CHAPTER VI

RESULTS AND DISCUSSION

6.1 INTRODUCTION

The main goal of SuVa Security Framework is to perform the process of data migration in a secure fashion. Data migration is the process of transferring data from one place to the other. Usually, this process happens between the data owner and the cloud server. However, achieving hassle-free data migration is not simpler and highly challenging. The reason is that mostly, the data owners prefer to hire cloud space, when they possess voluminous data.

6.2 EXPERIMENTAL RESULTS AND DISCUSSION

Shifting voluminous data in a stretch is quite challenging and during the process of migration, security attacks may happen. For instance, data duplication may occur, which is a highly sensitive issue. In addition to this, the vulnerability may be present in the data to be outsourced, which may harm the cloud server in turn. Hence, it is a better option to check the data for vulnerabilities before the initiation of outsourcing. This idea conserves time and resources.

Taking all these factors into account, this work proposes a security framework namely SuVa Security Framework and the performance of the proposed approach is compared against by Wei L. et al. [2014] and CloudZone presented by Talib A.M. et al. [2011] in terms of penetration testing and F-measure analysis.

The real-time data is utilized for the research. The performance of the proposed approach is compared with two state-of-the-art techniques such as SecCloud and CloudZone. SecCloud is meant for providing security and privacy for the cloud stored data. CloudZone is a multi-agent system architecture that works on the integrity layer of the cloud data storage.

This chapter not only analyses the execution time with respect to the count of vulnerabilities, but the F-measure analysis is also presented. The F-measure analysis is the evidence for the better reliability of the proposed framework.

The framework is not analysed in terms of OS, web applications and network based vulnerability assessments. In future, this work can be extended by analysing these scenar-
ios. The test experiments are carried out in a computer system with 16 GB RAM and 7th generation Intel core processor with 4 MB cache, 3.5 GHz.

6.3 PENETRATION TESTING

Penetration testing is to measure the robustness of a security mechanism in subjection to security breaches. This work utilizes Metasploit to have viruses and Trojans. The main intention of this testing is to figure out the count of viruses and Trojans being detected by SuVa during the process of data migration.

Table 6.1: Vulnerability Detection Analysis

<table>
<thead>
<tr>
<th>Performance Measures</th>
<th>Cloud Zone</th>
<th>Sec Cloud</th>
<th>SuVa</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability Detection</td>
<td>568</td>
<td>1600</td>
<td>1938</td>
</tr>
</tbody>
</table>

Table 6.1 displays the vulnerability detection analysis, in which the performance measures for the vulnerability detection for number of counts of vulnerabilities detected has been presented for all three scenarios of CloudZone, SecCloud and SuVa Security Framework.

For test purposes, vulnerability has been introduced with 2000 different viruses and Trojans to the data before the start of the data migration. The Figure 6.1 shows the count of viruses and Trojans detected by SuVa Security Framework and the results are compared.

On analysis, it can be observed that the SuVa Security Framework detects the maximum count of viruses and Trojans. Though CloudZone and SecCloud are developed for providing security to the data storage, this work just employed them during data migration.
On the other hand, CloudZone is the least performer and SecCloud is a potential competitor to SuVa Security Framework. During the process of experimentation, CloudZone could detect 568 viruses and Trojans and SecCloud was able to capture 1600 viruses and Trojans. The proposed SuVa framework detects around 97% of the viruses and Trojans and the exact count is 1938. Hence, the potentiality of SuVa Security Framework is proven with the greatest count of detected viruses and Trojans.

6.4 EXECUTION TIME ANALYSIS W.R.T VULNERABILITY DETECTION AND DATA VOLUME

In this session, the SuVa Security Framework’s execution time analysis of detection of vulnerabilities and its performance with the data volume has been compared with both Cloud-Zone and SecCloud. Note that only for the first time while uploading the time taken is more than normal.

6.4.1 Execution Time Analysis SuVa Security Framework

Next intention is to check the execution time of the security framework to detect the viruses and Trojans, which is discussed above. The execution time analysis is presented in the below given Figure 6.2.

It is great to observe that the proposed SuVa Security Framework has detected the
maximum count of viruses and Trojans, however the time it takes to detect the viruses and Trojans is equally important.

Table 6.2: Execution Time Analysis

<table>
<thead>
<tr>
<th>Performance Measures</th>
<th>Cloud Zone</th>
<th>Sec Cloud</th>
<th>SuVa</th>
</tr>
</thead>
<tbody>
<tr>
<td>Execution Time w.r.t Virus and Trojan Detection (ms)</td>
<td>458</td>
<td>210</td>
<td>148</td>
</tr>
</tbody>
</table>

The reason is that the maximum time consumption for virus detection results in maximum energy consumption and reduces the Quality of Service (QoS) as well. A security framework can be considered optimal, when it can detect the maximum count of viruses and Trojans in a minimal amount of time. From the Table 6.2 of time analysis, the performance measures for the execution time with respect to viruses and Trojan detection (ms) against the CloudZone, SecCloud and SuVa Security Framework is being analyzed.

Figure 6.2: Execution Time Analysis

On analysis, it is proven that the SuVa Security Framework consumes lesser period of time to detect the viruses and Trojans, as the framework employs different entities to perform different functionalities. This way of work distribution helps in minimizing the execution time. On comparison, CloudZone consumes the greatest time to detect viruses and Trojans, which is 458 ms.
SecCloud follows the CloudZone with 210 ms and finally, SuVa Security Framework proves 148 ms to detect viruses and Trojans, with regard to the total execution time of 500 ms. Hereby, it is proven that the SuVa Security Framework consumes lesser time to detect viruses and Trojans, which in turn reduces the computational overhead and energy consumption.

6.4.2 Time Analysis w.r.t Data Volume of SuVa Security Framework

In addition to this, this work analyses the execution time of the security frameworks by varying the volume of data. In order to analyze the work efficiency of the security frameworks, the volume of data is varied between 10 and 50 GB. The execution time analysis with respect to the volume of data is presented as follows.

Table 6.3: Execution Time Analysis w.r.t Data Volume

<table>
<thead>
<tr>
<th>Data Size (GB)</th>
<th>10</th>
<th>20</th>
<th>30</th>
<th>40</th>
<th>50</th>
</tr>
</thead>
<tbody>
<tr>
<td>CloudZone</td>
<td>2100</td>
<td>2987</td>
<td>3379</td>
<td>4176</td>
<td>5093</td>
</tr>
<tr>
<td>SecCloud</td>
<td>1890</td>
<td>2493</td>
<td>2978</td>
<td>3398</td>
<td>4358</td>
</tr>
<tr>
<td>SuVa</td>
<td>1236</td>
<td>1867</td>
<td>2354</td>
<td>3104</td>
<td>3876</td>
</tr>
</tbody>
</table>

Table 6.3 presents the experimental results of execution time analysis with respect to varying volume of data. The table clearly shows that SuVa consumes lesser period of time, when compared to the existing approaches, in spite of varying volume of data. The maximum time being consumed by SuVa is 3876 ms for handling 50 GB data, whereas the CloudZone and SecCloud show 5093 and 4358 ms respectively. The time gap clearly shows the efficiency of SuVa.

Figure 6.3 analyses the execution time of the security frameworks with respect to the volume of data. It is obvious that the execution time increases along with the data volume. However, the time gap between the security frameworks has to be noted. Among the three security frameworks, CloudZone consumes more time to deal with different volumes of data.
The range of execution time for the data volume between 10 and 50 GB for CloudZone is 2100 to 5093 ms. Secondly, the SecCloud framework shows the execution time between 1890 and 4358 ms. Finally, the proposed SuVa framework proves the execution time of 1236 to 3876 ms for different volumes of data.

The time difference between SuVa and CloudZone to handle 50 GB of data is 1217 ms. Similarly, 482 ms is the execution time difference between SuVa and SecCloud for tackling 50 GB of data. From the experimental results, it is evident that the SuVa consumes lesser period of time to handle different data volume.

Furthermore, the time gap between the proposed and the existing security frameworks is more. Preferably, a security framework should show minimal execution time. The reason-able execution time conserves energy and other resources along with the enhanced QoS. By showing minimal execution time, SuVa once again proves its efficiency.

Table 6.1, Table 6.2 and Table 6.3 illustrates all the performance measures along with the attained experimental results. From this table, it is evident that the proposed SuVa proves its best in all the performance tests. The SuVa detects the maximum viruses and Trojans, which is 1938 and is incomparable with the existing approaches. To our surprise, the time consumption to detect the maximum count of viruses and Trojans is the least.

The comparative techniques detect minimal number of viruses and Trojans at the cost of more time. However, SuVa consumes lesser time to detect the greater count of viruses and Trojans. Additionally, SuVa shows the greatest precision, recall and F-measure values, when
compared to the analogous approaches. The following Table 6.2 illustrates the execution time of the security frameworks with respect to the data volume.

6.5 F-MEASURE ANALYSIS

F-measure is a standard performance metric that can validate the results obtained. The F-measure relies on precision (P) and recall (R). Precision is measured by the correctly detected security breach to the total count of detected vulnerabilities. Recall is another measure that is computed by count of correctly detected vulnerability to the total count of vulnerabilities being found actually.

\[
F_M = \frac{2XPXR}{P+R} \quad \text{-- (1)}
\]

\[
P = \frac{\text{Correctly detected security breach}}{\text{Total count of detected vulnerabilities}} \quad \text{-- (2)}
\]

\[
R = \frac{\text{Correctly detected vulnerability}}{\text{Total vulnerabilities introduced}} \quad \text{-- (3)}
\]

When a system proves itself with maximum F-measure is considered to be more effective. F-measure is to measure the quality of the proposed approach. Hence, the greater the value of F-measure, the better is the quality of the system. The F-measure values are presented below.

Table 6.4: Vulnerability Detection Analysis

<table>
<thead>
<tr>
<th>Performance Measures</th>
<th>Cloud Zone</th>
<th>Sec Cloud</th>
<th>SuVa</th>
</tr>
</thead>
<tbody>
<tr>
<td>Precision (%)</td>
<td>38</td>
<td>45</td>
<td>100</td>
</tr>
<tr>
<td>Recall (%)</td>
<td>25</td>
<td>34</td>
<td>99</td>
</tr>
<tr>
<td>F-Measure (%)</td>
<td>30.15</td>
<td>38.73</td>
<td>99.44</td>
</tr>
</tbody>
</table>

From the Table 6.4 F-measure Analysis it clearly shows the performance measures of precision, recall and F-measures of CloudZone, SecCloud and SuVa Security Framework and can clearly see that SuVa Security Framework’s is performed well in all three precision, recall and F-measure performances.
The F-measure and quality of the system are directly proportional to each other. The F-measure analysis prove that the SuVa framework shows the greatest precision and recall values, which in turn improves the F-measure value. The precision and recall value being shown by the CloudZone is 0.38 and 0.25 respectively. Similarly, SecCloud proves 0.45 and 0.34 as its precision and recall values.

The SuVa framework proves its efficiency with the greatest precision and recall values, which are 1 and 0.99 respectively. The precision and recall values reflect in the F-measure values and hence, the SuVa framework shows the maximum F-measure value, which is 0.997 and is followed by SecCloud with 0.38. Here, a huge gap between the values can be noticed. Hence, SuVa is superlative, when compared to the existing cloud security frameworks. Finally, the experimental results are tabulated in Table 6.4 for detailed results.