each algorithm, provide valuable insights for future researchers, and enhance data security. The study aims to contribute to the advancement of more robust and adaptive solutions for SQL injection threats. Machine learning plays an important role in cybersecurity to detect threats. This paper focuses on the importance of choosing the right features understanding how the machine learning model makes decisions and applying the real-time to detect the SQL injection attacks. This paper highlights the need to tackle challenges like unbalanced datasets, high computational demands, and finding a balance between accuracy and efficiency. By exploring these areas, this study aims to provide useful insight into database security and create stronger detection systems for the future [26].

Vol. 3 No. 2 (2025)

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138

Print ISSN
3007-312X

Table 3: Comparison of Database- Security threats, Solutions and damage [27]

First level threats	Second level threats	Damage	Solutions
Data not effectively protected	Data tampering	Data distortion or invalid	Tamper detection, User authentication, data encryption, Tamper proof material
	Data exposure	Illegal use User' data	User authentication, data encryption, Audit, Construct machine learning model
	Data monitored or collected	Privacy disclosure	Establishment of special system, data encryption
User exception	Illegal act	Break the role code of conduct	Intrusion detection, Establishment of special system, User behavior analysis
	Unauthorized access	Illegal processing of data	Access control
	Weak safety awareness	Create a breakthrough for attackers	Empirical research
Vulnerability of Defense system	Bug	Used to destroy the database	Safety assessment, Empirical framework
	Inaccurate identification	Reject normal users and accept illegal users	User authentication

Challenges, and Opportunities of Traditional Detection Methods

Traditional security methods are used to protect the database from SQL injection attacks, which help prevent many attacks. These include techniques like input validation, parameterized queries, and web application firewalls. These approaches have significant limitations, especially, when cyberattacks become more sophisticated [28].

Input Validation

Input validation is the technique where the user input is checked to ensure they do not contain harmful SQL code. The input validation can block some basic attacks, but it is not foolproof. The attackers can sometimes bypass the input validation by using tricks, like encoding the malicious code or using unusual syntax. The input validation does

Spectrum of Engineering Sciences
Online ISSN
3007-3138
Print ISSN
3007-312X

not address the root cause of the vulnerability and can be misconfigured [29].

Parameterized Queries

Parameterized queries are designed to separate SQL commands from user inputs, making the harder for attackers to inject malicious SQL code. This method is more effective than the basic input validation. However, it still relies on developers' correct implementation[11]. If the developer does not use parameterized queries correctly in the SQL in the application, the system remains vulnerable to attacks [30].

Web Application Firewall

Web application firewalls are used to filter and monitor the traffic of websites or applications to block harmful data. Web application firewalls can detect harmful data and block the many types of SQL injection attacks. This relies on predefined patterns of known attacks, which makes them less effective against new or sophisticated attack techniques. Web application firewalls can introduce false positives, blocking the requests that resemble malicious ones, which can disrupt normal operations [31].

Static Nature of Traditional Methods

One of the biggest issues in the traditional methods is the static. These are designed to block the known attack patterns to detect the new methods of SQL injection. Cybercriminals find new ways to exploit vulnerabilities, and the traditional defenses cannot change tactics. As a result, systems protected by the methods remain at risk, and the attackers adapt and refine strategies over time [32].

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

Difficulty with Complex Systems

Modern applications become complex, the traditional methods increasing difficulty in detecting sophisticated SQL injection attacks. The attackers used multiple techniques like encoding and advanced payloads to make it harder for traditional systems to identify and block them. These advanced attacks can bypass the protection methods and leave databases exposed [33].

Literature Review

In the field of cybersecurity, various machine learning algorithms are used to detect and prevent SQL injection attacks. The main objective of the literature review is to analyze the machine learning algorithms performance and compare them. We analyze the various machine learning algorithms like Decision Tree (DT), Support Vector Machine (SVM), Random Forest (RF), and Artificial Neural Networks (ANN) and evaluate their unique strengths and limitations. SQL injection attacks have been a serious issue since the 1970s. The OWASP and CWE tools classified these vulnerabilities, which exploit the improper coding practices and generation of SQL queries. Common defenses like input validation, data stored procedures, and pattern matching have some limitations. Machine learning algorithms like Support Vector Machines (SVM), have achieved 94% accuracy in detecting SQL injection attacks [34, 35]. The objective is to compare the several machine learning algorithms and techniques explored to identify and prevent SQL injection attacks. We analyze and compare machine learning algorithms like Naive Bayes (NB), Decision Tree (DT), Support Vector Machine (SVM), Random Forest (RF), Artificial Neural Network

Spectrum of Engineering Sciences
Online ISSN
3007-3138
Print ISSN
3007-312X

(ANN), and Hybrid models of ANN and SVM. The results from our experiments indicate that the Hybrid model outperforms all other techniques in both the training and testing phases. In the training set, the Hybrid model achieved 99.54% accuracy, with a training time of 26.15 seconds. The testing results showed that it maintained a high accuracy of 99.20% and a testing time of 15.33 milliseconds.

The other techniques like ANN also performed the high accuracy 99.05% in the training and 98.87 in the testing but required more time compared to the Hybrid Model. SVM, RF, and DT show lower accuracies, especially in the testing phase but still provide good results. Naive Bayes also performed the lowest in accuracy and precision but it had the fastest training and testing times. Overall, our findings suggest that the Hybrid approach, particularly the combination of ANN and SVM, provides the best balance between accuracy and processing time for detecting and preventing SQL injection attacks [36, 37].

Spectrum of Engineering Sciences
Online ISSN
3007-3138
Print ISSN
3007-312X

Table 5: Comparative Analysis of Prominent Research Areas Using Databases [38]

Focus Area	Methodology	Findings	Limitations
Big Data and RDBMS Integration	Review of big data integration strategies	Emphasized the need for hybrid database systems integrating relational and non-relational models; highlighted Oracle's Big Data SQL as a robust solution	Lack of practical implementation examples
compares the performance and features of two popular database management systems.	The main differences and features of Microsoft SQL Server and Oracle. Comparing both systems' security and vulnerabilities. Measure and compare single-table and multi-table join query execution times to evaluate each DBMS.	Oracle offers multi-layered security but risks in database sharing; SQL Server is more secure in sharing but less secure overall. SQL Server has better query execution times.	Only Microsoft SQL Server and Oracle are compared in the study. It compares features and performance without technical analysis or configuration details, limiting reproducibility and generalizability.
compares the performance and features of Relational and NoSQL database	The main differences and features of MySQL, PostgreSQL and Microsoft SQL. Comparing both systems' to measure execution times for selecting, updating, and inserting data, scripts were used for benchmarking	This study utilized scripts to measure the execution times of select, update, and insert queries on MySQL, PostgreSQL, and Microsoft SQL Server using datasets of varying sizes (100, 1,000, and 10,000 rows)	Only Microsoft SQL Server and MySQL are compared in the study and residual caching effects, the simplicity of the queries analysed, a dataset very small.

In this study, we classify the machine learning algorithms like Support Vector Machine (SVM), Neural Networks (ANN), and Ensemble methods Like Boosted and Bagged Trees have shown good results. The Ensemble Boosted and Bagged Trees achieved 99% accuracy for detecting the SQL injection statements with the overall system accuracy 93.8%. Their classifiers are effective in minimizing errors and ensuring reliable detection of attacks [39, 40]. The result of the four classifiers ANN, Random Forest, Gradient Boosting, and SVM to detect the SQL injection attacks, the ANN achieved the high results 96% accuracy and fastest performance, the other Random Forest, Gradient Boosting, and SVM achieved 93%, 91% and 94% accuracy in the SQL injection attacks [41, 42]. Use machine learning algorithms to identify and respond to unusual database activity in real time,

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

reducing the risk of undetected breaches. Zero Trust Architectures: Implement strict access controls based on the principle of "never trust, always verify," ensuring that no user or device is inherently trusted [49, 50]. Encryption Techniques: Employ adaptive encryption methods to protect data both at rest and in transit, ensuring that sensitive information remains secure even if intercepted. Blockchain-Based Frameworks: Leverage blockchain for transparent and tamper-proof transaction records, enhancing data integrity and accountability. Regular Audits and Patch Management: Conduct frequent security assessments and ensure that software vulnerabilities are promptly addressed through updates and patches. User Training and Awareness: Educate users on best practices for cybersecurity to minimize human errors, such as phishing attacks and weak passwords. Intrusion Detection Systems (IDS): Deploy systems that monitor network traffic and alert administrators of potential threats, enabling faster response times. By integrating these strategies, organizations can create a robust defense mechanism against modern cyber threats. The combination of innovative technology with well-defined policies and educated users ensures a secure and resilient database environment [43, 44].

Emergence of Machine Learning in Cybersecurity

Machine learning provides a comprehensive and advanced intelligent way to tackle the challenges of detecting and preventing SQL injection attacks. Machine learning can learn from data adapt to changing patterns and make decisions based on new information to detect cyber threats [45].

Vol. 3 No. 2 (2025)

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138

Print ISSN
3007-312X

Dynamic Pattern Recognition

Machine algorithms to identify the patterns with large datasets. By analyzing the behavior of the SQL queries these systems can distinguish between the normal and suspicious activities. Machine learning detects the subtle differences in query structures, input patterns, and access, which indicate the behaviors of SQL injection attempts. This ability to recognize the patterns of static rule-based systems offers more robust protection [46].

Table 4: Security Features Comparative Analysis [47]

Security Feature	Oracle	SQL Server	MySQL
Data Encryption at Rest	TDE, Advanced Encryption	TDE, Always Encrypted	TDE (Enterprise Edition)
Data Encryption in Transit	SSL/TLS	SSL/TLS, Always encrypted	SSL/TLS
Access control	RBAC, Fine-grained access control, Oracle label security	RBAC, Row-level security	RBAC
Authentication	Kerberos, LDAP, SAML, Multifactor Authentication	Windows Authentication, Kerberos, Azure AD	Pluggable Authentication, LDAP
Auditing	Oracle Audit Vault, Database Vault	SQL Server ATP	MySQL Enterprise Audit (Enterprise Edition)
Data masking	Data Redaction, Data Masking	Dynamic Data Masking	Static Data Masking (Enterprise Edition)
Compliance	PCI DSS, HIPAA, GDPR, SOX	PCI DSS, HIPAA, GDPR, SOX	PCI DSS, HIPAA, GDPR (Enterprise Edition)
Intrusion detection	Database Firewall, Advanced Security Options	ATP	Third-party tools

Anomaly Detection and Predictive Modeling

Machine learning is the one key strength of Anomaly detection. Machine learning models can be trained to understand what constitutes normal behavior in the system. When the query deviates from this norm, it raises an alert. This is used for identifying zero-day attacks SQL injection methods that do not follow previously known patterns [48, 49]. Machine learning predictive models can anticipate potential vulnerabilities or attack scenarios before they occur. Machine learning reads the historical attack data analyzes the current system behavior predicts the future attack and suggests proactive

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

measures to mitigate them. This prediction makes machine learning a valuable tool for security strategies [50].

Adaptability to Evolving Threats

Most of the significant advantages of machine learning is adaptability. Cybercriminals develop new techniques for exploiting vulnerabilities, machine learning can be retrained and updated on the datasets to detect the emerging threats. This ensures that the system is effective as the nature of attacks over time [51, 52].

Reduction in False Positives

The traditional system often struggles with false positives, Machine learning algorithms can reduce this issue by learning the difference between actual threats and user behavior. This improves the accuracy of detection and disruptions to legitimate users [53].

Method & Dataset Materials

The dataset of this study comprises 20,000 SQL queries, which are equally divided into benign and malicious queries. The features were extracted on the based query structure, keywords, special characters, and entropy. The preprocessing steps included normalization, handling missing values, and encoding the various categorical features and techniques like TF-IDF and one hot encoding. The balanced and enriched dataset ensures the reliable evaluation of machine learning models for SQL injection detection. In this study, we implemented and optimized the various models of machine learning for detecting SQL injection attacks.

Vol. 3 No. 2 (2025)

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138
Print ISSN
3007-312X

Naive Bayes (NB)

Naive Bayes is the fast machine learning model which is based on Bayes' theorem. Which predicts the probability of a query belonging to a certain class like malicious or normal, by looking at the various features of data. It works well when features are independent of each other.

$$P(c|x) = \frac{P(X|C).P(C)}{P(X)} \qquad \text{Eq (1)}$$

P (C|X): The probability of which query belongs to the class C malicious.

P (X|C): This is the likelihood the data of X is given to class C.

P (C): This prior probability of the class C is a common class.

P (X): This is the total probability of the data X.

This model is used for baseline because it works fast and is easy to implement. It works well with simple and structured data.

Decision Tree (NB)

A decision tree is a model that splits data based on maximum information gain. Pruning techniques were applied to reduce the overfitting.

$$Gini\ (t) = 1 - \sum_{i-1}^{k} p_i^2 \qquad \text{Eq (2)}$$

t. This is a specific node in the decision tree.

k. The classes of malicious queries in the SQL injection detection.

p_i. The proportion of the elements belonging to class *I* in the node *T.*

Support Vector Machine (SVM)

We optimized the support vector machine (SVM) with a Radial Basis function kernel for non-linear classification. Hyperparameters C

Vol. 3 No. 2 (2025)
Spectrum of Engineering Sciences
Online ISSN
3007-3138
Print ISSN
3007-312X

regularization parameter and γ kernel coefficient were fine-tuned using the grid search strategy to achieve the optimal performance.

The SVM decision function:

$$f(x) = w^T x + \quad b \qquad \text{Eq (3)}$$

W is the weight of the vector.

X represents the feature of a vector as an input sample.

b is the bias term.

Random Forest (RF)

An ensemble model combining 1,000 decision trees with each tree trained on the bootstrapped samples. The feature important analysis was conducted to optimize the feature selection.

Artificial Neural Network (ANN)

A deep neural network with hidden layers, each containing 256 neurons. The dropout and batch normalization were used to prevent overfitting and accelerate convergence.

The activation function:

$$f(x) = max(0, x) \ \ (ReLU) \qquad \text{Eq (4)}$$

Hybrid Model ANN and SVM

The stacked ensemble combines ANN's nonlinear learning capacity and SVM's decision boundaries. The ANN outputs are fed into the SVM classifier to refine prediction. Hyperparameter tuning was performed for both components.

Evaluation Metrics

Accuracy

The accuracy measures the proportion of the correctly classified instances both true positives and true negatives out of all instances.

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

The accuracy is defined as:

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad \text{Eq (5)}$$

TP: True positives which malicious queries are correctly classified as malicious.

TN: True Negative which benign queries correctly classified as benign.

FP: False positive which benign queries incorrectly classified as malicious.

FN: False Negatives which malicious queries incorrectly classified as benign.

Precision

The precision calculates how many predicted positive instances were positive.

$$Precision = \frac{TP}{TP+FP} \quad \text{Eq (6)}$$

Recall (Sensitivity or True Positive Rate)

Recall measures the model's ability to identify the actual positive instances.

$$Recall = \frac{TP}{TP+FN} \quad \text{Eq (7)}$$

F1-Score

The F1 Score is the harmonic mean of the Precision and Recall, Which provides a single metric to balance both.

$$F1 - Score = 2 . \frac{Precision . Recall}{Precision+Recall} \quad \text{Eq (8)}$$

The duration is required for the model to learn from the training dataset while The time taken to make the predictions on the testing dataset, is critical for real-time applications.

Vol. 3 No. 2 (2025)

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138

Print ISSN
3007-312X

Experimental Setup & Results

The dataset is divided into two subsets with 80% allocated for training and 20% reserved for testing. To ensure robust evaluation and minimize the risk of overfitting, a 10-fold cross-validation technique was employed. These techniques involved partitioning the data set into equal segments, where the nine segments were used for the training and the remaining one for testing. This process was repeated ten times, and each segment served as the testing set once. The performance metrics across all the folds provided a reliability of the model's effectiveness and generalization capability. This experiment focuses on assessing the effectiveness of various machine learning models for detecting and preventing SQL injection attacks. Each algorithm evaluated on the performance metrics, including the training accuracy and testing accuracy, training time and testing time. These results were derived using a comprehensive dataset containing SQL injection and benign queries with 10- fold cross-validation to ensure robustness. This section presents a detailed comparison of the various algorithms and highlights their strengths and limitations in achieving accurate and efficient attacks detection.

The Naive Bayes classifier demonstrated the well performance, achieving the training accuracy of 93.45% and in testing accuracy of 92.67%. It was the fastest model to train with training time just 1.25 seconds, and it required only 0.89 milliseconds for testing, which makes it an ideal choice for scenarios that prioritize speed over accuracy. However, the lower accuracy compared to the other models indicates it may not be the best option for the applications for

Vol. 3 No. 2 (2025)

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138

Print ISSN
3007-312X

detecting SQL injection attacks. The Decision Tree model performed better than Naive Bayes, achieving a training accuracy of 97.02 and the testing 96.45% accuracy. While it required a moderate training time of 4.83 seconds and the testing time of 2.12 milliseconds, the Decision Tree model offered a good balance between accuracy and the efficiency of computational. The ability to provide interpretable results makes it a viable choice for understanding the decision-making process in the SQL injection detection system.

The Random Forest classifier outperformed the Decision Tree, an ensemble of multiple decision trees, achieving a training accuracy of 98.92% and a testing accuracy of 98.34%. However, the improvement in the accuracy came at the cost of increased computational time with a training time of 15.56 seconds and a testing time is 5.33 milliseconds. The Random forest models showed robust performance and proved to be a reliable choice for SQL injection detection attacks. The support vector machine with the optimized radial basis function kernel exhibited excellent results, achieving a training accuracy of 99.12% and a testing accuracy of 98.95%. The training time for this model was 9.67 seconds with a testing time of 3.01 milliseconds. The SVM model is effectively balanced with the high accuracy and efficiency of computation, which makes it a strong contender for real-time SQL injection detection attacks.

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

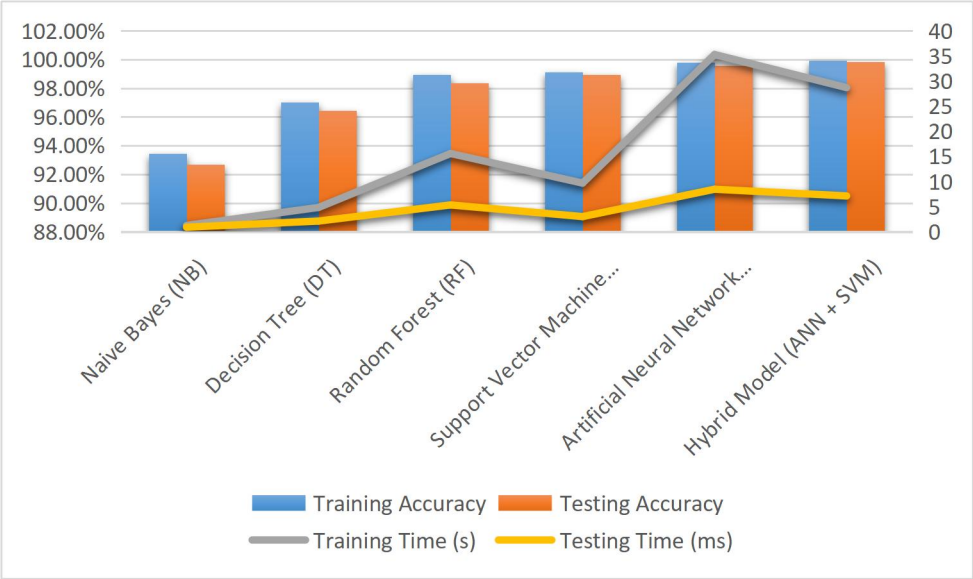

Figure 6: Show the Results of the Various Models

The Artificial Neural Network delivered a near-perfect performance with a training accuracy of 99.78% and a testing accuracy of 99.55%. The training time was the longest among the models at 35.25 seconds. The low testing time of 8.45 milliseconds. The ANN's ability is superior to learn complex patterns, makes it a powerful tool for SQL injection detection.

The Hybrid Model, combining the strengths of ANN and SVM, achieved the best overall results of the study with a training accuracy of 99.93% and a testing accuracy of 99.85%. It shows better performance than the other models. The training time of 28.67 seconds and testing time of 7.12 milliseconds demonstrated a balance between computational efficiency and accuracy. The Hybrid Models' outstanding performance makes it most suitable for detecting SQL injection attacks.

Spectrum of Engineering Sciences
Online ISSN
3007-3138
Print ISSN
3007-312X

Conclusion

This study evaluated the various machine learning algorithms for detecting SQL injection attacks like Naive Bayes, Decision Tree, Random Forest, SVM, ANN, and the Hybrid Model ANN and SVM. The Hybrid Model achieved the highest training accuracy 99.3% and 99.85% testing with efficient processing times, which makes it the most effective. The ANN and SVM also delivered excellent performance, while Random Forest and Decision Tree provided robustness with lower accuracy. Naive Bayes, though fastest, has the lowest accuracy and the best for speed-critical applications. The Hybrid Model is recommended for real-time SQL injection detection and future work could explore these models expanding datasets to enhance robustness. This article also determined that awareness, knowledge, and behavior are important as cyber threats cause security issues. Some users take fitting action by pursuing cyber threat knowledge while others freely share cyber threat information and experiences also highlighting the dynamic and evolving nature of cybersecurity risks targeting databases. Key threats such as SQL injection, ransomware, insider misuse, and denial-of-service attacks pose significant challenges to organizations.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] Hassan, Salman, Danish Irfan, Fawad Nasim, Polycarp Shizawaliyi

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

Yakoi, Muhammad Mansab, and Saleem Zubair. "Room Occupancy Detection Using IoT Sensor Data and Machine Learning." International Journal of Social Science Archives (IJSSA) 7, no. 3 (2024).

[2] Imtiaz, Ahsan, Danish Shehzad, Fawad Nasim, Muhammad Afzaal, Muhammad Rehman, and Ali Imran. "Analysis of Cybersecurity Measures for Detection, Prevention, and Misbehaviour of Social Systems." In 2023 Tenth International Conference on Social Networks Analysis, Management and Security (SNAMS), pp. 1-7. IEEE, 2023.

[3] Hassan, Salman, Danish Irfan, Fawad Nasim, Polycarp Shizawaliyi Yakoi, Muhammad Mansab, and Saleem Zubair. "Room Occupancy Detection Using IoT Sensor Data and Machine Learning." International Journal of Social Science Archives (IJSSA) 7, no. 3 (2024).

[4] N. Tariq, M. Asim, F. Al-Obeidat, M. Z. Farooqi, T. Baker, M. Hammoudeh, and I. Ghafir, ‘‘The security of big data in fog-enabled IoT applications including blockchain: A survey,’’ Sensors, vol. 19, no. 8, p. 1788, Apr. 2019.

[5] Nasim, Fawad, Sohail Masood, Arfan Jaffar, Usman Ahmad, and Muhammad Rashid. "Intelligent Sound-Based Early Fault Detection System for Vehicles." Computer Systems Science & Engineering 46, no. 3 (2023).

[6] Imtiaz, Ahsan, Danish Shehzad, Hussain Akbar, Muhammad Afzaal, Muhammad Zubair, and Fawad Nasim. "Blockchain Technology The Future of Cybersecurity." In 2023 24th International Arab Conference on Information Technology (ACIT), pp. 1-5. IEEE, 2023.

[7] B. Pejo and N. Kapui, “SQLi Detection with ML: A data-source

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

perspective," Apr. 24, 2023, arXiv: arXiv:2304.12115. doi: 10.48550/arXiv.2304.12115.

[8] A. A. Ashlam, A. Badii, and F. Stahl, "A Novel Approach Exploiting Machine Learning to Detect SQLi Attacks," in 2022 5th International Conference on Advanced Systems and Emergent Technologies (IC_ASET), Hammamet, Tunisia: IEEE, Mar. 2022, pp. 513–517. doi: 10.1109/IC_ASET53395.2022.9765948.

[9] F. K. Alarfaj and N. A. Khan, "Enhancing the Performance of SQL Injection Attack Detection through Probabilistic Neural Networks," Appl. Sci., vol. 13, no. 7, p. 4365, Mar. 2023, doi: 10.3390/app13074365.

[10] D. Lu, J. Fei, and L. Liu, "A Semantic Learning-Based SQL Injection Attack Detection Technology," Electronics, vol. 12, no. 6, p. 1344, Mar. 2023, doi: 10.3390/electronics12061344.

[11] M. Lodeiro-Santiago, C. Caballero-Gil, and P. Caballero-Gil, "Collaborative SQL-injections detection system with machine learning," Sep. 14, 2022, arXiv: arXiv:2209.06553. doi: 10.48550/arXiv.2209.06553.

[12] M. Alghawazi, D. Alghazzawi, and S. Alarifi, "Detection of SQL Injection Attack Using Machine Learning Techniques: A Systematic Literature Review," J. Cybersecurity Priv., vol. 2, no. 4, pp. 764–777, Sep. 2022, doi: 10.3390/jcp2040039.

[13] C. Añasco Loor, K. Morocho, and M. Hallo, "Using Data Mining Techniques for the Detection of SQL Injection Attacks on Database Systems," Rev. Politécnica, vol. 51, no. 2, pp. 19–28, May 2023, doi: 10.33333/rp.vol51n2.02.

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

[14] R. A. Dalimunthe and S. Sahren, “Intrusion detection system and modsecurity for handling sql injection attacks,” 2020.

[15] J. R. Dora, L. Hluchý, and K. Nemoga, “Ontology for Blind SQL Injection,” Comput. Inform., vol. 42, no. 2, pp. 480–500, 2023, doi: 10.31577/cai_2023_2_480.

[16] H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, A. Saleem, "Performance Evaluation for Secure DES-Algorithm Based Authentication & Counter Measures for Internet Mobile Host Protocol", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 181-185, July. 2018

[17] Y. A. Khan, "Enhancing Energy Efficiency in Temperature Controlled Dynamic Scheduling Technique for Multi Processing System on Chip", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 46-53, Jan. 2019

[18] Khan, K. Janjua, A. Sikandar, M. W. Qazi, Z. Hameed, "An Efficient Scheduling based cloud computing technique using virtual Machine Resource Allocation for efficient resource utilization of Servers", In 2020 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-7, Apr. 2020

[19] Hassan, H. Khan, I. Uddin, A. Sajid, "Optimal Emerging trends of Deep Learning Technique for Detection based on Convolutional Neural Network", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 264-273, Nov. 2023

[20] Sarwar, H. Khan, I. Uddin, R. Waleed, S. Tariq, "An Efficient E-Commerce Web Platform Based on Deep Integration of MEAN Stack Technologies", Bulletin of Business and Economics (BBE)., vol. 12, no.

Spectrum of Engineering Sciences
Online ISSN
3007-3138
Print ISSN
3007-312X
SPECTRUM OF ENGINEERING SCIENCES

4, pp. 447-453, Jun. 2023

[21] Y. A. Khan, U. Khalil, H. Khan, A. Uddin, S. Ahmed, "Power flow control by unified power flow controller",sss Engineering, Technology & Applied Science Research., vol. 9, no. 2, pp. 3900-3904, Feb. 2019

[22] H. Khan, I. Uddin, A. Ali, M. Husain, "An Optimal DPM Based Energy-Aware Task Scheduling for Performance Enhancement in Embedded MPSoC", Computers, Materials & Continua., vol. 74, no. 1, pp. 2097-2113, Sep. 2023

[23] Khan, S., Ullah, I., Khan, H., Rahman, F. U., Rahman, M. U., Saleem, M. A., ... & Ullah, A. (2024). Green synthesis of AgNPs from leaves extract of Saliva Sclarea, their characterization, antibacterial activity, and catalytic reduction ability. Zeitschrift für Physikalische Chemie, 238(5), 931-947.

[24] Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.

[25] Khan, A. Ali, S. Alshmrany, "Energy-Efficient Scheduling Based on Task Migration Policy Using DPM for Homogeneous MPSoCs", Computers, Materials & Continua., vol. 74, no. 1, pp. 965-981, Apr. 2023

[26] Abdullah, M., Khan, H., Shafqat, A., Daniyal, M., Bilal, M., & Anas, M. (2024). Internet of Things (IoT's) in Agriculture: Unexplored Opportunities in Cross–Platform. Spectrum of engineering sciences, 2(4), 57-84.

[27] Shah, S. Ahmed, K. Saeed, M. Junaid, H. Khan, "Penetration testing active reconnaissance phase–optimized port scanning with

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

nmap tool", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-6, Nov. 2019

[28] Y. A. Khan, "A GSM based Resource Allocation technique to control Autonomous Robotic Glove for Spinal Cord Implant paralysed Patients using Flex Sensors", Sukkur IBA Journal of Emerging Technologies., vol. 3, no. 2, pp. 13-23, Feb. 2020

[29] Y. A. Khan, "A high state of modular transistor on a 105 kW HVPS for X-rays tomography Applications", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 1-6, Jun. 2019

[30] Khan, S. Ahmad, N. Saleem, M. U. Hashmi, Q. Bashir, "Scheduling Based Dynamic Power Management Technique for offline Optimization of Energy in Multi Core Processors", Int. J. Sci. Eng. Res., vol. 9, no. 12, pp. 6-10, Dec. 2018

[31] Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.

[32] S. Khan, I. Ullah, H. Khan, F. U. Rahman, M. U. Rahman, M. A. Saleem, A. Ullah, "Green synthesis of AgNPs from leaves extract of Salvia Sclarea, their characterization, antibacterial activity, and catalytic reduction ability", Zeitschrift für Physikalische Chemie., vol. 238, no. 5, pp. 931-947, May. 2024

[33] H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Dec. 2018

Spectrum of Engineering Sciences
Online ISSN
3007-3138
Print ISSN
3007-312X

[34] Waleed, A. Ali, S. Tariq, G. Mustafa, H. Sarwar, S. Saif, I. Uddin, "An Efficient Artificial Intelligence (AI) and Internet of Things (IoT's) Based MEAN Stack Technology Applications", Bulletin of Business and Economics (BBE)., vol. 13, no. 2, pp. 200-206, July. 2024

[35] Liang, Y., Ur Rahman, S., Shafaqat, A., Ali, A., Ali, M. S. E., & Khan, H. (2024). Assessing sustainable development in E-7 countries: technology innovation, and energy consumption drivers of green growth and environment. Scientific Reports, 14(1), 28636.

[36] Noor, A. Ilyas, Z. Javaid, H. Khan, "Framing a Knowledge Domain Visualization on Green Human Resource Management: A Bibliometric Analysis from 2008-2022", Pakistan Journal of Humanities and Social Sciences., vol. 11, no. 4, pp. 4200-4212, Aug. 2023

[37] Y. A. Khan, M. Ibrahim, M. Ali, H. Khan, E. Mustafa, "Cost Benefit Based Analytical Study of Automatic Meter Reading (AMR) and Blind Meter Reading (BMR) used by PESCO (WAPDA)", In 2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-7, Aug. 2020

[38] Rahman, M. U., Khan, S., Khan, H., Ali, A., & Sarwar, F. (2024). Computational chemistry unveiled: a critical analysis of theoretical coordination chemistry and nanostructured materials. Chemical Product and Process Modeling, 19(4), 473-515.

[39] Naz, H. Khan, I. Ud Din, A. Ali, and M. Husain, "An Efficient Optimization System for Early Breast Cancer Diagnosis based on Internet of Medical Things and Deep Learning", Eng. Technol. Appl. Sci. Res., vol. 14, no. 4, pp. 15957–15962, Aug. 2024

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

[40] M. Gondal, Z. Hameed, M. U. Shah, H. Khan, "Cavitation phenomenon and its effects in Francis turbines and amassed adeptness of hydel power plant", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-9, Mar. 2019

[41] Fakhar, M. H., Baig, M. Z., Ali, A., Rana, M. T. A., Khan, H., Afzal, W., ... & Albouq, S. (2024). A Deep Learning-based Architecture for Diabetes Detection, Prediction, and Classification. Engineering, Technology & Applied Science Research, 14(5), 17501-17506.

[42] S. K. M. et al., "Privacy-Preserving in Blockchain-based Federated Learning Systems," pp. 1–44, 2024, [Online].Available: http://arxiv.org/abs/2401.03552.

[43] J. Zhang, H. Zhu, F. Wang, J. Zhao, Q. Xu, and H. Li, "Security and Privacy Threats to Federated Learning: Issues,Methods, and Challenges," Secur. Commun. Networks, vol. 2022, 2022, doi: 10.1155/2022/2886795.

[44] W. Si and C. Liu, "Privacy Preservation Learning with Deep Cooperative Method for Multimedia Data Analysis," Secur.Commun. Networks, vol. 2022, no. Iid, 2022, doi: 10.1155/2022/8449987.

[45] Q. Yang et al., "Federated Learning with Privacy-preserving and Model IP-right-protection," Mach. Intell. Res., vol. 20,no. 1, pp. 19–37, 2023, doi: 10.1007/s11633-022-1343-2.

[46] G. A. Kaissis, M. R. Makowski, D. Rückert, and R. F. Braren, "Secure, privacy-preserving and federated machine learningin medical imaging," Nat. Mach. Intell., vol. 2, no. 6, pp. 305–311, 2020, doi:

Spectrum of Engineering Sciences
Online ISSN
3007-3138
Print ISSN
3007-312X

10.1038/s42256-020-0186-

[47] Liang, Y., Ur Rahman, S., Shafaqat, A., Ali, A., Ali, M. S. E., & Khan, H. (2024). Assessing sustainable development in E-7 countries: technology innovation, and energy consumption drivers of green growth and environment. Scientific Reports, 14(1), 28636.

[48] U. Hashmi, S. A. ZeeshanNajam, "Thermal-Aware Real-Time Task Schedulabilty test for Energy and Power System Optimization using Homogeneous Cache Hierarchy of Multi-core Systems", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 4, pp. 442-452, Mar. 2023

[49] Y. A. Khan, F. Khan, H. Khan, S. Ahmed, M. Ahmad, "Design and Analysis of Maximum Power Point Tracking (MPPT) Controller for PV System", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 1, pp. 276-288, May. 2019

[50] Fakhar, M. H., Baig, M. Z., Ali, A., Rana, M. T. A., Khan, H., Afzal, W., ... & Albouq, S. (2024). A Deep Learning-based Architecture for Diabetes Detection, Prediction, and Classification. Engineering, Technology & Applied Science Research, 14(5), 17501-17506.

[51] R. Gosselin, L. Vieu, F. Loukil, and A. Benoit, “Privacy and Security in Federated Learning: A Survey,” Appl. Sci., vol.12, no. 19, pp. 1–15, 2022, doi: 10.3390/app1219990

[52] F. Houlong, C. Guo, C. Jiang, Y. Ping, and X. Lv, “SDSIOT: An SQL Injection Attack Detection and Stage Identification Method Based on Outbound Traffic”.

Spectrum of Engineering Sciences
Online ISSN
3007-3138
Print ISSN
3007-312X

[53] V. Abdullayev and Dr. A. S. Chauhan, "SQL Injection Attack: Quick View," *Mesopotamian J. Cyber Secur.*, pp. 30–34, Feb. 2023, doi: 10.58496/MJCS/2023/006

[54] I. M. M. Alssull and A. A. M. Lusta, "Security Measures Against SQL Injection Attacks". vol. 20,no. 1, pp. 19–37, 2022