JOURNAL OF CRITICAL REVIEWS

ISSN- 2394-5125 VOL 10, ISSUE 04, 2023

SQL Injection Detection Using Machine Learning Techniques

C. Gazala Akhtar[1], M Harshini Reddy [2], P Keerthana [2], P Likitha[2], S Nithya Sri[2]

[1]Assistant Professor, [2]UG Scholar, [1,2]Department of CSE-Cyber Security

[1,2]Malla Reddy Engineering College for Women (A), Maisammaguda, Medchal, Telangana.

Abstract

SQL injection attacks pose a serious threat to web applications, as they exploit vulnerabilities in the database layer by injecting malicious SQL code into user input fields. These attacks can have severe consequences, including unauthorized access, data breaches, and even the complete compromise of the application and underlying database. Although traditional methods like input validation and parameterized queries exist to counter SQL injection, they have their limitations. These methods often rely on manual coding practices and may not cover all possible attack vectors. As attackers continually evolve their techniques, there is a pressing need for advanced and automated solutions that can proactively identify and mitigate SQL injection attacks. This is where artificial intelligence (AI) proves its significance in predicting and combating SQL injection attacks. AI has the capacity to analyze vast amounts of data, detect patterns, and learn from previous attacks, making it an invaluable tool in this context. AI brings significant benefits to the prediction of SQL injection attacks. Its ability to detect anomalies, learn from new attack patterns, recognize complex patterns, reduce false positives, provide real-time protection, and scale to handle large applications makes it an indispensable tool. By leveraging AI, organizations can bolster their defenses against SQL injection attacks, mitigating risks and ensuring the security of their web applications and databases.

Keywords: SQL injection attack, Artificial Intelligence, Prediction.

1. Introduction

SQL Injection is a type of cyber-attack that has been around for a long time. It involves injecting malicious SQL code into an application's input fields, which allows attackers to gain unauthorized access to the application's database. This can lead to severe consequences, such as data breaches and system compromises. In recent years, Artificial Intelligence (AI) and machine learning have become popular in various fields, including cybersecurity [1]. The idea of using AI to predict SQL Injection attacks emerged to bolster security measures and counter sophisticated attack techniques. By developing AI models that can analyze application input data, we can identify patterns that indicate the presence of an SQL Injection attack.

The traditional methods used to prevent SQL Injection attacks rely on simple rule-based approaches or static pattern matching. However, these methods can sometimes be bypassed by well-crafted attacks. This is where AI-based prediction of SQL Injection attacks becomes essential. We need AI-based prediction because cyber attackers continuously evolve their methods, making it challenging to rely solely on traditional approaches [2]. AI-powered systems can process large amounts of data, discover hidden patterns, and adapt to new attack techniques, making them more effective in identifying SQL Injection attacks.

The significance of AI-based prediction lies in its ability to enhance detection accuracy. AI models can learn from historical attack data and identify even subtle patterns that might go unnoticed by traditional methods. By doing so, they can reduce false positives, which helps minimize disruptions to legitimate user activities. Additionally, AI can serve as a proactive defense mechanism, continuously monitoring and protecting applications from potential threats, including novel and previously unseen SQL Injection attacks [3].

Artificial Intelligence, particularly machine learning, has shown promise in various cybersecurity applications due to its ability to analyze vast amounts of data, detect patterns, and make predictions. By harnessing the power of AI, security professionals can enhance their capabilities in detecting and mitigating SQL injection attacks [4].

Benefits of AI-based Prediction of SQL Injection Attacks:

- High Accuracy: AI models can achieve high accuracy in distinguishing between legitimate and malicious SQL queries, reducing false positives and false negatives.
- Real-time Detection: AI-based prediction can quickly assess incoming queries, providing a swift response to potential threats in real-time.
- Adaptability: The model can adapt to new attack patterns and variations, making it more resilient against emerging SQL injection techniques.
- Reduced Manual Effort: By automating the detection process, security teams can focus on other critical security tasks, allowing for a more efficient use of resources.
- Enhanced Security: Implementing AI-based prediction can significantly improve the security posture of web applications, safeguarding sensitive data and preventing unauthorized access.

Problem definition

The problem of "Artificial Intelligence based prediction of SQL Injection attack" involves utilizing AI techniques to detect and predict instances of SQL Injection attacks in computer systems or web applications. SQL Injection is a critical cybersecurity threat where attackers exploit vulnerabilities to inject malicious SQL code into a web application's backend database, potentially gaining unauthorized access or manipulating data. Traditional security measures might not fully prevent such attacks, making AI a valuable tool. By collecting a diverse dataset of legitimate inputs and known attack examples, training AI models like decision trees, random forests, or neural networks, and deploying the best-performing model into the application's security infrastructure, organizations can proactively defend against SQL Injection attacks and strengthen their web application security. Periodic updates and continuous monitoring ensure the model's effectiveness in tackling evolving threats.

2. Literature survey

Alghawazi et al. [5] applied techniques from different areas to detect and deterrence of SQL injection attacks, for which to improve the detect ability of the attack, is not a new area of research but it is still relevant. Artificial intelligence and machine learning techniques have been tested and used to control SQL injection attacks, showing promising results. The main contribution of this paper is to cover relevant work related to different machine learning and deep learning models used to detect SQL injection attacks. With this systematic review, this work aimed to keep researchers up-to-date and contribute to the understanding of the intersection between SQL injection attacks and the artificial intelligence field.

Zhang et al. [6] proposed a SQLNN deep neural network model. The core method is to convert the data into word vector form by word pause and then form a sparse matrix and pass it into the model for training to build a multi hidden layer deep neural network model containing ReLU function, which optimized the traditional loss function and introduces the Dropout method to improve the generalization ability of this model.

Uwagbole et al. [7] explored the generation of data set containing extraction from known attack patterns including SQL tokens and symbols present at injection points. Also, as a test case, this work build a web application that expects dictionary word list as vector variables to demonstrate massive quantities of learning data. The data set is pre-processed, labelled and feature hashing for supervised learning. This paper demonstrated a full proof of concept implementation of an ML predictive analytics and deployment of resultant web service that accurately predicts and prevents SQLIA with empirical evaluations presented in Confusion Matrix (CM) and Receiver Operating Curve (ROC).

Gandhi et al. [8] proposed a hybrid CNN-BiLSTM based approach for SQLI attack detection. The proposed CNN-BiLSTM model had significant accuracy of 98% and superior performance compared to other machine learning algorithms. Also, paper presented a comparative study of different types of machine learning algorithms used for the purpose of SQLI attack detection. The study showed the performance of various algorithms based on accuracy, precision, recall, and F1 score with respect to proposed CNN-BiLSTM model in detection of SQL injection attacks.

Ali et al. [9] studied the top 10 security threats identified by the OWASP are injection attacks. The most common vulnerability is SQL injection and is the most dangerous security vulnerability due to the multiplicity of its types and the rapid changes that can be caused by SQL injection and may lead to financial loss, data leakage, and significant damage to the database, and this causes the site to be paralyzed. Machine learning is used to analysed and identified security vulnerabilities. It used classic machine learning algorithms and deep learning to evaluate the classified model using input validation features.

Sharma et al. [10] used various classification algorithms to determine whether a particular code is malicious or plain. Some of the neural network and machine learning algorithms are Naive Bayes classifier, LSTM, MLP, and SVM which can be used for the detection of SQL Injection attacks. This work compared various algorithms on a common dataset in this study.

Roy et al. [11] penetrated the logical section of the database. If the database has a logical flaw, the attackers send a new type of logical payload and get all of the user's credentials. Despite the fact that technology has advanced significantly in recent years, SQL injections can still be carried out by taking advantage of security flaws.

Falor et al. [12] reviewed the different types of SQL Injection attacks and existing techniques for the detection of SQL injection attacks. We have compiled and prepared own dataset for the study including all major types of SQL attacks and have analysed the performance of Machine learning algorithms like Naïve Bayes, Decision trees, Support Vector Machine, and K-nearest neighbour. This work have also analysed the performance of Convolutional Neural Networks (CNN) on the dataset using performance measures like accuracy, precision, Recall, and area of the ROC curve.

Tripathy et al. [13] investigated the potential of using machine learning techniques for SQL injection detection on the application level. The algorithms to be tested are classifiers trained on different malicious and benign payloads. They take a payload as input and decide whether the input contains a malicious code or not. The results showed that these algorithms can distinguish normal payloads from malicious payloads with a detection rate higher than 98%. The paper also compared the performance of different machine learning models in detecting SQL injection attacks.

Hubskyi et al. [14] developed a neural network model for identifying SQL injection attacks based on HTTP request analysis. The model allowed classifying URL values by attributing them into one of two classes: attack or normal activity. An additional advantage is the provision of a quantitative identification value which describes the predicted accuracy of SQL injection determination.

Tang et al. [15] presented a high accuracy SQL injection detection method based on neural network. This work first acquired authentic user URL access log data from the Internet Service Provider (ISP), ensuring that our approach is real, effective, and practical. Then conduct statistical research on normal data and SQL injection data. Based on the statistical results, designed eight types of features, and train an MLP model. The accuracy of the model maintained over 99%. Meanwhile, this work compared and evaluated the training effect of other machine learning algorithms (LSTM, for example), the results revealed that the accuracy of this method is superior to the relevant machine learning algorithms.

3. Proposed System

Firstly, we collect a diverse dataset that includes both legitimate user input and various types of SQL Injection attacks. This dataset should be representative of the application's user base and encompass different attack scenarios. Next, we preprocess the collected data, removing any noise, irrelevant information, and personally identifiable data that may violate privacy regulations. After preprocessing, we perform feature engineering, extracting relevant features from the data that effectively represent the characteristics of input patterns and potential attacks. The next step is to select appropriate AI algorithm for the task. Depending on the available data and prediction requirements, we can choose from supervised learning (such as neural networks or support vector machines) or unsupervised learning (such as anomaly detection). With the algorithms selected, we proceed to train the AI model using the pre-processed dataset. During this phase, we adjust the model's parameters to optimize its performance in predicting SQL Injection attacks. To ensure the model's effectiveness and reliability, we evaluate its performance on a separate validation dataset and fine-tune it further if needed. We conduct extensive testing to validate its capabilities in real-world scenarios.

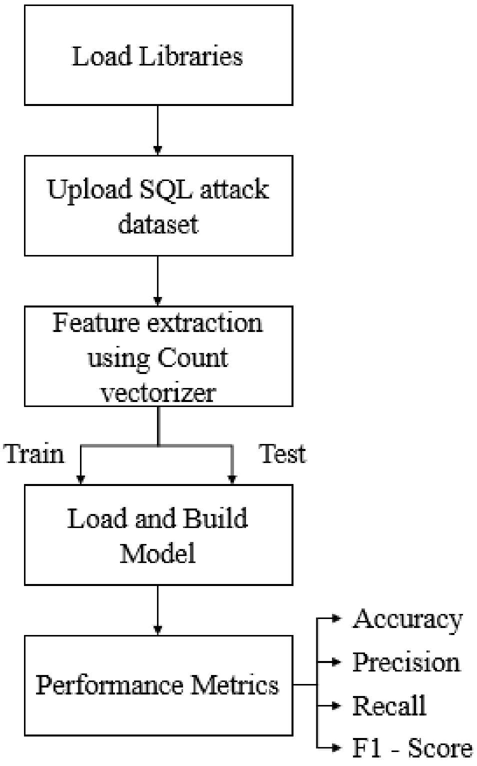


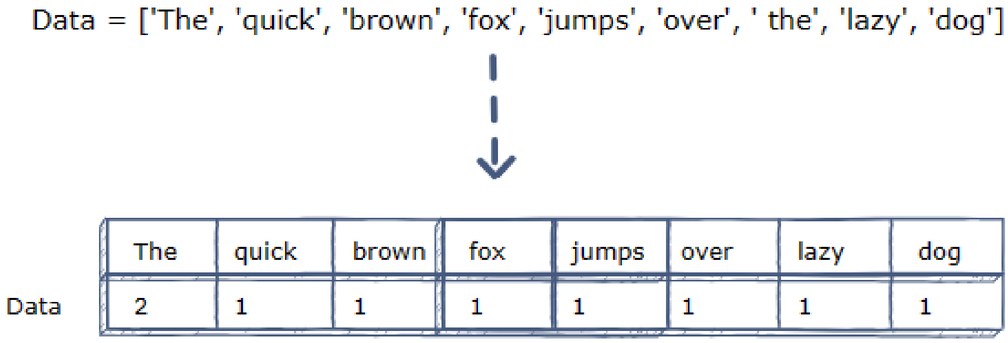
Fig. 1: Block diagram of proposed system.

Once the model has been thoroughly tested and proven effective, we integrate it into the application's security infrastructure. This enables the AI model to predict and prevent SQL Injection attacks in real-time. As the threat landscape constantly evolves, continuous monitoring and updating of the AI model are crucial. Regularly updating the model with new data allows it to adapt to emerging attack patterns and maintain its effectiveness over time.

3.1 Count Vectorizer

Machines cannot understand characters and words. So, when dealing with text data we need to represent it in numbers to be understood by the machine. Count vectorizer is a method to convert text to numerical data.

Count Vectorizer converts a collection of text documents to a matrix of token counts: the occurrences of tokens in each document. This implementation produces a sparse representation of the counts. It creates a matrix in which each unique word is represented by a column of the matrix, and each text sample from the document is a row in the matrix. The value of each cell is nothing but the count of the word in that text sample.



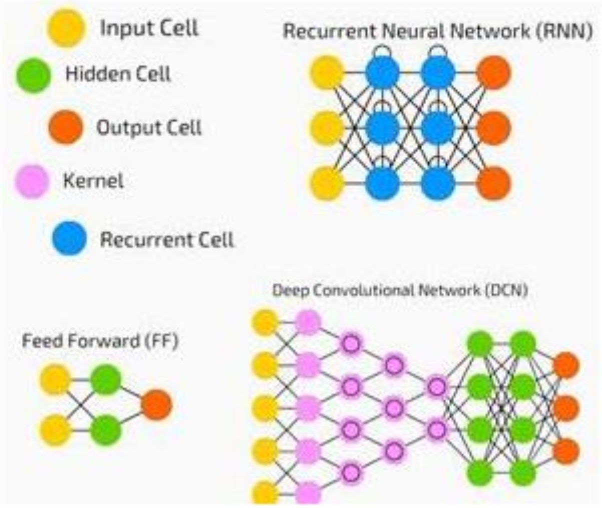
Data = ['The', 'quick', 'brown', 'fox', 'jumps', 'over', ' the', 'lazy', 'dog']

	The	quick	brown	fox	jumps	over	lazy	dog
Data	2	1	1	1	1	1	1	1

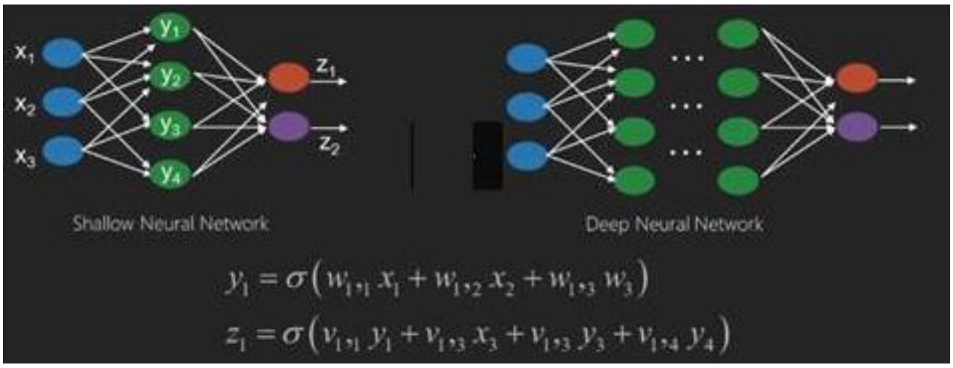
Fig. 2: Example of count vectorizer.

3.2 Deep Neural network

A deep neural network (DNN) is an ANN with multiple hidden layers between the input and output layers. Similar to shallow ANNs, DNNs can model complex non-linear relationships. The main purpose of a neural network is to receive a set of inputs, perform progressively complex calculations on them, and give output to solve real world problems like classification. We restrict ourselves to feed forward neural networks. It has an input, an output, and a flow of sequential data in a deep network.

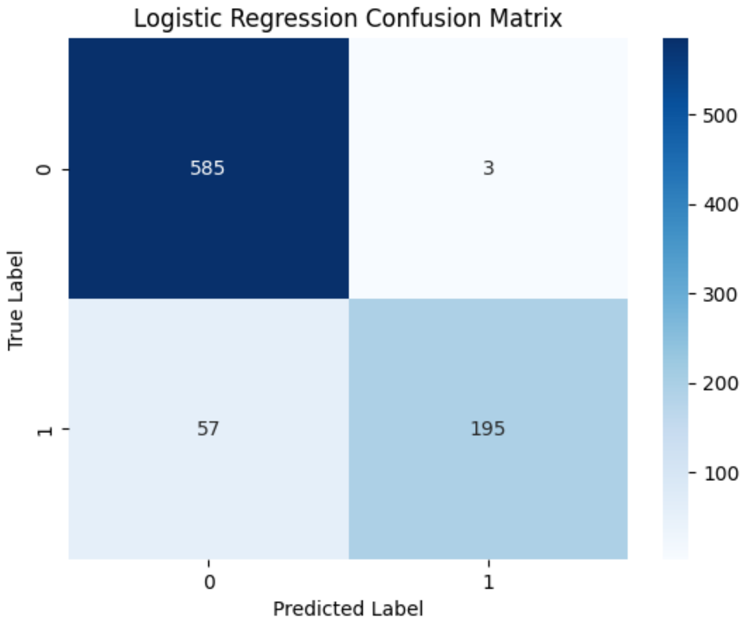


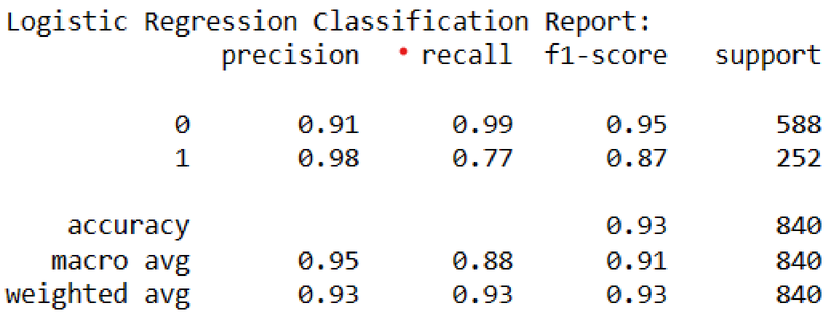
Neural networks are widely used in supervised learning and reinforcement learning problems. These networks are based on a set of layers connected to each other. In deep learning, the number of hidden layers, mostly non-linear, can be large; say about 1000 layers. DL models produce much better results than normal ML networks. We mostly use the gradient descent method for optimizing the network and minimising the loss function. One example of DL is the mapping of a photo to the name of the person(s) in photo as they do on social networks and describing a picture with a phrase is another recent application of DL.


x_1
x_2
x_3
y_1
y_2
y_3
y_4
z_1
z_2
Shallow Neural Network
Deep Neural Network
$y_1 = \sigma(w_{1,1} x_1 + w_{1,2} x_2 + w_{1,3} w_3)$
$z_1 = \sigma(v_{1,1} y_1 + v_{1,3} x_3 + v_{1,3} y_3 + v_{1,4} y_4)$

Neural networks are functions that have inputs like x1, x2, x3…that are transformed to outputs like z1, z2, z3 and so on in two (shallow networks) or several intermediate operations also called layers (deep networks). The weights and biases change from layer to layer. ‘w’ and ‘v’ are the weights or synapses of layers of the neural networks. The best use case of deep learning is the supervised learning problem. Here, it has large set of data inputs with a desired set of outputs.

4. Results and Discussion

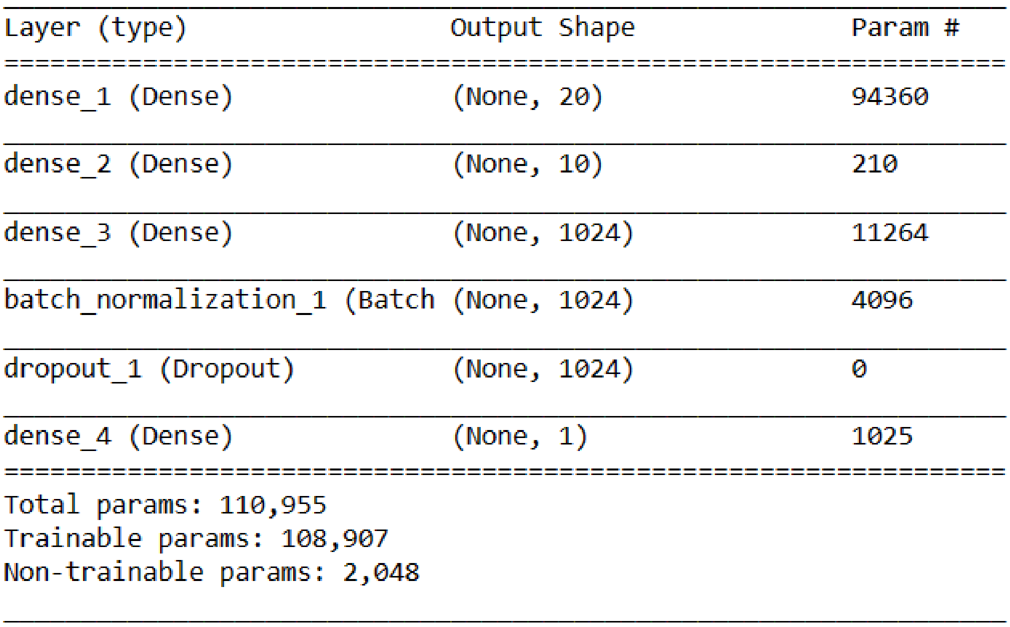




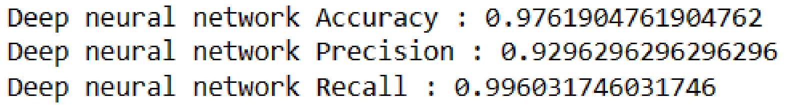
```
Logistic Regression Classification Report:
              precision    recall  f1-score   support

           0       0.91      0.99      0.95       588
           1       0.98      0.77      0.87       252

    accuracy                           0.93       840
   macro avg       0.95      0.88      0.91       840
weighted avg       0.93      0.93      0.93       840
```



```
_________________________________________________________________
Layer (type)                 Output Shape              Param #
=================================================================
dense_1 (Dense)              (None, 20)                94360
_________________________________________________________________
dense_2 (Dense)              (None, 10)                210
_________________________________________________________________
dense_3 (Dense)              (None, 1024)              11264
_________________________________________________________________
batch_normalization_1 (Batch (None, 1024)              4096
_________________________________________________________________
dropout_1 (Dropout)          (None, 1024)              0
_________________________________________________________________
dense_4 (Dense)              (None, 1)                 1025
=================================================================
Total params: 110,955
Trainable params: 108,907
Non-trainable params: 2,048
_________________________________________________________________
```



```
Deep neural network Accuracy : 0.9761904761904762
Deep neural network Precision : 0.9296296296296296
Deep neural network Recall : 0.996031746031746
```

5. Conclusion and Future Scope

In conclusion, SQL injection attacks pose a significant threat to web applications, potentially leading to unauthorized access, data breaches, and complete compromise of the application and underlying database. While traditional methods such as input validation and parameterized queries offer some level of protection, they have limitations and may not cover all attack vectors. Therefore, this work implemented AI solution to proactively identify and mitigate SQL injection attacks. The future scope of this project lies in leveraging AI to combat SQL injection attacks. AI has proven to be highly effective in analyzing vast amounts of data, detecting patterns, and learning from previous attacks. By using AI techniques, organizations can enhance their defenses against SQL injection attacks and ensure the security of their web applications and databases.

The benefits of AI in predicting SQL injection attacks are significant. AI can detect anomalies and learn from new attack patterns, which enables it to recognize complex attack vectors that traditional methods might miss. Furthermore, AI can reduce false positives, provide real-time protection, and scale to handle large applications efficiently. These capabilities make AI an indispensable tool in defending against SQL injection attacks. To further enhance the effectiveness of

AI-based solutions, ongoing research and development efforts should focus on continuously updating AI models with the latest attack patterns and vulnerabilities. This would ensure that the AI system remains up-to-date and can effectively counter emerging SQL injection threats.

References

[1] Martins, N.; Cruz, J.M.; Cruz, T.; Abreu, P.H. Adversarial Machine Learning Applied to Intrusion and Malware Scenarios: ASystematic Review. IEEE Access 2020,8, 35403–35419.

[2] Mishra, P.; Varadharajan, V.; Tupakula, U.; Pilli, E.S. A Detailed Investigation and Analysis of using Machine Learning Techniquesfor Intrusion Detection. IEEE Commun. Surv. Tutor. 2018,21, 686–728.

[3] Yan, R.; Xiao, X.; Hu, G.; Peng, S.; Jiang, Y. New deep learning method to detect code injection attacks on hybrid applications. J.Syst. Softw. 2018,137, 67–77.

[4] Aliero, M.S.; Qureshi, K.N.; Pasha, M.F.; Ghani, I.; Yauri, R.A. Systematic Review Analysis with SQLIA Detection and PreventionApproaches. Wirel. Pers. Commun. 2020,112, 2297–2333.

[5] Alghawazi, Maha & Alghazzawi, Daniyal & Alarifi, Suaad. (2022). Detection of SQL Injection Attack Using Machine Learning Techniques: A Systematic Literature Review. Journal of Cybersecurity and Privacy. 2. 764-777. 10.3390/jcp2040039.

[6] W. Zhang, Y. Li, X. Li, M. Shao, Y. Mi, H. Zhang, G. Zhi, "Deep Neural Network-Based SQL Injection Detection Method", Security and Communication Networks, vol. 2022, Article ID 4836289, 9 pages, 2022. https://doi.org/10.1155/2022/4836289

[7] S. O. Uwagbole, W. J. Buchanan and L. Fan, "Applied Machine Learning predictive analytics to SQL Injection Attack detection and prevention," 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), Lisbon, Portugal, 2017, pp. 1087-1090, doi: 10.23919/INM.2017.7987433.

[8] N. Gandhi, J. Patel, R. Sisodiya, N. Doshi and S. Mishra, "A CNN-BiLSTM based Approach for Detection of SQL Injection Attacks," 2021 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), Dubai, United Arab Emirates, 2021, pp. 378-383, doi: 10.1109/ICCIKE51210.2021.9410675.

[9] M. H. Ali AL-Maliki; Mahdi Nsaif Jasim. "Review of SQL injection attacks: Detection, to enhance the security of the website from client-side attacks". International Journal of Nonlinear Analysis and Applications, 13, 1, 2022, 3773-3782. doi: 10.22075/ijnaa.2022.6152

[10] Sharma, V., Kumar, S. (2023). Comparative Study of Machine Learning Algorithms for Prediction of SQL Injections. In: Shukla, P.K., Singh, K.P., Tripathi, A.K., Engelbrecht, A. (eds) Computer Vision and Robotics. Algorithms for Intelligent Systems. Springer, Singapore. https://doi.org/10.1007/978-981-19-7892-0_36

[11] P. Roy, R. Kumar and P. Rani, "SQL Injection Attack Detection by Machine Learning Classifier," 2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC), Salem, India, 2022, pp. 394-400, doi: 10.1109/ICAAIC53929.2022.9792964.

[12] 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: Gupta, D., Polkowski, Z., Khanna, A., Bhattacharyya, S., Castillo, O. (eds) Proceedings of Data Analytics and Management . Lecture Notes on Data Engineering and Communications Technologies, vol 91. Springer, Singapore. https://doi.org/10.1007/978-981-16-6285-0_24

[13] D. Tripathy, R. Gohil and T. Halabi, "Detecting SQL Injection Attacks in Cloud SaaS using Machine Learning," 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), Baltimore, MD, USA, 2020, pp. 145-150, doi: 10.1109/BigDataSecurity-HPSC-IDS49724.2020.00035.

[14] Hubskyi, O., Babenko, T., Myrutenko, L., Oksiiuk, O. (2021). Detection of SQL Injection Attack Using Neural Networks. In: Shkarlet, S., Morozov, A., Palagin, A. (eds) Mathematical Modeling and Simulation of Systems (MODS'2020). MODS 2020. Advances in Intelligent Systems and Computing, vol 1265. Springer, Cham. https://doi.org/10.1007/978-3-030-58124-4_27

[15] P. Tang, W. Qiu, Z. Huang, H. Lian, G. Liu, Detection of SQL injection based on artificial neural network, Knowledge-Based Systems, Volume 190, 2020, 105528, ISSN 0950-7051, https://doi.org/10.1016/j.knosys.2020.105528.