ISSN (Print)   : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 5, July 2013

Physical Security for Mobile Devices Using Novel Application Lockbox

Prof. PrashantJawade[1], Mrs. Suwarna S. Thakre[2]

Assistant Professor, Government College of Engineering, Karad, India[1]

Senior Lecturer, Dept. of Information Technology, Thakur polytechnic, Mumbai, India[2]

***ABSTRACT*:**The pervasive use of wireless networks and mobile devices has been changing our living style significantly. Along with great convenience and efficiency, there are new challenges in protecting sensitive and/or private data carried in these devices. The most challenging part lies in a dilemma: while it should be computationally infeasible for adversaries to decrypt the data. The security requirements for mobile devices are inherently different from stationary Mobility exposes them to different threat environments and excludes them from relying on external physical security. Productive application from enterprise, government, and military will invariably deal with sensitive data. A risk management and security framework is needed to protect applications and data on mobile devices when they are lost. We propose annovalapplication lockbox concept that compartmentalizes mobile devices at the application level. It is a practical approach that improves the security of mobile devices without requiring significant changes in the current mobile technology.In this paper we have created application such as lockbox in this we can store Sensitive data such as ATM PIN, password for online transaction etc.this information will in encrypted form on mobile device we can decrypt it on mobile but encryption and decryption keys will store on server. To open application longitude and latitude parameters parameter should match.All these parameters act as the policy decision point.Here we are providing physical security to mobile devices like pc, because of mobility now a days mobile devices work like pc,it is easy to handle in crowded area so physical security for mobile device is must. If mobile is lostwe can protect the data in mobile from adversaries[8].

Keywords: DPA,Encryption, Decryption,MAP, SCC etc.

I. INTRODUCTION

Smart phones and other mobile devices are becoming common. They pack a tremendous amount of capabilities into a small handheld form factor. They are as powerful as desktop workstations from a few years ago and fully capable of running sophisticated applications. Therefore enterprises,governments and the military are showing a great deal of interest in utilizing them fully as productivity platform[2],[8].·However, concerns over security remain a significant obstacle. Productive applications will often deal with Sensitive and secret data.Existing mobile devices do not provide sufficient protection for these applications and their data. Currently, themain concern over security in mobile devices is the immaturity of security in some mobile operating systems. Devices such as the iPhone and Android smart phones are not designed to support enterprise and military grade security. Even if mobile operating systems are hardened to the degree of desktop operating systems, additional concerns would remain. It must be recognized that security requirements formobile devices are inherently different from stationary machines. Mobile devices, which include smart phones as well as laptops, are able to move around.

Stationary Machines at Least Somewhat Rely on External Physical Security.

- Desktops are used inside homes and offices.
- Servers are locked inside data centers.
- Military systems that handle classified data are secured inside vaultsprotected by armed guards.
- Data center in dangerous locations have more guards

The amount of physicalsecurity usually commiserates with the sensitivity of the data as well as the level of threat in the environment. Thisassumption cannot be made for mobile devices Mobile devices can move around todifferent environments with different threat levels. They can be used in the office, on a crowded train, inside a secured base, or on the battlefield. Security mechanisms in mobile devices must compensate for the lack of physical security and deal with the risk of device loss appropriately. So our paper we are providing physical security to mobile devices

II. DIFFERENT TECHNIQUES

A number of techniques have been developed to provide data security in mobile devices MAPBox, Sandbox, GeoLocking,SE(Self Encryption),location dependent data encryption etc.

A. SANDBOX

Sandbox is capable of performing static and dynamic analysis. In the static part, the sandbox decompresses installation files and disassembles corresponding executables. This can be used for cheap and fast pre-checks that might already indicate malicious code fragments and characteristics.
In the dynamic part, we make use of the android emulator which is normally used for testing and debugging ordinary android application Investigated Applications are installed to the emulated and isolated environment[6].After that, applications are executed and can beused within the sandbox for performing behavioral analysis. For improving the dynamic analysis process, the possibility of automated generation of user inputs is investigated.Since these analyses requires extensive resource capabilities, our system is intended to be run as a cloud service. Software distributors, like the Android Market or the AppStore, can run this analyses on each submitted application or users, in turn, can upload suspicious applications to their convenience.

B.GEO LOCKING

In this paper they have used two techniques data in mobile devices from being compromised. We use twolevel data hiding technique, where in its first level data is encrypted and stored in special records and the second level being a typical password protection scheme. The second level is for secure access ofinformation from the device. In the first level, encryption of the data is done using the locationcoordinates as key. Location Coordinates are rounded up Figures of longitude and latitude information.
In the second phase the password entry differs from conventional schemes. Here we have used thepatterns of traditional Rangoli for specifying the password and gaining access, thus minimizing thechances of data leak in hostile situations. The proposed structure would be a better trade off incomparison with the previous models which use Bio Metric authentication – a relatively costly way ofauthentication[1].

C.SE SCHEME

In this technique the sensitive data is broken into two parts using our self-encryption stream cipher scheme. The major part (Part A: ciphertext) is stored in the mobile device carried by the company employee, and the minor part (Part B: keystream + other parameters) is protected in the secure server of the company. Part A is encrypted using part B. When the user needs to access the data, he or she has to input a correct PINto pass the authentication procedure. Then the server will send part B to decrypt part A and merge them together to recover the original plaintext. When a mobile device is lost, at most the adversary can access the part A, from which it is computationally infeasible to get meaningful information .

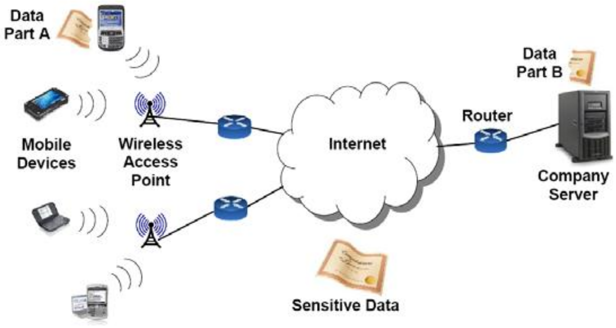


Fig.1 Overview of the Self-Encryption framework.

Physical attacks have been proved effective in breakingsomewell designed ciphers in practice [4].unfortunately,it is challenging to designers to theoretically investigate therobustness of a cipher scheme against various physicalattacks. To address this problem, a prototype is going to beimplemented on top of reconfigurable hardware devices

(i.e.FPGAs). to avoid attacks like DPA(differential power analysis)they try to implement SE protocol on NetFPGA board which is inserted in pc
And SE stream cipher on the mobile deviceDevices such as oscillograph will be used to monitor and record Devices such as oscillograph will be used to monitor and record the electromagnetic leakage when the SE stream cipher is being executed to encrypt/decrypt the data attacks by analyzing the variance of leaking electromagnetic wave. Actually, they expect that SE stream is not vulnerable to DPA attacks due to the uniqueness of each key stream and a much larger keystream space.

D.LOCATION DEPENDENTDATA ENCRYPTION

There are two phases: register and operation phases. Firstly, a mobile client requests a random seed and a MAC function C from the information server in the register phase. The information server records the issued random seed and the function C for each individual client. They are very important for ensuring data security in the operation phase. So, they must be transmitted under a secure channel, such as Intranet or VPN (virtual private network). The random seed is the initial value of one-way hash function, such as MD5. A series of session keys is generated according to the random seed. When the mobile client is moving under an insecure channel in the operation phase, the mobile client submits a target coordinate before message transmission. The information server sends the message encrypted by using the coordinate and a specific session key[3],[8].The session key is changed for every session. Since the information server and the mobile client own the same set of session keys, a key synchronization process is also designed for information server to identify the correct session key. When a secure channel is available for a mobile client, the client can request a new random seed and MAC function C. The proposed approach can provide a novel

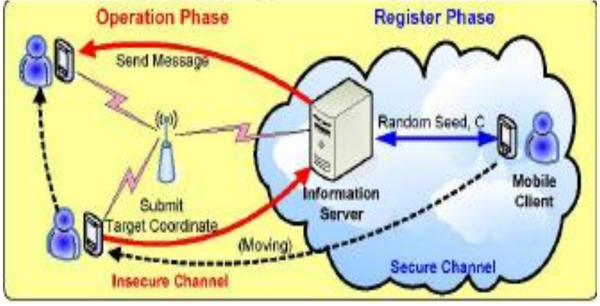


Fig. 2 Communication between mobile users[3]

.

E.MAPBOX:-

MAPbox(Multipurpose application profile) retains the ease of use of application-class-specific sandboxes while providing significantly more flexibility. The key idea is to group application behaviors into classes based on the expected functionality and the resources required to achieve that functionality. Examples of behavior classes includes filters,compilers,editors etc. Classification of the behavior of an application provides a label.which can be used by its provider to conciselydescribe its expected functionality to its users. Thisis similar to MIME-types which are widely usedto concisely describe the expected format offiles.We refer to the label assigned to an application asits Multi-purpose Application Profile-type (or MAP- type). At end-user species the set of application behaviors willing to allow as a set of MAP-types listed in a .mapcap file with each map type .associates a suitable sandbox when untrusted application is to be run, this file is consulted.if the map type associated with the application is not present in the .mapcapfile,the application is not allowed to run. MAP type that would allow the application to access resources that it would not be allowed to if correctly labeled[5].

III. PROBLEM STATEMENT

Different techniques (GEO locking[1], self encryption etc.) were implemented toprotect the mobile devices from adversaries. Still Security remains a significant obstacle in mobile devices. Now day’s mobile devices are common in many applications like Military, government and enterprises invariably deal with sensitive data Existing mobile devices does not provide sufficient protection for these applications and their data. So we propose enhanced application lockbox for mobile device security. To overcome above problems we propose an application lockbox concept that compartmentalizes mobile devices at the application level. It combines policy enforcement mechanisms and support for sophisticated access polices to mitigate the exposure when the device is lost. It is a practical approach that improves the security of mobile devices without requiring significant changes in the current mobile technology.There is an application sandbox in existing system to protect the system from the malicious application by providing the strong separation between the running process. Application sandboxes can exert full control over applications running inside and restrain their malicious actions. Sensitive applications and data inside the lockbox will be protected from attacks originating from the outside system will have full control over the application lockbox. Our goal is to provide the ability to lockout sensitive applications and data. If thelockbox is locked, applications and data inside it should be protected from the operating system and physical attacks. The application lockbox will serve as the compartmentalization enforcement mechanism for the risk management and security framework. Lockboxes for sensitive applications should be automatically locked when the mobile device is deemed to be in high-risk situations. The goal is for sensitive application and data to be already locked when the enemy or a thief captures the device. Applications should be able to run inside application lockboxes without modification. It is unrealistic to expect organizations to adopt a brand new software framework.

IV. PROPOSED METHOD

In previous paper they have mentioned various techniques such as GEO locking, self encryption, MAP box, MDMS etc. to protect the sensitive data in mobile from adversaries. Still there are some problems in security of mobile devices. They have used cryptographic techniques to secure the data. In above techniques data encryption done on mobile device, keys are also stored on mobile devices. In some cases encrypted data sent to client by server and client will onlydecrypt the data. In case mobile is lost thereare chances of data hacking. By using above concept we propose application lockbox concepts for data security in mobile device . In Application lockbox secure data stored in separate memory space. In this encryption and decryption keys stored on server, the user is authenticated by considering three parameters such as password, location parameter and time. To develop a risk management and security framework that compartmentalizes sensitive applications and data. Supports fine-grained access policies. The physical security of mobile devices can change access control should be managed according to the threat level.Location based application locked (Applications deemed too risky for the current physical environment should be locked)Eg. Some application should only run while the device is in the office or secured area.office data we can access only in the office not outside the office. Sensitive application that is not actively being used should be automatically locked.Application lockbox concepts are used.Keys ,location parameter & time will stored on server sideonly.Sensitive application and data to be already locked, when the enemy or a thief captures the device. Applications should be able to run insideapplication lockbox without modification. It useful in military, enterprise and government[8].

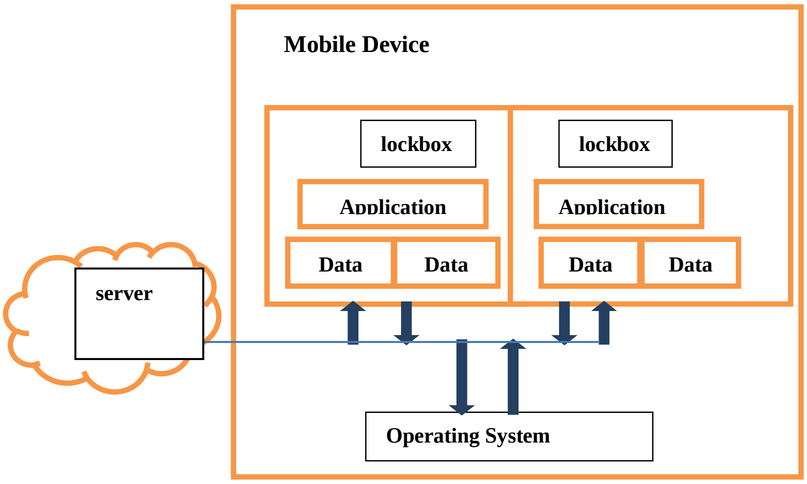


Fig. 3Architecture of annovelapplication lockbox

To use this Application Mobile should have android operating system. Sensitive applications and data will be placed inside lockbox(created application).Encryption and Decryption keys will be placed on server . The key store will also act as the policy decision point. It will take inputs from server and require a secured network channel. Applications should be able to run inside lockbox without modification. To open data which is stored in lockbox need to enter password/key if match found then only we can see that contents we can modify data again, data will encrypt and stored on mobile device. we can also encrypt and decrypt file.Suppose confidential document is there in mobile and user enter into risky area in that case our application will automatically lock that document by using longitude and latitude parameter if parameter match within that area then only we can open application otherwise there is no access to that document.

V. HIGH LEVEL OF INFORMATION SECURITY FOR EXISTING MOBILE DEVICES

If the corporation or other organization has an internal safety policy that regulates information security Table 4 shows how to use certain security techniques as a leverage to mitigate the risk of threats to mobile devices.

Table 1. Security Techniques Used to Mitigate Information Security Risks.[7]

Mobile device access	Power-on authentication – Require a power-on password or PIN, so the device cannot even be powered by an unauthorized user. Implement a standard process for creating unique user names and PINs.
	Auto-lock – ConFig. device to automatically lock up after a certain period of time
	Two-factor authentication – Implement two-factor authentication for access to systems that contain PHI.Consider the use of tokens, call-back, and biometrics
Data storage	Data encryption – Establish data encryption for mobile devices. Identify the types of hardware and electronic media that must be tracked (hard drives, digital memory cards) and develop inventory control systems.
	Auto-run applications – Prevent memory cards from automatically running specific programs.
Data transmission	Encryption – Implement and andate appropriately strong encryption solutions for transmission of PHI. For example access can be implemented over SSL, IPSecora similar VPN technology.
	Signed applications – Allow only signed applications to be loaded onto the devices (S/MIME, token-based).
Data access	Role-based – Employ role-based access as part of a user-provisioning solution. Different users may require different levels of access based on job function.Develop and employ proper clearance procedures and verify training of workforce members prior to granting access.
	Logging and auditing – Implement logging and auditing on device and parent network. Ensure that the issue of unauthorized access of PHI is appropriately addressed in the required sanction policy.

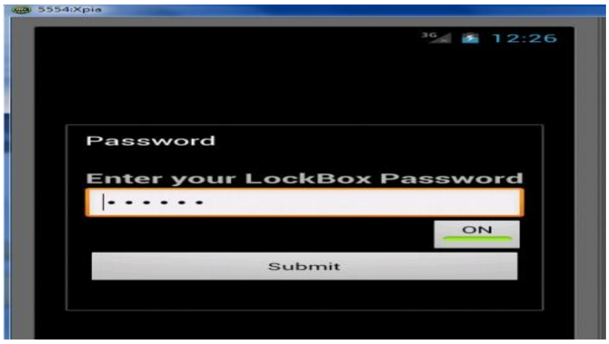
VI. SYSTEM OVERVIEW

By considering above problem in this paper we implement application lockbox concept to secure our data .In previous paper they have mention security like authentication, malware detection, remote wipe,network security etc.Encryption and Decryption keys stored on mobile only so any one will find keys very easily. We thought why not to provide physical security to mobile device likepc.e.g. suppose confidential data is there in user mobile and he/she entered in some risky zone in that case[8].

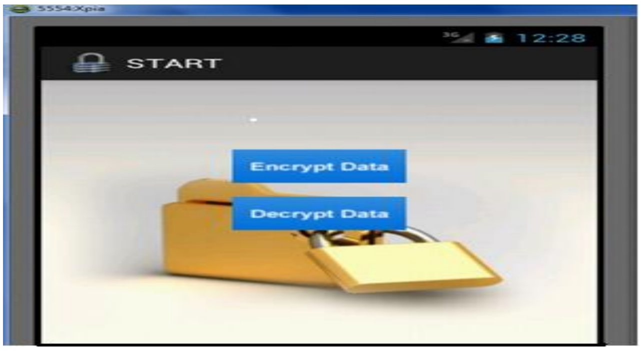
- our application will automatically lock the data by using longitude and latitude parameter(if no match found)
- we will assign time suppose user office timing is 9.30am to 5.00 pm he /she work on that data during above timing if we are at home we cannot open that application.
- main advantage of this application is encryption and decryption keys stored on sever so it very difficult to get the key when mobile is lost.
- We are providing physical security to mobile device so our data will safe if mobile is stolen.

Step1First switch on mobile device(should have android) and click on lockbox(created application name)

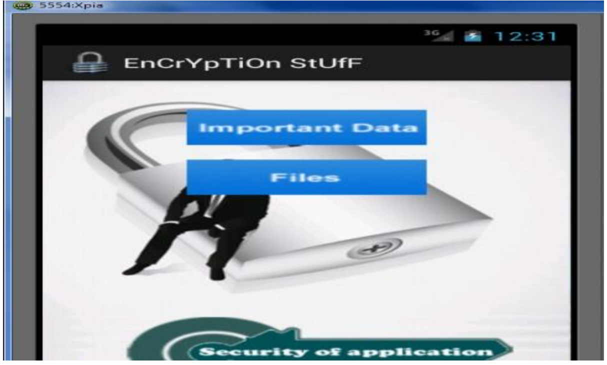
Step2Once open application enter password (it is unique key)


Password
Enter your LockBox Password

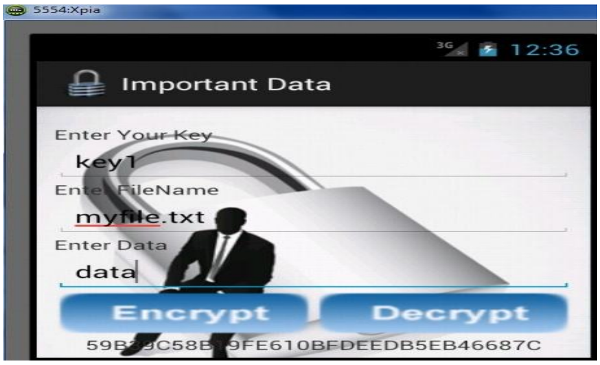
Step3Once password match will get another screen in that we can encrypt and decrypt file[8]



Step4when we click on encrypt data will get following screen[8].



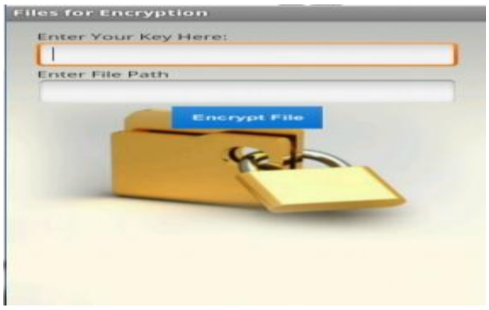
Step5Once we click on important data will get screen here we have three fields ,enter corresponding data intofieldsand then click on encrypt. (Data is veryconfidential so entersomething which is very sensitive like acc no, atmpin,pan card no and other small stuffs) This will encrypt data and show the result .Encrypt button do many task will save our key and file on server it will also create folder lockbox into SDCardSDcard will have those files we have created here[8].



Enter Your Key
key1
Enter FileName
myfile.txt
Enter Data
data

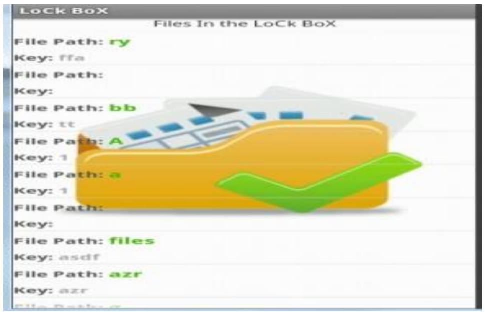
59B[illegible]C58B[illegible]9FE610BFDEEDB5EB46687C

Step6once we click on file option in in step-4 will get screen in which we can browse file and encrypt that file.



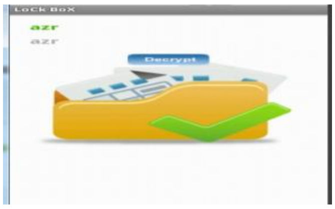
Enter Your Key Here:
Enter File Path

Step7we can extract file from lockbox which is available on mobile this page has file name and key lists.Here we have to select file name for decrypt data.(the file which is already store in lockbox i.e.encrypted form the same file we can decrypt in step-8



Files In the LoCk BoX
File Path: ry
Key: ffa
File Path:
Key:
File Path: bb
Key: tt
File Path: A
Key: 1
File Path: a
Key: 1
File Path:
Key:
File Path: files
Key: asdf
File Path: azr
Key: azr

Step8 Enter decryption password to decrypt a file



azr
azr

VII. CONCLUSION

A risk management and security framework is needed to protect applications and data on mobile devices when they are lost. Our approach is to develop a risk management and security framework that compartmentalizes sensitive applications and data, and supports fine-grained access policies. Since the physical security of mobile devices can change, access control should be managed according to the threat level. Applications deemed too risky for the current physical environment should be locked[8]. Application lockbox provides another layer of protection for sensitive applications and data in mobile devices. It can provide meaningful protection without significant changes in current technology and is intended to work with existing applications without modification. It will be able to protect locked applications and data even if the enemy has physical possession of the device. It will allow for fine-grained risk-adaptive access control policies since applications can be selectively locked without disabling the entire device. The application lockbox will encapsulate individual applications and all their associated data to allow for access control on the application level. The application lockboxes need to provide robust protection when they are locked. Therefore, a robust policy framework is needed for risk management and mitigation that takes into account the risk in the environment as well as the least privilege principle. Effectiveness of the security framework will be driven by the risk-adaptive access controlpolicy. Lockboxes for sensitive applications should be automatically locked when the mobile device is deemed to bein high-risk situations. The goal is for sensitive application and data to be already locked when the enemy or a thief captures the device.

ACKNOWLEDGEMENT

I must thank, first and foremost, my guide Mr. PrashantJawade, Assistant Professor from Department of Information Technology who gave me opportunity to write this paper without his guidance and patience, this dissertation would not be possible. Finally, I thank him to review my paper and his valuable suggestion that make to improve quality of my paper.

REFERENCES

[1] M Prabu Kumar1 and K Praneesh Kumar Yadav, Data Security in Mobile Devices by GEO Locking, International Journal of Network Security & Its Applications (IJNSA), Vol.1, No.3, pp.52-61,October 2009.

[2] JimLuo ,Myong Kang ,Application lockbox for mobile device security,Naval Research Laboratory 2011 Eighth International Conference on Information Technology: New Generations,pp.336-341

[3] Hsien-Chou Liao, Po-Ching Lee, Yun-Hsiang Chao, and Chin-Ling Chen,A Location-Dependent Data Encryption Approach for Enhancing Mobile Information System Security ISBN 978-89-5519-131-8 93560,625-628.

[4] Yu Chen Self-Encryption Scheme for Data Security in Mobile Devices Manuscript submitted on Oct. 2, 2008 to CCNC'09, Las Vegas, NV, USA, Jan. 10 – 13, 2009., E-mail: ychen@binghamton.edu, Tel.: (607) 777-6133

[5] Acharya, and M. Raje,MAPbox: Using Parameterized Behavior Classes to Con[12]A. "MAPbox: using parameterized behavior classes to confine untrusted applications."

[6] Thomas Bl¨asing, Leonid Batyuk, Aubrey-Derrick Schmidt,SeyitAhmetCamtepe,andSahinAlbayrakTechnischeUniversit¨at Berlin - DAI-Labor An Android Application Sandbox System for Suspicious Software Detection,2010 5th International Conference on Malicious and Unwanted Software,pp.55-62.

[7]BlažMarkelj, Igor Bernik,Mobile Devices and Corporate Data Security International journal of education and information technologies,Issue 1, Volume 6, 2012.

[8] PrashantJawade,SuwarnaThakre,Design and Implementation of Enhanced application lockbox for mobile devicesecurity,Issue 6,Volume 2, pp.3342-3348 , June 2013.