AES Encryption And Decryption

Shweta.B. Parekh[1], Girish Mishra[2], Prof. Dipali Bhole[3]
[1, 2, 3] Dept of Computer Engineering
[1, 2, 3] Shree L.R. Tiwari College of Engineering, Maharashtra, India

Abstract- *Now days, Mobile phones have become our day to day necessity. In traditional approach most of the users think that their personal mobile device is secure to store the confidential information. They simply store their data without providing any security to the data, but nowadays due to rapidly growing mobile users, so it is challenging task to maintain privacy of our mobile data in this approach.In case if mobile phone device has been stolen or lost it is very simply to access confidential data without efforts. That's why we use this application. This application allows user to store sensitive data and confidential information on their mobile devices without having to worry about confidentiality even if the mobile is lost. This system is developed so that employees and other mobile users can store and operate on sensitive data on their mobile phones without having to worry of it being leaked. This project concentrates on securing data on mobile phones by storing it in an encrypted form.*

Keywords- AES, Data security, Mobile devices, Self-Encryption.

I. INTRODUCTION

In traditional approach, Most of the user thinks that their personal mobile device is secure to store the confidential information. They simply store their data without providing any security to the data. But now a day's due to the rapidly growing mobile user population, so it challenging task to maintain privacy of our mobile data in this approach. In case if mobile device has stolen or lost it's very simple to access Confidential data without efforts. That's why we use this system. This system allows users to store sensitive data and confidential information on their mobile devices without having to worry about confidentiality even if the mobile is lost. This system is developed so that employees and other mobile users can store and operate on sensitive data on their mobile phones without having to worry of it being leaked. This software project concentrates on securing data on mobile devices by storing it in encrypted form. This data is encrypted with a stream cipher whose key is stored on a server. This system enables the user to store sensitive data on their android mobile phones. System will encrypt the data and store the data online. User can access the system data by login to the system using his user ID and password than the data will be displayed to the user. Other malicious user can't access the data. Even if malicious user access online database, data will be displayed in encrypted format which is not in understandable format

By using this system user is free from worrying about leakage of his confidential data. Even if user loses his mobile phone he can access his sensitive data by login to the system using other mobile phone. Since confidential data is stored in encrypted format other malicious would not able to access the data even if he accesses the data he won't able to understand. This application is used by many people who want to keep their confidential data secretly. This application is a web application developed in android. User can access this system anywhere at any time he just has to use his user ID and password to access the system. We use java technology for the coding of our system. The Self-Encryption (SE) Scheme for Data Security in Mobile Devices was introduced in their paper they have investigated whether it is possible to implement a lightweight encryption algorithm which provides data confidentiality by exploiting the availability of a secure connection with a central server. Portability makes mobile devices prone to being stolen or lost. It is very challenging to protect the weakly encrypted information on a mobile device, which might end up in the hands of an adversary, who could then use powerful cryptanalysis tools to break the encryption. Therefore, security solutions developed for general distributed data storage systems cannot be adopted directly for this new frontier.

1.2 MOTIVATION:

In existing system presented security issues of Mobile database system as well as Mobile network and discussed the solutions for it. They classified the security issues in four different areas such as Security of mobile device, security of operating system on mobile device, security of mobile database and security of mobile network. They also identified a set of vulnerabilities on mobile database and provided some techniques to decrease the side effect of vulnerability of mobile database.

II. LITERATUREREVIEW

"Role of Encryption in Mobile Database Security", D. Roselin Selvarani and Dr. T. N. Ravi Volume 3, Issue 12, December 2014 in this paper the authors presented security issues of Mobile database system as well as Mobile network and discussed the solutions for it. They classified the security issues in four different areas such as Security of mobile device, security of operating system on mobile device, security of mobile database and security of mobile network. They also identified a set of vulnerabilities on mobile database and provided some techniques to decrease the side effect of vulnerability of mobile database [12].

Mobile Database Review and Security Aspects" Bhagat.A.R Prof. Bhagat.V.B, JCSMC, Vol. 3, Issue. 3, March2014, pg.11741182 In a mobile database application a part or a replica of the database is locally installed on the mobile device. This is a significant difference compared to a conventional client-server application where all data is centrally stored in a database server. The approach with a mobile database provides the necessary autonomy to the mobile device to work independently from the central database. The client application can work with the mobile database asynchronously, and needs to connect to the central database only when it is necessary to synchronize. This approach has several advantages compared to a conventional approach where the clients do not use local storage[11].

"Distributed Certified information Access for Mobile Devices," C. Galdi, A. Del Sorbo, and G. Persiano, Workshop in Information Security Theory and Practices(WISTP'07), Crete, Greece, May 8-11, 2007. this paper we describe a primitive, which we call, Certified Information Access, in which a database answers to a query by providing the information matching the query along with a proof that such information are consistent with the actual content of the database. Adv:-We have shown that it is possible to securely distribute the load of the most time-consuming operations among a set of Untrusted peers[2].

"Multiple Key Sharing and Distribution Scheme with (n, t) Threshold for NEMO Group Communications," Y. Jiang, C. Lin, M. Shi, and X. Shen, IEEE Journal on Selected Areas in Communications, Vol. 24, No. 9, Sep. 2006.In this paper, a novel secure key sharing and distribution scheme for network mobility (NEMO) group communications is proposed. The scheme offers the capability of multiple key sharing and distribution for current and future application scenarios, and a threshold mechanism that effectively improves flexibility and robustness of the key sharing and distribution process. Both forward and backward secrecy are guaranteed by compulsive key refreshment and automatic key refreshment mechanisms, which provide dynamic in-progress group communication joining/ leaving and periodic keys renewal, respectively. Adv:- The scheme offers the capability of multiple key sharing and distribution for current and future application scenarios, and a threshold mechanism that effectively improves flexibility and robustness of the key sharing and distribution process. Adv:- The scheme offers the capability of multiple key sharing and distribution for current and future application scenarios, and a threshold mechanism that effectively improves flexibility and robustness of the key sharing and distribution process[3].

"Securing Distributed Storage: Challenges, Techniques, and Systems," V. Kher and Y. Kim StorageSS'05,Fairfax, Virginia, USA, Nov. 11, 2005The rapid increase of sensitive data and the growing number of government regulations that require long-term data retention and protection have forced enterprises to pay serious attention to storage security. In this paper, we discuss important security issues related to storage and present a comprehensive survey of the security services provided by the existing storage systems The main advantage of SIDS (running directly on the storage server or on the disk firmware) as compared to host-based IDS is that an intruder having full access to the host can disable a host-based IDS, whereas a SIDS can still continue to function properly and are independent of host (or OS) compromise [4].

III. PROBLEM DEFINATION

From the platform-agnostic encryption model shown in Figure 1, general assets and threats can be derived. In general, encryption systems are developed and used to assure the confidentiality of data. Hence, data represents the primary assets that needs to be considered for systematic assessments of encryption systems on smartphone platforms. The security of encryption systems on smartphone platforms and the confidentiality of the asset data can be compromised by different threats. Due to their mobility and their broad support for third-party applications, theft and malware represent the main threats for mobile devices. Hence, encryption systems for mobile devices need to be designed such that encrypted data stored on the smartphone cannot be decrypted by an illegitimate user or by malware running on the mobile device.

Attack Scenarios

Based on the defined assets, threats, and assumptions, a set of generic attack scenarios can be derived from the platform-agnostic encryption model shown in Figure 1. Attacks on the encryption system include attacks on properties of the encryption system and its integration into the platform. The following specific attacks need to be considered here: (1) Circumventing the encryption system by utilizing jail breaking/rooting on a stolen smartphone, (2) attacking backups that are either stored on disk or in the cloud, and (3) attacking cloud storage that is provided by the platform for data-synchronization purposes. Under the assumptions that the encryption system is implemented correctly, attacks on key derivation are considered to be the most likely attacks: (1) Some encryption systems do not use the user's passcode to derive encryption keys, which enables jail breaking/rooting attacks, (2) even when the passcode is used for deriving encryption keys, the system is still susceptible to brute-force attacks on the passcode. The time required to carry out such attacks primarily depends on the employed key derivation function, and the inclusion of a secure element in the key derivation process. Finally, attacks on user configurations or developer decisions need to be considered due to the various properties and parameters that can be influenced by the administrators, the users and the developers. Depending on the specific properties of the system (e.g. brute-force times on the passcode), appropriate passcodes must be chosen, or the system might not be enabled by default (poor configuration option). Application developers can influence the way, in which smartphone applications make use of available security features. Depending on the particular platform, an application developer can decide where to store data, which security level to use, and whether data is transmitted to external backup and cloud components. If poor developer decisions are made, attacks can potentially circumvent integrated security features.

The system focuses on predicting bankruptcy of the firms by considering the following financial terms listed in the United States of America's stock market.

Central Index Key which is a unique identification number for company registered in United States of America.

There are two kind of filings which will be the first level in generation of the bankruptcy score.10-Q filings are generated annually; 10-K filings are registered quarterly, summing of these two filings will make four filings in the year which are extracted through CIK (central index key) which in turn are found through ISIN (International securities identification number) and company names. Each of these links consists of financial statements; commentaries are drawn out with the help of these 10k, 10Q filings links. These statements explains the company scenario for the past three months, on how the company managed through its financials comparing its various portfolios present in their organization.

iOS Analysis The analysis of the iOS system is more complex than the Android analysis, because there are three systems (Figure 2) that need to be considered for data and credentials protection (two, when external backups are not counted). Especially, the file-based data protection system offers a high level of security due to the inclusion of a secure element. However, this high level of security can only be achieved when the right configuration and developer choices are made. The information in the subsequent analysis is based on Apple documentation [1], third-party analysis [6], [13], and our own analysis within the context of secure application development and external consulting projects. 4.1 Encryption System The first file-system encryption system – depicted in the left part of Figure 2 – is available since the iPhone 3gs (iOS 3.x) and encrypts the whole file-system. The file system key (EMF key) is randomly created when the device is started for the very first time. It is stored in the so-called Effaceable Storage, which is a Smartphone File System Key Derivation Module Encryption Module Key Derivation Function File File Key Chain Cre Cre Secure Element File System Encryption iTunes/iCloud Backup iCloud D D Smartphone File System Key Derivation Module Encryption Module File Encryption Credential Encryption Key Derivation Function PIN or Passcode Security Level A File Security Level B File Key Chain Security Level X Cre Security Level Y Cre Secure Element iTunes/iCloud Backup iCloud C D DDDDDD C C D DD C CCC .This capability is employed for fast remote wiping, which only deletes the cryptographic keys instead of the whole file-system. The EMF key itself is encrypted by the unique device identifier (UID) AES key, which is stored within a secure element. The employment of a secure element eliminates the possibility to gain access to file-system images that are either gained by cloning or ripping out the flash memory. In other words, any attack must be executed on an iOS device due to the presence of the secure element. The system can easily be attacked via Jailbreaking/Rooting

IV. SYSTEM ARCHITECTURE

In our application, the user of the mobile will be able to store data in the form of image, audio, video, text files, pdf. In mobile storage and memory card, simultaneously the data will be stored on database.

STEP 1: Firstly the user have to register on the app. After registration process, now user will be able to log in on the app with appropriate user-id and password.

STEP 2: After successfully login, user is now able to store their confidential data like images, audio, video, text files

STEP 3: The all data is stored in mobile micro SD, or Mobile storage and cloud in encrypted format. It mean unauthorized user can't access our data.

STEP 4: If in case, our mobile device is lost then we have to log in on another mobile phone and click on button "key destroyed”. the key will be destroyed and data will remain in encrypted format.

STEP 5: If we want our data on another phone then log in with existing user-id and password. Press on decrypt button, it will ask one key. After providing key, the data will be retrived.

For the past years, Apple’s iOS platform and Google’s Android platform have been dominating the market. During this time, both companies have introduced a wide range of security related features for their smartphone platforms in order to make their platforms ready for business applications. Recently, the market power of iOS and Android has been challenged by a new Windows Phone 8 release2 and a new version of RIM’s BlackBerry platform. For all major smartphone platforms, encryption represents a core feature that is advertised for its strong security345. However, encryption systems of smartphone platforms differ in various security related aspects. For instance, different platforms rely on different approaches to encrypt data (file based encryption vs. file-system based encryption) and implement different methods to derive required encryption keys from user input (e.g. PIN or passcodes). Furthermore, different platforms offer both developers and end users different options to use and configure provided encryption features. The choice of these parameters also significantly influences the security of provided encryption systems.

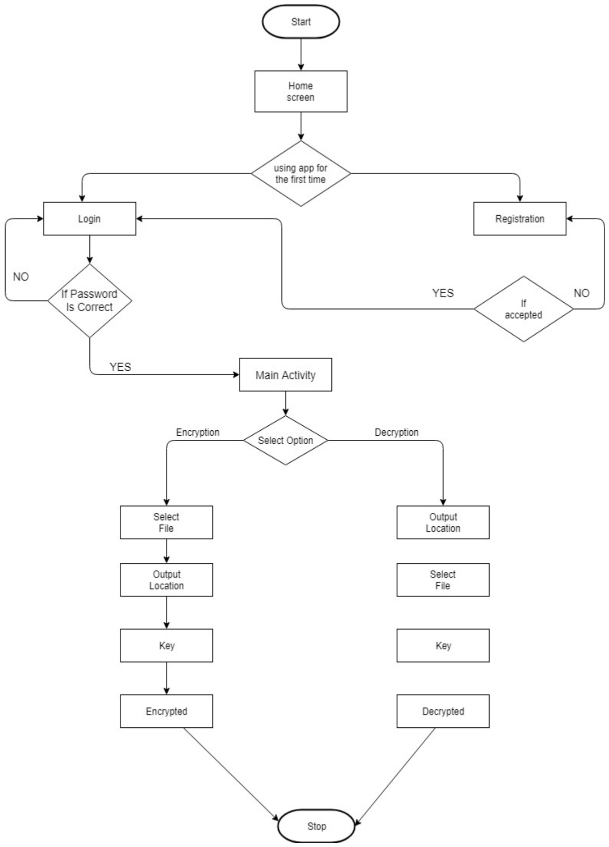

Fig -2: System Architecture

V. IMPLEMENTATION OF THESYSTEM

Here we will discuss about how we implemented our system and is partially represented in a flow chart manner in Figure 1.

Text Pre-processing

Foreachlinked10-Kfiling,weremovetheHTMLtags,tables, and exhibits. Extraction of MD&A section is done using Python scripts. In the text pre-processing stage, we transform the original MD&A section from 10-K annual filings to plain-text documents in three phases: (1) We tokenize each filing in to individual words using the Natural Language Toolkit (NLTK) ; (2) We also use NLTK stem to lemmatize each word and remove the inflectional forms of words and return them to understandable forms. For instance, connection and connecting become connect; (3) Removal of low-frequency words & stop words with help of NLTK corpus and only include15,000 most frequent words. Such filtering procedure is a common practice in NLP as it can help reduce the complexity of statistical models.

Algorithms

Encryption:

step 1:128-bit data block
step 2-key expansion
step3: add round key
step4:sub byte ,shift row,mix columns ,add round key
step5:sub byte ,shift rows, add round key
step6-128 but encrypted bloc

Mean Embedding Vectorizer Decryption:

step1-128 but encrypted block
step2-key expansion
step3-add round keys ,shiftrows, subbytes
step4-add round keys ,mix columns, shift rows ,sub bytes
step5-add round key step6-128 bit block.

VI. RESULTS

Present a novel scheme for storing mobile data securely on server. If in case mobile device is lost user will get secure data on another mobile number of user. User will get OTP and decryption key on second mobile number of user. User has to enter key within session time. Here stored data on cloud is in encrypted format. So no one can recognize that stored data on server.Infuturepdf data will store on server from android application.

VII. CONCLUSION

The conducted analysis shows, that although encryption systems are present on all current platforms, their heterogeneity causes security issues that need to be considered when deploying a mobile device platform. When looking at iOS and Android, the following summary can be given. Due to the strong key derivation function based on the user's passcode and the device's secure element, the iOS systems offer a good level of protection. However, this level can only be achieved when the developer as well as the user/administrator make the right decisions. Since, there are multiple systems that need to be considered, an in-depth knowledge is required by the developer and the user/administrator. One of the most disturbing facts is that neither the user nor the administrator can verify whether an application uses the appropriate protection classes. We have addressed this problem by creating a backup analysis tool that extracts the protection classes of application files, which can then be used to asses the security of application data. On Android, the employed encryption system is much simpler than that on iOS.

REFERENCES

[1] Apple: iOS Security. Tech. Rep. May, Apple Inc. (2012), http://images.apple. com/ipad/business/docs/iOS_Security_May12.pdf

[2] Belenko, A., Sklyarov, D.: Evolution of iOS Data Protection and iPhone Forensics: from iPhone OS to iOS 5 (2011)

[3] Chen, Y.C.Y., Ku, W.S.K.W.S.: Self-Encryption Scheme for Data Security in Mobile Devices (2009), http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4784733

[4] Enck, W., Ongtang, M., McDaniel, P.: Understanding Android Security (2009), http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4768655

[5] Goadrich, M.H., Rogers, M.P.: Smart Smartphone Development : iOS versus Android. Science Education pp. 607–612 (2011), http://dl.acm.org/citation.cfm?id=1953330

[6] Heider, J., Khayari, R.E.: iOS Keychain Weakness FAQ - Further Information on iOS Password Protection (2012), http://sit.sit.fraunhofer.de/studies/en/ sc-iphone-passwords-faq.pdf

[7] Kaliski, B.: PKCS #5: Password-Based Cryptography Specification Version 2.0 (2000), http://www.ietf.org/rfc/rfc2898.txt

[8] Pacatilu, P.: Android Applications Security. Informatica Economica 15(3), 163–171 (2011), http://search.ebscohost.com/login.aspx?direct=true\&db=bth\&AN= 69706020\&site=ehost-live