CHAPTER 8
Concluding Remarks

The thesis covers some of the research investigations towards the improvement in developing secured software product. It includes understanding the need for security to be considered from pre-development stage. The thesis also focuses on developing framework and mechanism for incorporating security throughout the development process, with special focus on gathering security requirements and lastly security metrics that acts as control mechanism for the various software development stages. We summarize the following important conclusions:

1. We have classified security into various dimensions at six hierarchical levels. At level 1, security is classified as hardware security, logical security, and security management. Further, the security at level 1 has been classified into 5 levels ranging from level 2 to level 6 to achieve parent level security. Based on the classification, various security domains have been identified such as application and system software security, communications security, server security etc. We then discussed various types of projects along with the security issues. It has been observed that software security is the key to secure the software systems followed by security management. Network security also plays a vital role in securing all the types of networked systems. Security considered during development mainly focuses on login, passwords and biometric identification. These mechanisms cannot provide right kind of security to the software systems leading to the importance of considering security throughout the development process. The classification can be beneficial to the management, development team and the administrators to focus on the key security aspects to secure the software systems.
2. To understand the umbrella of networks, we classified networks based on six dimensions namely, size, design, network architecture, organizational scope, computing models and topologies. The dimensions are further categorized hierarchically along with their security issues. We then attempted to identify the dominance of security during the development of software based on different types of networks on SDP. Moreover, the dominance is also identified by an empirical survey method. It has been revealed that there is more reliance on network security through secure configuration and perimeter defense. The security consideration during requirements gathering and maintenance phase has been low during the development of the software system. Developers largely establish login and passwords as the most common way of securing the applications. Securing the networks does not provide complete solution towards securing the system. It indicates the need to gather security requirements explicitly and plan security throughout the development process. The research domain shall be beneficial to system designers and developers to be concerned about security throughout SDP rather than relying only on network security.

3. Secured software development is mainly the concern of two aspects namely, technical and process management. We have analyzed the two aspects leading to techno-management view of security. The links of techno-management view indicate the need of misuse cases and attack pattern in gathering security requirements, assessment of reusable components and platform for security, metrics for secure development etc. It can be established that the links can bridge the gap between the technical and process management aspects of security. Further, we have attempted to develop security product security (SPS) framework for systematic inclusion of security throughout the development process. The SPS framework comprise of three layers viz. control, security aspect and development layer. The control layer focus on the
governance control, security aspects helps in identification of security features to be incorporated while development layer centers on secure development along with process management. The three layers shall support security concerns since the pre-development stage of software development. The SPS framework shall guide the development team in considering security holistically and systematically throughout the development process and analyze non-conformity, if exists. Besides, we formulated a mathematical model to identify security factor \( F_s \) of a product following SPS framework. It has been observed that \( F_s \) shall help evaluate and judge the security concerns throughout the software development process.

4. The first step towards secure implementation is by gathering security requirements. Our SSRGI being developed illustrates the various types of security requirements to be gathered namely, \( SFR \), \( Drivers \), \( FSR \), \( NFSR \), \( SDR \) and \( STR \). The security requirements can be gathered from the different roles such as customers, managers, designers, coders, and QA/ testers. SSRGI is then integrated in the SRS document so that the security requirements can be gathered along with the other functional requirements. Based on the case studies, it has been revealed that SSRGI promotes methodical gathering of security requirements. It is flexible and can be used for gathering security requirements for various types of software systems. Further, we developed SSDP that focuses on the security issues of each of the development phases. It also emphasizes on the actions and tools required to combat security issues during each of the development phases. It has been observed from the case study that SSDP considers security during SDP in a systematic manner. It can support the development team by taking into account various tools and techniques required throughout the development process.

5. The metrics acts as feedback mechanism to control the software development process. We investigated various security metrics
available in the literature. It has been observed that most of metrics could access security later in the development process or after deployment. Also, most of the process metrics do not provide enough details regarding implementation. Moreover, none of them focused on the security issues of the software development stages. Our research is based on the security consideration during software development stages. Thus, we developed metrics and effectiveness factors covering all the stages of SDP. The developed metrics may help the development team to reflect and measure security efforts during the development process. The usefulness of the developed metrics and the effectiveness factor has been judged with the help of case studies. Case studies revealed that security concerns for web-based software are moderately high as compared to client/ server based systems. The developed metrics shall support the development team to monitor security efforts throughout the development process.

There is a scope for enhancements in secured software development process. The classification of security can be extended to other types of software designed for mobile applications, embedded software, and real-time online games. Inclusion of risk management may further enhance secured SDP. The cost/ benefit analysis can be performed for implementation of security in SDP. Metric values can be segregated on the basis of type of software viz. on the basis of size, type (desktop, client/ server based, web-based etc.), and level of security required. This may provide benchmark for different kinds of software. The SPS framework can be enhanced to establish minimum security needs for different kinds of software. The work can be extended to identify the efforts required to include security in various types of software development methodologies and frameworks.