Name of Scholar: **Rajendra Kumar**

Name of Supervisor: **Prof. K. Mustafa**

Department: **Computer Science**

Title of Thesis: **Development of Security Requirements for Web Applications**

ABSTRACT

The importance of Requirements Engineering as a branch of Software Engineering is now well recognized. The prime reason behind this recognition is the opinion of industry as well as academia that about 70% of the projects fail due to problems in requirements phase. On the other hand, security is a burning issue and it has become not only the requirement but a necessity for the software industry. Keeping in mind both the vibrant issues, it becomes essential to take care of security related aspects as early as possible in the development life cycle. Requirements phase is the foremost opportunity for the same. The right approach should be to incorporate security requirements and the corresponding mechanism for achieving them. It is very necessary to incorporate the security requirements for building a secure software.

In the present scenario, web applications play a great role in different domains due to its useful efficiency. Due to the sensitivity and importance of these applications, security is at high demanding rate. Keeping in mind these issues, it becomes significant to have a framework/model/roadmap to develop security requirements for web applications. Studies reveal that various approaches are underway to propose security requirements but the methodology through vulnerabilities analysis and their impact on security attributes is high demanding and especially for web applications. It is also revealed that the existing methodologies are not enough and there is a sufficient scope to propose a prescriptive methodology for developing security requirements of web applications. Hence, research is accomplished for the development of such a framework in the light of the existing literature and studies. The current research has three major areas, our proposal: ^{S}RDF, validation data, and interpretation of results.

The first component is the identification and classification of web application related security vulnerabilities on the basis of existing databases viz. OWASP, WASC, SANS, CWE, and CERT-In. These vulnerabilities are the most common one in the web applications. Afterwards, classification of these identified vulnerabilities is done on the basis of globally accepted security attributes namely Confidentially, Integrity, Availability, Likelihood of Exploit and their Time of Introduction. This classification may be useful for analyzing the impact of a particular vulnerability on its various related attributes.

The second component is the severity determination of these identified vulnerabilities. Based on the aforementioned attributes, severity is assessed with the help of statistical formulation. An expert's feedback is also taken to apply the regression analysis. Finally, a mathematical formulation was established to assess the severity.

In the third major component, a prescriptive framework, ^{S}RDF has been proposed. To address the security related issue from the beginning in the SDLC, it is necessary to integrate security in the requirements phase. As discussed above, in the absence of a framework for the development of security requirements especially for web applications, ^{S}RDF may be useful. A structured representation model of security requirements has also been proposed that may be considered a major contribution. ^{S}RDF has been validated by tryouts on five SRS's of the live industry projects namely, Web Store System (WSS), Smart Government (SGovt.), Online Bidding System (OBS), Personal Investment Management System (PIMS), Online Medical Consultancy (OMS). The results obtained by using ^{S}RDF are also compared with the final results/recommendations of the industry and these are found to be highly similar to the results obtained by using ^{S}RDF.

It appears to be an evolving process as new vulnerabilities and their corresponding security requirements shall be identified. Therefore, extension/modification and proposal of new security requirements may also be done. In future, new vulnerabilities and security requirements must be added in ^{S}RDF. A software tool may also be developed for the automation of complete process. Future contributions on the similar line will be required to be compared and discussed the results in the light of our proposal, ^{S}RDF. This work may provide guidance to the industry as well as academia for developing more secure software.