March - April 2020
ISSN: 0193-4120 Page No. 9301 - 9313

Detecting the Abnormal SQL Query using Hybrid SVM Classification Technique in Web Application

R. Shobana[1], Dr. M. Suriakala[2]
[1]Part time Research Scholar, University of Madras,
Assistant Professor, Department of Computer Science and Applications,
D.K.M. College for Women, Vellore- 1
[2]Assistant Professor, Department of Computer science, Government Arts College for Men, Nandanam, Chennai-35
shobanavasu.mca@gmail.com[1], suryasubash@gmail.com[2]

Article Info
Volume 83
Page Number: 9301 - 9313
Publication Issue:
March - April 2020

Article History
Article Received*: 24 July 2019*
Revised*: 12 September 2019*
Accepted*: 15 February 2020*
Publication*: 09 April 2020*

Abstract

SQL Injection Attacks (SQLIAs) are playing a significant role in database driven sites due to its automatic nature. Previously, many works had been carried out to reduce this SQLIAs at the application side but, they result in failure in many ways. Many techniques were tended to minimize the usage of less number of support vectors. In this paper, the proposed methodology will be fully concentrate on minimizing the dataset points and that leads to improvement of SVM classification. The main idea is to calculate the approximate rate of decision boundary rate of decision boundary of SVM by the assistance of binary trees. The finally obtained tree is considered as the hybrid tree that will helps to sense both of theuni-variant and multi-variant nodes. The hybrid tree takes SVM's assistance just in ordering significant information focuses lying close choice limit, staying less urgent datapoints are grouped by quick uni-variant nodes.

Keywords; *Support Vector machine, Classification, Binary tree, SQL query*

I. INTRODUCTION

The evolution of big data leads to massive development in Relational Database Management Systems (RDBMS) because of its enlarged storage nature. Various companies and institutions are using these databases due to its security[1]. If the data misusage or data loss happens, it will not only affect the organizations but also the customers. To reduce the data loss issues many companies opted RDBMS due to its efficiency in storage and security from malicious attacks [2].If a security framework should be effective, it has to protect the database from all intrusions technically it is named as Intrusion Detection Systems (IDS). These IDS initially find the availability of intrusions and tries to neglect it by generating any data-integrity report towards the users. Still now there are more research are going on under IDS. Basically IDS is divided into network based & host-based which can find the malicious activity at all types of databases[3]. Malicious attacks explicitly coordinated to the database are probably going to be undetectable at the system and working systems level and along these lines, imperceptible to the finders on that level. Along these lines, organize based and host-based IDS's are rendered futile notwithstanding database-explicit attacks. In accordance with this, irregularity based IDS utilizing information mining methodologies are increasing increasingly more consideration in the field of database abnormality detection in light of their high intrusion detection exactness, effectiveness, and mechanization highlights [4].Many research works had done in the area of SQL queries to extract the abnormalities of the detected anomalies, But they are not considered due to the limitation of SQL syntax. When the usage of internet is more, the attacks also increases rapidly that will further makes huge risk among the users[5].

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 9301 - 9313

This attacks can be done by various injection ways, enhancing the query, Data rehabilitation and hence it leads to drastic report among the unauthorized users[6]. The researchers had undergone survey and found that around 92% of real time applications are running in web affected by some types of attacks[7]

Support Vector Machines are the best classification method for supervised machine learning that will solve the regression problems. SVMs are motivated by statistical Learning Theory(SLT)&Bayesian Arguments (BA). The basic terminology of SVM is as follows. Initially it will discover the optimal point by splitting the +ve and –ve cases of hyperplane. The definition of optimal hyperplane is obtained by the related hyperplane. The applications of SVM re handwritten classification, face identification, iris recognition, particle splitting etc..,[8]. Among other classification techniques the support vector machine is best due to its low computational cost and reducing training set during multivariate data points. The complexity is very less in SVM [9]. If the amount of data point are large that will make drastic change upon the classification process at both the testing and training phase.

In the database there are 2 important types of intrusion attack. First one is the malicious users directly try to access the database by hacking the username & password by any structures Query Language (SQL). Second one is by indirectly accessing the database by picking up the SQL syntax. This second case is totally depend upon the input rated values and hence it is named as “SQL injection attack” (SQILA). While deeply analyzing both types the first type of malicious attack is due to the divergent behavior of the user whereas the second type is due to the upcoming queries at any application. mHealth applications are thusly characterized as programming programs that give wellbeing related administrations through cell phones and tablets. mHealth is a developing field which can possibly make medicinal services experts progressively effective, increment tolerant fulfillment and decrease the social insurance cost. The general idea of mHealth incorporates therapeutic applications. There are a few sorts of medicinal applications, some are utilizing outside gadgets, for example, therapeutic sensors, and some applications are utilizing cell phone assets, for example, the camera for the handling of the patient. Now a days the healthcare apps are emerging due to its better relationship between the patient and doctor through their headset. Doctors give the proper medications and suggestions to them for their better improvement in health. The knowledge of these apps are improving day by day and that makes more relational content by giving the solution for various questions. They are termed as the functional demand. There are unfunctonal demand also included and that is over to all ages of people. But the thing is these apps also undergoing many insecurity issues with various risk among user level. Sometimes, the issues cannot be solve by the user itsels due to its complicaitons. While programming this apps the user built it with sensing circuits, medical equipment & evaluation metrics. It has to be noted that all these equipment will undergo with some security issues and create the attacks. To reduce this security issues the equipment has to be built with more security aspect in the application case of operating system with some inter or intra process communication and android permission scape.

Some of the categories of SQL injection are discussed here:

String SQL Injection –It is also known as AND/OR attack. Initially, the SQL tokens are taken as input and tries to evaluate the obtain expression is true or false. The key point of the expression is if the statement is true for one row it will automatically create the strings for all other rows and hence everything in the database will be affected.

Numeric SQL Injection – This is same as that of string SQL injection. But here, the numbers are

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 9301 - 9313

playing an important role. So the input query will be number for checking the expression

Remarks Attack - This sort of attack exploits the SQL to inline remarking permitted - the malicious code as well as remarks anything comes after the "- - " in the WHERE statement. The fact is that everything after the remark characters will be overlooked. Remarks Attack can be joined with either String or Numeric SQL Injection so it executes as a repetition which consistently assesses to a genuine statement

Blind SQL Injection - In this kind of attack, valuable data for abusing the backend database is gathered by deriving from the answers of the page subsequent to scrutinizing the server some obvious/false questions. It is fundamentally the same as a typical SQL Injection Still, as attacker endeavors to misuse an application, as opposed to getting a helpful mistake message; they get a conventional page determined by the designer. This makes abusing a potential SQL Injection attack increasingly troublesome yet not feasible. An attacker can in any case gain admittance to delicate information by soliciting an arrangement from True and False inquiries through SQL statements.

Timing Attacks - An attacker gathers data by watching the reaction time (conduct) of the database. Here the primary concern is to watch the reaction time that will assist the attacker with deciding astutely on the fitting injection approach.

Normally, the SQL attacks are denoted by the special case of language in various applications that will further form the queries in meaningful manner. Sometimes it will be even harmful for many applications due to abnormal query and that is named as injection attack. This can be explain between users and attack case whereas the users can develop the query either validate or invalidated which can further elevate the coding based machine learning process. For an attack to be happen in the network the affected website had to be check with proper SQL statement. Further, the user has to supply the payload activities at the server with application level.

Inside the database there are list of injections are available as follows,

- Tautology-based SQL Injection
- Piggy-backed Queries/Statement Injection
- Union Query
- Illegal/Logically Incorrect Queries
- Inference
- Stored Procedure Injection

Under the tautology attacks “OR” operator is used with condition based and checks for “true” or “false” statement for each authentication. While the process is going on “WHERE” clause is used at each query which helps to transform the original statement at all rows and columns. Finally, ’OR’ clause came to arise and produce the operands which makes the condition so difficult.

The problem in classification of query can be two way method by separating the unique classes and its functions. The final goal of this classification is to achieve the generalized task. There are many possible ways are available to split the information with application of margin ended by extending the distance to the maximized data point of each attribute. This is named as hyper plane division based classification intruded with boundaries.

II. LITERATURE SURVEY

Sherykhkanloo et al., [12] proposed a novel approach based on combination Artificial Intelligence (AI) & Neural Network system (NNs for finding the type of SQL injection in database. This is basically done by using 3 elements namely, URL generator, classifier and neural network model. Among these elements the classifiers & generator enhance the detection of malicious activities by the steps such as testing, validating & training under neural network.

Wang ET. al., [13] suggested a susceptibility detection method using PHP based application SQL

Published by: The Mattingley Publishing Co., Inc.

by injection analysis techniques. This performance ius done with elaborated analysis of singly injection with the case of flowchart and programmable based on structure with stable and unstable conditions. This suggestion method is further compared with lexical feature comparison.

Bujaet. al., in [14] proposed a method for to elaborate the susceptibility of attacks in web. This proposed method mainly follows the detection module by evaluating the statement using Boyer Moore string matching method. Here, the matching process is done by 4 panels namely, crawler panel, parameter panel, exploration panes and solution giving panel.

Bockerman et al.,[15] dealed with kernel based tree classification method to explore the reality of SQL syntax. They ended with the advantage with exhibiting the machine learning thechniques.

Osunaet al., [16] suggested some methods to minimize the usage of support vector machine during learning process. This minimization can be achieved by using regression method and discriminant approach with optimization concept.

Downs et al.., [17] executed a methodology to neglect the support vector by replacing the linearization and decision concept.

Elshazly et al.,[18] analyzed by using HTML scripts in real-time application by evolving the PHP and ASP components

Bertino et al. [19] enchanted many applications with dataset by extending the reputed queries by evaluation the recursive rules along with derivations of association rules.

Kemalis et al.,[20] extended Structural Query Language Intrusion detection system (SQL-IDS) on abnormal queries which then aggregated with execution and evaluation time. This method is further applicable to build the profiled description of many types of attacks.

Liu et al. [21] constructed probability model named as SQLProb which unstably purifies the input with paired manner and then compare with its tree structure for high efficiency and accuracy.

Zhang et al. [22] evaluated transcriptional structure query language method by perpetuating the duplication of database with Lightweight Dictionary Access Protocol (LDAP) form. Hence the input queries are confronted into LDAP system and then evaluate with starts SQL statement. This method is not suitable for all injection attacks due to its duplication manner and hence ended up with failure.

Low et al. [23] suggested a method by using fingerprint. Initially, the fingerprints are extracted from authorized user and it has to be match during the further proceedings. This method is normal to user and makes many useful possibilities in various applications.

Wei et al. [24] enchanted a novel method for protecting SQLIA at storing area. This novel method made perfect analysis at static level and validate the real-time coding error.

Kim and Lee [25] recommended a data mining techniques with tree based structure. This tree has to be apply on internal query and make to protect the server with the perseverance of accessing techniques.

Boyd et al.,[26] presented SQLR model with key based code structure. This method is applicable to the proxy server and then randomly generate the key. This method is perfect for various database till the key is revealed to the attackers.

Vigna et al. [27] recommended the combination of HTTP proxy server & intrusion detector at application level to minimize the complexity issues.

Le et al. [28] planned Double Guard dependent on a comparative methodology comprising of an IDS at the web server as well as an additional at the back-end database

Published by: The Mattingley Publishing Co., Inc.

Pinzón et al. [29] proposed idMAS-SQL, a progressive multi-specialist framework checking at different layers. These methodologies yield better exactness at the expense of higher handling overhead, and are hard to send, train and keep up.

Inyong Lee et. al.[30] exhibited that SQL injection or SQL insertion attack is a code injection procedure that endeavors a security vulnerability happening in the database layer of an application and an administration. This is frequently found inside website pages with dynamic substance. This paper proposes a basic and powerful detection strategy for SQL injection attacks. The technique expels the estimation of a SQL query quality of site pages when parameters are submitted and after that contrasts it and a foreordained one. This technique uses joined static and dynamic investigation. The examinations demonstrate that the proposed technique is exceptionally compelling and straightforward than some other strategies. [30]

A method named as AMNESIA (Analysis and Monitoring of NEutrilization SQL Injection Attacks) [31] is used for detecting the query and protect it by continuously giving notification on it. This method is best for protecting illegal queries.

In SQLrand [32] rather than ordinary SQL watchwords engineers make queries utilizing randomized directions. In this methodology an intermediary channel captures queries to the database and de-randomizes the catchphrases. By utilizing the randomized guidance set, attacker's infused code couldn't have been developed. As it utilizes a mystery key to adjust directions, security of the methodology is reliant on attacker capacity to hold onto the key. It requires the mix of an intermediary for the database in the framework as equivalent to engineer preparing.

Ivan Ristic et al., [33] used signature attack detection by enhancing the complemented parameters. This will be exhibiting related to postal process in the website. The limitation of this process is more complex.

Problem identification:

- During the perusal of string method it may result in structuration SQL model which makes the entire database to be unprogressive in nature.
- At the time of having legal queries to produce its duplication with the conditional phase model it would result in violation.

In this paper, an individual idea is made using SVM-BT (Support Vector Machine-Binary Tree) with the target of classification to be incorporated on normal and abnormal query. This is planned to be done by using the learning concept at the mid-level.

III. PROPOSED METHODOLOGY

The proposed method is a hybrid approach to embedding SVM in binary Tree (SVM-BT) for pre-pruning the tree while carrying out the classification. This resulting hybrid system is categorized as embedded hybrid system where the technologies participating are integrated in such a manner that they appear to be inter-twined. The proposed model is based on the traditional recursive partitioning schemes, except that the leaf nodes created are categorizers for Support Vector Machine instead of nodes predicting a single class. Root node of the decision tree is selected based on a chosen threshold value of the continuous attribute. For this the standard entropy minimization technique is used.

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 9301 - 9313

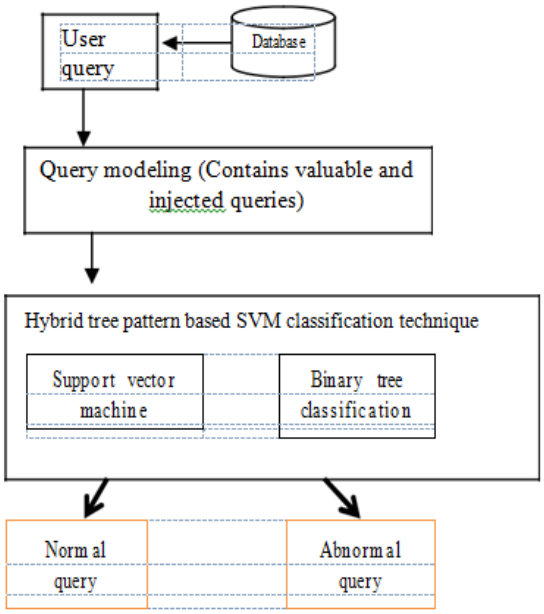

Figure-1 System architecture of the proposed model to classify the normal and abnormal queries

3.1 SQL injection

Normally, the websites are addictable to various SQL due to its black box nature with 3-tier architecture. It is automatically built when HTTP request is given with is perfect response. Sometimes this request may given by the attackers for the illegal purpose and tries to produce the abnormal query to access the database illegally.

In this SQL injection static analysis is used to maximize the detection and prevention of SQLIA with remaking process. The aim of this method to be apply here is to use the JAVA string base computation library. This will eluded the user is making the recursion by analyzing the proper format of syntax or not.

3.2 Detection Method

In the anomaly detection method the normal behavior of the users are stored in the database. They may be their username, password, their personal identification, their secret questions. Once the user is trying to access the database these has to check with their present attribute and hence the identification of authorized or unauthorized user is done with the elucidation concept. At the time of impersonation of the user the injection attack with DDOS may happen in the application layer when diffusing with other users which may have the features as follows:

- From the server point of view the illegal users prevalence is more than normal users.
- While analyzing the sequence of illegal and legal users there should be some difference in the sequential order of illegal user.

Here, query tree is an option to protect the database from SQL injection attacks. This uses the regression and post regression model with structure query language statements. There are some of the commands are given here. For debugging process: 'SET' DEBUG_PRINT_PLAN="ON" and 'SET'CLIENT_MIN_MESSAGE="DEBUG1"

These commands are tree minimized files that has to be store in the post regression database. Whereas the queries are informally evicted to the authorized user.Now, the query is submitted and the training process is about to start with its allocated level. After the training process the classification will happen by extracting the features of each query and comparing with its tree surfaced model. When the user elucidates the query and try to access the information from the database the query is compared with the trained dataset and noted as malicious or not

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 9301 - 9313

If admin=1,2,3,4
User: xxx
Password: yyy
Type of injection: and,or, string,numeric, comments
Attack type = y
FQ = Fixed query for web application
DQ = Dynamic query for web application
Input : Query= user generation
Db = static list with stored SQL injection
DB= d1,d2,d3....dn
d1: select user where id1='admin1/user1 (xxx) and p/w=(yyy)
D2: select user where id2='admin1/user2 (xxx) and p/w=(yyy)
N= Total fixed queries in database (db)
If [db(string,union,numeric,comment)]==null
Calculate the anomaly score (AS)
$AS = \frac{Matching\ value\ (query)}{string\ length} \times 100$
If (AS ≥ threshold)
Then go to classification
Abn is abnormal
Nm is normal
Return by giving indicaiton alarm to asmininstrator
Else
Result= normal
else if
result= abnormal
end if

3.3 Classification Process

Assuming that the space region where the two classes of samples are located in R, SVM-BT first divides R into two sub-regions R1 and R2. Then, it recursively divides each sub-region by repeating this process until gets satisfied the stop condition. If the stop condition is satisfied for sub-region then the division of this area is completed. Accordingly a decision node is generated.

With the size of the problem reduced, the algorithm is eventually converging. Based on the key value the node is identified in binary search tree also use vector (K dimension) for counting the values in that node. This Kind of vector class Totals [k] include the counts for example, which one is key Value that can be labeled with class k. Each node manage the pointer left and right for its child whether its left child corresponds to ≤ key Value, while its right child corresponds to > key Value. To get the best split point, every numerical attribute manages a head pointer. If the attacker can change the SQL command, then it can be execute with same statement as the application user, While SQL serve need to execute the SQL command which interact with Operating system, then the process remains same permissions will run as the component which execute the command (e.g., database server, application server, or Web server).

Training as well as testing data task is involved in classification part which contains few data instances. In training set, every instance has one “target value” I.e. class labels as well as several “Attributes” i.e. features. SVM-BT goal is to make a model that can predict the target value instance in testing data which can be given the attributes only.

Create the training set

- SQL Query string as input
- To create a model the training set is given into the SVM-BT Train process
- Now we are prepared to make forecast made by Classifier made in training process
- Using SVM-BT classifier Now we can arrange the Model
- Through Labeled result it will give the precision of our calculation.
- Repeat input the SQL query string to marked yield till the right classification precision is accomplished.

IV. PERFORMANCE ANALYSIS

The classification accuracy rate is measured by the dataset in the proposed system. For instances, the two classes having the classification dilemma namely positive as well as negative, there are four possibilities in single prediction. In classification accuracy have true positive rate (TP) as well as true negative rate (TN).A False Positive (FP) happens when the result is incorrectly anticipated as positive

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 9301 - 9313

when it is truly negative. A False Negative (FN) happens when the result is mistakenly anticipated as negative when it is really positive.

1. Accuracy – It is measured as total number records which is correctly classified by the classifier.

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$

2. Classification Error – Dataset which is misclassified accurately from classified records.

3. True Positive Rate (TP): It is accurately predicted by the classification model which is number of positively predicted.

4. False Positive Rate (FP): It is accurately predict the negative which is inaccurately predicted by the classification model.

5. Precision -is retrievethe fraction of instanceswhich is correlated.

$$\text{Precision} = \frac{TP}{TP + FP}$$

6.Recall- is the fraction of correlated instances which is

Retrieved.

$$\text{Recall} = \frac{TP}{TP + FN}$$

AnSQLi attack which is classified mistakenly that is false negative of legitimate content and the legitimate content mistakenly classified is false positive. In this model, false negative cost is better than false positive cost. Certainly, The legitimate request analyzing is wasting time which is more acceptable when the malicious code is passing to the Web application.

By using query tree and the SVM classification is used to detect the user behavior in the proposed system. The malicious user entered the query then the user is malicious one the alert message is transfer to the admin. Then the database will save for the data future purpose which is requested. Based on timestamp the user is classified which one is malicious.

Table-1 Comparison table for existing and proposed system

Parameters	SVMclassification	Proposed Classification
Accuracy	85	92.3
Precision	83.4	91
Recall	81.5	89

Table-1 gives the comparison between existing algorithm and proposed SVM classification. It compares the accuracy, precision and recall values, where proposed SVM classification algorithm gives optimized values than existing algorithm.

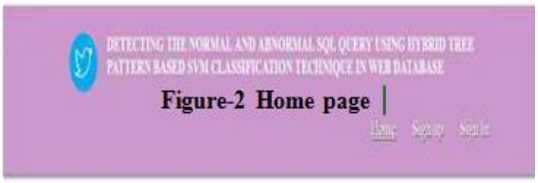

Figure-2 Home page

Figure-3 signup process

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 9301 - 9313

Fig 3 and 4 indicates the signup process and its successful registration under healthcare application to access the particular dataset

Figure-4Succesful registration

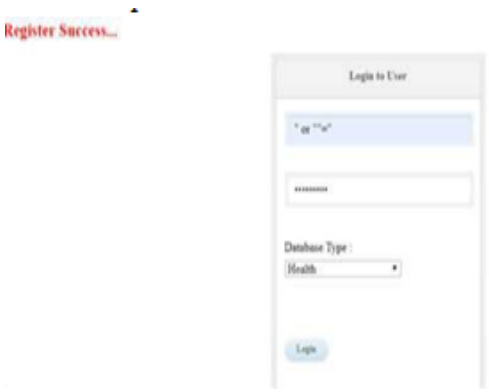

Figure-5 Login page –PreventSql injection

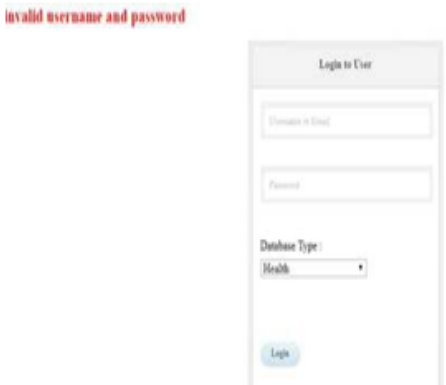

Figure-6 SVM Prevent the sql injection

Fig 5 and 6 shows the prevention of malicious SQL injection to access the dataset and it is efficiently prevented by using our proposed technique

Figure-7 Health care Management

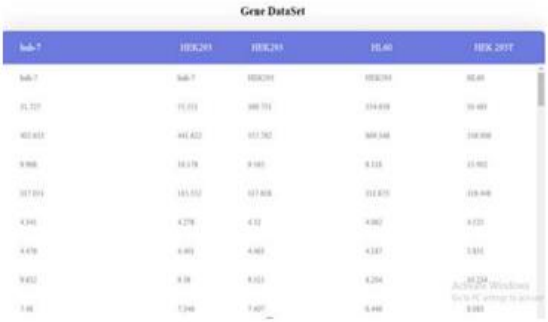

Figure 8- Healthcare dataset

Fig 7 and 8 indicates the invalid accessing of healthcare database system

Figure 9 Banking management

Figure 10 Banking dataset

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 9301 - 9313

Fig 9 and 10 indicates the invalid access of banking database system

Figure 11-Employee management

Figure 12-Employee dataset

Figure 13 Finance management

Figure 14 Finance dataset

Fig 13 and 14 indicates the invalid access of finance database system

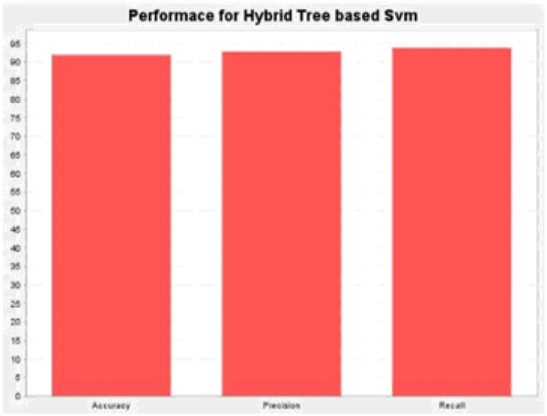

Figure 15 Performance in healthcare field

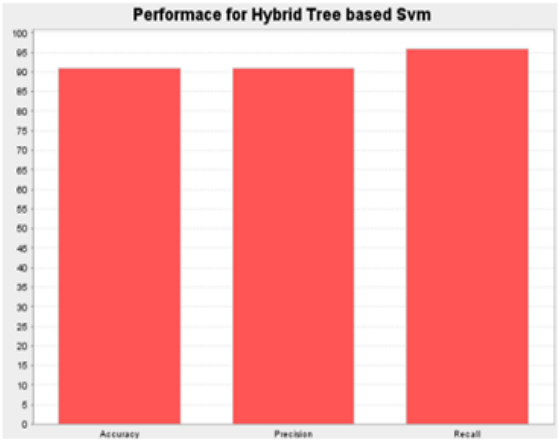

Figure 16 Performance in banking sector

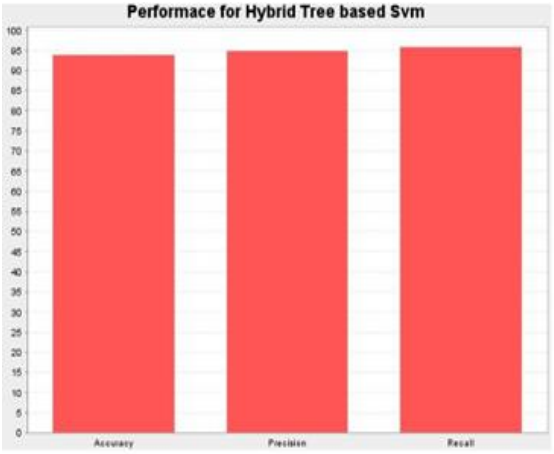

Figure 17 Performance in finance sector

Published by: The Mattingley Publishing Co., Inc.

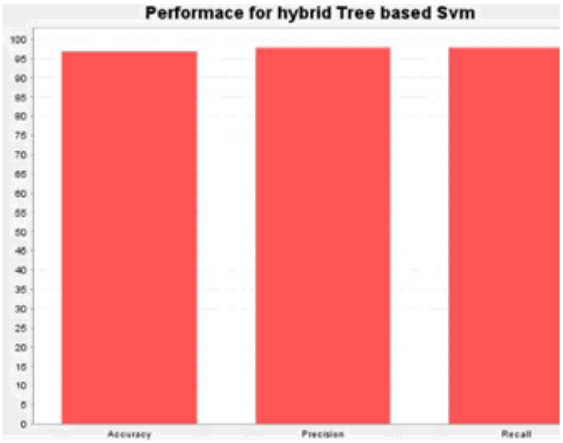

Figure 18-Performanceinemployeesector

Figure-15,16,17,18 shows the performance of proposed SVM classification in graphical form. It gives the accuracy, precision and recall comparison using SVM technique.

V. CONCLUSION

In this paper we have displayed a novel strategy to forestall SQL injection attacks by an effective classification plan to change over SQL inquiries into their auxiliary structure and after that applying half breed tree technique for each lawful query gathered during typical use. At run-time, hash key for each powerful query is produced in a similar way and coordinated against the recently put away hash keys to forestall SQL injection attacks. This methodology limits the size of the authentic query storehouse and encourages quick and productive looking at run-time utilizing an essential list. Our trial results demonstrate that this methodology can successfully counteract a wide range of SQL injection attacks.

REFERENCES

[1] Lee, S.-Y., Low, W.L., Wong, P.Y.: Learning fingerprints for a database intrusion detection system. In: Gollmann, D., Karjoth, G., Waidner, M. (eds.) ESORICS 2002. LNCS, vol. 2502, pp. 264– 279. Springer, Heidelberg (2002)

[2] Huynh, V.H., Le, and A.N.: Process miningand security: visualization in databaseintrusion detection. In: Chau, M., Wang, G., Yue, W.T., Chen, H. (eds.) PAISI 2012. LNCS, vol. 7299, pp. 81–95. Springer, Heidelberg (2012)

[3] Jin, X., Osborn, S.L.: Architecture for data collection in database intrusion detection systems. In: Jonker, W., Petković, M. (eds.)SDM 2007. LNCS, vol. 4721, pp. 96–107. Springer, Heidelberg (2007)

[4] Rajput, I.J., Shrivastava, D.: Data Mining based Database Intrusion Detection System: A Survey. Int'l Journal of Engineering Research and Applications (IJERA) 2(4), 1752–1755 (2012)

[5] Buehrer G., Weide B. W., Sivilotti P. A. G., "Using Parse Tree Validation to Prevent SQL Injection Attacks", 5th International Workshop on Software Engineering and Middleware, Lisbon, Portugal, 2005, pp. 106–113.

[6] Gupta, Himanshu; Sharma, VinodKumar;"ROLE OF MULTIPLE ENCRYPTIONSIN SECURE ELECTRONIC TRANSACTION", International Journal of Network Security & Its Applications, Nov 2011, pp: 89-96.

[7] Gupta, Himanshu; Sharma, Vinod Kumar; "Multiphase Encryption: A New Concept in Modern Cryptography",] International Journal of Computer Theory and Engineering, Aug 2013, pp: 638-641.

[8] B. Fei, J. Liu, Binary tree of SVM: a new fast multiclass training and classification algorithm, IEEE Transactions on Neural Networks 17 (2006) 696–704.

[9] AtefehTajpour, Ibrahim Suhaimi, Masrom Maslin; "Evaluation of SQL Injection Detection and Prevention Techniques"; International Journal of Advancements in Computing Technology,Korea; year 2011; pp. 1-20.

[10] Algergawy, A., Mesiti, M., Nayak, R., &Saake, G. (2011). XML data clustering: An overview. ACM Computing Surveys,

[11] Ben-Hur, A., & Weston, J. (2010). A user's guide to support vector machines.In Data mining techniques for the life sciences (pp. 223–239). Humana Press.

[12] NaghmehMoradpoorSheykhkanloo, "Employing Neural Networks for the Detection of SQL Injection Attack", SIN '14, September 09 - 11 2014, Glasgow, Scotland Uk , 2014.

[13] Yaohui Wang, Dan Wang, Wenbing Zhao, Yuan Liu," Detecting SQL Vulnerability Attack based on the Dynamic and Static Analysis Technology", IEEE 39th Annual International Computers, Software & Applications Conference, 2015.

[14] GeogianaBuja, Dr. Kamarularifin Bin AbdJalil, Dr. Fakariah Bt. HjMohd Ali, TehFaradilla Abdul Rahman," Detection Model for SQL Injection Attack: An Approach for Preventing a Web Application from the SQL Injection Attack", IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE) , April 7 - 8, 2014, Penang, Malaysia, 2014.

[15] Bockermann, C., Apel, M., Meier, M.: Learning SQL for database intrusion detection using context-sensitive modelling (Extended Abstract). In: Flegel, U., Bruschi,D. (eds.) DIMVA 2009. LNCS, vol. 5587, pp. 196–205. Springer, Heidelberg (2009)

[16] E.Osuna, F.Girosi,Reducingtherun-timecomplexityofsupportvector machines. AdvancesinKernelMethods—Support VectorLearning,MITPress, 2011, pp.271– 283.

[17] T. Downs, K. Gates, A. Masters, Exact simplification of support vector solutions, Journal of Machine Learning Research 2 (2012) 293–297.

[18] Elshazly, K., Fouad, Y., Saleh, M., Sewisty,A. A survey of SQL injection attack detection and prevention. Journal of Computer and Communications, vol 2, no 8 2014;:1–9.

[19] Kemalis K, Tzouramanis T. SQL-IDS: A Specification-based Approach for SQL-injection Detection. In: Proceedings of the 2008 ACM symposium on Applied computing. ACM; 2008. p. 2153–8.

[20] Liu A, Yuan Y, Wijesekera D, Stavrou A. SQLProb: A Proxy-based Architecture towards Preventing SQL Injection Attacks. In: Proceedings of the 2009 ACM symposium on Applied Computing. ACM; 2009. p. 2054–61.

[21] Zhang K, Lin C, Chen S, Hwang Y, Huang H, Hsu F. TransSQL: A Translation and Validation-Based Solution for SQL-injection Attacks. In: Robot, Vision and Signal Processing (RVSP), 2011 First International Conference on. IEEE; 2011. p. 248–51.

[22] Low W, Lee J, Teoh P. DIDAFIT: DetectingIntrusions in Databases through Fingerprinting Transactions. In: Proceedings of the 4th International Conference on Enterprise Information Systems (ICEIS). Citeseer; volume 264; 2002. p. 265–7.

[23] Wei K, Muthuprasanna M, Kothari S. Preventing SQL Injection Attacks in Stored Procedures. In: Software Engineering Conference, 2006. Australian.IEEE; 2006.p.191–8.

[24] Kim MY, Lee DH. Data-mining based SQL Injection Attack Detection using Internal Query Trees. Expert Systems with Applications 2014;41(11):5416–30.

[25] Boyd S, Keromytis A. SQLrand: PreventingSQL injection attacks. In: Applied Cryptography and Network Security. Springer; 2004. p. 292–302

[26] Vigna G, Valeur F, Balzarotti D, Robertson W, Kruegel C, Kirda E. Reducing Errors in the Anomaly-based Detection of Web-based Attacks through the Combined Analysis of Web Requests and SQL Queries. Journal of Computer Security 2009;17(3):305–29.

[27] Le M, Stavrou A, Kang BB. Doubleguard: Detecting intrusions in multitier web applications. Dependable and SecureComputing, IEEE Transactions on 2012;9(4):512–25

March - April 2020
ISSN: 0193-4120 Page No. 9301 - 9313

[28] Pinzón CI, De Paz JF, Herrero A, Corchado E, Bajo J, Corchado JM. idmas-sql: intrusion detection based on mas to detect and block sql injection through data mining. Information Sciences 2013;231:15–31.

[29] Inyong Lee et. al./A novel method for SQL injection attack detection based on removing SQL query attribute values/Elsevier 2012.

[30] W.G. Halfond and A. Orso, AMNESIA: Analysis and Monitoring for NEutralizing SQL-Injection Attacks, Proc. 20th IEEE and ACM Intl Conf. Automated Software Eng.,pp.174-183, Nov. 2005

[31] S. W. Boyd and A. D. Keromytis. SQLrand: Preventing SQL Injection Attacks. In Proceedings of the 2nd Applied Cryptography and Network Security (ACNS) Conference, pages 292-302. June 2004

[32] Van Ristic :ModSecurity Handbook: The Complete Guide to the Popular Open Source Web Application Firewall, 2010 Feisty Duck Ltd Edition ISBN: 1907117024