Journal Homepage: - www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

ISSN NO. 2320-5407

Article DOI: 10.21474/IJAR01/3698
DOI URL: http://dx.doi.org/10.21474/IJAR01/3698

*RESEARCH ARTICLE*

# DATA SECURITY IN SMARTPHONES USING BIT-LOCKER TECHNOLOGY.

**Dilip V[1] and Shoney Sebastian[2].**

1. Student, Department of Computer Science, Christ University, 560029, India.
2. Associate Professor, Department of Computer Science, Christ University, 560029, India.

## Manuscript Info

*Manuscript History*

Received: 14 January 2017
Final Accepted: 03 February 2017
Published: March 2017

*Key words:-*
AES algorithm, Personal data, Encrypt Once and Decrypt in Any Operation System [ EODAOS], Self-encryption, Reset Operations.

## Abstract

**Objectives**: Securing portable devices with the help of existing technology of Bit-Locker drive encryption, with more security of reset operations, if you lost your portable devices like memory cards, pen drive etc. The main objective is to make Data more secured and unauthorized access is denied when they try to access the personal information that are present in SD card after the User lost his/her Mobile/SD card.

**Methods**: a performance difference between Bit-Locker enabled device and Bit-Locker not enabled device with varying of read/write operation is more in non-enabled Bit-Locker device, so we will suggest to encrypt SD card using Existing Method Bit-Locker and also we suggest an Idea that User can Encrypt once in Windows Platform and Decrypt in Other Platform ( Ex: Ubuntu) better way of protecting the SD card.

**Findings:** The issues of Bit-Locker device that is we enabled Bit-Locker drive encryption, even the drive is locked but the user can be able to format the entire drive without any interruption.so we have given better solution for these type of problem and also if you lost your portable device without encrypting the unknown user can easily misuse the data present in portable device, so we provided a solution if any unknown user wants to access your data it will ask for password, if unknown user enters 5 times wrong password the portable device will be locked and all the data is format the unknown user cannot perform any read/write operation on portable device. And also if we enabled bit-locker drive encrypted it will have decrypted in windows operating system so we introduced a concept of encrypt once and decrypt in any operating system [EODAOS].

**Improvements:** The privacy data is more secured compared to Bit-Locker technology, with reset operation if unknown user enters five times wrong password the portable device will be format and lock the portable device with read/write operations. Performance is more improved.

**Corresponding Author:- Dilip V.**
Address:- Student, Department of Computer Science, Christ University, 560029, India.

## Introduction:-

Data security is the main challenges that prevents the wider acceptance of mobile devices especially within business[1]. Mobile Technologies are rapidly replacing the traditional cellular phones because of its PC-like features which allow them to use many services like (browsing, money transaction etc.). all the smartphone as the feature to install the third-party application and if not enough storage is available in the internal memory the user can explicitly move all the installed third party application to SD card as the installed application are moved to SD card the user data stored on this SD card and the services that they provide becomes more and more vital. Mobile operating systems naturally become the target for security inspection as they are responsible for managing all the information and services. [2] studied on the analysis of security weakness in bit-locker technology and puts forward some measures to improve its security.

So, the existing problem in Bit-Locker technology we encrypt SD card and It cannot be decrypted in any other operating system and it takes lot of time for encrypting. Unfortunately, we discovered that Bit-Locker possesses some critical weaknesses. In this paper, we illustrate our discoveries about the vulnerabilities of the scheme. We also suggest a way to take advantage of the ideas introduced with Bit-Locker technology using standard tools in order to provide an efficient and strongly secure encryption scheme, if the Smartphone lost/stolen the content of SD card can easily misuse by any person like SD card consists of personal photos, videos, third party applications data (WhatsApp backup file, Account password text file etc.) for better way to eliminate this problem our paper explain the different way of encrypting the SD card that helps protect your files and folders from unauthorized access in case your SD card is lost or stolen. To Provide better security we introduce a concept called Encrypt once and Decrypt in any Operating system (EODAOS) usually if the user encrypts SD card in Android Operating System, the user can only decrypt in that particular operating system, our paper will explain about encrypt in one operating system and decrypt in any operating system with secure password/passcode authentication.

## Literature Review:-

An algorithm of SE (self-encryption)[1,2] is an efficient encryption for sensitive files requiring the user to enter password or PIN code, the author explains detailed analysis of the weaknesses of the SE scheme.

The algorithm takes better way when using AES encryption [3] algorithms based on the high-performance computing of GPU, usually encrypting time of traditional AES algorithm is too long to meet fast encryption. The author come up with better way to encrypt with High performance computing with GPU Using AES Encryption.

A comparison between DES, BLOWFISH and AES, the author [4,5,11] explains the different Cipher type, Possible keys, Key length and rounds, and time consumption for each algorithm with specific cipher type. Discusses an algorithm the increasing need for Secured data communication [6] has led to development of several cryptographic algorithms, the author explains secured High throughput implementation of AES algorithm, author explains complete detailed explanation of AES algorithm and comparison between AES Versions, Key Length, Block Size and Number of Rounds.

The key-based security for document encryption [7] system, utilizing the security key on the key usage of effective administration to guarantee that exclusively approved clients can decode the document and make the proper operation, and utilize the hash calculation for document honesty check, and in this way successfully enhance the security of electronic records, guaranteeing its respectability , proposed a new design to give a safe authentication [8] such that the Hardware and security measures executed in the system vanquishes any endeavors of unauthorized access to retrieve the information and to keep up extreme control to secure information and prevent theft, by dealing with outline measurements also, proposed discusses Mobile security [9,10,13] testing targets to detect vulnerabilities and malicious apps on a mobile devices explains various mobile security model like Android security model, IOS security model, Windows Phone security model and briefly explains about Application-based Mobile Threats in all mobile platforms [12,14,15] explains about image encryption in mobile devices and explains elliptic curve cryptography (ECC) and apply the same for convenient encryption and decryption of an image [16,17] author explains the securing applications in windows phone, To have an excellent security to the windows phone the developers and Microsoft will utilize the better methodology, By utilizing the sandbox idea, applications won't have the entrance to utilize the information of different applications.

## Existing System:-

In order to encrypt the disk, we currently use Bit locker (or) other third party software (Ex: True crypt, File vault, McAfee Drive Encryption (safe boot), private disk etc.).So using Existing Method we are going to Explain How to Securing SD card with Bit Locker Drive encryption.

### Bit Locker:-

BitLocker Drive Encryption[19] is built into the Windows operating system and uses Advanced Encryption Standard (AES) with configurable key lengths of either 128 bit (default) or 256 bit (as to configure in Group Policy). The idea behind the BitLocker Drive Encryption [18] is that once you secure your drive, only you, or someone who has your password and recovery key, will be able to get to your data. Explains the attack strategies [20] against Bit-Locker which goal the way Bit-Locker is using the TPM sealing device.
Bit Locker Drive encryption encrypts your entire drive.

### Bit Locker Performance:-

Enabling Bit Locker drive encryption in PC/Mobile to protect the personal files/folders, but we have to think about the performance. If we configure Bit Locker drive encryption there is a performance degradation in both read and write operation of the disk. Performance depends on the combination of processor, RAM and hard disk type (SSD, HDD).

The Performance was tested the performance of read/write operation using a free tool called AS-SSD-Benchmark version number 1.9 with laptop configuration of 1.50 GHZ AMD A4-5000 APU with Radeon™ HD Graphics with 4 GB RAM and 16 GB SanDisk Ultra USB 3.0 pen drive with Bit Locker Drive Encryption and without Bit Locker Drive Encryption.

### Tool Explanation:-

Article [21] explains the tool as test the sequential or random read/write performance without using the cache. AS SSD Benchmark reads/writes a 1 GByte file as well as randomly select 4K blocks. Moreover, it performs the tests using 1 or 64 threads and it determines the SSD's access time.
Two extra benchmark tests inspect the drive's behavior when (1) copying a few big files, a lot of small files and a combination of file sizes by using cached copy functions of your OS as well as (2) Reading/writing data depending on the data's compressibility.

### Read operation:-

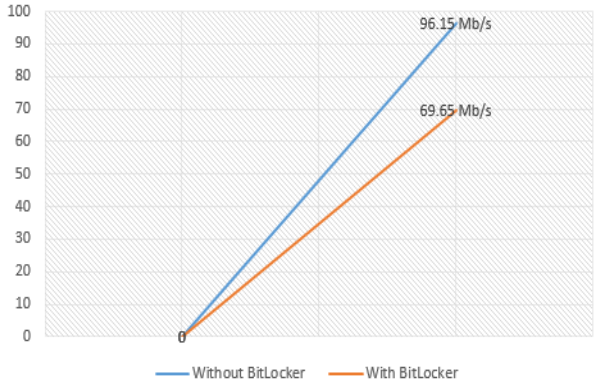


**Figure 1:-** Read operation.

Read operation takes data out of a specified address in the memory. In Figure [1] explains the performance of varying in Without Bit locker, the reading speed will be more, if we Enable Bit Locker Drive encryption then the speed will be less than 25 %. Taking more time to retrieve the address of specified block in Bit Locker drive encryption because of each block encrypted and taking more time to decryption, for increasing the speed of Bit Locker drive encryption the processing as done both using GPU and CPU to increase the efficiency of an encryption.

**Write operation:-**

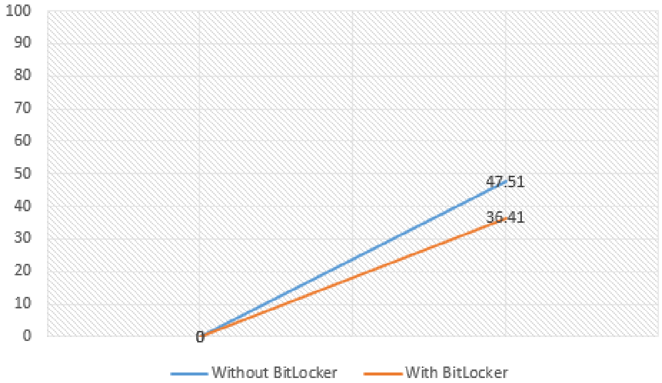


**Figure 2:-** Write operation.

In Figure [2] explains the performance of varying in Write operation puts data into a specified address in the memory. If you are copying small file, the file copied very fast. But think if you are copying more than 10 – 20 GB in Bit Locker Drive Encryption disk it takes lot of time to get copied.

## Proposed System:-

our algorithm and it's working, algorithm follows two fundamental operations. This include a phase of reset operations, increases the speed of encryption process in bit-locker. Since it undergoes two operations (phases) the overall complexity increases and algorithm becomes quite difficult to attack from hackers or attackers. The fixed length of key is generated which must be kept secret. Even through the complexity is very high, but time taken by the algorithm for encryption is less and

Procedure to encrypt the portable device is simple. Thus, algorithm can be used to any portable devices, such as camera SD card, PC, Mobile etc. The following section discusses the procedure to encrypt the SD card.

**Algorithm for Encrypting: -**

1. User has to Select Key length (64 bits, 128 bits, 256 bits).
   Note: if we select lower bits for encryption it will take less time to complete encryption.
2. The key is generated and stored in Flash memory i.e. Root folder of SD card [System Volume Information]
3. The SD card blocks are divided based on the Key Size that user as selected.
4. Temporary master file is created in User selected local disk. By default, master file is secured by AES cipher encryption.
5. All the block address is stored in the master file.
   Initial password has been written in master file.
   M=AES (BA)
   Where,
   M=master File
   BA=Block Address

6. After successful store of master file, the shift rows or mix column Sub-programs will execute with all blocks.
7. Encrypt all the blocks with key size if not go to step 6.
8. After encrypting the master file consists of two separate section one is before encrypting block address and after encrypting block address.
9. Now master file, reset program and auto run programs are flashed to SD card.
10. Now SD card is encrypted.

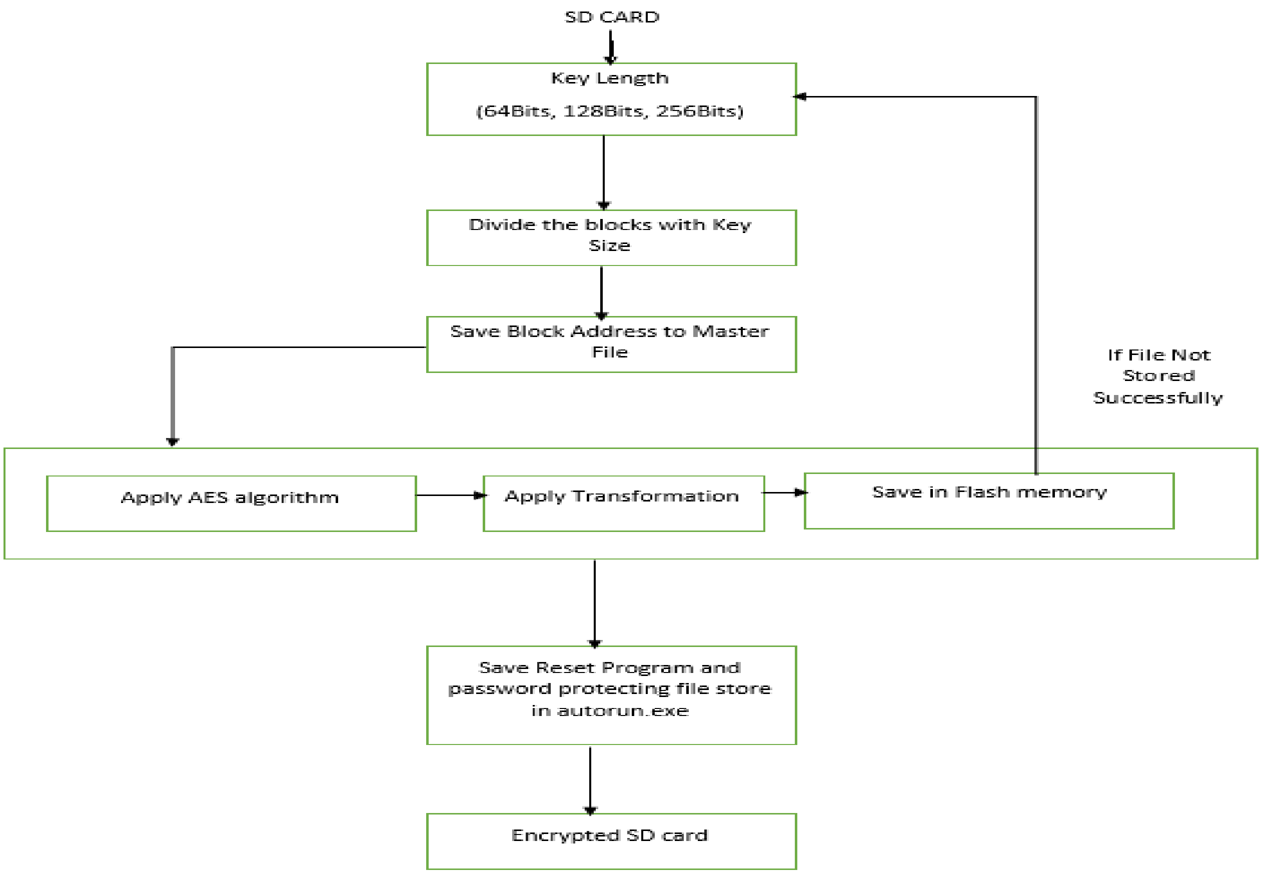

SD CARD
Key Length
(64Bits, 128Bits, 256Bits)
Divide the blocks with Key Size
Save Block Address to Master File
If File Not Stored Successfully
Apply AES algorithm
Apply Transformation
Save in Flash memory
Save Reset Program and password protecting file store in autorun.exe
Encrypted SD card

**Figure 3:-** Encryption Process of SD card.

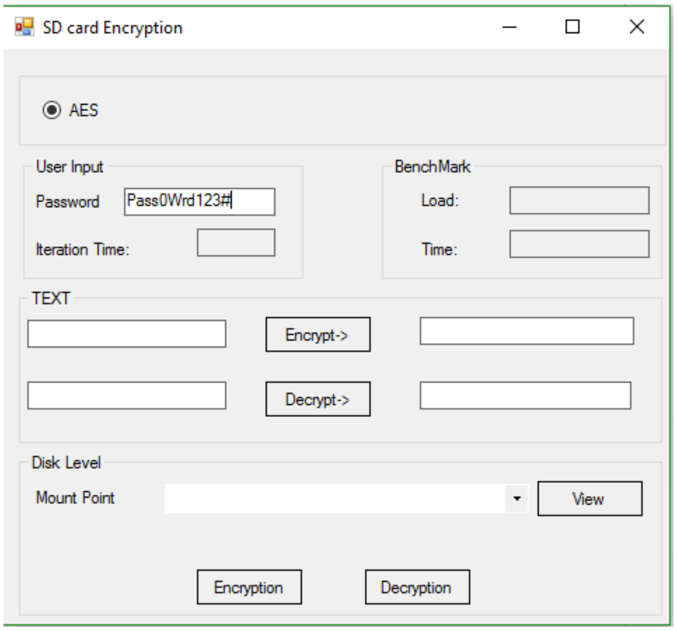
**Algorithm for Decrypting: -**

1. User Mounts SD card.
2. When User Opens the SD card Drive the Command prompt will be shown The user has to enter password, If password does not match the reset program will be executed will be formatted everything in SD card, after that the user still unable to save any content in SD card.
3. If password matches the block is divided with Key size.
4. After that the master file will assign the block with before encryption content.
5. Now the SD card is decrypted.

## Results:-

**Table 5.1:-** Comparison between existing method.

| | **Read** | **Write** | **Format** | **Platform support** | **Security** |
|---|---|---|---|---|---|
| Without Bitlocker | **YES** | **YES** | **YES** | **All platform** | **Less** |
| With Bitloker and Password | **YES** | **YES** | **YES** | **windows** | **More but not portable** |
| With Bitlocker and without Password | **NO** | **NO** | **YES** | **windows** | **Less** |
| With Bitlocker and EODAS without password | **NO** | **NO** | **NO** | **Windows, Ubuntu** | **More with portable** |
| With Bitlocker and EODAS with password | **YES** | **YES** | **YES** | **Windows, Ubuntu** | **More with portable** |



● AES

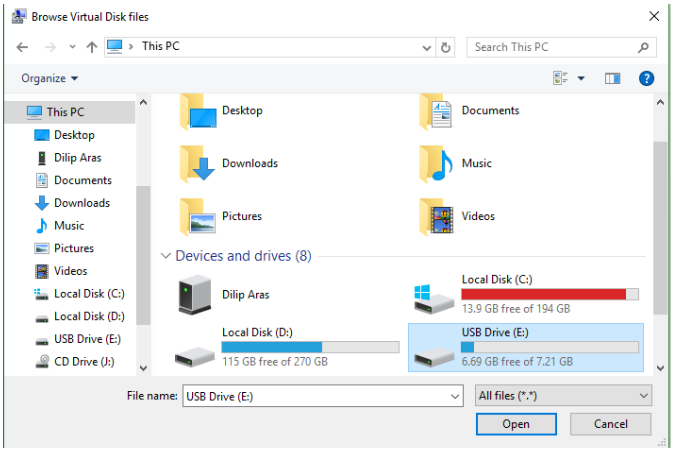
Password Pass0Wrd123#

Iteration Time:

**Figure 4:-** GUI for Mount Point.

In figure [4] the user select Mount Point and Enter password based on password the Key length will be taken,if user has given less time it will take less time to encrypt,It will display how much time it has taken for loading and how much time it takes for encrypting complete disk using this Approach.

**Select Disk Location:-**



File name: USB Drive (E:)

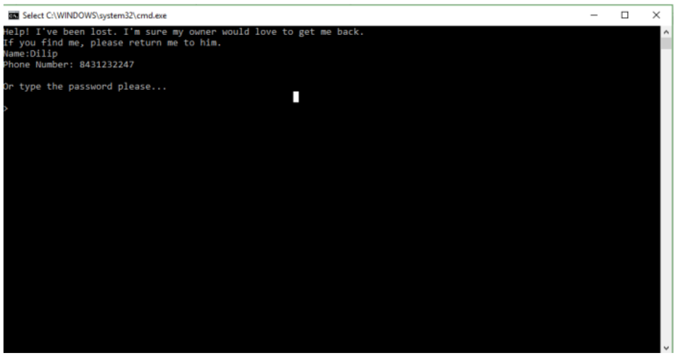
All files (*.*)

**Figure 5:-** Select Disk Location.

In figure [5] if the user wants to decrypt the disk he will first select disk location in my computer, If user decrypts SD card the SD card is no more secure it just clears the password and encryption information from Autorun.exe.

**SD Card Reset Operations:-**

When User Opens the SD card drive the Command prompt will show in which user has to enter password, if password does not match the reset program will be executed and will be formatted everything in SD card



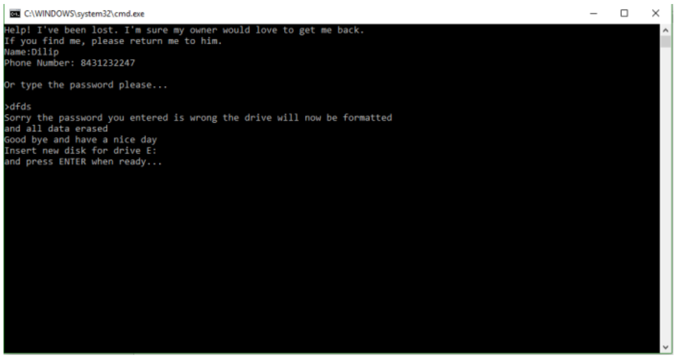
```
Help! I've been lost. I'm sure my owner would love to get me back.
If you find me, please return me to him.
Name:Dilip
Phone Number: 8431232247

Or type the password please...

>
```

**Figure 6:-** Enter Password Screen.

If user enters Wrong Password the Disk will be formatted.



```
Help! I've been lost. I'm sure my owner would love to get me back.
If you find me, please return me to him.
Name:Dilip
Phone Number: 8431232247

Or type the password please...

>dfds
Sorry the password you entered is wrong the drive will now be formatted
and all data erased
Good bye and have a nice day
Insert new disk for drive E:
and press ENTER when ready...
```

**Figure 7:-** Displays Error Message Screen.

The SD card data completely formated and hence unknown user can not get any information.

## Conclusions:-

The AS-SSD-Benchmark tool is used to help to determine the speed of the Bit Locker Disk encryption in both read/write operation. We suggest to encrypt the disk using Bit-Locker and new way of resetting the disk, if the password as entered wrong for 5 times the disk will be formatted.so far we tested in two platforms (windows, Ubuntu) if idea succeeded we will try to improve in all platforms.

The encryption is faster and more secure with reset option and disabling the format option under Context Menu which was the disadvantage in Bit locker drive encryption security. Then we proposed ideas in order to construct an encrypt once and decrypt in many devices, we verified the feasibility of our ideas by making a performance analysis which involves experiments on a popular mobile platform and popular desktop operating system.

## References:-

1. P Gasti and Y Chen, "Breaking and fixing the self encryption scheme for data security in mobile devices," in 18th Euromicro Conference on Parallel, Distributed and Network-Based Processing, PDP 2010, February 17, 2010 - February 19, 2010, Pisa, Italy, 2010, pp. 624-630.
2. Y Chen and WS Ku, "Self-Encryption Scheme for Data Security in Mobile Devices," 2009 6th IEEE Consumer Communications and Networking Conference, Las Vegas, NV, 2009, pp. 1-5.
3. F Shao, Z Chang and Y Zhang, "AES Encryption Algorithm Based on the High Performance Computing of GPU," 2010 Second International Conference on Communication Software and Networks, Singapore, 2010, pp. 588-590.
4. M Mathur and A Kesarwani, "Comparison between Des, 3des, Rc2, Rc6, Blowfish And Aes". In Proceedings of National Conference on New Horizons in IT-NCNHIT,2013.
5. T Nie and T Zhang, "A study of DES and Blowfish encryption algorithm," TENCON 2009 - 2009 IEEE Region 10 Conference, Singapore, 2009, pp. 1-4.
6. KN Manjesh and RK Karunavathi. "Secured High throughput implementation of AES Algorithm". International Journal, volume 3,Issue 5,May 2013.
7. Gang Hu, "Study of file encryption and decryption system using security key," 2010 2nd International Conference on Computer Engineering and Technology, Chengdu, 2010, pp. V7-121-V7-124.
8. N Agwankar,Dr.S Surve,Prof.S Prabhu,R Nayak, " Security For Portable Data Storage media." in IJARCCE International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 1, April 2013
9. Y Wang and Y Alshboul, "Mobile security testing approaches and challenges," 2015 First Conference on Mobile and Secure Services (MOBISECSERV), Gainesville, FL, 2015, pp. 1-5.
10. L Aron and P Hanacek, "Overview of security on mobile devices," 2015 2nd World Symposium on Web Applications and Networking (WSWAN), Sousse, 2015, pp. 1-11.
11. OP Verma, R Agarwal, D Dafouti and S Tyagi, "Peformance analysis of data encryption algorithms," 2011 3rd International Conference on Electronics Computer Technology, Kanyakumari, 2011, pp. 399-403.
12. TN Shankar, G Sahoo and S Niranjan, "Image Encryption for mobile devices," 2010 International Conference On Communication Control And Computing Technologies, Ramanathapuram, 2010, pp. 612-616.
13. L Yu, Z Wang and W Wang, "The Application of Hybrid Encryption Algorithm in Software Security," 2012 Fourth International Conference on Computational Intelligence and Communication Networks, Mathura, 2012, pp. 762-765.
14. WX Zhang, SY Xiao and Y Zhang, "Research on Image-Text Encryption Techniques in Mobile Communications," 2010 Second WRI Global Congress on Intelligent Systems, Wuhan, 2010, pp. 115-118.
15. V Shokeen and N Yadav,"Encryption and Decryption Technique for Message Communication" IJECT Vol 2,Issue 2,June 2011.
16. BV Sandeep, NG Cholli, and S Bandi, "Securing Applications in Windows Phone." In International Journal Of Electronics And Computer Science Engineering,2012.
17. P Srinivasarao, PV Lakshmipriya, PCS Azad, T Alekhya, K.Raghavendrarao, and K.Kishore, "A Technique for Data Encryption and Decryption." International Journal of Future Generation Communication and Networking, 2014, pp.117-126.
18. J Yi-ming and L Sheng-li, "The Analysis of Security Weakness in BitLocker Technology," 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing, Wuhan, Hubei, 2010, pp. 494-497.
19. H Rui,JZ Gang and WB Liang.,"Application research and Analysis based on Bitlocker-Data protection & Secure Start-up of Windows 7.", 2014 Journal of Chemical and Pharmaceutical Research,2014, pp.491-497.
20. S Turpe,A Poller and J Steffan.," Attacking the BitLocker boot process." In International Conference on Trusted Computing,April 2009, pp.183-196.
21. Article title. http://www.in.techspot.com/downloads/benchmarking/as-ssd-benchmark-1-8-5636/articleshow/47590422.cms. Date accessed: 09/08/2016.