1 Introduction

The Smartphones and PDA's are powerful multifunctional devices capable of hosting a broad range of applications with Wi-Fi, Bluetooth, NFC and GPS capabilities for both business and consumer use. The inception of the smartphone era can be seen as the beginning of smart applications with the new millennium. Portio research estimates that mobile subscribers worldwide will reach 6.9 billion by the end of 2013 and 8 billion by the end of 2016. The forecast says that mobile subscriptions will reach 9 billion by 2017. On the other hand, a mobile device is still a resource constrained one due to limitations such as processing power, low storage, less security, unpredictable Internet connection and few applications generally demand more resources than a mobile device can pay for. [4] [26] [49] [59] [60].

Over the past few years, the usage of mobile devices to access data has becoming more frequent, and the usage of mobile devices in the applications such as web-browsing, email, multimedia, entertainment applications, navigation, trading stocks, electronic purchase, banking and health care are increasing. Therefore, device and data security is a major challenge. The need for efficient security solutions for mobile devices is essential with new functionalities.

1.1 Key Aspects of Mobile Devices

An effective mobile devices strategy requires strong security controls. The five key aspects distinguish mobile security from conventional computer security [59] [60].

- **Mobility**: Each device comes with us anywhere we go and therefore, it can be easily stolen or physically tampered.
- **Strong personalization:** Owner of device is its unique user.
- **Strong connectivity:** Smartphone enables a user to send e-mails, to check her online banking account, to access lot of Internet services in this way, malware can infect the device, either through SMS or MMS or by exploiting the Internet connection.
- **Technology convergence**: Single device combines different technologies may enable an attacker to exploit different routes to perform the attacks.
- **Reduced capabilities:** Smartphones are like pocket PCs, there are some characteristic features that lack on smartphones.

1.2 Research Motivation

Mobile device access becomes very important and it is critical to assure secured mobile transactions with data integrity and confidentiality. The major objective of Mobile device security is to protect mobile users and mobile based applications from unauthorized access and attacks. To overcome these problems of authentication, attacks, storage and retrieval a clear knowledge of mobile device threats are essential. The forthcoming sections explain in detail the threats with their vulnerable propagation of various types of attacks in challenging mobile device security.

1.3 Mobile Device and Data Security Challenges

The growth in the wireless technology and the improvement of mobile device usage is increased in the mobile market. The growth in the creation and maintenance of secure identities for mobile devices has created challenges for individuals, society and businesses particularly in mobile added value services like mobile banking, mobile check-in, mobile ticket, etc. and government security services. The below are some of the mobile device challenges.

Weak Authentication

Today, many applications rely on password-based authentication, as a single factor. The owners of these applications do not enforce strong passwords and the securing of valuable credentials. Thus, users expose themselves to a host of threats, including stolen credentials.

Mobile Browsing

Mobile browsing is the best feature of any mobile device for providing the best use of internet applications. However, normally in mobile devices, a user cannot see the entire URL or web address, making it difficult to determine whether the web address or URL is safe. Thus, browsing can be used as a phishing related attack.

Insecure Data Storage

A user can suffer a data loss after losing a mobile device or experiencing interruption by some malicious application that deletes a user's most valuable information. In this way, all users are at risk by engaging in this type of activity. Some common pieces of data are stored at high risk, including personal information.

Physical Security

Physically securing a mobile device is difficult, but when a mobile user is constantly using their mobile device (24×7×365) and it is lost, then the task becomes seemingly impossible. Obviously, physical security is the greatest concern for risk-free mobile devices. If a person's mobile device is lost or stolen, the user's sensitive data may be misused by a thief, including personnel information, unsecured documents, business data, and files.

1.4 Threats and Vulnerabilities

A comprehensive overview of threats and vulnerabilities shows that cyber criminals are now focusing increasingly on mobile devices. Mobile devices use many useful applications on the internet, which makes them a prime target for attackers to destroy security mechanisms and cause threats, spread vulnerabilities. This tendency underlines the need for additional mobile device security cognizance, as well as more flexible, better integrated mobile device security solutions and policies. Some significant mobile threats and vulnerabilities are described.

Threats

A threat, in the context of security refers to anything that has the potential to cause serious harm to the device [66] [84]. It may or may not happen, but has the potential to cause serious damage. It can lead to attacks on device, networks and more. Mobile threats are basically divided into four categories in terms of user perspective, service/content provider perspective, and network perspective, as listed below

- Application-based threats
- Web-based threats
- Network-based threats
- Physical threats

Figure 1.1 shows the various mobile threats as discussed below.

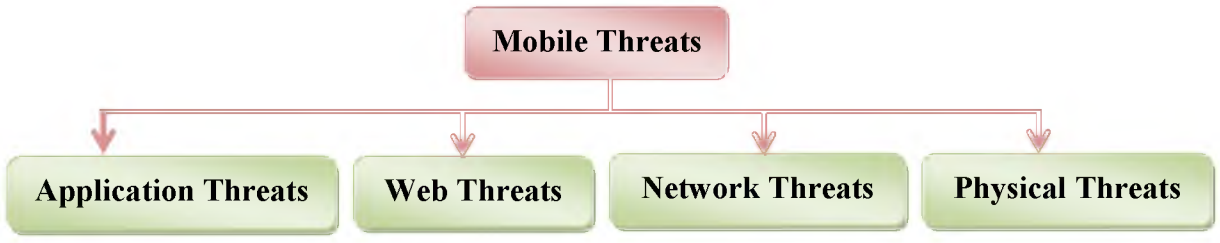

Figure 1.1 Different types of Mobile Threats

Application Based Threats

Many downloadable applications are available over the Internet, and most of these have multiple security problems. Malicious applications are available on websites, with the greatest concern being fraud or scams. Application-based threats can be classified as one or more of the following mobile applications [1][4][9].

Malware

Malware, a software accomplishes malicious action after being installed in a user's mobile device without the user's knowledge or approval. It can send unwanted messages and gives an attacker full control over the mobile device.

Spyware

This is designed to collect personal, private data without a user's knowledge or endorsement. Spyware-targeted data commonly include the user's location, contact list, private or financial photos, email address, browser history, and call history.

Privacy threats

Privacy threats can be caused by mobile applications in addition to malicious applications. An attacker or hacker can steal a user's information and identity, which can cause serious problems.

Vulnerable applications

Vulnerable applications are those applications that contain faults that can be exploited with malicious intent. They give an attacker permission to perform unwanted actions, access sensitive personal or business information, stop correctly performing activities, and download applications without approval.

Web-based Threats

In mobile devices, there are always mobile user's access web-based applications over the Internet [29]. Thus, threats related to such activity is a major concern, and some researches have proved that web-based threats are more serious problems for mobile devices. Some web-based threats are described below.

Phishing Scams

Phishing scams are a means of obtaining sensitive or business information from a user by representing oneself as a reliable unit using a link on a social networking website,

text message or email (spam) on a malicious website, or gaining information about login credentials.

Drive by Downloads

This is a concept involving the automatic download of an application when visiting a web page (malicious web address). When a user wants to see every downloaded item when clicking it, this causes the mobile device to become unstable. Thus, a user can take precautions against this type of activity associated within any website.

Browser Exploits

This type of attack benefits from the vulnerabilities of a user's mobile web browser or an application (software) launched by the browser, such as PDF reader, flash player, and image viewer. Generally, when visiting an unsafe website, clicking in a browser can install a malicious software or application on a mobile device.

Network-Based Threats

Mobile devices provide the best support to cellular networks, as well as wireless LAN IEEE 802.11, both of which have different types of threats for the user. Some network-based threats are described below.

Denial of Service Attack (DoS)

In Denial of service, an attacker or hacker denies access to application services or other services. In relation to mobile devices, this type of attack typically involves robust connectivity and compact capabilities.

Network Exploits

Network exploits the faults in the mobile device operating system or other application software that operates on a wireless or cellular network. When mobile devices are connected through a network, they (network) install some malicious application software on users' mobile devices without the approval of the users.

Mobile Network Services

Mobile network services like MMS, SMS, and voice calls can also be used for attacking mobile devices. In this case, a new attack like a phishing attack occurs in the mobile devices. Phishing is an attack strategy in which the attacker gains sensitive information from the user by presenting itself as a trustworthy entity.

Wi-Fi Sniffing

Wi-Fi sniffing means intercepting data between the mobile devices and Wi-Fi access point from the air. It also considers that every application and web page has some vulnerabilities. Thus, passing data in the Wi-Fi medium is a big risk. Unencrypted data can easily be grabbed by attackers or hackers.

Physical Threats

Mobile devices are designed to be used in daily life, and physical security is an important issue. Some of the physical threats are described below.

Bluetooth

This is a short-range radio technology that provides wireless connectivity in very short ranges, and many potential threats, vulnerabilities, and exploits have been recognized with Bluetooth. Malware can spread from device to device through Bluetooth services. When two devices come within a particular range and are paired using default Bluetooth passwords (code), malicious data are transferred to the other device by the Bluetooth services.

Lost or Stolen Mobile Devices

The loss or theft of valuable mobile devices is also a serious threat because these valuable applications and hardware devices can be resold on the market, which threatens a user's personal sensitive data.The mobile threat space for various mobile environments are shown in figure 1.2.

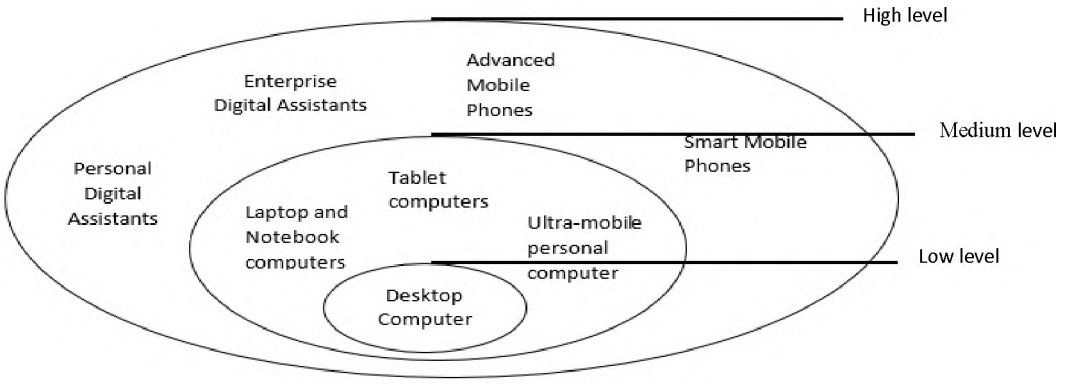

Figure 1.2 Mobile Threats Space

Vulnerabilities

Mobile vulnerability is a security exposer that results from a mobile device weakness that the application developer did not expect to introduce and will fix once when it is discovered. Vulnerability includes three steps, a device has susceptibility, attackers access the flaw, and a capable attacker exploits it.

Rootkit

Rootkits attain their malicious target by infecting the operating system. Generally, rootkits hide malicious user spaces and data files in the operating system or install some malicious application in the mobile device.

Worm

A worm is program code that makes multiple copies of itself from one mobile device to another, using diverse carriage techniques by the network. A worm damages or compromises the security of the mobile device.

Trojan horse

A Trojan horse installs other malicious (worm or botnet) applications and gathers sensitive information from the mobile devices. It is also used in a phishing attack. Trojan horses widely affect businesses with the purpose of stealing information from devices.

Botnet

A botnet is a collection of compromised devices that are infected by virus programs that give an attacker the capability of remotely supervising them. It represents a serious money-related security threat around the world. It is also responsible for sending spam mail to commit DoS attacks. The security of mobile devices deals with the same issues conventional computer security deals with confidentiality, integrity and availability. Table 1.1 shows the security objectives

Table 1.1. Security Objectives

Issues	*Description*
Confidentiality	Confidentiality determines who is allowed to access what.
Integrity	Integrity identifies who is allowed to modify or use a certain resource.
Availability	Availability describes the requirement that a resource be usable by its legitimate owner.

1.5 Defensive Mechanisms

Due to increasing use of mobile devices, the requirement of cloud computing on mobile device arises. The challenges faced by these devices are unauthorized access, vulnerabilities, data storage and data retrieval. The proposed integrated, comprehensive approach discussed in the forth coming chapters' focuses on providing mobile device security and data security for the above challenges together with improved performance and minimum computational complexity.

The proposed defensive mechanisms address the challenges through

- Improved and Accurate User Authentication in Mobile Devices using Iris Biometric.
- Enhanced 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.

Based on the challenges faced by mobile devices, it is necessary to create a defence mechanism to prevent mobile device and data. With the discussed challenges and issues in the Research Motivation section, the problem statement is stated.

1.6 Problem Statement

Given the propagation of vulnerabilities, attacks and threats, device a defensive mechanism for the user authentication, malware detection, secure data storage and efficient retrieval of encrypted data for mobile devices that have constrained resources. Devise an integrated and comprehensive approach to provide mobile device security and data security for the above challenges together with improved performance and minimum computational complexity.

1.7 Proposed Approaches

Mobile device applications offer a level of convenience that the world never before considered. At any location (home, office, hotel, playground, road, parking, museum, travelling in different countries, or anyplace in the world), any mobile user can use applications to fulfil their daily needs, including communicating, buying, searching, making payments, selling, entertainment, and finding general information. This extreme level of comfort has brought with it an extreme number of security risks. Some of the mobile device challenges are described below

- Authentication
- Malicious Applications
- Data Storage
- Data Retrieval

1.7.1 Authentication

Authentication is process of determining whether someone or something is who or what it is declared to be. Authentication is an important aspect of information security that aims to prevent unauthorized access and to decrease the risk against any theft or disclosure of sensitive information [26] [57]. Examples of authentication are passwords which are used to get access to computers, PIN codes that are used to get access to bank accounts or mobile phones and passports that are used at border control.

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 [69] [73] [74]. In this process, there are two main functions: enrolment and authentication (verification). The enrolment process is the first step for providing a user's specific information such as physiological (face, fingerprint, hand, iris, and DNA)and behavioral (keystroke, signature, and voice) data to generate a reference outline for succeeding authentication[18][77][99].In this process, a physiological or behavioral biometric sample (user related information) is scanned by a suitable sensor, and a reference outline is generated by extracting the user profile and its

training set, and then storing the data in the database that the system needs to use for comparison and authentication in the future.

1.7.2 Malicious Applications

Malware, as a malicious application can be installed on mobile devices, which in turn can gain access to these devices and collect user sensitive information [1][2][5] [25]. Malware has proven to be a serious problem for the mobile platform because malicious applications can be distributed through an application market. From the defender's perspective, how to effectively detect malware and enhance the cognitive performance of users and system administrators becomes a challenging issue. Mobile device users are looking for security solutions aimed at preventing malicious actions from damaging their smartphones.

1.7.3 Data Storage

Increase in mobile device sophistication also demands high storage sophistication. Mobile Cloud Computing (MCC) service, allows resource constrained mobile users to adaptively adjust processing and storage capabilities by transparently partitioning, offloading the computationally intensive and storage demanding jobs [33] [37] [64]. Also, increase in feature rich mobile applications like mobile wallets, banking apps, and healthcare app etc. exposes sensitive data of the users which are always prone to much vulnerability [21] [81]. The value of data is far more important than the value of device. The main issue in using MCC is securing the user data on mobile cloud since there is a high risk of unauthorized access to the data. So the main concern of cloud service provider is to provide data security by the same time providing ease of access to the authorized user.

1.7.4 Data Retrieval

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, the files are retrieved in a ranked order. They either support rank based single keyword search or multi-keyword search with static keyword dictionary [17] [33] [39] [44] [97]. There is a greater overhead

in updating the index file or the keyword dictionary when new files need to be uploaded. Also, efficient data discovery and user searching experience needs to be enhanced.

1.8 Objectives of the Thesis

With the above discussed security threats in Research Motivation section, the objectives of this research work are formulated. The objectives are formed after the study of Literature, to overcome the existing methods limitations. The primary objective of the research work is to devise a defence mechanism for achieving mobile device security and data security. The secondary objectives of the thesis are:

- Improve the detection and classification accuracy
- Increase precision value
- Maximize recall value
- Minimize time consumption
- Minimize Throughput
- Improves the user searching experience and
- Minimize Index generation time

A Four Component Methodology is proposed with four contributions to meet the above objectives and they are discussed in following chapters. The significant contributions of the research are discussed below.

1.9 Significant Contribution of Thesis

The contributions involved for defensive mechanisms for mobile device security and data security are based on

Contribution 1: ***PCA-SVMED Method*** *- Improved and Accurate User Authentication*

Contribution 2: ***MSGP-MS Method*** *- Detection of Malicious Malware Applications*

Contribution 3: ***MSAES Method*** *- Secured Outsourcing of Mobile Device over Cloud*

Contribution 4: ***RFMKS Method*** *- Efficient Search Scheme over Encrypted Cloud Data*

Contribution 1: Improved and Accurate User Authentication in Mobile Devices using Iris Biometric.

In contribution one, PCA-SVMED Method is proposed. PCA-SVMED method is a combination of Principal Component Analysis, Support Vector Machine and Euclidian Distance Algorithm. Here, the feature extraction of the iris image using Colour based Zero crossing transformation is proposed. The obtained features dimensionalities are further reduced using the Principal Component Analysis (PCA). The authentication via verification (one-to-one template matching) is based on Support Vector Machine (SVM) classification and Euclidean distance. The results obtained during authentication of iris image are compared with the existing SVMED method. The next possible threat on mobile devices is malicious application. To detect the presence of malware in mobile devices, Contribution two is proposed.

Contribution 2: Detection of Malicious Malware Applications using Optimized Machine Learning Classifiers

In contribution two, MSGP-MS Method is proposed. MSGP-MS method is a combination of Random Forest classifier with Particle Swarm Optimization Algorithm. The malware detection method identifies the presence of malware in android applications and enhance the security of the smartphone. The experimentation is done using the collected dataset and the results obtained by the proposed MSGP-MS classifier is compared with the existing classifier. For secured outsourcing of mobile device data over cloud using Hybrid Cryptographic algorithm, Contribution three is proposed.

Contribution 3: Secured Outsourcing of Mobile Device Data over Cloud using Hybrid Cryptographic Algorithms.

In contribution three, MSAES method is proposed. MSAES method is a combination of Message Digest signatures with Advance Encryption Standard. The analysis of the proposed method for secured outsourcing of mobile device data to cloud computing storage paradigm comes up with the following vulnerable threats like authentication, data leakage, modification, privacy of users. The proposed MSAES method is designed to tackle all these security issues efficiently. As the data needs to be transmitted over a cloud network, there are numerous means through which an attacker can easily get into the

internet based network and act as a cloud server to the owner of data, hence resulting into the loss of data. In secure data transfer, the hybrid approach MSAES shows high efficiency when compared with other algorithms based on the mean processing time, throughput, speed up ratio and turnaround time. This method ensures the security of the outsourced mobile data over cloud storage. For efficient retrieval of outsourced data, ranked fuzzy multi-keyword searching algorithm is explained in Contribution four.

Contribution 4: Efficient Search Scheme over Outsourced Encrypted Mobile Device Data in Cloud with Fuzzy Searching Techniques.

In contribution four, RFMKS method is proposed. RFMKS method is a combination of Ranked Fuzzy Multi keyword search algorithm. The proposed method discusses the privacy preserving fuzzy ranked multi keyword search approach on encrypted data in Cloud Computing. The experimentation is done using the collected dataset from the mobile device. The proposed method is efficient and improves the user searching experience in cloud storage.

1.10 Organization of the Thesis

This thesis is mainly divided into eight chapters and is framed around the research objectives. The organization of the thesis is as follows.

Chapter 1 presented the basis for the research work.

Chapter 2 presents the related works on the defensive mechanisms of mobile device security and data security.

Chapter 3 describes the research design based on the **Four-component Methodology**. The chapter discusses the four different contributions proposed using four-step methodology.

Chapter 4 presents the improved and accurate user authentication based on iris biometric using **PCA-SVMED** method. Experiments conducted and results obtained are presented.

Chapter 5 discusses the detection of malware applications using **MSGP-MS** method. The results obtained through experiments are presented.

Chapter 6 presents the confidentiality and integrity of outsourced data in cloud storage using **MSAES** method. Experimental results obtained are presented.

Chapter 7 presents the privacy preserving ranked fuzzy multi keyword search over encrypted data in Cloud storage using **RFMKS** method. The experiments performed with datasets and the results achieved are presented.

Chapter 8 provides the achievements of four contributions

Chapter 9 explores the further future research directions.

1.11 Chapter Summary

Threats and attacks are causing serious and challenging issues in the mobile device security and data security. Threats are malicious software that replicates and infects the systems within short period of time. This chapter discussed the various types of threats, vulnerabilities and attacks in mobile device. The defence mechanisms are framed for the mobile device security and data security. The objectives of the research are formulated and the contributions of the thesis are discussed. The Review of Literature for the research work is discussed in next chapter.