6. CONCLUSION

Creation of web pages as that of legitimate web page is known as phishing pages. Since phishing pages are almost similar in content and page image are as that of original page. Introduction of such fake pages into the internet resources pose a threat of loss of personal confidential data and financial loss to the users.

To overcome this internet crime, computer research workers have been finding several ways for their prediction and prevention. However new methods are not reliable or has not accurate in its functional aspects. In addition to the above burden, the phishers are also developing new ways of constructing fake pages to betray the users.

In view of the above constrain a research is attempted in this present work to develop a classifier for the prediction of phishing page and a new novel multilayer security authentication for prevention of phishing pages.

About 2700 web pages (2000 phishing and 700 legitimate pages) are analysed and most important sixteen pages characteristics are extracted. A synchronized feature vector is constructed. Three different values (-1, 0, & 1) are given to the sixteen page features. Classification of pages performed on the principle of neural network.

An algorithm of stepwise procedure is adopted to recognize the phishing pages as well as the legitimate pages. The predictive efficiency is tested with the confusion matrix concept. The result has yielded 99.6% accuracy and 0.4% error rate. In order to
rectify this error a multi level security authentication with small mathematical equation evaluation is proposed along with other conventional methods.

The results obtained in this present work are corroborated with earlier findings on the neural network classifier. However the modification is brought out high predictive accurate value (99.6).

It is desirable to undertake much more clear analysis with real online data to ascertain the new novel authentication as an extension of the present study.