International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-12, October 2019

Design and Implementation of Reliability Analysis Tool using Real Time Data

Gayathry G, Thirumalaiselvi R

Abstract: ***To estimate the reliability of software numerous statistical methods are in practice. To accomplish the software reliability prediction in more accurate way there is a huge demand for data sets. The data sets that can be acquired as a result of testing the software can be used for predicting the reliability. The research work focuses on creating a layer of software design and testing method namely web software testing. The main purpose is to collect the erroneous data from real time. The reliability of software can be measured in different aspects like traffic handling capability when there are a greater number of users, the security level for cracking the passwords and the possibility of different combinations of errors that occurs when inputting the data. This proposed software tool will read the software description, and will generate test patterns according to the input types and collects testing results, predicting the software reliability in real time and suggesting the possible ways to improve the software. For designing purpose PHP for web application will be used to give the testing results.***

Keywords**: Brute-force, failure rate, password, reliability.**

I. INTRODUCTION

In today modern world, there is a rapid change in the growth of science and technology. Dependent nature of human on computers is increasing day-by-day. There is always a need for highly reliable software. The main goal of software engineer is to develop a highly reliable software based on customer's satisfaction. The failures in software in turn causes the failures in system and results in undesirable results that affect the quality and reliability of system. The failures that occur in software increases the failure rate of software system. By identifying and removing these failures may cause a decrease in failure rate of software system. The faults are mainly design time faults, the classification, visualization and detection of these faults are not an easy job. The foremost task is to identify the data that need to be collected. The failure that causes at the time of testing and operating the system are recorded. Ensuring the accuracy and completeness of data collected is the need of hour.

Revised Manuscript Received on October 30, 2019.
***** Correspondence Author
Gayathry G*, Computer Science, Bharathiar University, Coimbatore, India.
Thirumalaiselvi R, Computer Science, Govt. Arts College (Men), Nandanam, Chennai, India.

II. PASSWORD CRACKING

Password cracking is defined as the process of retrieving password from the location where it is stored or from data transmission system. Various techniques are available to crack the password. Brute force attack is one among them. It always cracks the password no matter how complex it is. This method systematically tries all possible combinations for a password. This is most efficient when the length of password is short. The creative nature of user and the complexity of program defines the complexity of password.

A. Brute-force Algorithm

It is the simplest algorithm among the available pattern matching algorithm. It can be used to solve the pattern searching problem. This algorithm will search for the pattern within the given text. There is no uniformity exist in comparing the pattern. The pattern and text can be compared in any order. The main feature is that it does not require any preprocessing phase. The process done during searching process is given below

Step 1: Input the text and pattern to be matched.
Step 2: Search process begins from left to right and comparison done on character by character basis.
Step 3: Try to match patterns from the beginning of text
Step 4: If pattern and text are same then return the location of matching string
Step 5: if not same then continue the search process
Step 6: Return whether the search is successful or not

III. PROPOSED WORK

A. Web Testing

Main aim of this application is to test the reliability of the web application in security perspective. This paper attempts to redefine the software reliability metric in terms of Software/IO errors, Server capacity to cater the no of clients and also the security level of a web application in which multi user data's will be available online.

A variable length, non-sequential brute force algorithm is developed as a PHP server script and the website under test will be scrutinized for the level of security breach it can handle, after generating each of the password combination, the website will be tested for an automatic login attempt with a known username.

Password combination will be in uppercase, lowercase alphabets, numeric, symbols i.e. literally all the printing characters in the keyboard will be used for the password pattern generator. Since the length of the user password is unknown the brute force algorithm will take many days to crack the password, based on the number of hours taken for the brute force to crack the password, we can calculate the software reliability score.

B. Screen Shots

Fig. 1.Before Starting Brute Force

Fig. 2. Brute Force with 3 length password

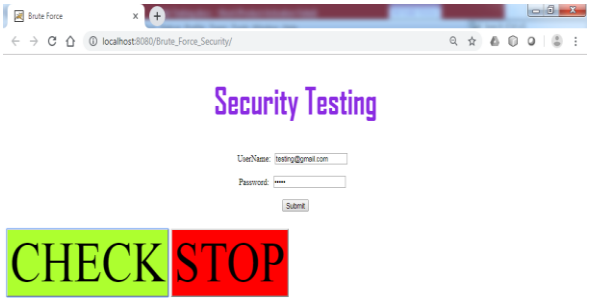

Fig. 3.Brute Force with 5 length password

IV. AUTOMATED RELIABILITY ANALYSIS TOOL

Macro-enabled worksheet has been designed to create the reliability analysis tool. Microsoft Excel Visual Basic for Application was used to design the tool. Labels, textboxes and command buttons are placed inside the form. A simple subroutine created that asks for input from the user. The reliability analysis of software in various scenarios like IO reliability, network reliability, security reliability is considered for illustration. The following code designed and using assign macro option the code assigned to the command button. To invoke the subroutine, choose the Run command that is available on the menu. The calculate button display the result in worksheet.

The factors along with its description are represented in Table 1.

Table I: Factors Affecting Reliability

FACTORS	DESCRIPTION
IO RELIABILITY	To measure the IO reliability a student database application created using java programming. The application records the exam results for each student. By applying Brute Force Non-Sequential Pattern Generator, the application can be auto tested. Error log report generated to record the occurrence of errors. The total errors based on number of test cases are given as input to calculate reliability.
NETWORK RELIABILITY	To measure the network reliability a python-based grid service created to test the load handling capability of server. This helps to measure the availability of RAM with respect to number of clients.
SECURITY RELIABILITY	To measure the security reliability a variable length, non-sequential brute force algorithm is developed as a PHP server script and the website under test will be scrutinized for the level of security breach it can handle.

The following Fig.4. represent the workflow nature of proposed tool.

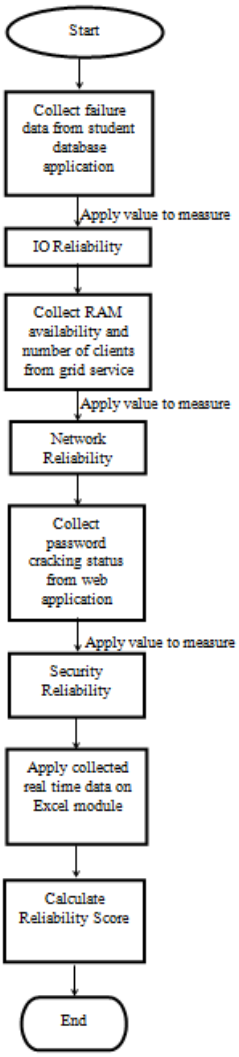

Fig. 4. Nature of Workflow in Proposed Tool

Sample coding to measure the reliability of software is Represented in Fig.5.

```
Sub Button1_Click ()
io_error = Range("E10")
io_count = Range("F10")

io_percent = 100 - (io_error / io_count)

net_ram = Range("E12")
net_client = Range("F12")

one_client = net_ram / net_client

ram = 8

net_percent = 100 - net_ram
sec_status = Range("E14")
sec_days = Range("F14")

sec_percent = 0

If sec_status = "cracked" Then

sec_percent = sec_days / 3
ElseIf sec_status = "not_cracked" Then
sec_percent = 100
Else
   MsgBox "Missing Fields"
End If

tot_percent = (sec_percent + net_percent + io_percent) / 3
Range("E20"). Value = CStr(tot_percent) + "%"
End Sub
```

Fig.5. Sample Coding

The tool that has been developed to measure and predict the reliability based on different factors is given below.

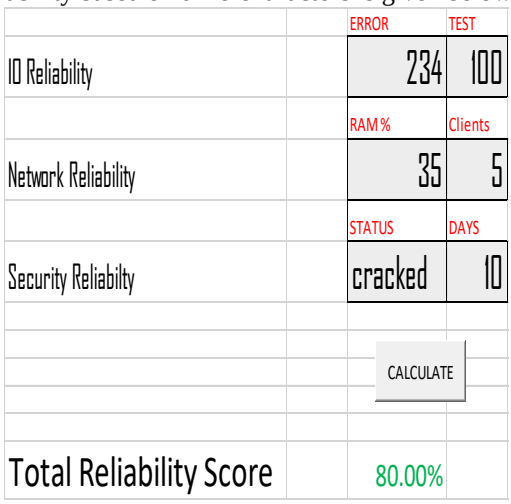

Fig.6. Reliability Analysis Tool

The tool provides reliability score by inputting the values such as total number of errors, test count, availability of RAM, number of clients, status of cracking the password and if cracked the total number of days taken.

V. CONCLUSION

The tool has been designed to evaluate and measure the reliability of software based on varying factors such as security, network and input/output reliability. When user inputs the needed data and choose the calculate button the score of reliability will be displayed in screen. From the predicted value the reliability can be identified.

REFERENCES

1. Farik , Ali, "Analysis of Default Passwords in Routers against Brute-Force Attack," International Journal of Scientific and Technology Research, vol. 4, no. 9, 2015.
2. Choi, Robles, Hong, Kim, "Wireless Network Security: Vulnerabilities, Threats, Countermeasures", International Journal of Multimedia and Ubiquitous Engineering, Vol. 3, No. 3, July, 2008.
3. Vidya Vijayan, Josna P Joy, Suchithra M S," A Review on Password Cracking Strategies", International Journal of Research in Computer and Communication Technology ISSN(O) 2278-5841 ISSN(P) 2320-5156.

4. Mudassar Raza, Muhammad Iqbal, Muhammad Sharif and Waqas Haider, (2012)," A Survey of Password Attacks and Comparative Analysis on Methods for Secure Authentication", World Applied Sciences Journal 19 (4): 439-444, 2012 ISSN 1818-4952.
5. Mohammed Farik, ABM Shawkat Ali," Algorithm to Ensure and Enforce Brute-Force Attack-Resilient Password in Routers", International Journal of Scientific & Technology Research Volume 4, Issue 10, October 2015 ISSN 2277-8616.
6. Konark Truptiben Dave," Brute-force Attack Seeking but Distressing", International Journal of Innovations in Engineering and Technology (IJIET), Vol. 2 Issue 3 June 2013, ISSN: 2319-1058.
7. Sajjad Rafique, Mamoona Humayun, Zartasha Gul, Ansar Abbas, Hasan Javed," Systematic Review of Web Application Security Vulnerabilities Detection Methods ", Journal of Computer and Communications, 2015, 3, 28-40.
8. Himanshu Kumar, Neelam Mathur," Password Cracking Technique: A Survey ", International Journal of Electrical Electronics & Computer Science Engineering Special Issue - ICSCAAIT-2018 | E-ISSN: 2348-2273 | P-ISSN: 2454-1222.
9. Rajdeep Bhanot1 and Rahul Hans2 "A Review and Comparative Analysis of Various Encryption Algorithms", International Journal of Security and Its Applications Vol. 9, No. 4 (2015).
10. Gayathry G, Thirumalaiselvi R, "Full Stack Software Development and Multi Aspect Testing", International Journal of Innovative Technology and Exploring Engineering, ISSN: 2278-3075, Volume-8 Issue-10, August 2019.

AUTHORS PROFILE

Ms.G.Gayathry is working as Assistant professor in the Department of Computer Science, Mar Gregorios Arts and Science College, Chennai. She is pursuing her Ph.D in the area of software engineering from Bharathiar University, India. She has 14 years of teaching experience

Dr. (Mrs.) R.Thirumalaiselvi is currently the Research Supervisor and Assistant Professor in the Department of Computer Science, Govt. Arts College (Men) (Autonomous), Chennai. She has over 20+ years of experience in various arts and science colleges and as a research supervisor. She is guiding many PhD students registered under various universities.