ABSTRACT

Security of user's information is at risk, as the increasing use of software makes it important to use software in every field. Nowadays, it is easy to build and use the software but to maintain its security is not an easy task because organizations are facing numerous issues related to security services of software. This introduces an urgent need to address security issues as security failure may lead to disastrous effects on human lives. Complex operations, rising cost, resource constraint, and a future of strategic uncertainty demand that software must deliver higher security with reducing cost. This will help in building software that will actually be able to defend itself from attacks despite being dependent upon any application security software (say, *antivirus*) for its protection against threats. The basic cause of the maximum of the security breaches is the presence of loopholes in the end product. The early detection and correction of these ambiguities may help reduce the occurrence of such attacks. In order to reduce the occurrence of security violations, it becomes indispensable to address the security issues during software development life cycle. Software developers are trying their best to achieve higher security of software. But, security of software is still not at its best. In addition, organizations are demanding optimal maintenance of security during working life of software services.

To fulfil the organization's demand, practitioners are always in search of better ways to manage security services for long duration. There is no straight forward solution available for problems of improving life span of security. Further, practitioners are trying to achieve durable software but unfortunately, they are ignoring the concept of security durability. Without a deep research of security durability, there is no way to get durable performance of software. If durable software is not secure then user will loss his/her trust on software. That is why, security of software is as much important as software durability. Hence, this makes the efforts of developing durable software worthless. After thoroughly reviewing literature, it is found that there is no work available in the area related to security durability assessment. With the critical examination of literature survey and best practices, Security durability is defined *as the duration during which the software performs securely*. Without paying attention on security durability, the software may start failing after deployment. Further, ignoring security durability may badly

affect service life of software. In addition, less durable security of software is likely to fail in the market.

It can be analysed that assessment of security durability is a significant step to improve the security, and without its consideration, potential of CIA (Confidentiality, Integrity and Availability) cannot be enhanced for a specific time period. Assessment of security durability is not possible without understanding the relation between security and durability. Further, durability of security services depends on budget and maintenance time. If it is possible to assess the durability of security services, the cost and time of maintenance would have been optimized. Security services of software must be longer with optimal maintenance as insecure services of software will gravitate to the insecure alternative. Security durability assessment is an important step towards improving durability of security as well as software services. Further, security durability measures may include one or more factors or attributes in it. To evaluate the security durability of software, there is need to assess the attributes which are related to security durability, directly or indirectly. In this row, the current research is done with three components in it, which are; development of framework, implementing the framework and assessment and third component is validation,done empirically as well as theoretically.

The first component referred to the development of the framework to identify security and durability attributes and its sub-attributes that affects security life span directly or indirectly. Correlate these attributes in order to assess the security durability of software. A framework for security durability assessment has been accomplished through the literature survey, gathering opinion from the practitioners, needed development, validations and revisions. The conceptualization phase is a brainstorming activity to precisely understand the problem and to gather related facts. Planning provides the roadmap to the design based on information from conceptualization phase. Designing is the most important and critical step towards the development of security models. Validation provides the supporting evidence as to whether a measure really captures the internal attributes that it purports to measure. Review and Revision phase facilitates the activity of ‘look back and change’, if required with a free-to-entre option to any of earlier phase.

The second component of the study is to implement the proposed framework for security durability assessment. In order to provide the significant and improved measurement of security durability, it is required to relate the durability attributes and desirable security attributes. Researcher establishes a correlation between durability and security attributes using Multiple Criteria Decision Analysis (MCDA) or Multiple Criteria Decision Making (MCDM) technique. Both hybrid and classical methods are used for assessment in this study, because, decision making process is a complicated phenomenon. Entrance Examination Software for Babasaheb Bhimrao Ambedkar University (A Central University), Lucknow, India (BBAU Software) is examined for assessing security services throughout the research work. Security services of BBAU Software are very crucial and important due to sensitive information of online entrance exam. The results of security durability assessment may help developers to improve longevity of secure software after development. Security durability consideration might help in reducing the maintenance effort incurred on security life span of software services.

The third component of the study is to confirm that how developed security durability assessment model is helpful for improvement of security life span of software services. Suggestions/rules/procedures are essential activities during development for improving the security service life span. It promotes the reengineering measures for improving working life of security as well as software services. The researcher made an effort in this regard to develop suggestions for longer security services. The given suggestions are helpful to manage security for longer life span. The proposed model calculates the security durability and revised version of BBAU Software is being influenced through suggestions. Sensitivity analysis analyzed to show the variations in results due to changing in values. Further, the validated results of statistical analysis with case study that reflect the usefulness and acceptability of developed model and suggestions is tested with hypothesis testing. The null hypothesis is strongly rejected on alpha level of significance for two tailed test. Hence, alternate hypothesis at a very good level of significance are accepted for improvements of security service life span.

This research work is done in the area of security life span and security is one of the biggest concerns in today's era. Software organizations need to focus on this area to get long-term performance of secure software with low maintenance cost. Therefore, developers need to focus

on secure as well as durable software. The study will help developers to improve the security for long life span. Further, the technique may be helpful for assessment in other areas.