3

Proposed Methodology

As discussed earlier, increasing use of mobile devices automatically demands the requirement and integration of cloud computing on mobile devices. Mobile devices have constraints such as limited battery power, low memory capacity and processing capability, small screen size and narrow bandwidth. Because of the limitations of mobile devices, implementing mobile security solutions must address the following needs and challenges in building mobile device security and data security. The challenges faced by these devices are unauthorized access, vulnerabilities, data storage and retrieval. Though many solutions are available in the literature as discussed in chapter 2, there are no attempts so far made to design and develop a comprehensive approach to meet all the challenges in a single stroke method. Therefore, this thesis proposes an integrated and comprehensive approach to provide mobile device security and data security to address all the above challenges together with improved performance and minimum computational complexity.

Suitable defensive mechanisms are discussed to address the above challenges through

- Enhanced Biometric Iris Authentication in Low Powered Resource Constrained Mobile Devices.
- Enhanced Permission Malware Detection in Mobile Device Applications using Optimized Machine Learning Classifiers.
- Secured Outsourcing of Mobile Device Data over Cloud using Hybrid Cryptographic Algorithms.
- Efficient Search Scheme over Outsourced Encrypted Mobile Device Data in Cloud with Fuzzy Searching Techniques.

This chapter discusses the proposed research design to handle the defensive mechanisms for Authentication, Detection, Security and Privacy of Mobile Device Security and its Data Security.

3.1 Steps involved in the Proposed Methodology

The main focus of the thesis is to develop an Integrated and Comprehensive Approach to Mobile Device Security and Data Security. A Four - Component methodology is followed. The four significant components are: Improved and Accurate User

Authentication, Detection of Mobile Malware, Secured outsourcing of Data and Retrieval of Encrypted Data. The methodology proposed is shown in figure.3.1.

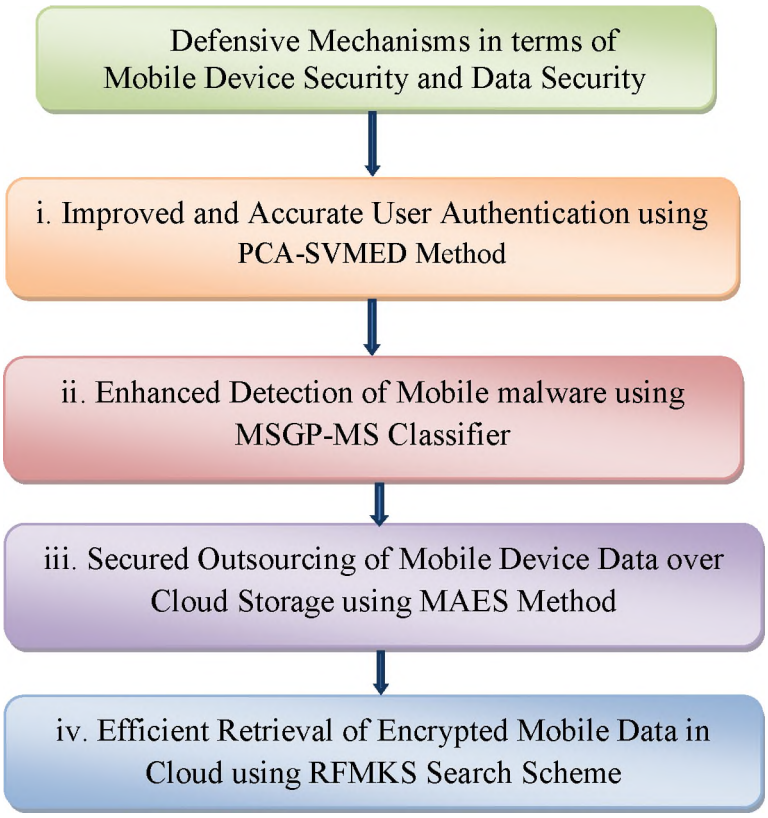

Figure 3.1 Proposed Four Component Methodology

Initially the real traces of data are collected from the communications between the devices and from different Internet web sources. The different techniques applied in the four-component methodology are explained below.

Step 1: Improved and Accurate User Authentication using PCA-SVMED Method

Restricting unauthorized access based on Iris Biometric authentication using the following methods

i. Rubber sheet model

ii. Colour Based Zero crossing transformation

iii. Principal Component Analysis

iv. Support Vector Machine with Euclidian Distance

Step 2: Enhanced Detection of Mobile malware using MSGP-MS Classifier

Enhanced Malware detection in Mobile Applications using optimized Machine Learning Classifiers by the following methods

i. K - means Clustering

ii. Classification based on J48, Classification and Regression Tree (CART) and Random Forest

iii. Particle Swarm Optimization with Random Forest

iv. Genetic Algorithm with Random Forest

Step 3: Secured Outsourcing of Mobile Device Data over Cloud using MAES Method

Secure Outsourcing of data to cloud through hybrid cryptographic algorithms using the following methods

i. Elliptic Curve Cryptography with Advanced Encryption Standard.

ii. Message Digest (MD5) with Advanced Encryption Standard.

iii. Message Digest (MD5) with Elliptic Curve Cryptography and Advanced Encryption Standard.

iv. Message Digest (MD5) with Rivest-Shamir-Adleman (RSA) and Advanced Encryption Standard.

Step 4: Efficient Retrieval of Encrypted Cloud Data using RFMKS Search Scheme

Secured ranked fuzzy multi-keyword searching on encrypted mobile data in cloud using the following methods:

i. Jaro Wrinkler Distance

ii. Sort Sorted index generation

iii. Fast Ranking

3.2 Specific Contributions of the Thesis

The entire research work is based on the four components. There are four research contributions following the four-step process. The significant contributions of the thesis is shown in figure 3.2.

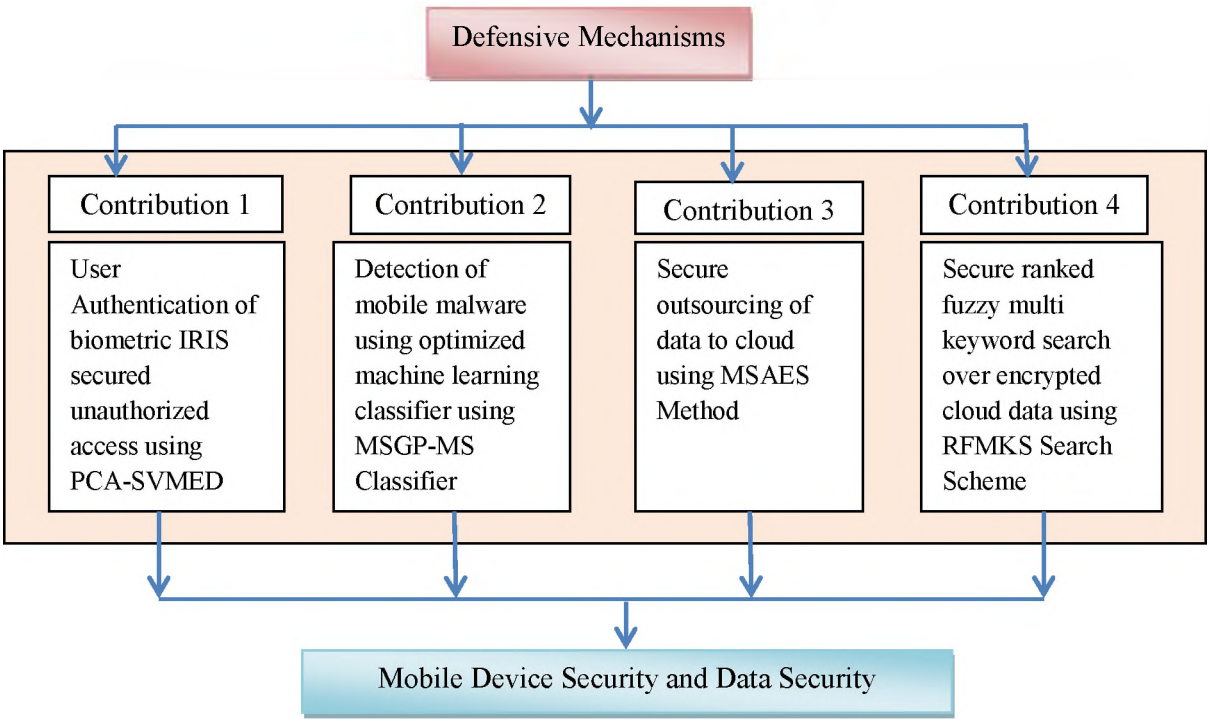

Figure 3.2 Contributions of the Thesis

The proposed work is designed to achieve mobile device and data security with improved performance with accuracy and computational complexity in terms of time. The proposed contributions detect the unauthorized access through iris biometric authentication, detection of mobile malware using optimized Machine Learning Classifiers Secure Outsourcing of mobile device data to cloud storage through hybrid cryptographic algorithms and Efficient Search scheme over outsourced encrypted mobile device data in cloud with Ranked Fuzzy Searching techniques. The consolidated view of the proposed methodology with the techniques applied and their outcomes is shown in figure.3.3.

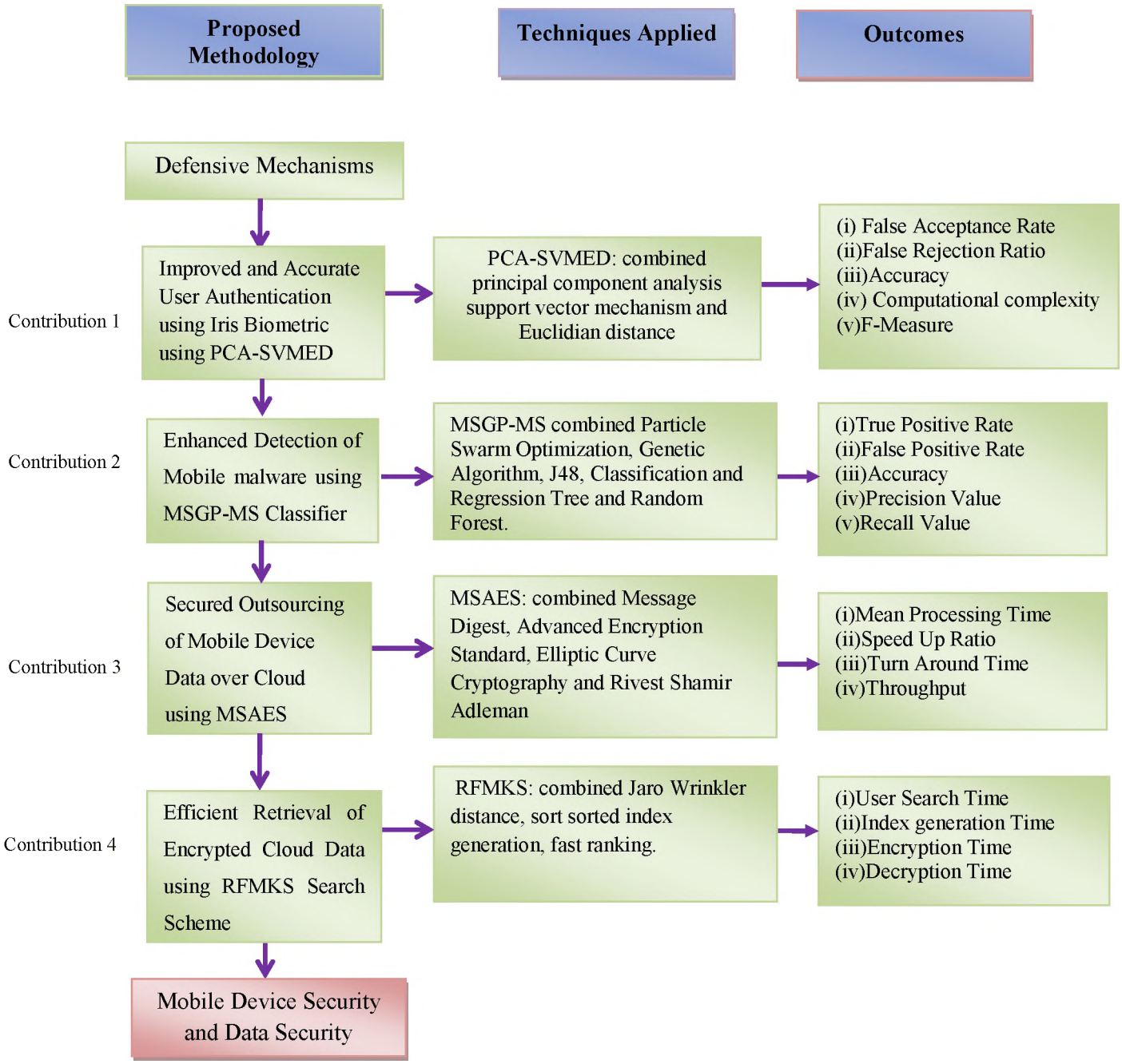

Figure 3.3 Consolidated View of the Proposed Methodology

The expanded view of the four major contributions of the thesis is shown in figure.3.4.

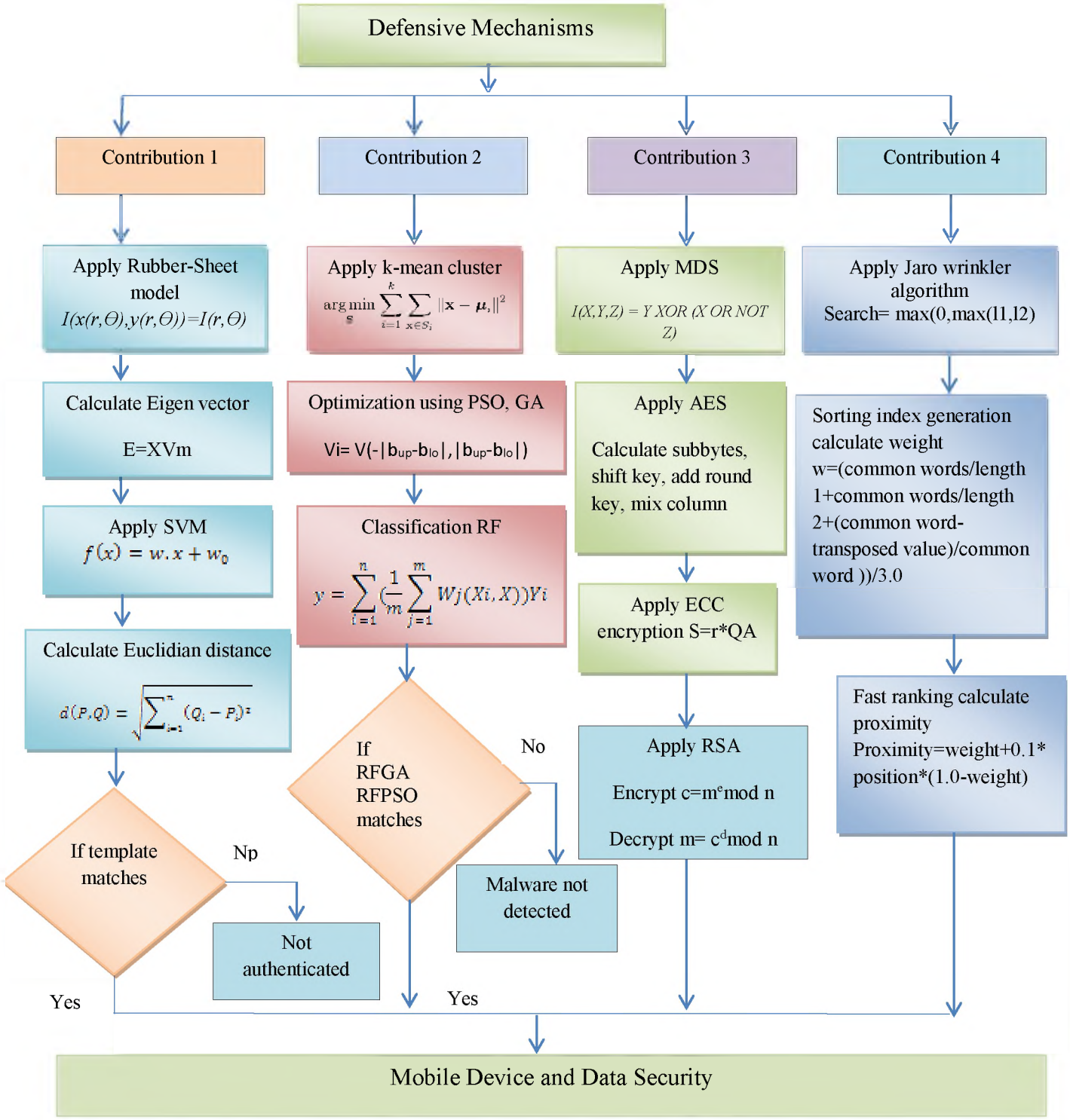

Figure 3.4 Technical details of Four Research Contributions

3.3. Chapter Summary

This chapter briefly discussed about the proposed Research Design. A Four Component Methodology is proposed to meet the objectives of the thesis. The entire research contributions are discussed in four phases based on the Four Component Methodology. The four major steps followed are discussed in detail. In the first contribution, namely the PCA-SVMED Method, an Improved and Accurate User Authentication is achieved by Iris Biometric in Mobile Devices. In the second contribution, namely the MSGP-MS Method, Detects the presence of malware in the Mobile Devices and it has higher accuracy in terms of correctly identified instances. In the third contribution, namely the MSAES Method, Secured Outsourcing of Mobile Device data to cloud storage is proposed which ensures higher efficiency when compared to other algorithms based on the mean processing time, throughput, speed-up ratio and turnaround time. In the fourth contribution, namely the RFMKS Method, Efficient Search scheme over outsourced encrypted data in cloud Storage is done and has better efficiency in terms of index generation and searching time.

The first and the second contributions, namely PCA-SVMED Method and MSGP-MS Method ensures the Mobile Device Security. The third and the forth contributions, namely MSAES Method and RFMKS Method promise the Mobile Device Data Security. All the four contributions are explained in detail in the forthcoming chapters.