MANAGING SECURITY RISK OF HEALTHCARE WEB APPLICATION: A DESIGN PERSPECTIVE

Thesis submitted in fulfilment of the requirement for

the degree of

Doctor of Philosophy

IN

INFORMATION TECHNOLOGY

Submitted by

Syed Anas Ansar

Supervised by

Prof.Raees Ahmad Khan

Co - Supervised by

Dr. AmitabhaYadav

Submitted to

DEPARTMENT OF INFORMATION TECHNOLOGY

BABASAHEB BHIMRAO AMBEDKAR UNIVERSITY

(A CENTRAL UNIVERSITY)

VIDYA VIHAR, RAEBARELI ROAD,

LUCKNOW – 226025, UTTAR PRADESH, INDIA

AUGUST 2021

ABSTRACT

The modern world is critically reliant on a broad range of software applications. Dependency on software applications 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, trading to online, buying and selling, booking an appointment to a doctor etc., are carried out unhesitatingly. These services require the privacy of the information and asset. When security intensive information is floating everywhere, anyone having malicious intent can misuse the information. This may harm an organization or individuals. Since decades, efforts are being made to estimate security risk in order to increase accountability, demonstrate compliance, and determine whether and by how much our investments in the product make our systems more secure.

Furthermore, the health sector is one of the most prime sectors where all the hi-tech applications are used. In this sector, medical personnel are entrusted with a vast number of responsibilities, and dealing with them is a more sophisticated as well challenging task. The healthcare sector has been linked to the technological world in order to ease the responsibilities as well as workloads of the healthcare staff. This was made possible by integrating IT (Information Technology) into the healthcare sector. Apart from these technological advancements, several statistics have demonstrated data breaches instances that have affected both, i.e., patients and Healthcare Information Systems (HISs). Thousands of healthcare records can be compromised by security breaches.

In addition, to secure an individual's as well as HIS's data, three major security factors and privacy goals are needed, which is commonly known as the CIA triad. The significant necessity of the CIA trio is;

confidentiality must be included for highly sensitive data, integrity is important because it may be fatal to provide an inaccurate procedure based on faulty data of medical, and availability is necessary because the data must be available on time for adequate treatment.

In the healthcare web application, the privacy of individual and organizational data is extremely important, and currently it has become a major challenge to shield healthcare information. The major challenge introduced in the healthcare web application is due to huge data growth. Furthermore, COVID-19 (i.e., the current pandemic situation) has resulted in an unexpected spike in healthcare data, which has impacted both the healthcare web applications and hospitals. Managing these healthcare data and securing it from intruders has become a complex task for security experts. Nowadays, the main objective of the researchers and security experts is to minimize security vulnerabilities in the healthcare web application by mitigating and assessing the security risk factors. So, some dedicated steps are required to enhance the security of healthcare web applications, which may help in securing and protecting them in order to ensure transparency and assess security risk. This is why security professionals prefer to take a step up on the design phase to reduce security risks. It will assist in designing secure web applications in the healthcare sector. Furthermore, it may also assist in overcoming from threats and protecting it from cyber-attacks by early detection and mitigation of security risk factors in the design phase.

In order to gain a competitive edge, developers and researchers need to create a viable security risk assessment framework so as to minimize critical healthcare web application failures. Though it is highly difficult to create a perfectly secure healthcare web application system, but one can surely reduce the security risks 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 security risk of the healthcare web application. This framework incorporates five phases, including Factors Identification, Mapping, Assessment, Statistical Analysis and Review and Revision.

The first phase, i.e., Factors Identification, in which the identification and selection of security risk factors as well as their corresponding security attributes have been made on the basis of a comprehensive literature review and expert's opinions. The relationship among security attributes and security risk factors has been developed in the second phase. In addition, an integrated Fuzzy AHP-TOPSIS approach is used for security risk assessment in the third phase. Where Fuzzy AHP is used to prioritize security risk factors, and the impact of security attributes on various alternatives is calculated with the help of Fuzzy AHP-TOPSIS. Furthermore, sensitivity analysis and empirical validation are carried out in the second last phase of the framework. In the last phase, review and revision will be undertaken only when required, which facilitates a retrospect of the entire development activity and aid in making changes whenever necessary.

It is apparent from the validation of the proposed framework that it may be significantly helpful to keep in check the potential risk and vulnerabilities from the early design 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 and implementation of the proposed model, further study may be conducted on large applications.