2

Literature Review

2.1 Security Challenges in Mobile Devices

Security is a major concern for any computing devices which contains sensitive data and accesses to the Internet. It is still more mandatory in the case of mobile computing devices such as Laptops, Notebooks, Tablets, Mobile Phones, Personal Digital Assistants (PDAs), Smart phones etc. Due to the inherent nature of these devices such as Mobility and Portability, they encounter additional security issues compared to the conventional computing devices. Now-a-days, business applications are going mobile and are using business data of an enterprise in a mobile context in order to improve the revenue by increasing the productivity [59]. So there is a need to secure these devices from the various attacks. The specifics of the mobile devices and data security are shown in figure 2.1.

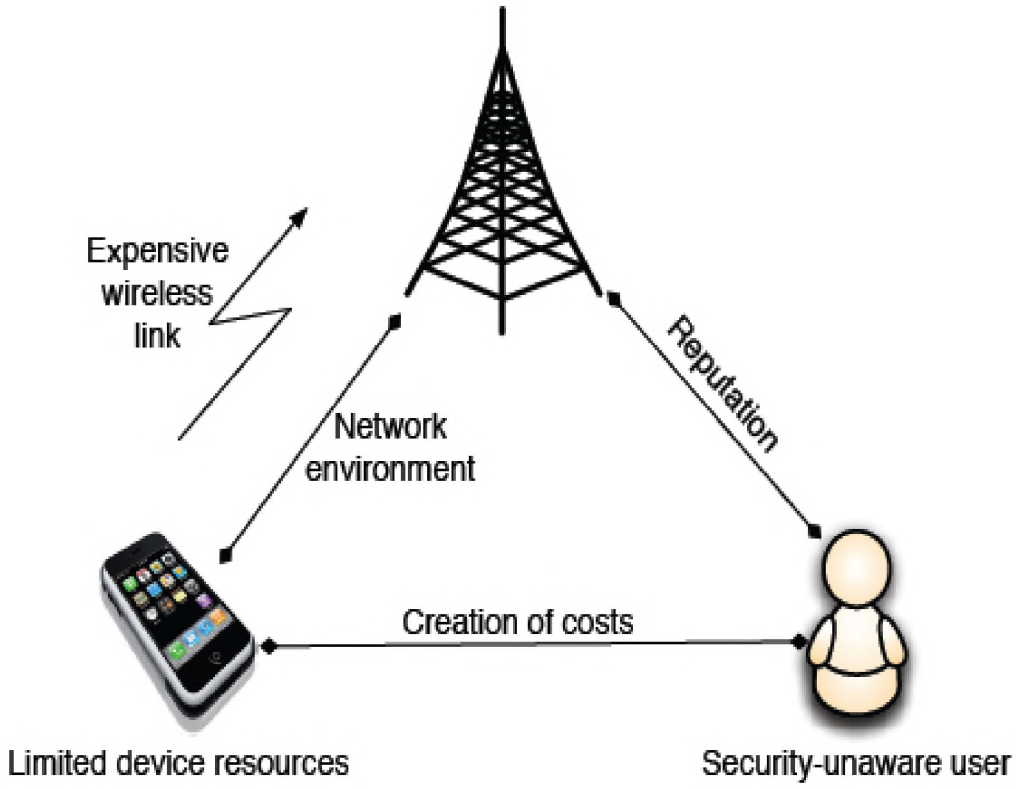

Figure 2.1 Specifics of Mobile Devices

Security and data privacy need multiple means of protection and restrictions on mobile devices. Smart phone's popularity and relatively lack of security have made them attractive targets for attackers. In general, the world now faces threats without correlation

among all aspects of security breaches. In this regard, it is essential to ensure appropriate security mechanisms in mobile devices. These involve correlations among the authentication approaches, application stores, data outsourcing in mobile devices to reduce security issues and data privacy threats, and provide a secure mobile ecosystem.

The proposed integrated and comprehensive approach shows the defensive mechanisms that need to be considered and implemented to solve mobile users' security issues and data privacy threats in the appropriate way. Some of the existing approaches to defend the challenges of the mobile device security are discussed below:

Roberta Cozza [72] forecasted the mobile device threats and vulnerabilities. They also discuss new attack patterns in emerging technologies such as social media, cloud computing, smartphone technology and critical infrastructure with user authentication

Polla M. et al. [48] describe high-level attacks as those against user and network specific for the mobile security and data privacy mechanisms

Yan Q. et al, [92] explore the security awareness of smartphone users who download applications from official application repositories.

Miettinen M. et al, [59] describe Host-Based Intrusion Detection techniques and the storage capabilities that are useful in android mobile devices and protecting against cybercrime by using a mobile ecosystem.

Zhangjie Fu et al, [97] developed a framework for Achieving effective cloud search services with respect to security and privacy of data.

Table 2.1 below analyses and discusses mobile devices security issues, data privacy in terms of types of attacks, security mechanisms, and the key emphasis of the research schemes.

Table 2.1 Mobile Device Security Challenges

Year	Scheme	Type of Attacks	Security Mechanism	Emphasis
2011	Mobile Device Threats, Vulnerabilities	All types of threats and vulnerabilities	Preferring biometric security in mobile devices	Suggesting iris biometric traits for their reliability and accuracy
2009	Malware Detection and Prevention on Mobile Phones	All types of attacks, especially malware threats and vulnerabilities	Based upon detection principles	Focusing on high-level attacks such as those against user-specific applications
2006	Mobile Devices Malware	Malware attacks on mobile devices	State of the Art mobile malware	Focusing on effective malware detection and prevention on mobile devices
2013	Mobile Devices Intrusion Detection	Based on intrusion, storage over Mobile devices	Host based intrusion detection and encryption approach	Computing power and Storage capabilities evolve into mobile devices
2014	Data search services	Based on security and privacy of mobile device data	Multi-keyword ranked search supporting synonym query	Focusing on effective Search techniques and security

Existing approaches only addresses the challenges separately and there is no integrated approach to solve these issues in a single stoke methodology. To overcome the challenges and to defend against these attacks, effective integrated defence mechanisms are necessary. The proposed methodology is framed with four contributions based on security and privacy of the mobile device and the data, the study is made in depth on these four factors only.

2.2 Defensive Mechanisms

The defensive mechanisms address the challenges of mobile device and data security in terms of Authentication, Malware Detection, Outsourcing Data to Cloud Storage and Retrieval of Outsourced Encrypted Data. The various existing defensive mechanism approaches are discussed in detail below.

2.2.1 Iris Biometric Authentication

With all these enhancements and developments of technology and with the rapid growth of smartphone usage, many advancements in technology have been taken place during the decade [76] [79] [99]. 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. Some of the approaches are existing in the literature and are discussed below

Chiara Galdi and Jean-Luc Dugelay et al. [18] proposed a novel system named as Cumulative SUMs that combines the recognition of user's iris and user's device. The approach is tested on MICHE, a database composed by iris images captured with different mobile devices in unconstrained acquisition conditions.

J Zuo and NA Schmid et al. [99] proposed three methods to improve performance of a single biometric matcher based on vectors of quality measures associated with biometric data. The first two methods adaptively select probe biometric data and matching scores based on predicted values of Quality of Sample (QS) index (defined here as d-prime) and Confidence in matching Scores (CS), respectively. The third method, Quality Sample and Template features (QST), treats quality measures as weak but useful features for discriminating between genuine and imposter matching scores. The experimental results obtained by means of feed forward neural network shows significant performance improvements for all three methods when applied to iris biometrics.

V.V.S. Tallapragad and E.G. Rajan et al. [82] developed a classifier named Support Vector Machine (SVM) and Hidden Markov model for iris recognition system. SVM classifier groups the large database into smaller groups where each group is linearly separable from the other and it is recognized by hidden Markov model (HMM) classifier which compares the features of the given image only with the other images of the same group. In order to meet this efficiency an average convergence time needed by the algorithm is found to be lesser than existing SVM-based technique.

Lagree S. and K.W. Bowye et al. [47] explained a technique named as texture filter spot, line and laws structure for predicting ethnicity from the iris features. It suggests that

the prediction of ethnicity is more difficult. This technique improves the texture recognition of biometric iris.

Esteban Vazquez-Fernandez, and Luis Perez-Freire et al. [23] proposed an algorithm named as Local Binary Patterns. It is automatically processed by already registered contacts that can be identified, so that the current picture can be sent to them in a smart, user-friendly manner. Table 2.2 describes some of the state-of–the-art technologies for iris recognition.

Table 2.2 Comparison of Iris Biometric Authentication Approaches

Year	Author	Countermeasure Schemes	Observations
2015	Chiara Galdi, Michele Nappi, Jean-Luc Dugelay	Cumulative SUMs, MICHE database	The sensor interoperability problem leveraging on the picture differences due to acquisition by different sensors
2013	J Zuo, NA Schmid	Feed Forward Neural Network (FFNN), Quality of samples, Confidence in matching Scores, Quality Sample and Template features	To improve iris quality using a multivariant prediction to better map quality values with matching performance.
2012	V.V.S. Tallapragada, E.G. Rajan	Support Vector Machine and Hidden Markov Model	To meet the efficiency of average convergence time for optimization process.
2011	Lagree, S. and K.W. Bowye	Texture filters spot, Line and Laws structure	Demographic attribute can search iris image by criteria, enhance ethnicity prediction
2011	E.V Fernandez, H.G-Pardo, D.Gonzalez-Jimenez, Luis Perez-Freire	LBP Face detection algorithm and adaptive illumination normalization	Obtain robust identification and the computational load of identification is negligible for a typical number of stored contact

The above section discussed various existing iris biometric authentication approaches proposed by different authors. From the above study, it observed that there are few limitations found in the existing authentication techniques. Some important observations are numerous features, classification delay and to enhance the detection rate.

2.2.2 Malware Detection

Security is one of the main concerns for Smartphone users today. The tremendous growth of smartphone usage makes it a target for malicious attackers to propagate malware attacks. Increased demand for mobile devices is due to the huge availability of applications that can be downloaded and installed easily on these devices. Malware, as a malicious application that can be installed on mobile devices, with the intention of breaching device security policy with respect to confidentiality, integrity and availability of data. Various approaches have been proposed by different authors for detecting malware in mobile devices. Some of them existing in the literature are discussed below.

Borja Sanz, and Borja, et al. [14] propose a method named as PUMA that detect malicious android application through machine-learning techniques by analyzing the extracted permissions from the application itself. The result obtained has high detection rate and also high false positive rate.

Glodek, W and Harang et al. [30] proposed a classifier named as Random Forest classification for malicious and benign applications. The combinations of frequently-occurring permissions in this manner significantly improves previous results, and provides true positive rates in excess while maintaining tractable false positive rates.

Vaibhav Rastogi and Jiang et al. [70] developed a framework called as DroidChameleon with various transformation techniques to improve the current state of malware detection on mobile devices.

Mohd Najwadi Yusoff and Aman Jantan et al. [62] propose an algorithm named as Genetic algorithm to optimize the malware classification system as well as help in malware prediction. The new malware classification system is based on malware target and its operation behavior. The result from this system also has an ability to train and learn by itself, so that it can predict the current and upcoming trend of malware attack.

Liang Xie and Zhu et al. [53] propose a novel behavior-based malware detection system named pBMDS which adopts a probabilistic approach through correlating user inputs with system calls to detect anomalous activities in cell phones. It achieves high detection accuracy and low false positive rates in protecting major applications in smartphones. Table.2.3 describes the various significant malware detection approaches discussed above.

Table 2.3 Comparison of Malware Detection Methods

Year	Author	Countermeasure Schemes	Observations
2013	Borja Sanz, Igor Santos, Carlos Laorden, Xabier Ugarte-Pedrero , Pablo Garcia Bringas, Gonzalo Alvarez.	Permission based Malware Detection (Machine-learning classifier, k-fold cross validation), PUMA method	To improve detection rate and false positive rate
2013	Glodek, W., & Harang	Random decision forest classification	To identify potentially malicious applications effectively
2013	Vaibhav Rastogi, Yan Chen, and Xuxian Jiang	DroidChameleon transformation	Improves signature and improve current state of malware detection on mobile device.
2011	Mohd Najwadi Yusoff, Aman Jantan	Genetic algorithm	To optimize the malware classification system and for prediction of malware in mobile application
2010	Liang Xie, Xinwen Zhang, Jean-Pierre Seifert, Sencun Zhu	Permission based malware detection	To achieve high detection accuracy and low false positive rates in protecting major applications in smartphones.

The above section discussed various malware detection approaches proposed by different authors. With explosive growth in the number of mobile devices mobile malware is rapidly spreading, making security one of the key issue. From the above study, it

observed that there are few limitations found in the existing detection techniques. Some important observations are based on the permission features, effective classifiers and to optimize the correctly identified instances.

2.2.3 Outsourcing Data to Cloud Storage

Due to increasing use of mobile devices, the need of cloud computing in mobile devices arises. While using the cloud storage services on resource constraint mobile device, the mobile user needs to ensure the confidentiality of the critical data before uploading and downloading data on the cloud storage. Various approaches have been proposed by different authors for secured outsourcing of mobile device data over cloud storage. Some of them existing in the literature are discussed below.

Xinlei Wang, Wei cheng, Mohapatra et al. [88] proposes a technique named as ART sense that solves the problem of "trust without identity" in mobile sensing. It consists of a privacy-preserving provenance model, a data trust assessment scheme and an anonymous reputation management protocol. On implementation in the Android demonstrates that ART Sense incurs minimal computation overhead on mobile devices.

Chonglei Mei and Abishek Chandra et al. [19] proposed the data mining techniques to detect data sharing across multiple applications, and developed novel scheduling algorithms that exploit such data sharing for better outsourcing performance. The results show that improvement in application performance, while achieving high efficiency in terms of computation resource and network usage.

P. Syam Kumar and D. Thamizh Selvam et al. [80] focus on Ensuring data storage security in cloud computing, which is an important aspect of Quality of Service (QoS). The results show that the system is more secured than existing system against Byzantine failure, unauthorized data modification attacks, and even cloud server colluding attacks.

Ayman Mousa and Elsayed Rabaie et al. [8] evaluate the performance of reverse encryption algorithm on the storages. The obtained results are compared with the existing encryption algorithms. The resulting design is able to facilitate secure data outsourcing.

Mohammed Alhanjouri and Ayman M. Al Derawi [61] developed a new method for encrypting the data using query based approach with hashing techniques. The result obtained shows that it greatly reduces the storage and representation overheads. Table.2.4 lists the various recent data outsourcing approaches discussed above.

Table 2.4 Comparison of Data Outsourcing Approaches

Year	Author	Countermeasure Schemes	Observations
2013	Xinlei Wang, Wei cheng, Mohapatra	ARTsense technique, privacy preserving model	Incurs minimal computation overhead on mobile devices and outsource task accurately
2012	Chonglei Mei, Daniel Taylor, Chenyu wang, Abishek Chandra	Data mining techniques and scheduling algorithm	Improves application performance, while achieving high efficiency in terms of computation resource and network usage.
2010	P. Syam Kumar, R. Subramanian and D. Thamizh Selvam	Sobol sequence, cloud computing	Improves security against Byzantine failure, unauthorized data modification attacks, and even cloud server colluding attacks.
2013	Ayman Mousa, Osama Faragallah, Elsayed Nigm, and Elsayed Rabaie	Cryptographic support, REA	The results of a set of experiments show the superiority of the REA over other encryption algorithm AES with regards to the query execution time.
2012	Mohammed Alhanjouri, Ayman M. Al Derawi	Test query and AES	Good comparable response time, the performance of is better than the traditional way to query over encrypted data

The above section discussed various data outsourcing approaches proposed by different authors. Outsourcing of data into cloud has become an effective trend in modern day computing due to its ability to provide low-cost, pay-as-you-go IT services. It is desirable to outsource sensitive data in an encrypted form but cost of encryption process would increase the heavy computational overhead on thin clients such as resource-

constrained mobile devices. From the above study, it observed that there are few limitations found in the existing detection techniques. Some important observations are based on the data transfer and security concern of the mobile data both in local device and cloud environment without any performance issue.

2.2.4 Retrieval of Outsourced Encrypted Data

As the power of cloud computing became prevalent in the recent years, enables the development of smart electronic mobile devices that can be integrated with the emerging cloud computing technologies. In this scenario, security and privacy become major concerns when data owners outsource their private data onto public cloud servers. In spite of the secured storage, retrieval of encrypted data becomes an intriguing task. Various approaches have been proposed by different authors for searching techniques. Some of them existing in the literature are discussed below.

Hongwei Li and Tom Luan et al. [33] developed the searchable encryption for multi-keyword ranked search over the storage data. The large number of outsourced documents (data) in the cloud, utilize the relevance score and k-nearest neighbour techniques to develop an efficient multi-keyword search scheme that can return the ranked search results based on the accuracy. The results show that improved efficiency in terms of search functionality and search time.

E. Lagerspetz and S. Tarkoma et al. [49] present the benefits and drawbacks of mobile desktop search coupled with cloud-assisted operations, such as operation offloading, cloud storage, and cloud-assisted search. The synergy between mobile platforms and cloud computing is under-utilized and should be explored further, particularly in the search and synchronization use case.

Zhangjie Fu and Lu Zhou et al. [98] propose a method synonym-based search to support synonym queries. It enables an effective searchable system with support of ranked search which remains a very challenging problem. The outcome is more accurate search results

C. Wang and Lou. et al. [85] proposed searchable symmetric encryption (SSE) and order-preserving symmetric encryption (OPSE) for secure index search. It protects

sensitive score information. The resulting design is able to facilitate efficient server-side ranking without losing keyword privacy.

J. Li, Q. Wang and W. Lou et al. [50] proposed systems namely Wild card based search and gram based fuzzy search over encrypted cloud data to solve problem of effective fuzzy keyword search. Fuzzy keyword search greatly enhances system usability by returning the matching files when users' searching inputs exactly match the predefined keywords or the closest possible matching files based on keyword similarity semantics, when exact match fails. The result obtained shows that the method greatly reduces the storage and representation overheads. Table.2.5 lists the various current searching data approaches discussed above.

Table 2.5 Comparison of Searching Techniques

Year	Author	Countermeasure Schemes	Observations
2014	Hongwei Li, Dongxiao Liu, Yuanshun Dai, Tom Luan	Multi-keyword ranked search, K-nearest neighbor technique	To achieve confidentiality of documents and index, trapdoor privacy, trapdoor unlinkability, and concealing access pattern of the search user
2011	E. Lagerspetz and S. Tarkoma	Cloud assisted search, synchronization	To improve Indexing performance and energy
2014	Zhangjie Fu; Xingming Sun; Linge, N and Lu Zhou	Synonym expansion, Rank function, Tree based search algorithm	To enhance the Precision and Privacy, Search Efficiency
2012	C. Wang, N. Cao, K. Ren and W. Lou.	searchable symmetric encryption (SSE), order-preserving symmetric encryption (OPSE)	To improve Index construction time and search efficiency
2010	J. Li, Q. Wang, C. Wang, N. Cao, K. Ren and W. Lou	Wild card based search, gram based fuzzy search	To improve Index construction time, searching time, efficiency

The above section discussed various recent searching approaches proposed by different authors. Existing search techniques are not effective in retrieval of encrypted data from cloud environment. Recently, several keyword searchable encryption schemes have been described in the literature. However, these schemes are not effective for resource-constrained mobile devices, because the adopted encryption system should not only support keyword search over the encrypted data but also offer high performance.

2.3 Observations due to Literature

From the above study, it observed that there are few limitations found in all the existing approaches. Some important observations due to the review of literature are

- Password or Personal Identification Number can be easily identified or bypassed. This will ultimately increase the risk of accessing information by unauthorized users.
- Malware attacks in mobile device can retrieve sensitive information, gaining control over user's browsing history, initiating telephone calls, initiating mobile device microphone or camera to secretly record information.
- In Data outsourcing over cloud storage, confidentiality of sensitive data is essential.
- Delay in searching the outsourced encrypted mobile data over cloud to be handled.
- There are no existing approaches found completely to address all the four challenges in a single defensive mechanism.

To overcome the above observed limitations from the study, the research work has proposed a Four-Component Methodology. The proposed integrated, comprehensive approach focuses on providing mobile device security and data security for the above challenges together with improved performance and minimum computational complexity. Thereby the research work provides better results based on the parameters such as Detection, Accuracy, Precision Value, Recall Value, Time Consumption, Throughput, User Searching Experience and Index Generation Time.

2.4 Chapter Summary

This chapter discussed briefly the various approaches used to provide mobile device and data security. Existing defensive mechanism approaches are not effective for Authentication, Malware Detection, Data Outsourcing and Data Retrieval. Moreover, the observations due to the study are also discussed. To overcome the limitations stated in the observations due to literature, a defensive mechanism of four component methodology has been proposed in this research work and is discussed in the subsequent chapter.