Detection of SQL Injection Attack Using Machine Learning Techniques: A Review

[1] Bhanu Pratap Singh, [2] Prof. Dr. Shekhar Nigam
[1]*M.Tech Scholar,* [2]*Professor & H.O.D*
[1,2]*Department of Information Technology (IT*)
[1,2]*NRI Institute of Information Science and Technology, Bhopal (MP), India,*

***Abstract*— SQL Injection (SQLi) attacks pose a significant threat to database security, enabling attackers to manipulate SQL queries and gain unauthorized access to sensitive data. Traditional security measures, such as signature-based detection and rule-based approaches, often fail to detect evolving SQLi attack patterns. To address these challenges, machine learning (ML) techniques have emerged as powerful tools for detecting and mitigating SQLi attacks. This review paper explores various ML-based approaches, including supervised, unsupervised, and deep learning models, for identifying SQLi attempts. It examines feature extraction methods, dataset challenges, model performance metrics, and comparative analyses of existing ML techniques. Additionally, the paper highlights the advantages and limitations of different ML models in real-world scenarios, emphasizing their effectiveness in improving detection accuracy and reducing false positives.**

Keywords- SQL Injection, Cross Side Scripting, Denial of Service Attack, Naïve Bias, Gradient Boosting, etc.

I. INTRODUCTION

The Securing web applications against cyber threats is a critical challenge in today's digital landscape, with SQL injection (SQLi) attacks remaining one of the most prevalent and damaging vulnerabilities. These attacks exploit weaknesses in database queries, allowing attackers to manipulate or access sensitive information. Traditional security measures, such as input validation and firewall protection, often fall short in detecting sophisticated SQLi attempts. In response, machine learning (ML) has emerged as a powerful tool for enhancing web security by identifying and mitigating such threats in real time. This paper explores the development of an ML-based model designed to detect and prevent SQL injection attacks. By leveraging techniques such as natural language processing (NLP) and anomaly detection, the model can analyze incoming queries, differentiate between legitimate and malicious inputs, and provide adaptive security measures. Implementing ML-driven security solutions not only strengthens web application defenses but also contributes to the evolving field of cyber security, ensuring safer and more resilient online environments.

Securing web applications against cyber threats is a critical challenge, with SQL injection being one of the most prevalent and damaging attacks. To enhance security, machine learning models can be employed to detect and prevent SQL injection attempts in real-time. These models analyze input patterns, identify anomalies, and classify malicious queries based on training data. Techniques such as natural language processing (NLP) and deep learning can improve detection accuracy by distinguishing between legitimate user inputs and SQL injection attempts. By integrating machine learning-based security mechanisms into web applications, developers can significantly reduce vulnerabilities, ensuring robust protection against unauthorized database access and potential data breaches.

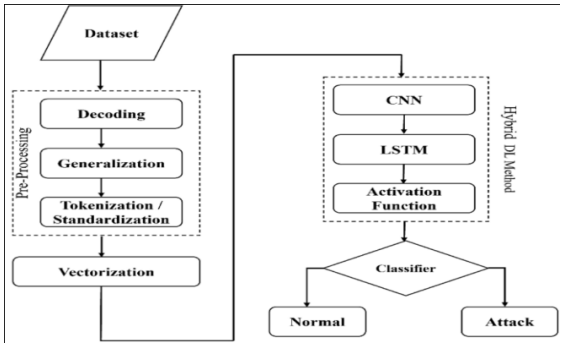

Fig 1 Securing Web Applications: A Machine Learning Model for SQL Injection

A. SQL Injection

SQL Injection is a type of cyber-attack that exploits vulnerabilities in a web application's database query

execution. It occurs when an attacker manipulates user input fields to inject malicious SQL code into a database query, potentially gaining unauthorized access to sensitive data, modifying database contents, or even executing administrative operations. This security flaw arises due to inadequate input validation and improper handling of user inputs in SQL statements. Attackers can use SQL Injection to bypass authentication, extract confidential information, or delete critical records, posing serious risks to data integrity and system security. To prevent SQL Injection, developers must implement secure coding practices, such as using prepared statements, parameterized queries, and proper input validation techniques.

B. Machine Learning

Machine learning is a branch of artificial intelligence that enables computers to learn from data and make predictions or decisions without being explicitly programmed. It relies on algorithms and statistical models to identify patterns and relationships in large datasets, improving performance over time as more data becomes available. Machine learning is widely used in various applications, including image and speech recognition, recommendation systems, fraud detection, and autonomous systems. It can be categorized into supervised learning, where models learn from labeled data; unsupervised learning, which identifies patterns in unlabeled data; and reinforcement learning, where agents learn by interacting with an environment to maximize rewards. As technology advances, machine learning continues to drive innovation across industries, enhancing efficiency and decision-making processes.

The success of machine learning depends on high-quality data, robust algorithms, and computational power. Data preprocessing, including cleaning, normalization, and feature selection, is crucial to ensuring accurate and reliable models. Popular algorithms include decision trees, support vector machines, neural networks, and deep learning models, each suited for different types of tasks. Deep learning, a subset of machine learning, uses artificial neural networks to process complex patterns, making it especially effective in areas such as natural language processing and computer vision. Despite its potential, machine learning also faces challenges, including biases in data, overfitting, and ethical concerns regarding privacy and security. As research progresses, advancements in explainable AI and fairness in machine learning aim to address these issues, making the technology more transparent and trustworthy. The continuous evolution of machine learning is expected to shape the future of industries like healthcare, finance, transportation, and more, driving intelligent automation and decision-making at an unprecedented scale.

II. LITERATURE SURVEY

Laila Aburashed et.al.(2024) - This research work presented, SQL Injection is one of the most common vulnerabilities exploited for both privacy breaches and financial damage. It remains the top vulnerability on the most recent OWASP Top 10 list, with the number of such attacks on the rise. The SQL Injection Detection Challenge is addressed using machine learning algorithms. By employing a classification method, communications are identified as either SQL Injection or plain text. This research proposes a machine learning framework to assess the feasibility of using a machine learning classifier to detect SQL Injection attacks. Classification algorithms such as Random Forest, Gradient Boosting, SVM, and ANN are utilized. As a result, ANN demonstrated superior performance and required less time to detect SQL Injection attacks [01].

S. Venkatramulu, et.al (2024), Author are presented The security in online applications cannot be guaranteed. Due to their accessibility, they are vulnerable to several flaws, and if these flaws are not fixed, they could have negative effects. One attack type that is simple to execute but difficult to detect is SQL Injection. This could lead to theft, the disclosure of private information, or the loss of property. This research effort has produced a novel method for detecting SQLi attacks utilizing word encoding techniques and machine learning algorithms. Our dataset includes legitimate, fraudulent SQL queries and plain text. We suggested a reliable methodology for differentiating plain text and regular queries from SQL injection attack queries. After evaluating the results, XGBoost algorithm with a unigram count vectorizer encoding of 70:30 split data ratio, gave us the best model with an F1-score of 0.992 and accuracy of 0.994. It has greater runtime as compared with other

machine learning algorithms used. As numerous simple classifiers are used, ensemble learning techniques are said to produce results with higher accuracy [02].

Michael S. Souza .et. al (2024) - Author are These services employ relational databases to store the collected data, thereby making them vulnerable to potential threats, including SQL Injection (SQLi) attacks. Hence, there is a demand for security solutions that improve detection efficiency and satisfy the response time and scalability requirements of this detection process. Based on this existing demand, this article proposes an SQLi detection solution that combines Regular Expressions (RegEx) and Machine Learning (ML), called Two Layer approach of SQLi Detection (2LDSQLi). The RegEx acts as a first layer of filtering for protection against SQLi inputs, improving the response time of 2LD-SQLi through RegEx filtering. From this filtering, it is analyzed by an ML model to detect SQLi, increasing the accuracy. Experiments, using a real dataset, suggest that 2LD-SQLi is suitable for detecting SQLi while meeting the efficiency and scalability issues [03].

Hakan Can Altunay et.al. (2023) - This research work presented, SQL injection attack is one of the cyber-attack types that puts individuals and institutions in a difficult situation in terms of data disclosure and material damage. This attack type, which is frequently preferred due to its case of use, has emerged with different usage features in recent years. In this study, various machine learning algorithms were tested to detect SQL Injection attacks. In the data pre-processing section, feature extraction was performed using Natural Language Processing techniques. While the relevance of expressions to each other was calculated with the Word Level TF-IDF method, term search was also performed [04].

Animesh Kumar et.al (2023), Author are study a from hosting websites to developing platforms and storing resources, cloud computing has tremendous use in the modern information technology industry. Although an emerging technique, it has many security challenges. In structured query language injection attacks, the attacker modifies some parts of the user query to still sensitive user information. This type of attack is challenging to detect and prevent. In this article, we have reviewed 65 research articles that address the issue of its prevention and detection in cloud and Traditional Networks, of which 11 research articles are related to general cloud attacks, and the rest of the 54 research articles are specifically on web security. Our result shows that Random Forest has an accuracy of 99.8% and a Precision rate of 99.9%, and the worst-performing model is Multi-Layer Perceptron (MLP) in the SQLIA Model. For recall value, Random Forest performs best while TensorFlow Linear Classifier performs worst. F1 score is best in Random Forest, while MLP is the most diminutive performer [05].

Babu R. Dawadi et.al, (2023) - Using LSTM as our deep learning approach, the proposed model detected DDoS, XSS, and SQL injection attacks with considerably good accuracy. The first detection layer was a DDoS attack detection model with an accuracy of 97.57%, and the second layer was for XSS and SQL injection attack detection with an accuracy of 89.34%. We analyzed features and parameters for attack detection, which reduced false positives during traffic filtering in the WAF. As DDoS traffic comes at a higher rate than normal traffic, the system's performance imporves when we check the traffic in a layered format, i.e., first checking for DDoS before testing for SQL injection and XSS. Moreover, we analyzed the performance perspective of the web application when an extra layer of filtering was added and found a slight impact on performance [07].

Yuting Guan et.al (2023) - SQL injection is a highly detrimental web attack technique that can result in significant data leakage and compromise system integrity. To counteract the harm caused by such attacks, researchers have devoted much attention to the examination of SQL injection detection techniques, which have progressed from traditional signature-based detection methods to machine- and deep-learning-based detection models. These detection techniques have demonstrated promising results on existing datasets; however, most studies have overlooked the impact of adversarial attacks, particularly blackbox adversarial attacks, on detection methods. This study addressed the shortcomings of current SQL injection detection techniques and proposed a reinforcement-learning-based black-box adversarial attack method. The proposal included an innovative vector transformation approach for the original SQL

injection payload, a comprehensive attack-rule matrix, and a reinforcement-learning-based method for the adaptive generation of adversarial examples. Our approach was evaluated on existing web application firewalls (WAF) and detection models based on machine- and deep-learning methods, and the generated adversarial examples successfully bypassed the detection method at a rate of up to 97.39% [06]

Ahmed Abadulla Ashlamr et.al (2022) - Author are study Structured Query Language (SQL) Injection constitutes a most challenging type of cyber-attack on the security of databases. SQLI attacks provide opportunities by malicious actors to exploit the data, particularly client personal data. To counter these attacks security measures, need to be deployed at all layers, namely application layer, network layer, and database layer; otherwise, the database remains vulnerable to attacks at all levels. Research studies have demonstrated that lack of input validation, incorrect use of dynamic SQL, and inconsistent error handling have continued to expose databased to SQLI attacks The security measures commonly deployed presently, being mostly focused on the network layer only, still leave the program code and the database at risk despite well-established approaches such as web server requests filtering, network firewalls and database access control [08].

Maha Alghawazi et. al. (2022) - This research work presented, An SQL injection attack, usually occur when the attacker(s) modify, delete, read, and copy data from database servers and are among the most damaging of web application attacks. A successful SQL injection attack can affect all aspects of security, including confidentiality, integrity, and data availability. SQL (structured query language) is used to represent queries to database management systems. Detection and deterrence of SQL injection attacks, for which techniques from different areas can be applied 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, we aims to keep researchers up-to-date and contribute to the understanding of the intersection between SQL injection attacks and the artificial intelligence field [09].

Ahmed Abadulla Ashlam et.al (2022) - A SQLi attack occurs as a result of flaws in query design which expose a vulnerability whereby an attacker can take advantage by inserting code into the query to alter the normal query, leading to unauthorised database access. This paper has proposed a Multi-Phase Algorithmic Framework which was designed, developed and evaluated in the lab through benchmarking as well as being tested with real-world data in the operational context of a university and a commercial bank to validate its performance. The results have shown improved parameterised machine learning and deep learning to enhance database security in real-time at the database layer. It can be concluded that the proposed algorithmic framework technique can efficiently detect and prevent a large subset of SQLi attacks in real-time [10].

III. METHOD

The goal of this project is to build a model that can detect SQL Injection (SQLi) attacks in SQL queries. SQLi attacks exploit vulnerabilities in the database query processing, leading to unauthorized access and data breaches. This model will classify SQL queries as either malicious (SQLi) or benign (safe), helping to prevent security vulnerabilities in web applications.

A. Dataset Description

The dataset used for this project consists of SQL queries labeled as:

- *Malicious (SQLi): Labeled as 1, representing a harmful SQL Injection attempt.*
- *Benign (Safe): Labeled as 0, representing a normal, safe SQL query.*

Each row in the dataset represents a single SQL query, and the associated label indicates whether the query is benign or malicious. The data is likely to be text-based, and pre-processing is necessary to convert the raw SQL queries into a usable form for machine learning.

B. Data Pre-processing

- Text Cleaning: The raw SQL queries may contain noise such as special characters, extra whitespace, or null values. This will be cleaned to ensure uniformity and to eliminate unwanted

elements that might interfere with model performance.

- Text Normalization: All text will be converted to lowercase to maintain consistency across all queries, as SQL queries may have different case conventions.
- Tokenization: The cleaned text will be split into smaller units, such as words or tokens, to better understand the structure of the query.
- Vectorization: The text data will be converted into numerical form. Techniques such as TF-IDF (Term Frequency-Inverse Document Frequency) will be used to represent the importance of each word or token in the context of the entire dataset. This allows the machine learning models to process text effectively.

Once the data is cleaned and vectorized, it will be divided into training, validation, and testing sets to evaluate the models' performance.

C. Feature Engineering

- TF-IDF Representation: The primary feature engineering technique involves transforming the SQL queries into numerical vectors using the TF-IDF method. This method assigns a weight to each word based on its frequency in the document and its rarity across the entire dataset.
- N-grams: In addition to individual words, sequences of words (n-grams) will also be considered as features. This helps capture contextual information in the queries, which may be crucial for identifying attack patterns in SQLi.

Embeddings (Optional): If necessary, pre-trained word embeddings like Word2Vec or GloVe could be used to capture semantic meaning between words, improving model performance by considering word relationships.

V. CONCLUSSION AND FUTURE SCOPE

Conclusion

Securing web applications against SQL injection attacks is a critical aspect of modern cybersecurity. The integration of machine learning models provides an effective and adaptive approach to detecting and mitigating such threats. By analyzing query patterns and identifying anomalies, these models enhance security beyond traditional rule-based methods. However, continuous updates and improvements are necessary to counter evolving attack techniques. Combining machine learning with other security measures, such as input validation and web application firewalls, ensures a robust defense against SQL injection vulnerabilities.

The effectiveness of a machine learning-based approach depends on the quality of the training data, feature selection, and model tuning. Regular monitoring and retraining of the model help maintain its accuracy in detecting new and sophisticated SQL injection techniques. Additionally, integrating this approach with real-time threat intelligence can further strengthen web application security. While machine learning offers a promising solution, it should be complemented by best security practices, including secure coding, access control mechanisms, and regular security audits. By adopting a multi-layered security strategy, organizations can significantly reduce the risk of SQL injection attacks and ensure the integrity and confidentiality of their data.

Future Scope

The future scope of securing web applications using machine learning, particularly for detecting and preventing SQL injection attacks, is vast and promising. As cyber threats continue to evolve, traditional security measures like rule-based detection systems often struggle to keep up with sophisticated attacks. Machine learning (ML) models can enhance security by analyzing vast amounts of data, identifying patterns, and detecting anomalies that may indicate SQL injection attempts. Future advancements in deep learning, natural language processing (NLP), and anomaly detection techniques will further improve the accuracy and efficiency of these models. Additionally, integrating ML-based security solutions with real-time monitoring systems and automated response mechanisms can significantly reduce the risk of data breaches. As organizations increasingly adopt AI-driven cybersecurity frameworks, the future will likely see more adaptive, self-learning security systems that can proactively defend against emerging SQL injection threats

REFERENCES

[1] Laila Aburashed1,Marah AL Amoush1, Wardeh Alrefai1 “SQL Injection Attack

Detection Using Machine Learning Algorithms ǁ ISSN: 3030-5241, 15 June 2024.

[2] S. Venkatramulu, Md. Sharfuddin Waseem, Arshiya Taneem, Sri Yashaswini Thoutam4 , Snigdha Apuri5 and Nachiketh. " Research on SQL Injection Attacks using Word Embedding Techniques and Machine Learning Vol.02(01), Mar 2024, pp.55-66.

[3] Michael S. Souza, Silvio E. S. B. Ribeiro, Vanessa C. Lima, Francisco J. Cardoso and Rafael L. Gomes. " Combining Regular Expressions and Machine Learning for SQL Injection Detection in Urban Computing." VOL. 15 NO. 1 (2024)

[4] Jaydeep R.Tadhani, VipulVekariya, Vishal Sorathiya, SamahAlshathri & Walid El-Shafa "Securing web applications against XSS and SQLi attacks using a novel deep learning approach" 20 January 2024, | https://doi.org/10.1038/s41598-023-48845-4.

[5] Hakan Can Altunay. "Detection of SQL Injection Attacks Using Machine Learning Algorithms Based on NLP-Based Feature Extraction" 11 December 2023.

[6] Animesh Kumar, Sandip Dutta, Prashant Pranav. "Analysis of SQL injection attacks in the cloud and in WEB applications" 18 January 2024, https://doi.org/10.1002/spy2.370

[7] Babu R. Dawadi, Bibek Adhikari and Devesh Kumar Srivastava. " Deep Learning Technique-Enabled Web Application Firewall for the Detection of Web Attacks." Volume 23, Issue 4, 12 February 2023.

[8] Yuting Guan, Junjiang He, Tao Li, Hui Zhao and Baoqiang Ma "SSQLi: A Black-Box Adversarial Attack Method for SQL Injection Based on Reinforcement Learning" Volume 15, Issue 4, 30 March 2023,| https://doi.org/10.3390/fi15040133,.

[9] . Manar Hasan Ali AL-Malikia, Mahdi Nusif Jasim "Comparison study for NLP using machine learning techniques to detecting SQL injection vulnerabilities" . Appl. 14 (2023) 8, 283–290 ISSN: 2008-6822, August 2023.

[10] Manar Hasan Ali AL-Malikia,∗ , Mahdi Nsaif Jasim. " SQL injection attacks: Detection, to enhance the security of the website from client-side attacks." Appl. 13 (2022) 1, 3773-3782 ISSN: 2008-6822.

[11] Ahmed Abadulla Ashlam, Atta Badii, Frederic Stahl. " Multi-Phase Algorithmic Framework to Prevent SQL Injection Attacks using Improved Machine learning and Deep learning to Enhance Database security in Real-time." November 2022, DOI: http://dx.doi.org/10.1109/SIN56466.2022.9970504

[12] Maha Alghawazi , Daniyal Alghazzawi and Suaad Alarifi "Detection of SQL Injection Attack Using Machine Learning Techniques" Volume 2, Issue 4 ,20 September 2022.

[13] Ashlam, A. A., Badii, A. and Stahl, F. ORCID "Multi-phase algorithmic framework to prevent SQL injection attacks using improved machine learning and deep learning to enhance database security in real-time" 2022.

[14] Rokia Lamrani Alaoui and El Habib Nfaoui "Deep Learning for Vulnerability and Attack Detection on Web Applications" Volume 14 , Issue 4, 13 April 2022.

[15] Bronjon Gogoi; Tasiruddin Ahmed; Arabinda Dutta "Defending against SQL Injection Attacks in Web Applications using Machine Learning and Natural Language Processing" 01 February 2021, 10.1109/INDICON52576.2021.9691740.

[16] Ravi Raj Choudhary; Susheela Verma; Gaurav Meena. "Detection of SQL Injection attack Using Machine Learning" 17-19 December 2021.

[17] Md. Maruf Hassan, R. Badlishah Ahmad, Tonmoy Ghosh "SQL Injection Vulnerability Detection Using Deep Learning: A Feature-based Approach" Indonesian Journal of Electrical Engineering and Informatics (IJEEI), Vol. 9, No. 3, September 2021, pp. 702~718 ISSN: 2089-3272, DOI: 10.52549/ijeei.v9i3.3131.

[18] László Erdődi, Åvald Åslaugson Sommervoll, Fabio Massimo Zennaro "Simulating SQL Injection Vulnerability Exploitation Using Q-Learning Reinforcement Learning Agents" Journal of Information Security and Applications,Volume 61, September 2021, 102903.

[19] Hacer Karacan And Mehmet Sevri "A Novel Data Augmentation Technique and Deep Learning Model for Web Application Security" Digital Object Identifier 10.1109/ACCESS.2021.3125785, 2021, accepted October 27, 2021.

[20] Binh An Pham, Vinitha Hannah Subburaj "An Experimental setup for Detecting SQLi

Attacks using Machine Learning Algorithms" Volume 8, No. 1, 2020.

[21] Luca Demetrio, Andrea Valenza, Gabriele Costa, and Giovanni Lagorio. " WAF-A-MoLE: Evading Web Application Firewalls through Adversarial Machine Learning." 7 Jan 2020.

[22] Mark A Aizerman. 1964. Theoretical foundations of the potential function method in pattern recognition learning. Automation and remote control 25 (1964), 821–837.

[23] Hyrum S Anderson, Anant Kharkar, Bobby Filar, and Phil Roth. 2017. Evading machine learning malware detection. Black Hat (2017).

[24] Dennis Appelt, Cu D Nguyen, and Lionel Briand. 2015. Behind an application firewall, are we safe from SQL Injection attacks? In 2015 IEEE 8th International Conference on Software Testing, Verification and Validation (ICST). IEEE, 1–10.

[25] Dennis Appelt, Cu D Nguyen, Annibale Panichella, and Lionel C Briand. 2018. A machine-learning-driven evolutionary approach for testing web application firewalls. IEEE Transactions on Reliability 67, 3 (2018), 733–757.

[26] Sruthi Bandhakavi, Prithvi Bisht, P Madhusudan, and VN Venkatakrishnan. 2007. CANDID: preventing sql injection attacks using dynamic candidate evaluations. In Proceedings of the 14th ACM conference on Computer and communications security. ACM, 12–24.

[27] Marco Barreno, Blaine Nelson, Russell Sears, Anthony D Joseph, and J Doug Tygar. 2006. Can machine learning be secure? In Proceedings of the 2006 ACM Symposium on Information, computer and communications security. ACM, 16–25.

[28] Battista Biggio, Igino Corona, Davide Maiorca, Blaine Nelson, Nedim Šrndić, Pavel Laskov, Giorgio Giacinto, and Fabio Roli. 2013. Evasion attacks against machine learning at test time. In Joint European conference on machine learning and knowledge discovery in databases. Springer, 387–402.

[29] Battista Biggio and Fabio Roli. 2018. Wild patterns: Ten years after the rise of adversarial machine learning. Pattern Recognition 84 (2018), 317–331.

[30] Kay Henning Brodersen, Cheng Soon Ong, Klaas Enno Stephan, and Joachim M Buhmann. 2010. The balanced accuracy and its posterior distribution. In 2010 20th International Conference on Pattern Recognition. IEEE, 3121–3124.

[31] Nicholas Carlini and David Wagner. 2017. Adversarial examples are not easily detected: Bypassing ten detection methods. In Proceedings of the 10th ACM Workshop on Artificial Intelligence and Security. ACM, 3–14.

[32] Mariano Ceccato, Cu D Nguyen, Dennis Appelt, and Lionel C Briand. 2016. SOFIA: an automated security oracle for black-box testing of SQL-injection vulnerabilities. In Proceedings of the 31st IEEE/ACM International Conference on Automated Software Engineering. ACM, 167–177.

[33] Kyunghyun Cho, Bart Van Merriënboer, Caglar Gulcehre, Dzmitry Bahdanau, Fethi Bougares, Holger Schwenk, and Yoshua Bengio. 2014. Learning phrase representations using RNN encoder-decoder for statistical machine translation. arXiv preprint arXiv:1406.1078 (2014).

[34] Corinna Cortes and Vladimir Vapnik. 1995. Support-vector networks. Machine learning 20, 3 (1995), 273–297.

[35] Luca Demetrio, Battista Biggio, Giovanni Lagorio, Fabio Roli, and Alessandro Armando. 2019. Explaining Vulnerabilities of Deep Learning to Adversarial Malware Binaries. arXiv preprint arXiv:1901.03583 (2019).

[36] Ambra Demontis, Marco Melis, Maura Pintor, Matthew Jagielski, Battista Biggio, Alina Oprea, Cristina Nita-Rotaru, and Fabio Roli. 2018. On the Intriguing Connections of Regularization, Input Gradients and Transferability of Evasion and Poisoning Attacks. arXiv preprint arXiv:1809.02861 (2018).