SQL injection attack: A Systematic Literature Review on Detection, Prevention and Classification with Machine Learning Approach

Conference Paper · July 2018

CITATIONS
0

READS
607

2 authors:

Abdullahi Egigogo Raji
Federal University of Technology Minna
10 PUBLICATIONS **3** CITATIONS
SEE PROFILE

Shafi'i Muhammad Abdulhamid
Federal University of Technology Minna
110 PUBLICATIONS **1,488** CITATIONS
SEE PROFILE

SQL INJECTION ATTACK: A SYSTEMATIC LITERATURE REVIEW ON DETECTION, PREVENTION AND CLASSIFICATION WITH MACHINE LEARNING APPROACH

[1]Morufu Olalere [2]Raji Abdullahi Egigogo, [3]Umar Rukayya, [4]Shafi'i Muhammad Abdulhamid [5]Yisa Victor Legbo, [6]Rasheed Gbenga Jimoh

[1,2,3,4,5]Department of Cyber Security Science, School of Information and Communication Technology, Federal University of Technology, Minna, Nigeria. [5]Department of Computer Science, Faculty of Information and Communication Technology, University of Ilorin, Nigeria.

[1]lerejide@futminna.edu.ng, [2]raji.pg610868@st.futminna.edu.ng, [3]umarrukayya1@gmail.com, [4]shafii.abdulhamid@futminna.edu.ng, [5]yisavictor@futminna.edu.ng, [6]jimoh_resheed@yahoo.com

ABSTRACT

When it comes to web application, confidentiality, availability and integrity of individuals and organizations data are not assured. Open Web Application Security Project (OWASP) has identified SQL injection attacks as common threat to the web application. Consequently, many researchers have proposed different approaches for either detection, prevention or classification/categorization of SQL injection attack. Machine learning approach is one of the approaches existing in the literature, though not very much research outputs with this approach are available in the literature. This implies that, future researchers can still apply machine learning approach in addressing SQL injection attack problem. For this reason, this study presents a systematic literature review on SQL injection attack detection, prevention and classification based on machine learning approach. In order to obtain SQL injection attack related articles, various search engines and scholar databases were visited. The authors review analysis revealed that most of the proposed machine leaning approaches were proposed to only detect whether an application is vulnerable to SQL injection attack or not. Very few were proposed to prevent and classify the injection based on the attack type. It is our hope that this review will provide a theoretical background for future research and enable future researches to identify how and where machine learning approaches have been used to address SQL injection attack.

Index Terms - *Categorization, Detection, Prevention, SQL injection Attack, Machine learning.*

1. INTRODUCTION

Technology has burgeoned to the degree that individuals, groups and organizations keep save of vital and confidential information such as date of birth, password, username, credit card information, email address, mobile phone, student and staff identification number, last and first name, staff identification number and work address number that relates to individuals, groups organizations and partners (customers) on the World Wide Web (WWW). When a particular database is attacked, information in the database can be revealed to illicit users, even modified by the hackers or totally moped out from the database through various web application vulnerabilities such Denial of Service (DoS), Cross Script (CSS) and Structural Query Language Injection Attacks (SQLI) [1].

The SQL Injection Attack (SQLIA) is a type of attack that injects malicious codes into the original query structure of a web application with the motive of modifying, deleting, retrieving/manipulating sensitive data that target databases connected web applications [2]. This vulnerability subsists when there is no proper input validation, standard error reporting and poor website administration [3]. Malicious code can be injected into a web application that is poorly designed in other to get access to the back end database. There are scores of location where users can input data in web applications such as URLs and login form, each leading to SQL injection attack opportunity resulting to loss of integrity, market value and confidentiality of an organization [4]. Various methods have been proposed to detect, prevent and even classify SQLI such as static, dynamic and machine learning based approach [2].

Machine learning is defined as a type of Artificial Intelligence (AI) that gives computers the ability to learn without being explicitly programmed. Machine learning focuses on the development of computer programs that can change when exposed to new data [5]. Addendum, machine learning has become one of the bases of information technology in which knowledge is discovered using different algorithms from a specified form of data over two decades [6]. The intrinsic ability to learn knowledge from data, technique of machine learning is believed to attract better attention in information retrieval, data mining and pattern recognition because data plays indispensable role in machine learning and learning algorithm that are used to learn knowledge and discover properties from the data [7]. There are various types of model in machine learning such as Neural Network (NN), Support Vector Machine (SMV) and Naive Bayes (NB) to mention but a few [8]. This study presents a systematic literature review on Detection, Prevention and Classification of SQL Injection Attacks using machine learning approach. The seven (7) most popular attack types of SQL injection [10] were considered in the review. The Table 1 below illustrates the seven (7) most SQL injection attack types.

Table 1: Seven (7) most SQL injection attack types

Types Number	SQL injection Type
Type 1	Tautology
Type 2	Illegal/logically incorrect queries
Type 3	Union query

Objectives of the Study

The following are the objectives of the study.

i. To identify the SQL injection causes, motives, and consequences.
ii. To identify the various ways of carrying out SQL injection.
iii. To identify SQL injection attack types and patterns/signatures widely used.
iv. To identify the proposed machine learning approaches that has been used for detection, prevention and classification of SQL injection.
v. To examine the effectiveness of the approaches in (iv).

2. RESEARCH METHODS

Research Questions

The following are the research questions formulated to guide his study

I. What are the major SQL injection causes, motives, and consequences?
II. What are the various ways of carrying out SQL injection?
III. What are the SQL injection types and patterns/signatures that are widely used?
IV. What are the proposed machine learning approaches that have been used for detection, prevention and classification of SQL injection?
V. How effective are these approaches in research question IV?

In responding to research question I, a comprehensive review was carried out with a view to identify the root causes, various motives of SQL injection attackers and consequences of SQL injection attack to the web applications security. To answer research question II, the study identified various ways/mechanism in which SQL injection is performed from sundry sources. Regarding the research question III, the study sorted out the widely used attack types and patterns/signatures which gave an insight into the nature of the attack. To address research question IV, various machine learning approaches that have been proposed was sorted with the view to identify approaches that were proposed for detection, prevention or classification of SQL injection attacks. Lastly, research question V was addressed by finding out the effectiveness of the proposed machine learning approaches in detecting, preventing and classifying different SQL injection attack types.

2.1 Procedures Used for the Research

In order to gather SQL injection attack related articles for this study, various search engines and scholar databases such as www.google.com, googlesclolar.com, ieeexplore.ieee.org, www.researchgate.net,academia.edu and www.sci-hub.com were used. The following terms were considered while searching for articles related to SQL injection attack:

i. SQL injection
ii. SQL injection detection and prevention
iii. Machine learning approaches for SQL injection
iv. Types of SQL Injection
v. SQL injection patterns/signatures
vi. SQL injection motives
vii. Effects of SQL injection
viii. SQL injection mechanism

Standard Adopted for Including a Paper

i. Conference and journals related SQL injection attack detection and prevention

ii. Articles that discuss SQL injection attacks
iii. Systematic literature review on SQL injection which was used as a guide
iv. Surveys that are in line with SQL injection
v. Surveys that are related to prevention, classification and prevention of SQL injection
vi. Books that are related to SQL injection

Data Collection

In order to collect research works that are relevant and related to this systematic review, online scholar databases and search engines were explored. Roughly 90 articles were downloaded including conference and journal articles. It is important to note that only 34 research works were useful for the review.

The following information was obtained from the research of all the studies.

i. Title, Author and Year
ii. Proposed approach
iii. Type of SQL injection attack (tautology, Illegal/Logically incorrect queries, union query, piggy-backed queries, stored procedures, inference and alternate encodings) tackled.
iv. Machine leaning area of focus (detection, classification and prevention) and the accuracy of the models

Various researchers such as [14], [16], [25], [26] and [27] have used different approaches in detection, prevention or classification of SQL injection attack. For the purpose of this systematic review, only machine learning approaches were reviewed. Table 2 below shows summary of SQL injection attacks researches based on machine learning approach.

Table 2: Summary of SQL Injection Attacks Researches Based on Machine Learning Approach

References	Research approach	Area of focus
[9]	Proposed a Support Vector Machine (SVM) for classification and prediction of SQL-Injection attack	Classification and prediction
[10]	Pattern recognition neural network model for detection and classification of SQL injection attacks was proposed	Detection and classification
[11]	This model enables detection of unknown attacks with reduced false positives and partial overhead and reduces the chance of implementing SQL-based imitation attacks.	Detection
[12]	SVM classification and Fisher score were proposed to detect SQL injection attacks. According to the query submitted by the users, the approach can classify them into either normal users or attackers	Detection
[14]	Proposes a genetic fuzzy system for detection of SQLI. In this research, accuracy is not the only priority, but also the learning and flexibility of the rules obtained. The algorithm was built on parameters, initial rules, enhancing function and data-dependent	Detection
[15]	A novel approach was introduced to dissect the HTTP traffic and inspect complex SQL injection attacks. A hybrid HIPS and a web application firewall architecture were used.	Dissect and inspection
[16]	Proposed Bayes classification for detection of SQL injection. The paper uses keywords rather than a statement of SQL query. Bayes theorem is applied on the keyword which improves the accuracy and performance of the detection.	Detection

3. RESULT AND DISCUSSION

Research Question I: What are the SQL injection causes, motives, and consequences?

The major root causes of SQL injection attacks as stated by [3] include the following:

i. Poor website administration
ii. Weak Input validation techniques
iii. Nonstandard error reporting.

For every invader to infiltrate any system there must be a motive behind the action, so do SQL injection attackers. The authors in [4], [3], [28], [29] and [35] stated the following as the motive behind SQL injection.

i. **Database finger printing (collected metadata information):** The main aim of attacking database is to collect certain technical information that is important and specific to the database.
ii. **Retrieving sensitive or regular data:** The aim of this, is to extract and have access to back-end database
iii. **Performing data manipulation:** The motive of the invader here is to have access to the database so to append, remove, insert, delete and update values of the data in the database.
iv. **Performing a Denial of Service:** The activities and processes of a web application is interrupted through performing some command in the database leading to denial of service.
v. **Bypassing Authentication:** The invader here bypasses the authentication of web application and gaining access to the database. This gives the invader some privileges and right as a legitimate user in the web application.
vi. **Executing Remote Commands**: This is done by executing illegal commands which give invaders total control of the whole system.
vii. **Performing Privilege Escalation**: These attacks centered on exploiting the database user privileges taking the advantage of implementation mistakes or logical errors in the database.

SQL injection can be very overwhelming if it successful, the damage an invader can cause has no limit. The following are consequences of SQL injection attack as stated by [28] and [29].

i. **Loss of Data**: When illicit user get access to the web application, user privilege can be changed and how to carry out a certain operation in the database can also be altered. If an unintended user gets access to the SQL database of the web application through the weakness, important information stored on this database is gained and modified leading to the loss of data.

ii. **Data Secrecy:** The secrecy of data is lost if the unauthorized user gets access to the information that is vital to individuals, group and organization.
iii. **Data Tempore**
iv. **Loss of Customer Trust and Loyalty:** Customers loyalty and trust is loss when they found out that the vital information their provided is been accessed/miss handled by someone without their permission.

Research Question II: What are the various ways of carrying out SQL injection?

There are various ways in which attackers used SQL injection to compromise the security of web application. [30], [31] highlighted the following as the most common mechanism used.

i. **User Input**: This is one of the media used by invaders to inject SQL command which is sent when forms are submitted to the web application.
ii. **Cookies:** This stores the state of information of a web page, when the content of the stored information is used to construct SQL queries, the invader can easily embed the attack in the cookies.
iii. **Server Variables**: These are variables that contain environmental, HTTP and network headers variables that are used in many ways web applications such as identifying browsing trends and logging usage statistics among others. The vulnerabilities are created when these variables are logged to a database without sanitization which paves a way to invaders to forge SQL commands into the headers.
iv. **Second Order Injection:** In the second-order injections, attackers send malicious inputs into a system or database to indirectly trigger SQLIA when that input is used at a later time

Research Question III: What are the SQL injection attack types and patterns/signatures that are widely used?

There are seven (7) most common SQL injection attack type each associated with its own attack patterns/signatures. Below are the SQL injection attack types with their attack signatures/patterns respectively by [10] [18], [28], [32] and [34].

i. **Tautology**: In this attack type, codes are injected into one or more conditional statement so that they always assess to true. Attackers made use of this technique to extract data and bypass authentication pages. The following are the patterns/signatures associated with this attack “‘”, “OR”, ”LIKE” and ”SELECT ”.
ii. **Stored Procedures**: As the name implies, they are set of operations that are stored which are mainly written in SQL and are stored in server side. These procedures can be modified by the client leading to denial of service and privilege escalation because they are available to the client and automatically obtain the new version. The following are the patterns/signatures associated

with this attack; “SHUTDOWN”, ”EXEC”, “XP_CMSHELL()”

iii. **Alternate Encodings**: Alternate encodings are employed to use vulnerabilities that might not otherwise be usable, evade prevention and detection schemes. The attack string unicode character, ASCII and hexadecimal are been concealed using alternate encodings. “EXEC ()”, “CHAR ()”, “ASCII ()”, “BIN ()”, “HEX ()”, “UNHEX ()”, “BASE64 () », « DEC () », and « ROT13 () among others » are the attack signatures/patterns

iv. **Union Query**: this is the type of attack in which invaders strive to extract data from a back-end database and bypass authentication by combining two separate SQL SELECT queries, which have nothing in common, using UNION SELECT statement. The attack pattern/signatures are “UNION” and “UNION SELECT”

v. **Illegal/Logically Incorrect Queries**: This is an attack in which invaders try obtaining information about the backend database from the malicious login page. Through this attack, data are extracted from the database, injectable parameters are discovered and database fingering is performed. Logical errors, syntax errors and type errors are the most common queries that are generated by the hackers. Below are the patterns/signatures peculiar to this type of attack; "ORDERBY", "CONVERT","INT", "CHAR", "VARCHAR","NVACHAR", and "AND" among others

vi. **Inference**: This type of attack is a time-based attack in which invaders employ time delay in order to make difference between true and false responses from a backend database. The following are the attack pattern/signatures; “IF”, “ELSE” and ”WAITFOR”

vii. Piggy-backed queries: In this type of attack, unauthorized user exploits database with the help of query delimiter, such as ";", by appending an extra query with the original SQL query. Below are the patterns/signatures peculiar to this type of attack;.

Table 3: Total number of Attack types Detected, prevented and classified by the approaches

Ref	Attack types	TADPC
[10], [11], [12], [13], [17], [18], [22]	Type1	7
[10], [11], [12], [13], [18], [21],[22]	Type 2	7
[10], [11], [12], [13],[17], [18], [22], [22]	Type 3	8

References = ref, Total Approaches Detected, Prevented and Classified (TADPC)

The table above shows the references, attack types and total number of machine learning approaches that detect SQL injection attack only. The Figure 3 below shows the approaches that detect SQL injection which indicated the number type of SQL injection attack. As shown in the Figure 1 type 3 is more detected by the approaches with the total number of 8. Type 5, 6, 7 has the same number of approaches that detected them which is 5.

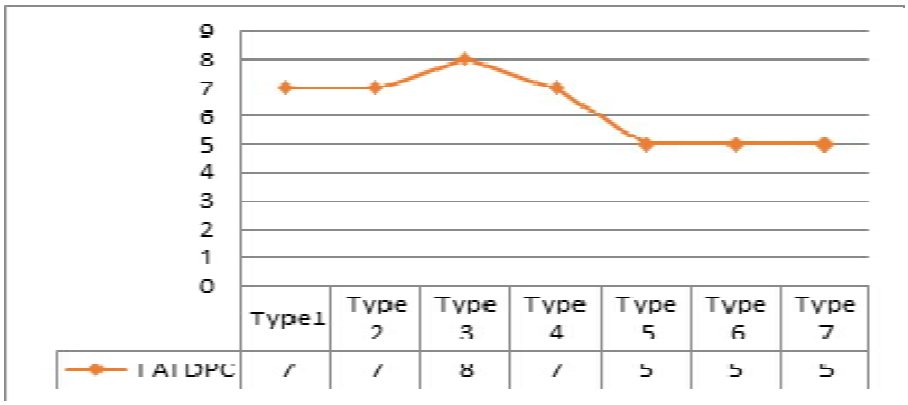

Figure 1: Total number of SQL Injection Attack Type Detected, Prevented and Classified

Research Question IV: What are the proposed machine learning approaches that have been used for detection, prevention and classification of SQL injection attack?

The table 4 below gives the proposed machine learning approaches that are used in detection, prevention and classification of SQL injection stating the Title, Author and Year (TA &Y), Proposed Approach Used (PPU), Types of SQLIA tackled (TSQLIAT), and Accuracy of the Approach (AoP)

Table 4: Proposed Machine Learning Approach used, Types of SQLIA tackled and Accuracy of the Approach

T, A &Y	PPU	TSQLIAT	AoP (%)
[9]	SVM	SQLI	96
[10]	NN	Type 1-7	96
[11]	NN	Type 1-7	NS
[12]	QT,FS & SVM	Type 1-7	94
[13]	NN	Type 1-7	NS
[14]	GFCS	SQLI	98
[15]	HIPPS	SQLI	NS
[16]	BC	SQLI	NS

Machine learning approaches that are used in either detection, prevention, classification or both are presented in the table 4 above each stated the type of type of attack tackled and their accuracy. The Figure 2 below showed the accuracy of the approaches

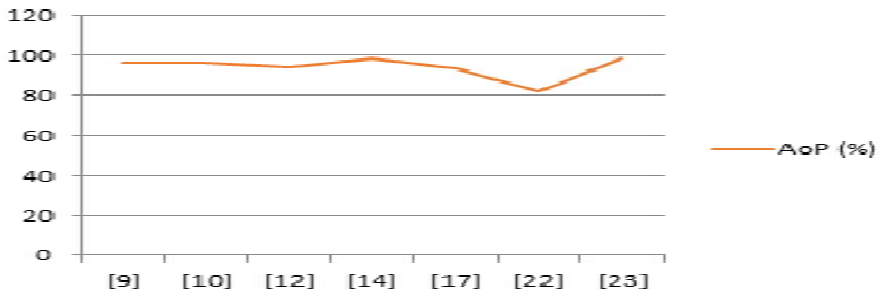

Table 5: Summary of the total number approaches used in detection, prevention classification and combined based on the machine learning

TNSVM	TNNN	TNDT	TNCA	TNGFCS
3	3	1	8	1

The above Table 5 shows the total number of Support Vector machine (TNSVM), Total Number of Neural Network (TNNN), Total Number of Decision Tree (TNDT), Total Number of Combined Approaches (TNCA) and Total number of Genetic Fuzzy System (TNGFCS). The Figure 3 below showed the machine learning approach that is used in detection, prevention, classification or combination of approach in the dealing with issues in the area of SQL injection attack.

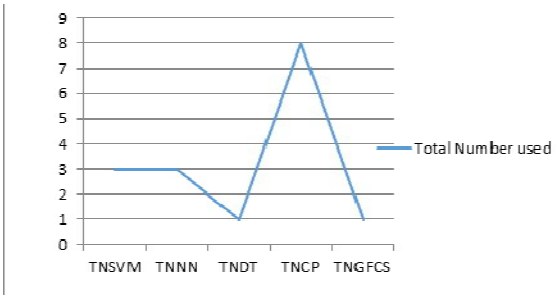

Figure 3: Approaches used in Detection, Prevention and Classification

Table 6 Area of focus and total number of approaches

Area of focus of the Approaches	**Total number of Approaches**
Detection	9
Prevention	2
Classification	0
Detection & Prevention	1
Detection &	1

Table 6 above showed the area of focus and total number of the approaches.
The Figure 4 below showed the area of focus and the total number of approaches that deals on them.

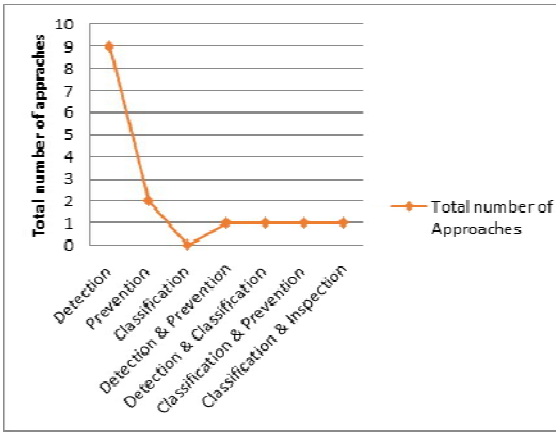

Figure 4: Area of Focus by the Approaches

Research Question V: How Effective are these Approaches in Research Question IV?

The effectiveness of these approaches was evaluated by checking how many attack type a specific approach is able to detect, prevent and classify. How often a particular approach has been used. In Table 3, [10], [11], [12], [13] considered the seven (attack) types, [17], [18], [21] and [22] considered few attack type and the remaining approaches [9], [14], [15], [16], [20], [23] and [24] did not state the particular attack type considered. Type 1, type 2 and type 4 have the same total number of approaches that detect, prevent and classified SQL injection attack. Type 5, 6 and 7 also have the

same total number of approaches, eight (8) approaches were able to detect, prevent and classified attack type 3 making it to be the highest attack type considered by the approaches. As indicated in Table 6 Out of 15 papers reviewed, nine (9) focuses on detection only, two (2) on prevention only, one (1) on detection and prevention one (1) on detection and classification, one (1) on prevention and classification, one (1) on classification and inspection and no approach focused on classification only. In table 5 above, the detection, prevention and classification of SQL injection attack, machine learning approaches are mostly combined. The combined learning approaches has the highest number of eight (8), SVM and NN three (3) and DT one (1). As shown in the 4, the support vector machine is the most commonly used machine learning approach in the detection, prevention and classification of SQL injection attack, though the model is been combined with other techniques such as query tree and Fisher score with the accuracy ranging from 94 to 98%.

4. CONCLUSION

This study presents a broad view of SQL injection attacks by providing theoretical foundations including causes, motives, consequences and way of carrying out SQL injection attack. The study conducts an exhaustive systematic literature review to identify SQL injection attack related publications that are based on machine learning approach. The identified publications were analyzed to determine whether a proposed machine learning approach detects, prevents or classifies SQL injection attack types. The result of the analysis revealed that most of the machine learning approaches is for detection of SQL injection attack. While very few are for either prevention or classification of SQL injection attack types. The authors believe this state-of-the-art systematic literature review on machine learning based approach on detection, prevention and classification of SQL injection attacks contributes to knowledge by providing future researchers with theoretical foundations and open issues in machine learning based approach for detection, prevention and classification of SQL injection attack.

REFERENCES

[1] Kumar, P. & Pateriya, R. k. (2012). A survey on SQL injection attacks, detection and prevention techniques. Proceedings of the 3rd International conference of computing communication and networking technomlogy. July, 26- 28.

[2] Sayyed, M., Sadegh, S. & Bahare. T. P. (2014). Study of SQL Injection Attacks and Countermeasures *International Journal of Computer and Communication Engineering*. 2(5). 2013. Retrieved from http://www.ijcce.org/papers/244-E091.pdf and accessed on 20th march 2017

[3] Jignesh, D. & Bhushan, T. (2017). Assessment of SQL Injection Solution Approaches. *International Journal of Advanced Research in Computer Science and Software Engineering*. . Retrieved from www.ijarcsse.com and accessed on 20th April 2017

[4] Lawal, M. A., Abubakar, M. D. & Ayanloye, O. S. (2016). Systematic literature review on SQL injection. *International Journal of Software Computing*,11(1), 26 32. 2016 Retrieved from http://docsdrive.com/pdfs/medwelljournals/ijscomp/26-35.pdf and accessed on 20th Aprill, 2017

[5] Sumit., D., et al (2015). Applications of Artificial Intelligence in Machine Learning: Review and Prospect. *International Journal of Computer Applications (0975 – 8887) 115 (9).* Retrieved from http://research.ijcaonline.org/volume115/number9/pxc3902402.pdf and accessed on 20th Aprill, 2017

[6] Alex, S., & Vishwanathan, S.V.N. (2008). Introduction to machine learning. University of Cambridge: Press Syndicate published by the press syndicate. Retrieved http://alex.smola.org/drafts/thebook.pdf and accessed on 10th January 2017

[7] Wei-Lun Machine Learning Tutorial 2011. Retrieved from http://disp.ee.ntu.edu.tw/~pujols/Machine%20Learning%20Tutorial.pdf and accessed on 25th January 2017

[8] Ian, H. W., & Eibe F.(2005) .Data mining: A Practical Machine learning tools and techniques. 2nd edition Morgan kaufmanna Publishers.

[9] Romil R., & Shailendra, K. S. (2012) SQL injection attack Detection using SVM. *International Journal of Computer Applications*, 42(13). 2012. Retrieved from http://research.ijcaonline.org/volume42/number13/pxc3877043.pdf and accessed on 15th March 2017

[10] Naghmeh, M. (2015). A Pattern Recognition Neural Network Model for Detection and Classification of SQL Injection Attacks. Retrieved from https://www.researchgate.net/publication/271072307 and accessed on 20th May 2017

[11] Fredrik, V. Darren, M. & Giovanni, V. (2005). A Learning-Based Approach to the Detection of SQL Attacks 2005. Retrived from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.94.9201&rep=rep1&type=pdf and accessed on 20th November, 2017.

[12] Aniruddh, L., & Phalke, D. A. (2016). SQL Injection Attack and User Behavior Detection by Using Query Tree, Fisher Score and SVM Classification. *International research journal of engineering and technology (IRJET*) 3 (6).

[13] Naghmeh, M. S. (2014). Employing Neural Networks for the Detection of SQL Injection Attack. Retrieved from https://www.researchgate.net/publication/264799665 and accessed on 4th April 2017

[14] Christine, B., Ahmed. E., & Saad D. (2016). Detection of SQL Injection Using a Genetic Fuzzy Classifier System. *International Journal of Advanced Computer Science and Applications (IJACSA),* 7(6). Retrieved from https://thesai.org and accessed on 25th January 2017

[15] Abdelhamid, M., Youcef, B. & Ahmed, S. (2014). Improving Web Application Firewalls to detect advanced SQL injection attacks. Information Assurance and Security (IAS). 10th International Conference. Retrieved from http://ieeexplore.ieee.org/document/7064617/ and accessed on 20th April 2017

[16] Amit, B and Tushar, V. (2016) SQL Injection detection using Baye's Classification. 3rd International Conference on Resent Innovation of Science Engineering and Management.

[17] Anamika J. & Geetha, V. (2014). SQL Injection Detection using Machine Learning. International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT). IEEE. Retrieved from http://ieeexplore.ieee.org/document/6993127/ accessed on 10th march 2017\

[18] Garima, S., Dev, K., Unique, G. & Akhilesh P. S. (2015). SQL Injection Detection and Correction Using Machine Learning Techniques. Emerging ICT for Bridging the Future - Proceedings of the 49th Annual Convention of the Computer Society of India (CSI) 1(1) pp 435 442.. Retrieved from https://link.springer.com/chapter/10.1007/978-3-319-13728-5_49 and accessed on 15th March 2017.

[19] Yi Wang & Zhoujun. L. (2012). SQL Injection Detection with Composite Kernel in Support Vector Machine International Journal of Security and Its Applications 6(2).

[20] Ritu, A., & Dharmendra, M. (2016). An Approach Based on SVM Classifier to Detect SQL Injection Attack *IJSRSET*,2(3) 2395-1990.

[21] Krit, K. & Chitsutha J. (2016). Machine Learning for SQL Injection Prevention on Server-Side Scripting Soomlek. Retrieved from http://ieeexplore.ieee.org/document/7859950/?denied and accessed on 15th March 2017.

[22] Hanmanthu, B., Raghu, B. R., ,. & Niranjan,. P. (2015). SQL Injection Attack Prevention Based on Decision Tree Classification IEEE Sponsored 9th International Conference on Intelligent Systems and Control (ISCO) 2015.

[23] Solomon, O. U. & J. William, B. (2017). Applied Machine Learning Predictive Analytics to SQL Injection Attack Detection and Prevention. IEEE. 2017. Retrieved from http://www.napier.ac.uk/~/media/worktribe/output-687590/applied-machine-learning-predictive-analytics.pdf and accessed on 26th April 2017.

[24] Cristian, et al. CBRid4SQL: A CBR Intrusion Detector for SQL Injection Attacks 2010. Retrieved from https://www.researchgate.net/publication/221053341_CBRid4SQL_A_CBR_Intrusion_Detector_for_SQL_Injection_Attacksand accessed on 25th January 2017

[25] Kanika, E. & Prabhjot, E. k. (2015). A dynamic approach to detect & prevent sql injection attack to overcome website vulnerability International Journal of Innovative Research In Science, Engineering And Technology 4 (12).

[26] Alexander, A. (2010). A Distributed System for Pattern Recognition and Machine Learning 2010. Retrieved from http://madm.dfki.de/_media/theses/alex-dispare-thesis.pdf and accessed on 7th April 2017

[27] Lambert N., & Lin, K. S. (2010). Use of Query Tokenization to detect and prevent SQL Injection Attacks, in Proc. 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), pp. 438-440.

[28] Atefeh. T., Suhaimi, I. & Maslin, M. (2011). SQL Injection Detection and Prevention Techniques. International Journal of Advancements in Computing Technology 3(7). 2011. Retrieved from https://pdfs.semanticscholar.org/0ff9/2dd1d6e0878347be94dae6c06365247aa46b.pdf accessed on 20th march 2017

[29] Rubidha, D.D., Venkatesan, R. & Raghuraman. K. (2016). A Study on Sql Injection Techniques. *International Journal of Pharmacy & Technology*. Retrieved from https://www.researchgate.net/publication/271072307 and accessed on 20th May 2017

[30] Avinash, K.S.(2011). Detection and Prevention of SQL Injection Attack in Web Application. 2011. Retrieved from http://dpSQLklk.og? and accessed on 25th January 2017

[31] W3resource. SQL injection September 2017. Retrieved from https://www.w3resource.com/sql/sql-injection/sql-injection.php and accessed on 23rd Desember, 2017.

[32] Joseph, R., Manoj A.C., & Anto, M. D. (2014). An Approach to Detect and Prevent Tautology Type SQL Injection in Web Service Based on XSchema

validation. International Journal Of Engineering And Computer Science 3(1), pg 3695-3699. 2014.

[33] Kuldeep, R. (2011). Classification of SQL Injection Attacks and using Encryption as a Countermeasure. International Journal of Advanced Research in Computer Science. 2 (1), Jan. –Feb,628-630

[34] San-Tsai, S., Ting, H. W., Stephen, L. & Sheung L. (2007). Classification of SQL Injection Attacks and using Encryption as a Countermeasure.2007. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.620.9731&rep=rep1&type=pdf and accessed on 30th October 017.