ABSTRACT

Nowadays, smart phones have become an integral part of daily life. These have proven to be a scientific invention that fills personal and business needs in a very efficient manner. In this era, the availability of smart phones has significantly increased because of the rich variety of smart phones and essential applications provided by the manufacturers. There are 6.9 billion mobile users around the world, which is equivalent to 95.5% of the world's population, as estimated by the International Telecommunication Union till May 2014.

A smartphone is a mobile device that offers more advanced computing ability and connectivity than a contemporary basic feature phone. Based on this feature, smartphone user can develop any programs which are customized in specific needs. Furthermore, smartphone user can trade their assets like stocks or use banking service with wireless network. However, to provide these services, smartphone needs more private information than feature phone, thus, it is very important to keep smartphone secure. At the same time, numerous mobile device security issues and data privacy threats are challenging both manufacturers and users. Therefore, mobile devices are an ideal target for various security issues and data privacy threats.

In present, there are many researches on smartphone security, but there is lack of effort to analyze all security threats of smartphone. This work is needed for design of security solution, to prevent against environment, vulnerabilities and resource constrained issues of smartphone. This extreme level of comfort has brought with it an extreme number of security risks. Some of the major challenges are due to Authentication, Malicious Applications, Data Storage and Data Retrieval. To overcome these mobile security issues and data privacy over threats, vulnerabilities and attacks, an effective defensive mechanism is essential.

For authentication, biometric approaches (authentication/ verifications) in mobile device is explored, which reduces the security issues and data privacy threats. Biometric approach for authentication of the users is considered to be more beneficial as biometric mechanism involves the automated use of behavioral or physiological features to determine or verify identity. Among the various attacks, malwares are vulnerable because they accomplish malicious action after being installed in a user's mobile device

without the user's knowledge or approval. Mobile malware detection schemes are categorized into three groups: static analysis, permission analysis, and dynamic analysis. To be specific, permission based detection techniques extract security configurations and check the applications against its installation.

Considering the high usability features of Mobile Devices there is need to find solution for the limited storage of Mobile Devices. Storage capacity is a constraint for mobile devices. To enable mobile device users to access and store the heavy files on cloud through wireless networks. Mobile cloud computing is developed enable mobile users to store and access the large data on the cloud through wireless networks. During the period between uploading and downloading files (data), the privacy and integrity of files need to be guaranteed. Keeping in mind the resource limitation of mobile device and need to ensure the confidentiality of the critical data, introduces the cryptographic approach for secure data storage on Cloud.

Encryption is the most effective way to achieve data security. Sensitive data have to be encrypted before outsourcing in spite of the fact that, retrieval of encrypted data becomes an intriguing task. Although various searching techniques are used for retrieving the encrypted cloud data through keywords. Among them the Ranked fuzzy Multikeyword search scheme is secure and privacy preserving. Also, efficient data discovery and user searching experience needs to be enhanced. Based on the challenges by threats, vulnerabilities and attacks, the objectives of this research work are formulated after studying significant literatures.

A four-component Methodology is proposed with four contributions to meet the objectives of the thesis. The proposed Principal Component Analysis with Support Vector Machine and Euclidean Distance Algorithm PCA-SVMED enhances the accurate user authentication in the mobile device based on iris biometric. The detection and the classification of the iris authentication reduces the false detection rate and provides better template matching. The proposed MSGP-MS which is a combination of Random Forest classifier with Particle Swarm Optimization detects the presence of malware in mobile applications. The detection and classification of malware applications are done using optimized machine learning techniques which ensures security for mobile device and data. The proposed Message Digest signatures with Advanced Encryption Standard MSAES method secures the outsourced mobile device data in cloud storage. The hybrid

MSAES method provides confidentiality and integrity of mobile data. The proposed Ranked Fuzzy Multi-Keyword Search- RFMKS method is used for the efficient retrieval of the encrypted cloud data.

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, F-measure, Accuracy, False Rejection rate, False Acceptance rate, 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. In contribution one, the recognition accuracy achieved by the proposed **PCA-*SVMED*** with 97% during detection and classification of biometric iris authentication. The proposed ***MSGP-MS***, Particle swarm optimization has high correctly identified instances of about 88.4% than compared to random forest of correctly identified instance 86.8%. The proposed hybrid ***MSAES*** method achieve high efficiency when comparing with other approach. Finally, ***RFMKS*** method produce exact search results based on ranking. The four contributions based on Defensive Mechanisms provide an improved performance in accuracy and computational complexity in terms of time as well. The proposed integrated, comprehensive approach focuses on providing mobile device security and data security.