7. CONCLUSION AND FUTURE WORK

Measurement is important in any engineering discipline. Software Engineering can be no exception. Metrics are quantitative indicators of some attribute of a software. Metrics can be of great aid to the Software Engineer and the project manager. Security Metrics are quantitative indicators of the amount of security present (or absent) in software. Security Metrics can be of great aid to Software Engineers and Security Professionals in their endeavor to create Secure Software.

In this regard, the research first investigated the applicability of existing metrics for measuring Software Security. The research proposed an enhancement to the Adaptive Vulnerability Analysis technique with Mutation Testing which improves the accuracy of the Security Metrics derived from the technique. These metrics are based on the dynamic or run-time behavior of the program.

The research also proposed a set of security metrics that are based on the static characteristics of the source code. The validity of the proposed metrics was established through an experimental study conducted on 3 running web applications.

Finally the research proposed a Genetic Algorithm for identifying the subset of metrics that are most effective in identifying the Security of the Software and found that the AccessSpecifier Metric, The Validated Parameters Metric and the Sensitive Data Accessed Metric were the most effective in indicating the Security of the Software.
As a part of future work, Security Metrics pertaining to the other phases of Software Engineering – Analysis & Design, can be developed and their effectiveness in measuring Security investigated. These metrics that can be derived early in the Software Life Cycle can be of greater utility to the Software Engineer in assessing the Security of the Software being engineered.