8

Conclusion

8.1 Summary and Conclusions

The rapid proliferation of smartphones that are equipped with a lot of features, multiple connections and sensors, it is vital to secure the mobile device and data from the vulnerabilities, threats and attacks. The goal of this research work is to provide better defensive mechanisms for security challenges of the low power resource constrained mobile devices. This chapter discusses the conclusion of this research work.

8.1. Summary and Conclusions

The chapter describes the discussed contents in the previous chapters and provides the summary of the thesis. In order to achieve the goal of this research work, a four-component methodology is proposed and defensive mechanisms are deployed. The proposed four contributions are based on accurate and improved user authentication, enhanced malware detection, secured data outsourcing to cloud storage and efficient search scheme over cloud storage. Based on the literature study, it is observed that the existing methods require few improvements for accurate authentication, enhancement in malware detection and data security over cloud storage. Moreover, there is no existing system to address all these challenges in a single stroke. Based on the above challenges, the proposed integrated, comprehensive approach focuses on providing mobile device security and data security together with better performance and computational complexity.

The proposed ***PCA-SVMED Method*** is introduced to authenticate the mobile device user. The unauthorized access to the mobile devices are restricted using improved iris biometric authentication. The false detection rate of authentication is reduced.

The proposed ***MSGP-MS Method*** is used to detect the presence of malware in mobile applications. The malicious applications are detected using optimized machine learning techniques to enhance mobile device security.

The proposed ***MSAES Method*** ensures the security of the outsourced mobile device data over cloud storage. The Mobile device data to be outsourced is encrypted using hybrid cryptographic algorithms.

The proposed ***RFMKS Method*** provides an efficient data retrieval mechanism in cloud storage. Encrypted Data retrieval is achieved using ranked fuzzy multiple keyword search scheme.

The proposed methods are implemented using Eclipse software in android v4.4 KitKat, Visual Studio 2013, Linux 3.10, Amazon EC2 cloud environment. The execution of the proposed method is evaluated using the parameters such as Computational Complexity in terms of time, False Acceptance Rate, False Rejection Rate, Accuracy, Correctly Identified Instances, Incorrectly Identified Instances, Mean Processing Time, Speed Up Ratio, Turnaround Time, Throughput, Search Time, Index Generation Time, Encryption Time and Decryption Time. The experimental results show that the proposed methods provide better results compared to that of the existing methods.

The recognition accuracy achieved by the proposed ***PCA-SVMED*** with 97% during detection and classification of iris biometric authentication. The proposed ***MSGP-MS***, Particle Swarm Optimization with Random Forest classifier has high correctly identified instances of about 88.4% when compared to Random Forest algorithm of correctly identified instances 86.8%. The proposed ***MSAES*** method achieves high efficiency when compared with other hybrid approaches. Finally, ***RFMKS*** method ensures efficient search results based on ranking. The combined four contributions provide the defensive mechanisms for mobile device security and data security with improved performance in accuracy and computational complexity in terms of time as well.