JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 5038-5046
https://publishoa.com
ISSN: 1309-3452

Smart Algorithms to Secure Web Based Applications from SQL Injection Attacks

[1]S.Shanmuganathan, [2]D.Srinivasan,
[1] Assistant Professor, Department of computer Science and Engineering,
Mailam Engineering College, Mailam
shanmuganathancse@mailamengg.com
[2] Assistant Professor, Department of computer Science and Engineering,
Mailam Engineering College, Mailam
help2srinivasan@gmail.com.

Received: 2022 March 15; **Revised:** 2022 April 20; **Accepted:** 2022 May 10

Abstract— This paper proposes a Multiplicative Inverse Based Data Encryption Module to secure Web Based Applications from SQL injections attacks. There are different methods to perform SQL injections attacks which are reviewed before this research work. The objective of this work is to enhance the security of Web based apps from SQL injections attacks. In order to enhance the security of Web based apps, Multiplicative Inverse based module is proposed. In the proposed Registration module, the user password is compressed and encrypted and saved it in Web Database. MATLAB Simulation tool is used for the simulation of results and output retrieved from proposed work. A comparative analysis of Proposed Work and Existing Security Technique is made to highlight the efficiency and applicability of this work. After encryption of data there should be negligible probability of attacking or hacking of Databases.

Keywords—Web based Applications, Attacks, SQL Injection, and Multiplicative Inverse Technique, Encryption, Decryption

I. INTRODUCTION

This document is a template. For questions on paper guidelines, please contact us via e-mail.

Program and applications are called Web based application when these are accessed over a network withthe help of Internet Connection. In order to access web applications, HTTP is used. Generally, these applications are used through a web browser that may be Google Chrome, Mozilla Firefox, Opera etc.The development and use of Web based Applications are increasing day by day. There is a lot of Web applications which are make our life easy. Several web based application are there such as online forms, shopping carts, word processors, spreadsheets, video and photo editing, file conversion, file scanning, and email programs such as Gmail, Yahoo and AOL. In computer system, basically there are client side and server side software application in a Web application. To access this app, the user make request or run in aweb browser. There are five different types of web apps having their own characteristics.

1) Static web application
2) Dynamic web application
3) E-commerce
4) Portal web app
5) Content Management System (CMS)

Web-based applications consist of three main components such as Web browser (or client), Web

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 5038-5046
https://publishoa.com
ISSN: 1309-3452

application Server, and Database Server. Basically, these apps depend on Database server, to provide the data. The development of cloud-based applications is increasing more quickly than ever before. As the development and use of these devices are increasing, the security threats with these apps are also increasing. The hackers are continuously engaged to develop different method and techniques to hack these web based applications. There are several types of threats and attacks which can be used to hack or attack on security of a web based app. These attacks are represented in above figure. Along with above discussed security threats, there are some other methods which are applied to hack a Web based application. For example Privilege Escalation is a considerable method that is used to attack on a web application. In addition to this, several other hacking techniques are there such as Virus, Worm, Trojan, Trojan horses, Spyware, Spam, Adware, Rootkits etc.

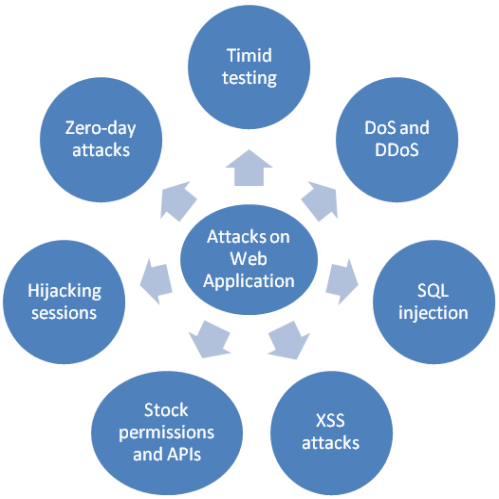

Fig 1 Different Security Threats to Web Application

II. SQL INJECTION

SQL injection has been known as a code injection technique. It can easily destroy and hack the important and sensitive data located in a database of a Web based app. Out of different Web hacking technique, SQL injection is one of them. In SQL injection technique, user of a web application inputs SQLstatements at the place of his information for example at the time of login, use may input a malicious code in the form of SQL statement instead of his user name. In order to secure a web site, it is essential to use SQL parameters.

Generally, SQL injection attacks take place by user of a web app when he is asked to ender his detail forlogin for example username/user id, and instead of a name/id. But instead of actual detail, he enters an SQL statement which runs on the Web database of his app for example.

User Id: 105 OR 1=1

As this input will reach in SQL, it becomes an SQL statement and behaves as a statement: SELECT * FROM Users WHERE UserId = 105 OR 1=1;

The SQL above is valid and will return ALL rows from the "Users" table, since OR 1=1 is always TRUE.

As it is discussed above that to avoid SQL Injection attack, it is essential to use statement parameters. It is required that SQL engine make proper checking of each input entered by user. The input must be correctaccording to its column. This input would be treated literally not as a part of SQL Query.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 5038-5046
https://publishoa.com
ISSN: 1309-3452

III. RELATED WORK

I proposed a model locked pattern,a frame work to detect, prevent sql injection and XSS attacks which has also been addressed and provides direct inputs for SQL injection prevention by Padma N Joshi et. al [1][2]. [3]. [5].

A. Multiplicative Inverse Algorithm

In Multiplicative inverse algorithm, the reciprocal of a number is calculated mathematically. For example the multiplicative of a will be 1/a. Multiplicative inverse of a fraction x/y will be y/x. to get the multiplicative inverse of a real number; it is essential to divide 1 by the real number. Here is another example to understand this concept such as reciprocal of 10 is 1/10 on the other hand, 2 is multiplicative inverse of 0.5. In order to calculate the multiplicative inverse of any number, simply divide 1 by the number whose multiplicative inverse is required. The function f(a) that maps a to 1/a, is simple example ofa function.

IV. OBJECTIVE OF RESEARCH WORK

There are several factors which are considered in this research work but some main objective of thisresearch is listed here:

1) To study different type of threats and attacks on the security of Web based Applications
2) To review the limitations of existing techniques and Module which are used to secure the Webbased Apps.
3) To propose a Multiplicative Inverse based module to avoid SQL Injection
4) To use MATLAB for the simulation of results and output retrieved from proposed work
5) To compare the Proposed Work to Existing Security Technique to highlight the efficiency and applicability of this work

V. TOOLS AND TECHNOLOGY

The tools which are used in this research work is discussed here

A. Structured Query Language (SQL)

Structured Query Language is also known as SQL. It is a set of commands used to access required information from the database of a Web based app. There are different data management systems for example SQL Server, My SQL, Oracle which are used to run the SQL commands and store the data ofWeb Applications. These data management systems are used according to language compatibility for example SQL Server is used with dot net based module whereas My SQL is compatible with Python basedprograms. There is different type of commands according to the requirement for example insertion, deletion, updating, Retrieval etc.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 5038-5046
https://publishoa.com
ISSN: 1309-3452

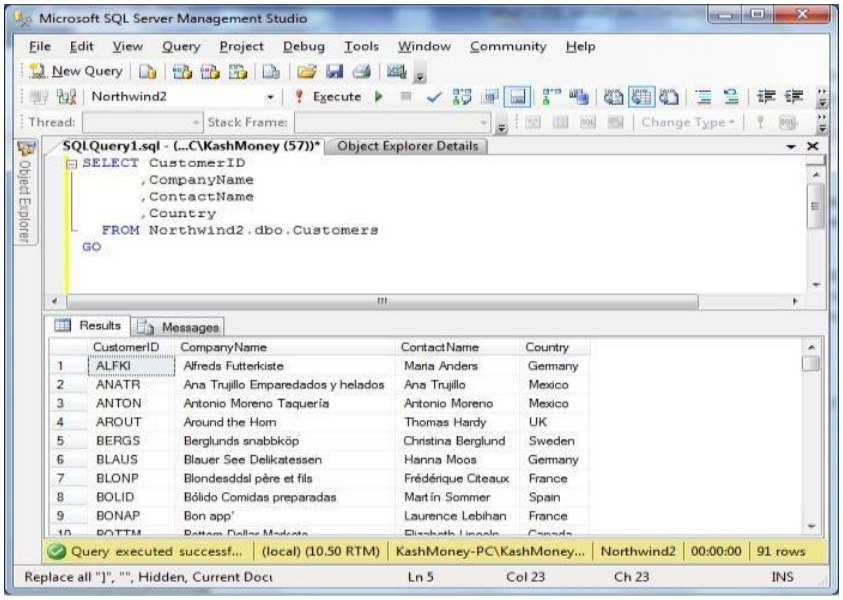

Fig 2 Retrieval of data in SQL Server

Out of different simulation tool, MATLAB is most popular simulation tool. The reason of its popularity is its interactive environment. In Matlab environment, high-level language is used which make easy to execute computationally without any delay. This simulation tool includes different feature for example it iseasy to perform addition, subtraction, multiplication and subtraction etc operation. This tool made it easy to plot line. One can plot line of any equation or using data located in a Notepad file. But it is essential to save this notepad file in Matlab folder. In addition to this, the files can be imported from any location to plot multiple lines. In addition to this, there are a lot of features and advantages which make oursimulation task easy. After installation of MATLAB, the first screen where we write command looks like as:

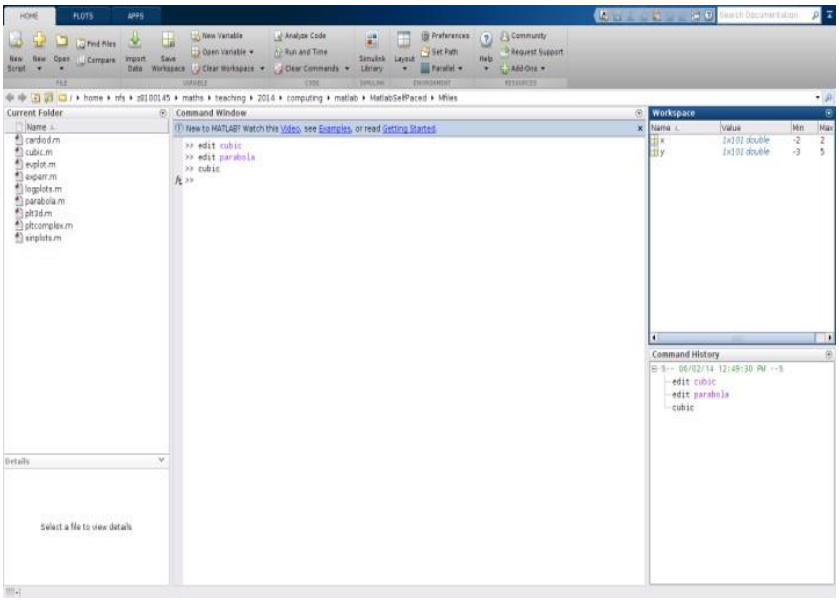

Fig 3 Matlab

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 5038-5046
https://publishoa.com
ISSN: 1309-3452

VI. PROBLEM STATEMENT

There are different techniques and modules which are proposed to secure Database of a based Web Application from SQL injection attacks. These methods are not sufficient and have own limitations. Some of researchers only review the different SQL attacks whereas some discussed less efficient way to avoid sql injection attacks such as Data Validation, Parameterized Query, Escaping and Firewall etc. In traditional SQL injection prevention systems, only authenticated user are enable to login in an application as admin specifies the authentic code for particular time session. But in these systems, the data of databases is not encrypted and remains in its actual form. Therefore it is essential to encrypt the data in order to enhance the security of Databases. For this purpose, more strong and efficient Data Encryption Technique should be used. After reviewing the traditional systems, it has comes to know that there is need of Efficient Encryption method. After encryption of data there should be negligible probability of attacking or hacking of Databases. Proposed model has provided triple layer security

1) Layer 1 is compressing the Data
2) Layer2 is encrypting the Data
3) Layer3 is security layer discussed in previous SQL Injection Prevention System

VII. PROPOSED MODEL

The working process of proposed Registration Module and Login Module is discussed here:

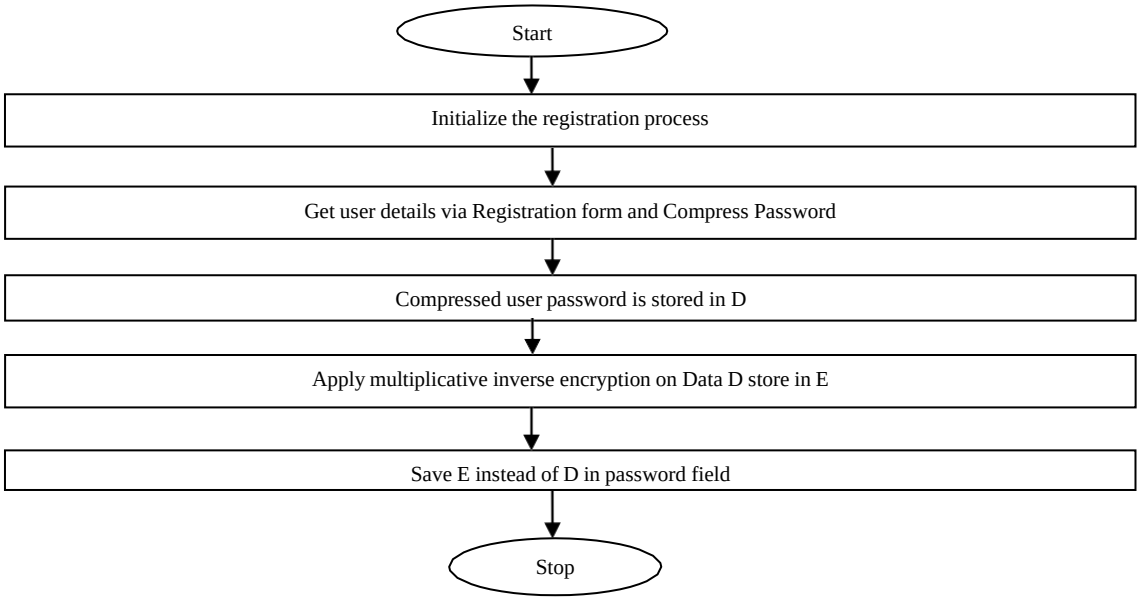

Fig 4 Process Flow during Registration Process

VIII. RESULT AND DISCUSSION

In this section, the Matlab Simulation of Packet Size, Time Taken and Error Rate in Case Of Traditional and Proposed Model is made. For the simulation of proposed result, MATLAB is used as a simulation tool.

A. Packet Size

Multiplicative Inverse is used to encrypt the data. As a result the packet of data becomes small in size.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 5038-5046
https://publishoa.com
ISSN: 1309-3452

The figure is showing comparison in packet size of existing and proposed work.

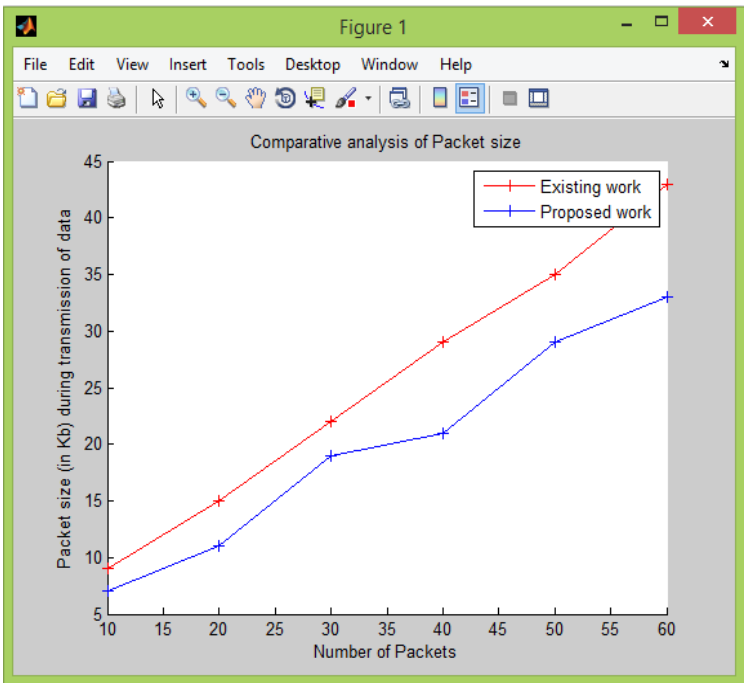

Fig 5 Packet Size

B.Time Consumption

The existing and proposed systems are also differentiated on the base of time consumption. As thepacket size is decreased with the use of Replacement method, the proposed system takes less time to reach on it destination. Therefore it takes less time which is indicated by below given table.

No of Packets	Time Consumed by Existing/Traditional model	Time Consumed by Proposed model
10	1	0.8
20	1.9	1.5
30	2.5	1.90
40	3.3	2.7
50	4	3.1
60	5	3.7

Table 1 Comparative Analysis Of Traditional System And Proposed System On The Base Of Time Consumption

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 5038-5046
https://publishoa.com
ISSN: 1309-3452

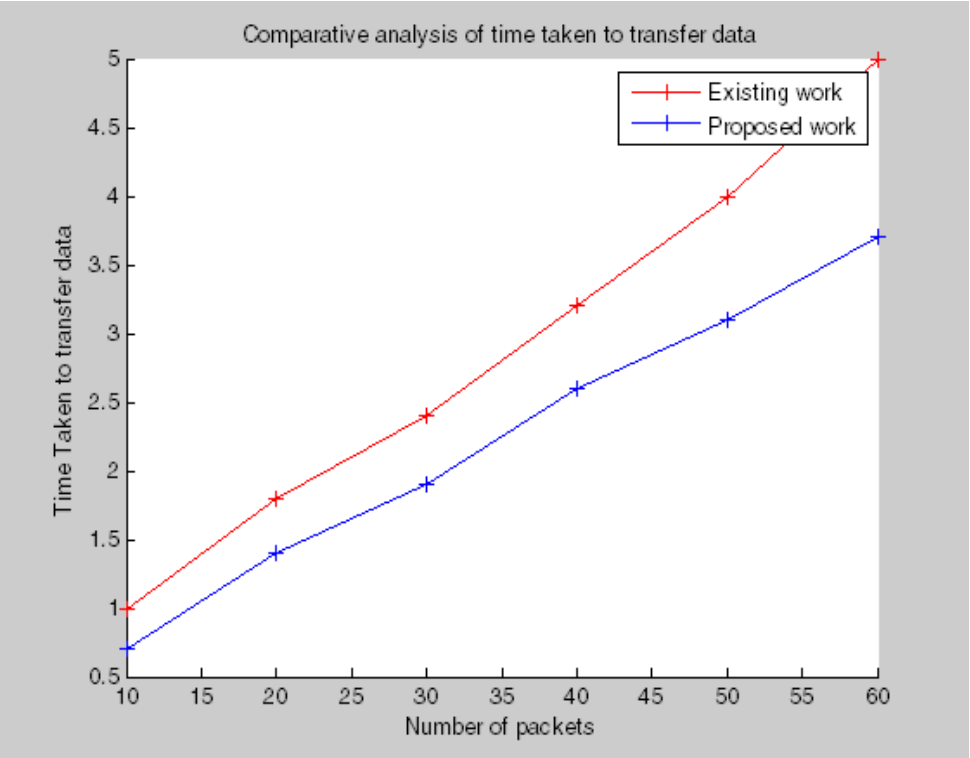

Fig 6 Time taken during Transmission

B.Error Rate

Triple layer security would be capable to avoid unauthentic access of data and control error rate. Therefore, it would be impossible to encrypt this data. Following figure is representing the error rate in case existing and proposed work.

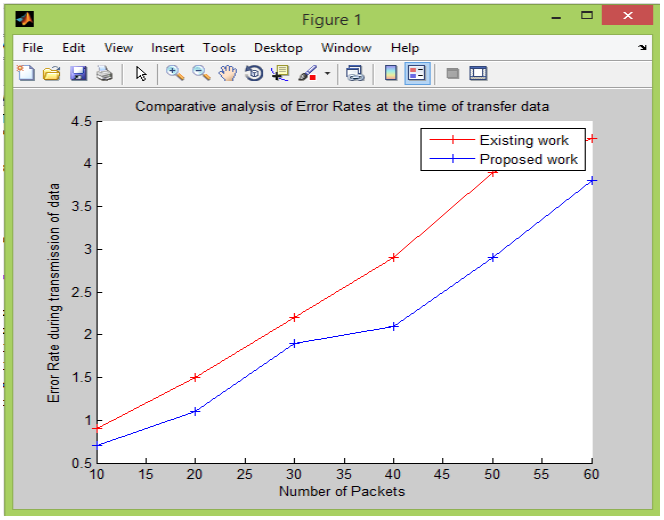

Fig 7 Error Rate

IX. CONCLUSION

Enhancement in this research work has increased the performance of Login System along with Security. The previously discussed model has enabled the security. But this enhancement provides Triple Layer Security along with better performance. The compression of content has improved the performance of Login System. In this work, Password is encrypted applying Multiplicative Inverse. As a result the password become small and secure before transmission in web application. When the data travels, there are less chances of error as small and encrypted data travels. To show the efficiency of proposed work, it

iscompared to existing work. For the comparative analysis, Security, Time Consumption, Data Size, Error Rate etc parameters are considered and Matlab simulation tool is used. The comparative analysis is clearly showing the applicability and efficiency of proposed work.

X. FUTURE SCOPE

This work would be beneficial to review the limitations of existing techniques and Module which are discovered in past to secure the Web based Apps. This work would be helpful as it proposes a Multiplicative Inverse based module to avoid SQL Injection. In addition to this, it also discusses MATLAB that is used for the simulation of results and output retrieved from proposed work. This paper contain the comparative analysis of Proposed Work to Existing Security Technique that would be helpfulto know the efficiency and applicability of this work

REFERENCES

[1] Joshi Padma, Dr.N.Ravishankar,Dr. M.B. Raju,N.Ch.SaiVyuha"Secure Software Immune receptors from Sql injection and Cross site scripting attacks in Content delivery Network Web applications" 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO 2021)DOI: 10.1109/ICRITO51393.2021,Sept. 2021

[2] Joshi Padma, Dr.N.Ravishankar, Dr. M.B. Raju, N.Ch.SaiVyuha "Defensive Walls for Detecting and Preventing SQL Injection and XSS attacks in Dynamic Content Delivery Network Web Applications" Design Engineering (Toronto) ,vol.2021,issue 7,2021,pp10019-10039

[3] Joshi Padma, Dr.N.Ravishankar,Dr. M.B. Raju, N.CH.Ravi(2018) "Encountering SQL Injection in Web Applications" Proceedings of the Second International IEEE Conference on Computing Methodologies and Communication.

[4] N.CH.Ravi,Joshi Padma,etal., "Inspecting Access Controls in Cloud Based Web Application" Proceedings of the Second International IEEE Conference on Computing Methodologies and Communication.2018

[5] Joshi Padma, Dr.N.Ravishankar,Dr. M.B. Raju, N.CH.Ravi(2017) "Contemplating Security of Http From Sql Injection and Cross Script" 2017 IEEE International Conference on Computational Intelligence and Computing Research

[6] Parveen Sadotra(2017) "SQL Injection Impact on Web Server & Their Risk Mitigation Policy Implementation Techniques: An Ultimate solution to Prevent Computer Network from Illegal Intrusion" Volume 8, No. 3, March – April 2017 International Journal of Advanced Research in Computer Science

[7] Nabeel Salih Ali (2016) "Protection Web Applications using Real-Time Technique to Detect Structured Query Language Injection Attacks"
International Journal of Computer Applications (0975 – 8887) Volume 149 – No.6, September 2016

[8] Swathy Joseph (2016) "Evaluating Electiveness' Of Conventional Fixes For standardized query language Injection Vulnerability" IEEE Computer Society, vol: 46, Issue: 3, pp.69 – 77

[9] Abirami J, (2015) "A Top Web Security Vulnerability standardized query language Injection attack – Survey standardized query language Injections in Online Applications

[10] Bharti Nagpal(2015) "SECSIX: security engine for CSRF, standardized query language injection & XSS"

[11] Rathod Mahesh Pandering (2015) "A Mapping-based Podel for Preventing Cross Site Scripting & standardized query language Injection Attacks on Web Application & its Impact Analysis" 2015

[12] Mukesh Kumar Gupta.(2015) "Predicting Cross Site Scripting (XSS) Security Vulnerabilities in Web

Applications", International Joint Conference on Computer Science and Software Engineering (IJCSE), IEEE, pp. 40-52, 2015.

[13] Sonewar, Piyush A., and Nalini A. Mhetre.(2015) "A novel approach for detection of SQL injection and cross site scripting attacks." Pervasive Computing (ICPC), 2015 International Conference on. IEEE, 2015.

[14] Wang, Rui, et al.(2015) "Improved N-gram approach for cross-site scripting detection in Online Social Network." Science and Information Conference (SAI), 2015. IEEE, 2015

[15] Habeeb Orotund (2014) "Mitigating standardized query language Injection Attacks Via Hybrid Threat Modelling" International Symposium on Secure Software Engineering. IEEE, Conference Proceedings, pp. 65–81. 2014

[16] Amirmohammad Sadeghian (2014) "Standardized Query language Injection Vulnerability General Patch Using Header Sanitization" international conference on World Wide Web, pp. 396-407. ACM, 2014.

[17] Rocha, Thiago S., and Eduardo Souto. (2014) "ETSS Detector: a tool to automatically detect Cross-Site Scripting vulnerabilities." Network Computing and Applications (NCA), 2014 IEEE 13th International Symposium on. IEEE, 2014.

[18] Dr. T.PriyaRadhikaDevi "Android Application Forspontaneous Soilconstant Monitoring And Controlling Systemusing Raspberry Pi"Journal Of Critical Review Vol 7 Issue 16.

[19] Murali. D, Prasanna. S, Mathavan. V,Priyaradhikadevi. T" Linear Regression And Neural Networks Algorithm To Predicting The Real-Time Parameters Of Temperature And Humidity" Journal of Critical Review Vol 7 Issue 16