International Journal on
"Technical and Physical Problems of Engineering"
(IJTPE)
Published by International Organization of IOTPE

ISSN 2077-3528
IJTPE Journal
www.iotpe.com
ijtpe@iotpe.com

December 2023 | Issue 57 | Volume 15 | Number 4 | Pages 256-261

A COMPREHENSIVE SYSTEMATIC REVIEW OF SQL INJECTION ATTACK DETECTION TECHNIQUES

B.H. Ali A.K. Al Azzawi

Department of Computer Science, College of Science, University of Diyala, Baqubah, Iraq
scicompms24@uodiyala.edu.iq, dr.abdulbasit@uodiyala.edu.iq

Abstract- Attacks using SQL injection provide a constant danger to websites and web applications. To prevent these attacks, and for identifying and thwarting SQL injection attacks, researchers and professionals have created a range of various techniques. In this systematic review, we analyze and evaluate the different techniques that have been developed for detecting SQL injection attacks, including Heuristic-Based Detection, Dynamic Analysis, signature-based, Static analysis, Machine Learning-Based Detection, and hybrid detection methods. Our review provides a comprehensive and authoritative overview of the current state of SQL injection attack detection techniques; and can be used by practitioners, researchers, and policymakers to inform decision-making and future research efforts in this area.

Keywords: SQL Injection Attack, Systematic Literature Review, Injection Detection Types, Injection Detection Sources.

1. INTRODUCTION

SQL injection is a type of cyber-attack that exploits security vulnerabilities in a website's SQL database. It occurs when an attacker inputs malicious SQL commands into a website's input fields, tricking the website into executing the commands, which can lead to data breaches, website defacements, and other harmful consequences [1]. As SQL injection attacks become more sophisticated, detecting them has become increasingly challenging. In response, researchers have developed various detection techniques to prevent such attacks from occurring [2]. An extensive examination of the various strategies that have been created to recognize and thwart SQL injection attacks is presented in A Comprehensive Systematic Review of SQL Injection Attack Detection Techniques. SQL injection attacks have been a persistent threat to websites and web applications for many years. These attacks can be launched by malicious actors to steal sensitive data, modify data, or even take control of an entire database. As a result, researchers have created a range of various methods to identify and stop SQL injection attacks.

The use of signature-based detection is one popular method for identifying SQL injection threats [3]. This technique involves searching for specific patterns or sequences of SQL commands that are known to be indicative of an attack. For example, a signature-based detection system might look for SQL commands that attempt to add or delete tables or columns from a database or contain certain keywords like "SELECT" or "UNION." While signature-based detection can be effective at detecting known attack patterns, it may not be as effective against new or evolving attack methods. Another approach to SQL injection detection is anomaly-based detection [4]. This technique involves looking for unusual or unexpected behavior within a database that might be indicative of an attack. For example, an anomaly-based detection system might look for a sudden increase in the number of failed logins attempts or the amount of data being requested from a database. While anomaly-based detection can be effective at detecting new or previously unknown attack methods, it can also generate false positives if legitimate user behavior is incorrectly identified as suspicious [5].

Some researchers have proposed hybrid approaches to SQL injection detection that combine elements of both signature-based and anomaly-based detection. These approaches attempt to leverage the strengths of both techniques to achieve higher accuracy and effectiveness.
This review aims to provide a comprehensive overview of the various techniques used for detecting SQL injection attacks, including signature-based, Dynamic Analysis, Heuristic-Based Detection, Machine Learning-Based Detection, and Static analysis. Overall, this systematic review provides a comprehensive analysis of the current state of SQL injection attack detection techniques. By evaluating and comparing the different detection methods, this review can help researchers and practitioners to select the most appropriate detection technique for their specific needs to identify areas for future research and development.

A thorough analysis of methods for detecting SQL Injection Attacks can significantly advance the field of cybersecurity research. including:
1. Comprehensive overview of the state-of-the-art: A systematic review can provide a comprehensive overview of the different techniques that have been developed for detecting SQL injection attacks. This can help practitioners and researchers to better understand the strengths and weaknesses of different approaches and to identify areas for improvement [6].

2. Evaluation of effectiveness: By evaluating the effectiveness of different detection techniques, a systematic review can help practitioners and researchers to select the most appropriate detection technique for their specific needs [7]. This can help to improve the overall effectiveness of SQL injection attack detection systems.
3. Identification of challenges and future research directions: A systematic review can help to identify the major challenges associated with SQL injection attack detection, such as the need for real-time detection and the difficulty of detecting previously unknown attack methods. This can help to guide future research efforts in this area and to identify new areas for innovation [8].
4. Standardization of methodology: By using a standardized methodology, a systematic review can help to ensure that the results are reliable and reproducible. This can help to increase confidence in the results and to promote greater collaboration and knowledge-sharing within the research community [9]. Overall, a Comprehensive Systematic Review of SQL Injection Attack Detection Techniques can provide valuable insights into the current state of research in this area and can help to guide future research and development efforts.

2. LITERATURE REVIEW

A frequent hazard to data-driven web applications is SQL injection attacks, where malicious code is inserted into SQL queries to access sensitive data or modify the database. Many detection and prevention techniques have been proposed to mitigate these attacks. A systematic literature review done by Nasereddin, et al., in 2021 [10] highlights the various techniques that have been improved and proposed to detect and mitigate SQL injection attacks. Another study in 2022 by Alghawazi, et al., provides A thorough analysis of SQL injection attacks and their effects on online applications. Machine learning has also been used to detect SQL injection attacks [11].

In [12] Mehta, et al. 2023 write A recent paper presents a method for comparing the accuracy of various machine learning models in detecting possible SQL threats. Lawal conducted a further investigation in 2016 suggests using machine learning to identify SQL injection attacks [13]. Overall, these studies highlight how crucial it is to recognize and stop SQL injection threats, and highlight the various techniques and approaches that have been proposed to address the issue. A comprehensive systematic review of these techniques would provide valuable insights for researchers and practitioners in the field.

3. RESEARCH QUESTIONS

Research Questions for SQL Injection Attack Detection Techniques:

- RQ1: What are SQL Injection Attack Detection Techniques, and what are techniques for that?
- RQ2: Which types of resources used SQL Injection Attack Detection Techniques?
- RQ3: What kinds of SQL injection detection Attack Techniques?
- RQ4: Which strategy analysis is used in SQL Injection Attack Detection Techniques?

➢ Question 1: These types identify the target and identify it through analysis, configuration, and the tools and techniques used. That's why this problem is always divided into two equal parts to determine and identify the target.
➢ Question 2: These types of questions tell the researcher what type of resource was used, especially when dealing with large databases.
➢ Question 3: These types of questions are used to inform the researchers about SQL injection detection Attack Techniques.
➢ Question 4: This type is used to identify different ways and mechanisms in the analysis of the above research addresses, which helps to extract a reasonable number of strategies to analyze and follow in large proportion.

4. SEARCH STRING

A search string used to conduct a systematic review study of SQL injection attack detection techniques:
("SQL injection" or "SQLi")
– And ("attack detection" or "intrusion detection" or "vulnerability detection" or "anomaly detection")
– And ("detection techniques" or "detection methods" or "detection systems" or "detection mechanisms" or "detection algorithms")
– And ("systematic review" or "meta-analysis" or "literature review" or "review article" or "comprehensive review").

This search string includes keywords related to SQL injection attacks, detection techniques, and systematic review methodologies. By using this search string, researchers can identify relevant academic papers, conference proceedings, and other sources of information that could be included in a systematic review study of SQL injection attack detection techniques.

4.1. Search in Databases

There are many different databases and platforms used by publishers to manage their content and information. However, some of the most widely used publisher databases include:
1) Scopus: An Elsevier-published bibliographic database of scientific literature that includes journals, books, and conference proceedings.
2) ACM digital library: A digital library with hundreds of academic journals, books, and original sources in the humanities, social sciences, and sciences at your fingertips.
3) ProQuest: A provider of digital information and research tools, including databases of academic journals, newspapers, and dissertations.
4) IEEE Xplore: A digital library with articles on science and technology that the Institute of Electrical and Electronics Engineers (IEEE) has published.
5) Springer: This is an international publisher that offers a wide range of opportunities for authors, customers, and partners. Springer is a leading scientific publisher that publishes in various fields.

These databases are just a few examples, and there are many other publisher databases available depending on the specific field or industry as Figure 1.

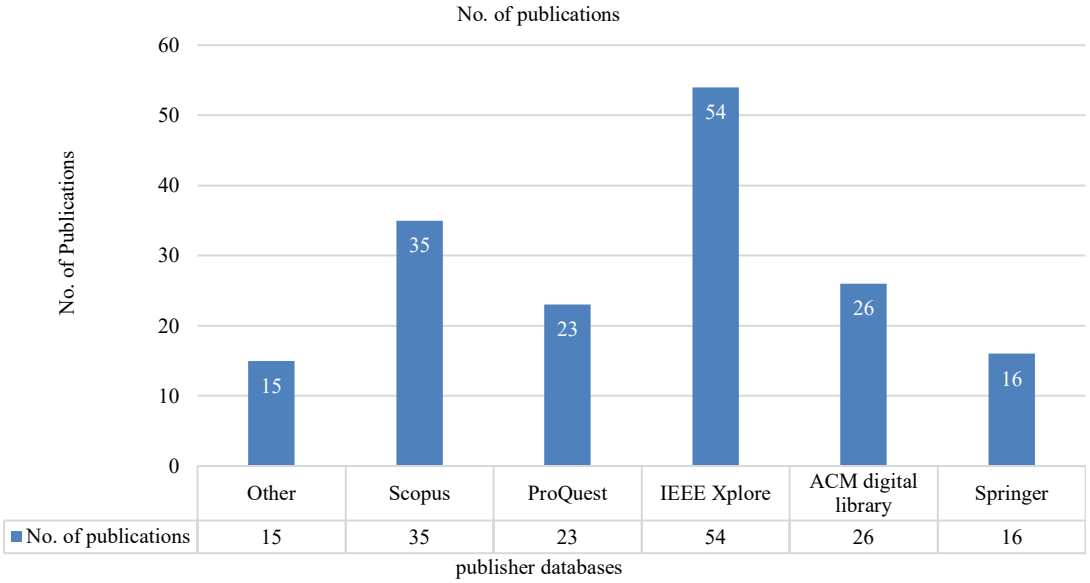

Figure 1. Many publications on the most widely used publisher databases

5. SCREENING OF PAPERS

In a systematic mapping review, the screening process typically involves several stages to identify relevant papers that will be included in the review [14]. The following are the general steps involved in the screening process:

5.1. Develop Inclusion and Exclusion Criteria

The first step is to establish clear and specific criteria for including or excluding papers in the review. This typically involves defining the research questions and objectives of the review and specifying types of studies, populations, interventions, and outcomes of interest.

5.2. Conduct a Preliminary Search

A preliminary search is conducted in relevant databases and other sources to identify potentially relevant papers based on the inclusion and exclusion criteria.

5.3. Screen Titles and Abstracts

The next step is to screen the titles and abstracts of the identified papers to determine their relevance. This is typically done by two or more reviewers independently, using the inclusion and exclusion criteria as a guide.

5.4. Retrieve Full-Text Papers

The full-text versions of the papers that pass the inclusion criteria based on title and abstract screening are obtained. The screening process is critical in ensuring that the systematic mapping review is comprehensive and includes all relevant studies. It also helps to minimize the risk of bias by ensuring that the selection of studies is based on predetermined and transparent criteria [15].

6. USE VARIOUS MODELS TO BUILD DIFFERENT PERSPECTIVES

We can explain any schema or description of any topic by constructing schemas. Define an overall vision for the article on each topic and approach it with some options. In this article, we show how to use these scenarios. as we explain below.

6.1. Distribution of Studies According to Years

This graph shows the distribution of the number of studies per year.

6.2. Venue Chart

The chart offers researchers a different perspective. Distribute papers by year and paper type for conferences and journals.

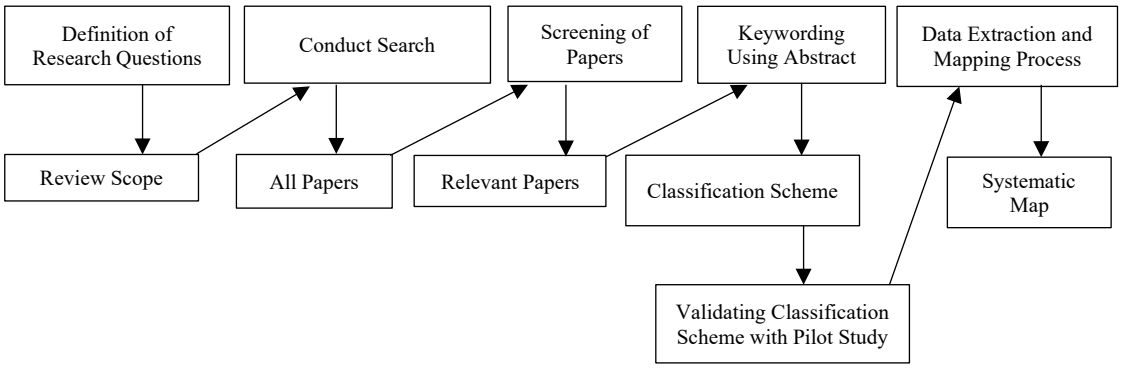

Figure 2. Systematic review process

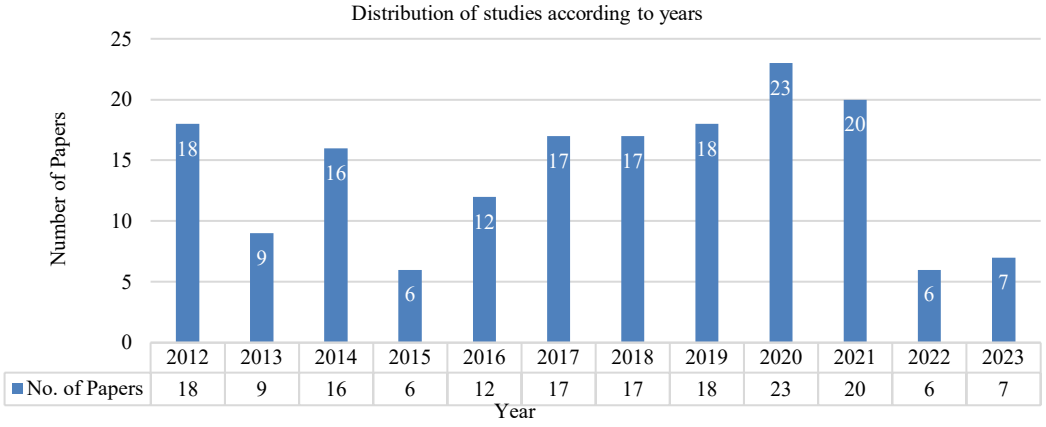

Figure 3. Depicts the distribution of research by year

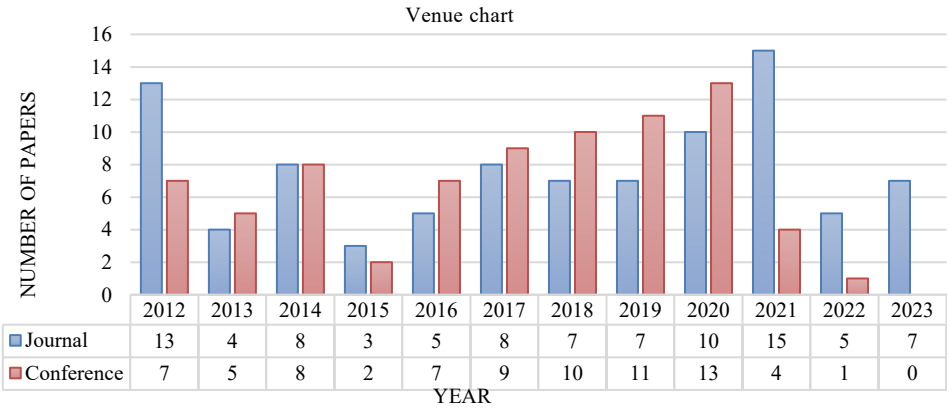

Figure 4. Venue chart

7. CLASSIFICATION SCHEMES

There are two facets to classification data schemes:

7.1. SQL Injection Detection Types

To recognize and stop SQL injection attacks, a variety of SQL injection detection approaches can be used:

1. Static Analysis: To do this, one must examine a web application's source code to find any possible SQL injection vulnerabilities [16]. Static analysis tools can identify coding patterns and practices that are commonly associated with SQL injection vulnerabilities.
2. Dynamic Analysis: To do this, analyze a web application's activity while it is running to find SQL injection attacks. Dynamic analysis tools can monitor web traffic and database queries to identify patterns and behaviors that are indicative of SQL injection attacks [17].
3. Signature-Based Detection: This involves searching for known SQL injection attack patterns in web traffic and database queries. Signature-based detection tools use a library of known SQL injection attack signatures to identify potential attacks [18].
4. Heuristic-Based Detection: This involves using algorithms and statistical models to detect patterns and behaviors that are indicative of SQL injection attacks. Heuristic-based detection tools can identify anomalies in web traffic and database queries that are consistent with SQL injection attacks [19].
5. Machine Learning-Based Detection: This involves identifying and categorizing SQL injection attacks using machine learning methods. Machine learning-based detection tools can be trained on a large dataset of known SQL injection attacks to identify new and previously unseen attacks [19].

Each detection technique has its advantages and disadvantages and is best suited for different situations. A combination of different techniques is often used to provide comprehensive SQL injection detection and prevention capabilities.

7.2. SQL Injection Detection Sources

Various sources can be used to detect SQL injection attacks:

1. Web Application Firewall (WAF): By examining web traffic and removing harmful requests, a WAF can be used to identify and stop SQL injection attacks [20]. A WAF can be implemented as a hardware or software appliance that sits between the web server and the internet, or it can be implemented as a cloud-based service.
2. Database Management System (DBMS) Logs: DBMS logs can be used to detect SQL injection attacks by analyzing database query logs. Anomalies in query patterns or unusual query parameters can be indicative of SQL injection attacks.
3. Network Intrusion Detection Systems (NIDS): A NIDS can be used to detect SQL injection attacks by analyzing

network traffic and filtering out malicious requests [21]. NIDS can be implemented as a hardware or software appliance that sits on the network and monitors network traffic for suspicious activity.

4. Web Server Logs: By examining online traffic logs, web server logs can be utilized to identify SQL injection attacks. Unusual request parameters or request patterns can be indicative of SQL injection attacks.

5. Web Application Scanners: Web application scanners can be used to detect SQL injection vulnerabilities by scanning web applications for known vulnerabilities and potential attack vectors. Scanners can be automated or manual and can be integrated into the software development lifecycle to improve the security of web applications.

Each detection source has its advantages and disadvantages and is best suited for different situations. A combination of different detection sources is often used to provide comprehensive SQL injection detection and prevention capabilities.

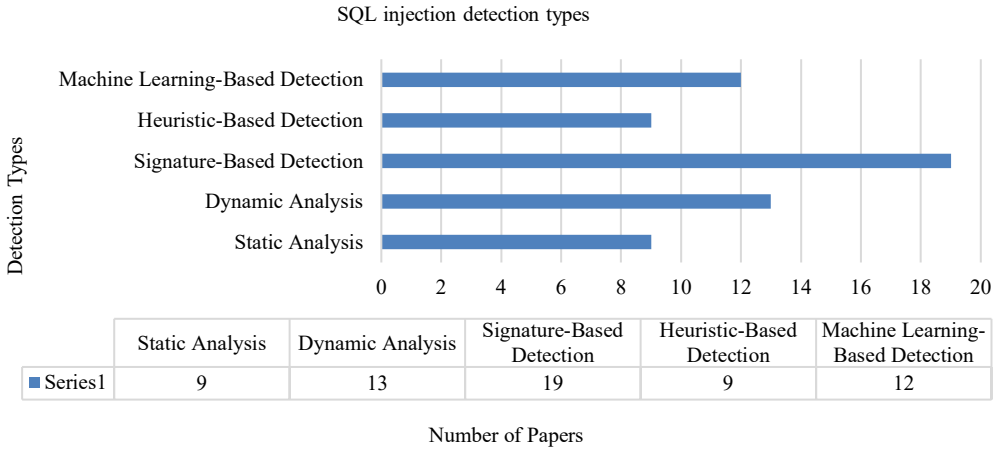

Figure 5. SQL Injection detection types

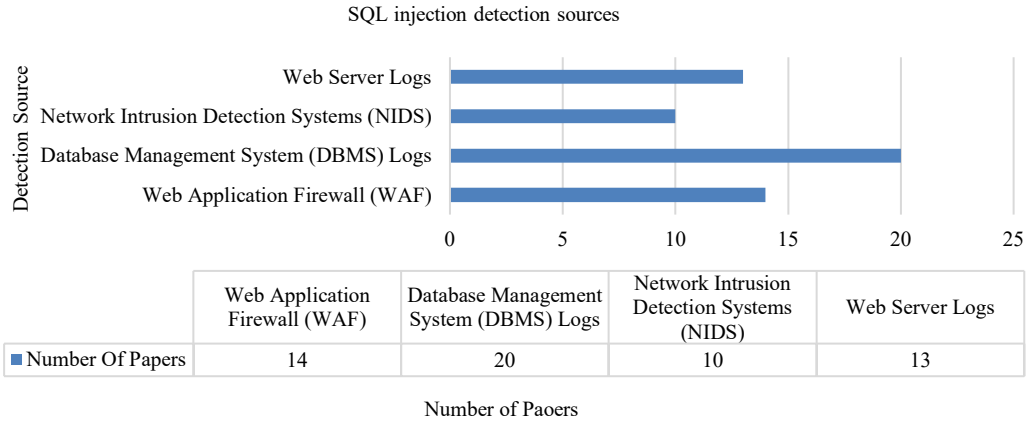

Figure 6. SQL injection detection sources

8. CONCLUSION

One of the most harmful web application threats is SQL injection, usually occurring when an attacker modifies, deletes, reads, and copies data from a database server. All security measures, such as data availability, confidentiality, and integrity, are jeopardized by a successful SQL injection attack. SQL is a language used to represent database management system queries. Although it is not a new area of study, the detection and prevention of SQL injection attacks, where approaches from other domains can be utilized to enhance detection of attacks, is still important. SQL injection attacks have been evaluated and controlled using artificial intelligence and machine learning approaches, with encouraging results.

This white paper's primary contribution is the coverage of research on several models for identifying SQL injection attacks. Through this overview of the system, we aim to inform researchers and help themunderstand the intersection between SQL injection attack techniques and attack sources.

REFERENCES

[1] P. Kumar, "The Multi-Tier Architecture for Developing Secure Website with Detection and Prevention of SQL-Injection Attacks", Int. J. Comput. Appl., Vol. 62, No. 9, 2013.

[2] Q. Li, W. Li, J. Wang, M. Cheng, "A SQL Injection Detection Method Based on Adaptive Deep Forest", IEEE Access, Vol. 7, pp. 145385-145394, 2019.
[3] R. Ezumalai, G. Aghila, "Combinatorial Approach for Preventing SQL Injection Attacks", The IEEE International Advance Computing Conference, pp. 1212-1217, 2009.
[4] M. Kiani, A. Clark, G. Mohay, "Evaluation of Anomaly-Based Character Distribution Models in the Detection of SQL Injection Attacks", The Third International Conference on Availability, Reliability and Security, pp. 47-55, 2008.
[5] S. Kim, C. Hwang, T. Lee, "Anomaly Based Unknown Intrusion Detection in Endpoint Environments", Electronics, Vol. 9, No. 6, p. 1022, 2020.
[6] A. Mardani, D. Kannan, R.E. Hooker, S. Ozkul, M. Alrasheedi, E.B. Tirkolaee, "Evaluation of Green and Sustainable Supply Chain Management Using Structural Equation Modelling: A Systematic Review of the State-of-the-Art Literature and Recommendations for Future Research", J. Clean. Prod., Vol. 249, p. 119383, 2020.
[7] R. Malhotra, "A Systematic Review of Machine Learning Techniques for Software Fault Prediction", Appl. Soft Comput., Vol. 27, pp. 504-518, 2015.
[8] M.T. Muslihi, D. Alghazzawi, "Detecting SQL Injection on Web Application Using Deep Learning Techniques: A Systematic Literature Review", The Third International Conference on Vocational Education and Electrical Engineering (ICVEE), pp. 1-6, 2020.
[9] C. Wanden Berghe, J. Sanz Valero, "Systematic Reviews in Nutrition: Standardized Methodology", Br. J. Nutr., Vol. 107, No. S2, pp. S3-S7, 2012.
[10] M. Nasereddin, A. Al Khamaiseh, M. Qasaimeh, R. Al Qassas, "A Systematic Review of Detection and Prevention Techniques of SQL Injection Attacks", Inf. Secur. J. A Glob. Perspect., pp. 1-14, 2021.
[11] M. Alghawazi, D. Alghazzawi, 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, 2022.
[12] D. Mehta, H. Suhagiya, H. Gandhi, M. Jha, P. Kanani, A. Kore, "SQLIML: A Comprehensive Analysis for SQL Injection Detection Using Multiple Supervised and Unsupervised Learning Schemes", SN Comput. Sci., Vol. 4, No. 3, p. 281, 2023.
[13] M.A. Lawal, A.B.M. Sultan, A.O. Shakiru, "Systematic Literature Review on SQL Injection Attack", Int. J. Soft Comput., Vol. 11, No. 1, pp. 26-35, 2016.
[14] N.R. Haddaway, et al., "On the Use of Computer-Assistance to Facilitate Systematic Mapping", Campbell Syst. Rev., Vol. 16, No. 4, p. e1129, 2020.
[15] K.L. James, N.P. Randall, N.R. Haddaway, "A Methodology for Systematic Mapping in Environmental Sciences", Environ. Evid., Vol. 5, pp. 1-13, 2016.
[16] I. Medeiros, N. Neves, M. Correia, "Detecting and Removing Web Application Vulnerabilities with Static Analysis and Data Mining", IEEE Trans. Reliab., Vol. 65, No. 1, pp. 54-69, 2015.
[17] I. Lee, S. Jeong, S. Yeo, J. Moon, "A Novel Method for SQL Injection Attack Detection Based on Removing SQL Query Attribute Values", Math. Comput. Model., Vol. 55, No. 1-2, pp. 58-68, 2012.
[18] K. Ross, M. Moh, T.S. Moh, J. Yao, "Multi-Source Data Analysis and Evaluation of Machine Learning Techniques for SQL Injection Detection", The ACMSE 2018 Conference, pp. 1-8, 2018.
[19] K. Aryal, M. Gupta, M. Abdelsalam, "A Survey on Adversarial Attacks for Malware Analysis", arXiv Prepr. arXiv2111.08223, 2021.
[20] A.Z. Ablahd, "Detect Malicious Emails Using Dart Language", International Journal on Technical and Physical Problems of Engineering (IJTPE), Issue 54, Vol. 15, No. 1, pp. 116-120, March 2023.
[21] J. Vimalrosy, S. Brittorameshkumar, "OSS-RF: Intrusion Detection Using Optimized Sine Swarm Based Random Forest Classifier on UNSW-NB15 Dataset", International Journal on Technical and Physical Problems of Engineering (IJTPE), Issue 51, Vol. 14, No. 2, pp. 275-283, June 2022.

BIOGRAPHIES

Name: **Basim**
Middle Name: **Hussein**
Surname: **Ali**
Birthday: 25. 03.1978
Birthplace: Diyala, Iraq
Bachelor: Computer Science, Yarmouk University College, Diyala, Iraq, 2001
Master: Student, Computer Science, University of Diyala, Baqubah, Iraq, 2023
Research Interests: Image Processing, Image Captioning, and Machine and Deep Learning Algorithms

Name: **Abdulbasit**
Middle Name: **Kadhim**
Surname: **Alazzawi**
Birthday: 01.07.1974
Birthplace: Baghdad, Iraq
Bachelor: Computer Science Department, Faculty of Computer Science, Baghdad University, Baghdad, Iraq, 1999
Master: Computer vision, Computer science, University of Technology, Baghdad, Iraq, 2005
Doctorate: Electrical and Electronic Engineering, Altinbas University, Istanbul, Turkey, 2018
The Last Scientific Position: Director of Deep Learning for Graduate, Collage of Science, University of Diyala, Baqubah, Iraq, 2018
Research Interests: Deep Learning, Machine Learning, Image Processing
Scientific Publications: 15 Papers, 2 Theses