International Journal of Informatics, Information System and Computer Engineering

Detection of SQL Injection Attacks Based on Supervised Machine Learning Algorithms: A Review

Hilmi Salih Abdullah, Adnan Mohsin Abdulazeez***

*Technical Informatics College, Akre University for Applied Sciences, Iraq
**Technical College of Engineering, Duhok Polytechnic University, Iraq
*Corresponding Email: Hilmi.Salih@auas.edu.krd

ABSTRACTS

In the ever-changing world of cybersecurity, it is becoming more important to ensure integrity of web applications as well as securing sensitive data. Among a variety of vulnerabilities, SQL injection is considered a significant risk with severe consequences. Addressing this crucial threat has always attracted the researchers to explore various approaches to identify and detect SQL injection attacks. The machine learning has captured the attention of the researchers to explore its potential due to its success in several different fields and the limitation of other rule-based approaches. This study provides a comprehensive review on a variety of the most recent researches that have been carried out using supervised learning algorithms. The study reveals that machine learning has a huge potential in the process of identification and detection of SQL injection attacks.

ARTICLE INFO

Article History:
Received 18 Feb 2024
Revised 02 Mar 2024
Accepted 28s Mar 2024
Available online 25 Apr 2024
Publication date 01 Dec 2024

Keywords:
SQL Injection,
Machine Learning,
Supervised ML Algorithms

1. INTRODUCTION

In the rapidly evolving cybersecurity landscape, ensuring the confidentiality and integrity of sensitive data is extremely important by securing web applications against vulnerabilities. Among the various security threats, SQL injection vulnerability is considered a serious threat that poses a serious risk to web applications. Based on the Open Web Application Security Project (OWASP), SQL Injection is a crucial vulnerability and ranked in the list of top 10 vulnerabilities (Demilie & Deriba, 2022). SQL injection vulnerability is exploited by attackers via injecting malicious SQL code to web applications in order to gain unauthorized access to sensitive data stored in the databases (Bharati & Kumar, 2022) (Goyal & Matta, 2023). SQL injection can be classified into several types which exploits various weaknesses in web applications (Hubskyi, et al., 2020; Singh, et al., 2015). Researchers have tried to eliminate the risk of this threat and utilized various approaches such as static, dynamic and hybrid approaches to identify and detect SQL injection vulnerabilities and attacks (Zhumabekova et al., 2023) (Sadeeq & Abdulazeez, 2023). However, due to the limitations of these rule-based approaches, the researchers investigated about more robust and versatile solutions (Abdulmalik, 2021; Hasan, et al., 2019; Nasereddin, et al., 2023). Therefore, the success of machine learning in many fields, attracted the researchers to explore its capabilities it in the field of security. Moreover, machine learning approaches have proved to be a good solution to identify SQL injection attacks instead of rule-based approaches (Deriba, et. al., 2022; Roy, et. al., 2022) (Kunang, et al., 2021). This paper aims to review recent researches that utilized supervised machine learning algorithms to identify, detect and prevent SQL injection attacks. First a comprehensive review has been conducted on recent researches. Then the methods and algorithms of each research have been analyzed and extracted as well as the accuracy results. Moreover, according to the conducted review, the supervised machine learning algorithms have obtained promising results in SQL injection attacks identification and detection. The paper's organization is as follows: Section 2 introduces the background of SQL injection, its types, and prevention methods as well as supervised machine learning algorithms. Section 3 explains the method of the research. Section 4 presents the results and discussions of the review. Finally, Section 5 provides the conclusion.

2. BACKGROUND STUDY

2.1. SQL Injection

SQL injection is a security vulnerability in web applications which enables attackers to access sensitive information stored in the databases of web applications via injecting malicious SQL code (Lakhani, et al., 2022) (T. Zhang & Guo, 2020). This vulnerability emerges when the user input data is not handled properly by the web application. Generally, this vulnerability is considered crucial due to its severe impact on revealing sensitive data (Brindavathi, et al., 2023; Mondal, et al., 2022). For this reason, it is listed in the top ten vulnerabilities issued by Open Web Application Security Project (OWASP) (Demilie & Deriba, 2022). Typically, the attacker inserts SQL code into a web form or other input field and then executed by the backend database as in Fig. 1 (Roy et al., 2022). However, the source of the attack might be cookies, server variables and stored procedures too (Padmaja, et al., 2022). The malicious SQL code could be executed in case the user input is not sanitized or validated properly by the application (Fidalgo, et al., 2020; Johny, et al., 2021). Usually, successful SQL injection attacks enable the attacker to access sensitive data, modify and delete data or even have access to the underlying system, which are considered severe and serious consequences (Sivasangari, et al., 2021). In order to prevent SQL injection attacks, the user input data needs to be checked and validated, as well as other security measures should be implemented, such as firewalls and access controls in addition to secure coding practices that should be followed by Web application developers and finally, stay up-to-date with the latest security vulnerabilities and patches (Jemal, et al., 2020; Tasevski & Jakimoski, 2020). There are various types of SQL injection attacks as in the following (Saran, et a., 2022) (Azman, et al., 2021).

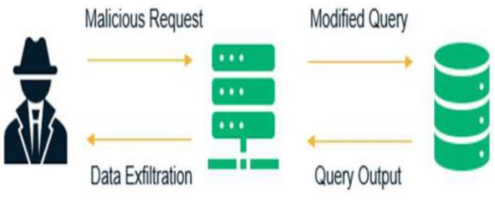

Fig. 1. SQL injection attack procedure.

2.1.1. Classic SQL Injection

It is considered as the most common type of SQL injection attacks. The way it works is by injecting malicious SQL code into the vulnerable SQL Statement. Usually, when the web application doesn't validate user input in a proper way, this vulnerability arises, which in turn enables the attacker to enter SQL commands into the input fields such as login and search boxes (Sommervoll, et al., 2023). Furthermore, in order to exploit this vulnerability, the attackers might use several techniques such as using a single quote character (‘) to add their malicious code at the end of the original SQL statement. Thus, the injected code will always be true which will return information from the database, and hence bypass the authentication process. The consequences of Classic SQL injection attacks might be data loss or corruption and unauthorized access to sensitive information. Therefore, to prevent Classic SQL injection attacks, the validation of user input is necessary in addition to the use of parametrized queries (Azman et al., 2021; Sommervoll, et al., 2023).

2.1.2. Blind SQL Injection

The reason it is called “blind” is because no feedback about the query result is returned to the attacker. Typically, with this type of injection, the attacker tries to extract sensitive information or modify database contents by exploiting a vulnerability in the web application. When sending SQL query to the database it will behave in a certain way. Therefore, by observing the behavior of the application, the attackers can determine whether the condition is true or false (Jemal et al., 2020). Later, they can construct more complex queries based on the obtained information. Usually, this type of attack is difficult to detect and mitigate compared to other SQL injection attacks because no direct feedback is received from the database. In order to mitigated the risk of this attack, prepared statements and input validation techniques should be used as well as implementing strict access controls (Erd

Hodi, et al., 2021; Jemal et al., 2020) (Erd Hodi et al., 2021).

2.1.3. Error-Based SQL Injection

This type of attack tries to extract useful information from the database depending on the error messages returned from the database after executing malformed SQL queries. Typically, these useful information include database structure, tables names as well as usernames and passwords in some cases. To prevent this type of attack, the developers must take into consideration using parametrized queries and sanitize user input before sending it to the database (Crespo Mart'inez et al., 2023) (Tasevski & Jakimoski, 2020) (Mondal et al., 2022).

2.1.4. Union-Based SQL Injection

In this type of attack, the results of two or more SELECT statements are combined into a single result set using UNION operator. Typically, the attack involves injecting malicious SQL code into input fields like login forms or contact forms in order to change the behavior of the application or get useful information from the database (Mondal et al., 2022). The prevention from the this type of SQL injection attack involves the use of prepared statements which don't allow the injection of any additional code by separating the user input from the SQL code. Additionally, validation is necessary to ensure the limit of user input (Sommervoll, et al., 2023) (Abdulmalik, 2021).

2.1.5. Time-Based SQL Injection

The idea behind this type of attack is inferring information about the database structure based on the time delay of the database response. Typically, the attacker observes the response time for each of the injected malicious SQL statements then analyzes the response time to extract sensitive information from the database. The method of prevention againt this attack is to perform regular security assessments to identify and mitigate vulnerabilities (Azman et al., 2021) (Erd Hodi et al., 2021).

2.1.6. Out-of-Band SQL Injection

It is called "out-of-band" because it doesn't use the normal method of retrieving data. Instead it uses HTTP or DNS requests for obtaining data from the database. This method is useful when the web application allows functions that make HTTP requests or send emails. When the application is exploited, the response of the malicious SQL code is received on a different channel. Typically, this attack is more difficult to detect compared to in-band attacks because it doesn't show any signs of being exploited. However, there are ways of protection against this attack such as monitoring the network traffic for any suspicious requests (Azman et al., 2021; Johny et al., 2021; Pinzon et al., 2013) (McIvera, et al., 2017).

2.1.7. Second-Order SQL Injection

This type of SQL injection is also known as persistent or stored SQL Injection. Typically, it involves two steps, first, when the user input is saved in the database. Second, which might happen at a later time, when the saved user input is used in the SQL Query to get or modify data in the database. Usually this attack happens when the application allows the user to store some data in the database. Therefore, the attacker might store malicious SQL code. Another way is when the attacker successfully injects malicious SQL code in a stored procedure. As a result, every time the stored procedure is called the malicious SQL code is executed. To prevent this type of attack, the developers must take into consideration using parametrized queries and sanitize user input before storing in the database (Johny et al., 2021) (Tasevski & Jakimoski, 2020).

2.2. Machine Learning

The researchers have used several approaches to detect SQL Injection attacks. First approach was static analysis, which relies on validating user input to identify syntactic and grammatical errors. The downside of this approach is that it cannot detect malicious SQL code when the syntax is correct (Abdulmalik, 2021) (Saleem, et al., 2020) (Hassan, et al., 2022). The second approach is Dynamic analysis, which is based on scanning and comparing the web application response for the queries sent, however the limitation of this method is that it can only identify predefined vulnerabilities (Singh et al., 2015) (Abdulmalik, 2021). The third approach is combined analysis, which is basically benefiting from both static and dynamic analysis techniques to detect SQL injection attack. All the previously mentioned approaches are rule-based, meaning they cannot detect attacks which are not covered by the rules (Abdulmalik, 2021) (Nasereddin et al., 2023). For this reason, there was a strong need for a more robust and reliable approach. The success of machine learning in a variety of fields has motivated many researchers to explore its capabilities in detecting SQL injection attack (Falor, et al.,2022) (Ashlam, et al., 2022). Machine learning based approaches to detect SQL injection attacks are considered a replacement for the rule-based one. Since, machine learning approach can detect new SQL injection attack types (McIvera et al., 2017) (Singh et al., 2015) (Zolanvari, et al., 2019). There are three types of machine learning which are supervised, unsupervised, and reinforcement learning (Salih & Abdulazeez, 2021) (D. M. Abdullah & Abdulazeez, 2021) (R. M. Abdullah, et al., 2021). The supervised algorithms has successfully proven to be effective in analyzing a broad and annotated training data. Below are some useful algorithms of supervised learning for identifying and detecting SQL injection attacks (Praveen, et al., 2022) (Islam, et al., 2019) (Kunang et al., 2021; Zolanvari et al., 2019).

2.2.1. Naive Bayes

This algorithm has been used in detecting SQL injection attacks. It is based on Bayes Theorem which depends on conditional probability. It simple and fast which is mainly used in text classification (R. Gupta, et al., 2020; Pinzon et al., 2013).

2.2.2. SVM

Support Vector Machine it used mainly in classification of problems. The target of this algorithm is separating the data into two groups by finding the best line which is called hyperplane with the aim of increasing the margin between the two groups (V. Gupta, et al., 2022) (R. Gupta, al., 2020) (D. M. Abdullah & Abdulazeez, 2021).

2.2.3. Logistic Regression

It is a predictive modeling technique which determines the relationship between a dependent variable and an independent variable or variables. It is considered prediction model because it is fast and simple (R. Gupta, et al., 2020; V. Gupta et al., 2022).

2.2.4. Decision Tree

Decision tree is one of the most used algorithms in machine learning. It can be with classification and regression too. It is a good way to decide between various actions. However, one of the most obvious challenges with this algorithm is overfitting which can cause errors in the the final decisions (R. Gupta, et al., 2020; V. Gupta, et al., 2022; Sadeeq, et al., 2022).

2.2.5. Random Forest

Random Forest (RF) is an algorithm which uses supervised learning methods to solve regression and classification problems. Random forest forms subsets of data which solves overfitting issues present in decision tree (Islam et al., 2019) (R. Gupta, et al., 2020; Islam, et al., 2019).

3. METHOD

First of all, a literature review has been conducted by utilizing the most popular digital libraries Science Direct, IEEE Xplore, Springer and Scopus. The aim of the study is to review papers in these databases that discuss the process of identification, detection and prevention of SQL Injection attacks. The period covered was papers from 2018 till 2023. The selection process included removing duplicates and review the most relevant papers.

4. RESULT AND DISCUSSION

In this work we reviewed and compared many researches that used supervised machine learning algorithms to identify and detect SQL Injection attacks. The summary of the reviewed papers is presented in Table 1, which contains the algorithms used, the method of the research and the results in terms of accuracy. Natarajan et al. used Naïve Bayes, logistic regression, CNN and random forests algorithms. In addition, they utilized two datasets, one for training and the other on for validation and testing. They have obtained 99.29% accuracy with CNN (Natarajan, et al, 2022). Ibrohim et al. utilized two algorithms only, SVM and Naïve Bayes. The result of SVM was better than Naïve with 93.98% accuracy (Ibrohim & Suryani, 2023). Roy et al. used Kaggle dataset to detect SQL injection attacks with a variety of machine learning algorithms such as Logistic Regression and Naïve Bayes. The results showed that Naive Bayes was the best model with 98.3% accuracy (Roy et al., 2022). Deriba et al. developed a comprehensive framework for SQL injection detection and prevention using a hybrid approach and machine learning techniques. Other models like ANN and SVM were tested as well. According to the results, the best performing model was the hybrid approach with 99.2% accuracy (Deriba et al., 2022). Krishnan et al. tested various machine learning models to identify and detect SQL injection attack, including SVM,CNN, Naïve Bayes and Logistic regression. The best performing model was CNN with 97% accuracy (Krishnan, et al., 2021). Gandhi et al. compared various types of machine learning algorithm in terms of detecting SQL injection attack. A hybrid CNN-BiLSTM model has been proposed by the authors with the accuracy of 98% (Gandhi, et al., 2021). Ahmed and Uddin tested and compared a variety of supervised learning algorithms such as SVM, Naïve Bayes, KNN random forest and decision tree together with Natural Language Processing (NLP) and obtained 98.15% accuracy with random forest and NLP

(Ahmed & Uddin, 2020). Tang et. al, used SVM and neural networks LSTM and CNN algorithms for detecting SQL injection attacks and obtained 99.85% accuracy with LSTM (Tang, et al., 2020). Tripathy et al. trained a variety of supervised learning models such as decision trees and random forest on the dataset. The results obtained from the random forest classifier was the best with 99.8% accuracy (Tripathy, et al., 2020). Hasan and Tarique created datasets which contained malicious SQL syntax. They tested and compared many machine learning algorithms including SVM, ensemble bagged and boosted trees, as well as cubic KNN. The results showed that the best performing model was ensemble bagged and boosted trees with 93.8% accuracy (Hasan et al., 2019). Xie et al. used Elastic-Pooling CNN (EP CNN) to detect SQL injection attack. The authors compared the result of the other methods. The accuracy of EP CNN was outstanding with 99.98% (Xie, et al., 2019) .Luo et al. used the network traffic to extract SQL injection payloads. The authors used a CNN-Based model for their experiment which resulted in an outstanding accuracy of 99.5% (Luo, et al., 2019). Li et al. used offline and online training stages. They tested and evaluated various methods like KNN, Adaptive random forest (ADF), SVM . The result showed that ADF was the model with the highest accuracy of 98% (Li, et al., 2019). Zhang utilized several machine learning models such as SVM, CNN, MLP, LSTM. The result of the evaluation presented that CNN outperformed other models with the accuracy of 95.4% (K. Zhang, 2019). Ross et al. created a system containing three phases; creating traffic, capturing data and data pre-processing. They tested various models such as ANN, random forest and SVM which presented the best result of 95.7% accuracy (Ross, et al., 2018). From the reviewed papers, it can be noticed that CNN, SVM and random forest were the most used supervised machine learning algorithms to detect SQL Injection as shown in Figure 2. Furthermore, the results of CNN and random forest algorithms were the best among other algorithms in terms of accuracy.

Table 1. Comparison of the reviewed papers.

Authors	Year	Algorithms	Methods	Accuracy
Natarajan et. al	2023	Naïve Bayes, Logistic Regression , Random forest and CNN	Using two datasets, one for training and the other one for validation and testing. NLP is applied to increase the accuracy of text processing.	99.29% with CNN
Ibrohim et al.	2023	Naïve Bayes and SVM	Merging penetration testing payloads with Kaggle dataset.	93.98% with SVM
Roy et. al	2022	Naïve Bayes, Logistic Regression	Testing the classifiers with the chosen dataset	98.33% with Naïve Bayes

Authors	Year	Algorithms	Methods	Accuracy
		and Random forest.	and then analyze the performance	
Deriba et al.	2022	Naïve Bayes, SVM, ANN , Decision tree, Hybrid	developing a comprehensive framework for SQL injection detection and prevention using a hybrid approach and machine learning techniques	99.27% with Hybrid
S.S. Anandha Krishnan et al.	2021	Naive Baye s, CNN, Logistic Regression, SVM	NLP techniques and feature Extraction)	Highest accuracy was 97% in CNN and 95% in Naïve Bayes
Gandhi et al.	2021	CNN-BiLSTM	extracting the information of queries by using convolutional layers. Then BiLSTM for data processing in forward and backward directions.	98%
Ahmed, M. et al.	2020	SVM, KNN, Naïve Bayes, Decision Tree, Random forest and NLP.	Dataset collecting, labeling , splitting, extracting features and BOW Model Generation	98.15 % with Random forest and NLP
P. Tang et al.	2020	LSTM SVM, MLP, CNN	Converting the URL into vector then using the vector as the input of LSTM for model training	99.85% with LSTM
D. Tripathy et al.	2020	Random Forest, SGD Classifier, Deep ANN, Decision Tree	feature engineering process performed on the payloads	99.8% with Random Forest and 99.5% with Decision Tree
Hasan, M. et al.	2019	Cubic SVM, Ensemble Boosted Trees, Ensemble	Loading the injected and non-injected SQL statements then Extract the features	93.8 with Cubic Ensemble Boosted and Bagged Tree

Authors	Year	Algorithms	Methods	Accuracy
Xie, X et al.	2019	Naive Bayes, EPCNN, SVM, Random Forest, Decision Tree, CNN	EP-CNN extracts the hidden common features of SQL injection and identifies the attack traffic .	99.98% with EP-CNN
A. Luo et al.	2019	CNN	Construct the CNN network model, use payload data as the input for model detection and report if the traffic contains SQL injection attack.	99.5%
Q. Li et al.	2019	KNN, SVM, Random forest, ADF, CNN	1-offline and online training stages. feature vectors are used as the input of the deep forest model.	98% with ADF
K. Zhang	2019	Logistic Regression, Decision tree, CNN, Random forest, SVM, LSTM	Training and evaluating classification models y performing input validation and sanitization features .	CNN 95.4%
K. Ross et al.	2018	RF ,SVM ,ANN	data pre-processing, creating traffic and capturing data	SVM 95.715%

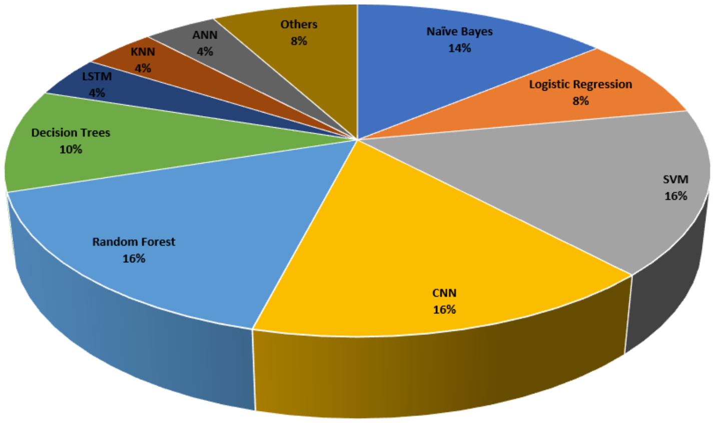

Fig. 2. The most used algorithms in detection of SQL injection.

5. CONCLUSION

SQL injection poses a significant threat to the security of web applications and their sensitive information. Many researches have been carried out to identify and detect this threat and help protect the web applications from such attacks. Machine learning has proved to be successful in eliminating the risk of this threat. This study has reviewed many researches that utilized various supervised machine learning algorithms to detect this type of attack. The study revealed that some algorithms such as CNN and random forest has achieved promising results in terms of accuracy.

REFERENCES

Abdullah, D. M. & Abdulazeez, A. M. (2021). Machine Learning Applications Based on SVM Classification a Review. *Qubahan Academic Journal*, *1*(2), pp. 81–90.

Abdullah, R. M., Abdulazeez, A. M. & Al-Zebari, A. (2021). Machine Learning Algorithm of Intrusion Detection System. *Asian Journal of Research in Computer Science*, *9*(3), pp. 1–12.

Abdulmalik, Y. (2021). An Improved SQL Injection Attack Detection Model Using Machine Learning Techniques. *International Journal of Innovative Computing, 11*(1), pp. 53–57.

Ahmed, M. & Uddin, M. N. (2020). Cyber Attack Detection Method Based on Nlp and Ensemble Learning Approach. In *2020 23rd International Conference on Computer and Information Technology (ICCIT)*, pp. 1–6.

Ashlam, A. A., Badii, A. & Stahl, F. (2022). A Novel Approach Exploiting Machine Learning to Detect Sqli Attacks. In *2022 5th International Conference on Advanced Systems and Emergent Technologies (ICASET)*, pp. 513–517.

Azman, M. A., Marhusin, M. F. & Sulaiman, R. (2021). Machine Learning-Based Technique to Detect SQL Injection Attack. *Journal f Computer Science*.

Bharati, V. & Kumar, A. (2022). An Efficient Approach Toward Security of Web Application Using SQL Attack Detection and Prevention Technique. In *Inventive Computation and Information Technologies: Proceedings Of ICICIT 2021*, pp. 781–792. Springer.

Brindavathi, B., Karrothu, A. & Anilkumar, C. (2023). An Analysis of AI-Based SQL Injection (Sqli) Attack Detection. In *2023 Second International Conference on Augmented Intelligence and Sustainable Systems (ICAISS)*, pp. 31–35.

Crespo-Mart'Inez, I. S., Campazas-Vega, A., Guerrero-Higueras, Á. M., Riego-Delcastillo, V., Álvarez-Aparicio, C. & Fernández-Llamas, C. (2023). SQL Injection Attack Detection in Network Flow Data. *Computers and Security*, *127*, pp. 103093.

Demilie, W. B. & Deriba, F. G. (2022). Detection and Prevention Of SQLI Attacks and Developing Compressive Framework Using Machine Learning and Hybrid Techniques. *Journal of Big Data*, *9*(1), pp. 124.

Deriba, F., Salau, A. O., Mohammed, S. H., Kassa, T. M. & Demilie, W. B. (2022). Development of a Compressive Framework Using Machine Learning Approaches for SQL Injection Attacks. *PRZEGLKad ELEKTROTECHNICZNY*, *1*(7), pp. 183–189.

Erd\Hodi, L., Sommervoll, Å. Å. & Zennaro, F. M. (2021). Simulating SQL Injection Vulnerability Exploitation Using Q-Learning Reinforcement Learning Agents. *Journal of Information Security and Applications*, *61*, pp. 102903.

Falor, A., Hirani, M., Vedant, H., Mehta, P. & Krishnan, D. (2022). A Deep Learning Approach for Detection Of SQL Injection Attacks Using Convolutional Neural Networks. In *Proceedings of Data Analytics and Management: ICDAM 2021, Volume 2*, pp. 293–304.

Fidalgo, A., Medeiros, I., Antunes, P. & Neves, N. (2020). Towards A Deep Learning Model for Vulnerability Detection on Web Application Variants. In *2020 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW)*, pp. 465–476.

Gandhi, N., Patel, J., Sisodiya, R., Doshi, N. & Mishra, S. (2021). A CNN-Bilstm Based Approach for Detection of SQL Injection Attacks. In *2021 International Conference on Computational Intelligence And Knowledge Economy (ICCIKE)*, pp. 378–383.

Goyal, A. & Matta, P. (2023). Beyond The Basics: A Study Of Advanced Techniques for Detecting and Preventing SQL Injection Attacks. In *2023 4th International Conference on Smart Electronics And Communication (ICOSEC)*, pp. 628–631.

Gupta, R. & Others. (2020). A Survey On Machine Learning Approaches and Its Techniques. In *2020 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS)*, pp. 1–6.

Gupta, V., Mishra, V. K., Singhal, P. & Kumar, A. (2022). An Overview of Supervised Machine Learning Algorithm. In *2022 11th International Conference on System Modeling and Advancement In Research Trends (SMART)*, pp. 87–92.

Hasan, M., Balbahaith, Z. & Tarique, M. (2019). Detection Of SQL Injection Attacks: A Machine Learning Approach. In *2019 International Conference On Electrical And Computing Technologies And Applications (ICECTA)*, pp. 1–6.

Hassan, M. M., Risha, R. & Esha, A. (2022). ADT-Sqli: An Automated Detection Of SQL Injection Vulnerability In Web Applications. In *Proceedings Of International Conference on Frontiers In Computing And Systems: COMSYS 2021*, pp. 433–443.

Hubskyi, O., Babenko, T., Myrutenko, L. & Oksiiuk, O. (2020). Detection Of Sql Injection Attack Using Neural Networks. In *International Scientific-Practical Conference*, pp. 277–286.

Ibrohim, M. M. & Suryani, V. (2023). Classification Of SQL Injection Attacks Using Ensemble Learning SVM And Na"Ive Bayes. In *2023 International Conference on Data Science and Its Applications (Icodsa)*, pp. 230–236.

Islam, M. R. U., Islam, M. S., Ahmed, Z., Iqbal, A. & Shahriyar, R. (2019). Automatic Detection Of Nosql Injection Using Supervised Learning. In *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*. Vol. 1, pp. 760–769.

Jemal, I., Cheikhrouhou, O., Hamam, H. & Mahfoudhi, A. (2020). Sql Injection Attack Detection and Prevention Techniques Using Machine Learning. *International Journal Of Applied Engineering Research*, *15*(6), pp. 569–580.

Johny, J. H. B., Nordin, W. A. F. B., Lahapi, N. M. B. & Leau, Y.-B. (2021). SQL Injection Prevention in Web Application: A Review. In *Advances In Cyber Security: Third International Conference, Aces 2021, Penang, Malaysia, August 24-25, 2021, Revised Selected Papers 3*, pp. 568–585.

Krishnan, S. A., Sabu, A. N., Sajan, P. P. & Sreedeep, A. (2021). SQL Injection Detection Using Machine Learning. *Vol*, *11*, pp. 11.

Kunang, Y. N., Nurmaini, S., Stiawan, D. & Suprapto, B. Y. (2021). Attack Classification of an Intrusion Detection System Using Deep Learning and Hyperparameter Optimization. *Journal Of Information Security And Applications*, *58*, pp. 102804.

Lakhani, S., Yadav, A. & Singh, V. (2022). Detecting SQL Injection Attack Using Natural Language Processing. In *2022 IEEE 9th Uttar Pradesh Section International Conference On Electrical, Electronics And Computer Engineering (UPCON)*, pp. 1–5.

Li, Q., Li, W., Wang, J. & Cheng, M. (2019). A SQL Injection Detection Method Based on Adaptive Deep Forest. *IEEE Access*, *7*, pp. 145385–145394.

Luo, A., Huang, W. & Fan, W. (2019). A CNN-Based Approach to The Detection of SQL Injection Attacks. In *2019 IEEE/ACIS 18th International Conference on Computer and Information Science (ICIS)*, pp. 320–324.

Mcivera, A., Rabehajaa, T., Wenb, R. & Morganb, C. (2017). Journal of Information Security and Applications.

Mondal, B., Banerjee, A. & Gupta, S. (2022). A Review of SQLI Detection Strategies Using Machine Learning. *Machine Learning*, *6*(S2), pp. 9664–9677.

Nasereddin, M., Alkhamaiseh, A., Qasaimeh, M. & Al-Qassas, R. (2023). A Systematic Review of Detection And Prevention Techniques of SQL Injection Attacks. *Information Security Journal: A Global Perspective*, *32*(4), pp. 252–265.

Natarajan, Y., Karthikeyan, B., Wadhwa, G., Srinivasan, S. & Akilesh, A. P. (2022). A Deep Learning Based Natural Language Processing Approach for Detecting SQL Injection Attack. In *International Conference on Intelligent Systems Design and Applications*, pp. 396–406.

Padmaja, B., Sekhar, G. C., Rama Padmaja, C. V., Chandana, P. & Krishna Rao Patro, E. (2022). Tool-Based Prediction of SQL Injection Vulnerabilities and Attacks on Web Applications. In *Communication, Software and Networks: Proceedings of India 2022*, pp. 535–543. Springer.

Pinzon, C. I., De Paz, J. F., Herrero, A., Corchado, E., Bajo, J. & Corchado, J. M. (2013). Idmas-SQL: Intrusion Detection Based on MAS To Detect and Block SQL Injection Through Data Mining. *Information Sciences*, *231*, pp. 15–31.

Praveen, S., Dcouth, A. & Mahesh, A. (2022). Nosql Injection Detection Using Supervised Text Classification. In *2022 2nd International Conference on Intelligent Technologies (CONIT)*, pp. 1–5.

Ross, K., Moh, M., Moh, T.-S. & Yao, J. (2018). Multi-Source Data Analysis And Evaluation Of Machine Learning Techniques For SQL Injection Detection. In *Proceedings of The ACMSE 2018 Conference*, pp. 1–8.

Roy, P., Kumar, R. & Rani, P. (2022). SQL Injection Attack Detection By Machine Learning Classifier. In *2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC)*, pp. 394–400.

Sadeeq, H. T. & Abdulazeez, A. M. (2023). Metaheuristics: A Review of Algorithms. *International Journal of Online and Biomedical Engineering*, *19*(9).

Sadeeq, H. T., Ameen, S. Y. & Abdulazeez, A. M. (2022). Cancer Diagnosis Based On Artificial Intelligence, Machine Learning, And Deep Learning. In *2022 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, pp. 656–661.

Saleem, S., Sheeraz, M., Hanif, M. & Farooq, U. (2020). Web Server Attack Detection Using Machine Learning. In *2020 International Conference on Cyber Warfare and Security (ICCWS)*, pp. 1–7.

Salih, A. A. & Abdulazeez, A. M. (2021). Evaluation Of Classification Algorithms For Intrusion Detection System: A Review. *Journal Of Soft Computing and Data Mining*, *2*(1), pp. 31–40.

Saran, M., Yadav, R. K., Maurya, P., Devi, S. & Tripathi, U. N. (2022). A Comprehensive Review For Detection And Prevention Techniques For SQL Injection Attack In Cloud Computing. *International Journal of Innovative Research In Engineering and Management*, *9*(5), pp. 11–17.

Singh, G., Kant, D., Gangwar, U. & Singh, A. P. (2015). Sql Injection Detection And Correction Using Machine Learning Techniques. In *Emerging ICT For Bridging The Future-Proceedings Of The 49th Annual Convention of The Computer Society Of India (CSI) Volume 1*, pp. 435–442.

Sivasangari, A., Jyotsna, J. & Pravalika, K. (2021). SQL Injection Attack Detection Using Machine Learning Algorithm. In *2021 5th International Conference on Trends in Electronics And Informatics (ICOEI)*, pp. 1166–1169.

Sommervoll, Å. Å., Erd\Hodi, L. & Zennaro, F. M. (2023). Simulating All Archetypes Of SQL Injection Vulnerability Exploitation Using Reinforcement Learning Agents. *International Journal of Information Security*, pp. 1–22.

Tang, P., Qiu, W., Huang, Z., Lian, H. & Liu, G. (2020). Detection of SQL Injection Based on Artificial Neural Network. *Knowledge-Based Systems, 190*, pp. 105528.

Tasevski, I. & Jakimoski, K. (2020). Overview Of Sql Injection Defense Mechanisms. In 2020 28th Telecommunications Forum (TELFOR).

Tripathy, D., Gohil, R. & Halabi, T. (2020). Detecting SQL Injection Attacks In Cloud Saas Using Machine Learning. In *2020 IEEE 6th Intl Conference on Big Data Security on Cloud (Bigdatasecurity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS),* pp. 145–150.

Xie, X., Ren, C., Fu, Y., Xu, J. & Guo, J. (2019). Sql Injection Detection For Web Applications Based On Elastic-Pooling Cnn. *IEEE Access*, *7*, pp. 151475–151481.

Zhang, K. (2019). A Machine Learning Based Approach To Identify SQL Injection Vulnerabilities. In *2019 34th IEEE/ACM International Conference on Automated Software Engineering (ASE)*, pp. 1286–1288.

Zhang, T. & Guo, X. (2020). Research On SQL Injection Vulnerabilities And Its Detection Methods. In *2020 4th Annual International Conference on Data Science and Business Analytics (ICDSBA)*, pp. 251–254.

Zhumabekova, A., Matson, E. T., Karyukin, V., Zhumabekova, K., Zhuandykov, B., Ussatova, O. & Telbayeva, T. (2023). Determining Web Application Vulnerabilities Using Machine Learning Methods. In *2023 19th International Asian School-Seminar on Optimization Problems of Complex Systems (OPCS)*, pp. 136–139.

Zolanvari, M., Teixeira, M. A., Gupta, L., Khan, K. M. & Jain, R. (2019). Machine Learning-Based Network Vulnerability Analysis of Industrial Internet of Things. *IEEE Internet of Things Journal*, *6*(4), pp. 6822–6834.