EVALUATING SOFTWARE SECURITY THROUGH QUANTUM TECHNIQUES

Abstract Submitted to the
Babasaheb Bhimrao Ambedkar University, Lucknow
in Fulfillment of Requirement for the Award of Degree of

Doctor of Philosophy
in Information Technology

BY
Mohd. Nadeem
Enrollment No. 1525/19

CO-SUPERVISOR
Dr. Rajeev Kumar
Assistant Professor at Centre for Innovation and Technology, Administrative Staff College of India, Hyderabad, Telangana

SUPERVISOR
Professor Raees Ahmad Khan

Department of Information Technology
School of Information Science & Technology,
Babasaheb Bhimrao Ambedkar University, (A Central University)
Lucknow, Uttar Pradesh-226025

2022

ABSTRACT

In the exponential growth of computing in the era of quantum computers, the security of software is the main objective in the field of Information Technology (IT) and Artificial Intelligence (AI). Dependency on software is so high that life cannot be imagined without them. Information, no matter to which part of the globe it belongs, is available with a click of the mouse. Intensive security-oriented services ranging from internet banking, and trading to online, buying and selling, booking an appointment with a doctor etc., are carried out unhesitatingly. These services require the privacy of the information and asset. Security-intensive information is floating everywhere anyone having malicious intent can misuse the information. This may harm an organization or individuals. For decades, efforts are being made to evaluate security in order to increase accountability, demonstrate compliance, and determine whether and by how much our investment in the product makes our systems more secure.

A quantum enabled security techniques gives several method or algorithms to ensure software security. Software security evaluation is a vital factor in assessing, administrating, and controlling security to improve the nature of security. It is to be realized that assessment of security at the early stage of development of software helps in identifying security loopholes in the software. This thesis states the definition and characterization of quantum computing techniques, software security factors, attributes of security, Fuzzy Analytic Network Process (F-ANP), and Fuzzy Technique for Order of Preference by Similarity to Ideal Solution (F-TOPSIS).

In order to gain a competitive edge, developers and researchers need to create a viable security assessment framework so as to minimize critical software security failures. Though it is highly

difficult to create a perfectly secure software system, but one can surely reduce the security by following a fool-proof and meticulously designed strategy with the inclusion of security attributes. In addition to this, the researcher has made an effort to overcome this issue and proposed a framework to assess the security of software in the era of quantum computers. This thesis presents a framework that incorporates five phases, including Factors Identification, Mapping, Assessment, Statistical Analysis, Review and Revision.

In this thesis, software security is evaluated by the different quantum techniques of security. The impact of security factors and their attributes are evaluated by the F-ANP and F-TOPSIS. Quantum computer innovation indicates the advent of a large qubit-based quantum computer in the future. Since the security mechanism of software can be solved by quantum computers, the present security mechanism would be rendered obsolete. Hence, it is imperative to focus more on intensive research in the context of the present quantum enable security techniques. The security of software is depending on the factors their attribute that may affect the security in the era of the quantum computer. The security factors of software are such as Confidentiality, Integrity, Durability, and Availability, further, we classified it in its attributes. The intention of the evaluation of the impact on security in the quantum era is to estimate and access the security of software.

The results obtained and the route used in this evaluation would sustain future researchers and developers in organizing software security in the presence of a quantum computer. The developers are constantly working on techniques that would ensure an ideal blend of highly user-friendly software with the desired level of security. The present evaluation of software security in the era of quantum computer investigation intends to posit feasible solutions that would overcome the gap between software securities, thereby providing far enhanced security of software services. Various research

studies have been done on software security assessment to bridge the security gap. The quantitative assessment of software security is validated by the Wilcoxon rank test. The quantum enables security techniques are considered as alternatives. However, there are very few research endeavours that are currently based on using the integrated approach of Fuzzy-ANP with the Fuzzy-TOPSIS method for assessing software security.

To address this research possible, the present empirical study assesses software security by using the quantum computing approach. The attributes considered for the assessment are four factors at the first level, and thirteen attributes of security at the second level with six quantum computing techniques as alternatives. F-ANP has been applied for estimating the weights of the attributes and their relationship with one another. Finally, the F-TOPSIS technique has been applied and alternatives ranking has been estimated. The results of the study conclude that LBCA-1 provides better software security. Furthermore, as analyzed, F-TOPSIS produced more convincing results in assessing the software security of the quantum computing technique. This research analysis also corroborates that when compared with the Classical ANP TOPSIS. The sensitivity analysis validated the results of the evaluation.

It is apparent from the validation of the proposed framework that it may be significantly helpful to keep in check the security of software from the early phase till the end. The proposed framework has shown satisfactory results with respect to other mentioned approaches. It may also form the basis for the development of new modified or refined approaches. Like any other research, the current work may also suffer from certain limitations therefore to achieve a generalized result further study may be conducted on a large scale.