Improvements in Secure Deletion Mechanism for Crucial Data on Android Gadgets

M. Ali Tariq[1] and M. J. Arshad[2]

[1,2]Department of Computer Science and Engineering, University of Engineering and Technology, Lahore, Pakistan

[1]alitariq16@gmail.com

***Abstract*– In the current era, due to the advancement of technology and improved services, use of smartphones is becoming more popular day by day. The use of smartphones is not only restricted to instant messages and calls but people also perform business transactions and social networking as well. But with the massive use of phones the safety and security of data is always a critical issue if the phone is stolen, lost or fell into the custody of an adversary. While mostly data communication is secured through encryption but due to the efficiency issues whole data can never be encrypted. Anyhow, normal deletion method also misleads the user into considering that all data had been removed but that's not the situation. On the other hand, once removed data from normal operations can be retained using various methods. We did analyze work done on the way to secure removal of data. Furthermore, to delete critical data, it offers some mechanism assuring that once data deleted this way can never be retained by any adversary.**

***Keywords*– Secure Deletion, Android OS, Flash Memory, Critical Data and Mobile Security**

I. INTRODUCTION

Nowadays, the utilization of advanced cell phones has turned into a fundamental piece of our life. With the progression of time, there has been a fast exponential development in the field of cell phone innovation also. The utilization of advanced cells is restricted not only for calls and texts as well as it performs different exercises like playing games, listening music, long range informal communication [9] and furthermore utilize it industrially for business exchanges.

However, by the speedy improvement of mobile phone advancement, the enthusiasm of people has been growing step by step. We can evaluate the significance of cell phone such that, in the first quarter of 2017, the International Data Corporations assembled data from their Worldwide Quarterly Mobile Phone Tracker [10] showing that Android rules showcase with 85% offer before iOS at 14.7% and Windows Phone at 0.1%. The market generally is so far making with Android showing new appearances on devices, for instance, TVs, Autos and splendid watches [11]. Information security is an expanding trade-off as more personal and critical data is put away in mobile phones. In this way, its security is an extremely basic issue for a man in any shape. However, when a gadget is stolen, lost or incidents whenever or on the off chance that anybody sales his/her gadget at that point there is a noteworthy security issue of information procurement by any outsider and which is extremely critical [1].

As indicated by these security issues there is a need of such a framework situation, to the point that must be given Android Operating System (OS) which offers information covering up or encryption at deletion time and at storage time. However, a great deal of work has been done in this field yet insufficient that can give contentment to the client about their information.

In this manner, the work theory is that "It is conceivable to present a procedure that will give an answer for protected erasure of basic information from personal gadget." Critical information that can be a few messages, pictures, sound, videos, and so on however our system is specific about the pictures. Consequently, the clients can have the capacity to erase their information safely and couldn't be recovered by any outsider.

Normal deletion method also misleads the user into considering that all data had been removed but that's not the situation. On the other hand, once removed data using normal operations can be retained using various methods. Secure data eradication in our work is meaning to a product based procedure for thoroughly deleting data from memory to the degree that can't be recovered. In the present age, deleting any report isn't secure eradication, yet rather to oust pointers by stamping it as open or free memory space.

It is, all things considered, in light of the fact that to the typical customer deleting a record is every now and again done just to recuperate the storage room instead of ensuring that his information can't be stolen or spilled. There is another factor which is that the protected deletion of information turns out to be exorbitant in the feeling of assets since it includes additional activities when contrasted with eradicating pointers. This strategy makes the evacuated data exist in the physical memory disregarding the way that they are not being referenced by anything anymore [2].

II. LITERATURE SURVEY

Secure deletion is a portion of the circumstances came to as lost, erased, deleted, completely expelled, reliably evacuated, self-destructed and destroyed [3]. The content in this stage is about the examination work that has been done already in the zone of secure erasure. We review different techniques that had been already gotten this field of research.

Normally, secure cancellation more regularly than overwriting the information to make it unrecoverable and information overwriting can be performed through coding program running on the OS. A few specialists like Joukov et al. [5] agreed that overwriting once is in all probability adequately secure, in spite of the way that this view isn't generally shared by others. For example Gutmann P. [6], recommended a 35-pass overwriting layout and in like way he cleared up that few passes (as opposed to 35 passes) ought to be sufficient in by far most of conditions. However, Joukov et al. [5] similarly cleared up that it is conceivable to recoup data utilizing a one-pass wipe is an immediate after effect of more old prepared hard drives having holes among "tracks" and such holes are not found in the present high-thickness hard drives. In any case, memory couldn't depend upon key information overwriting for secure erasure. File Translation Layer overwrites logical address, and additionally appropriates write access crosswise over storage.

Kang et al. [7] proposed another procedure for information wiping for mobile phones, instead of overwriting the entire data, it simply overwrites part of the data that will render it unidentifiable. Their approach is arranged only for data of the going with record outlines, specifically organizes Bitmap (BMP), Joint Photographic Experts Group (JPEG), Microsoft Excel Spreadsheet File (XLS), Flash Live Video (FLV), and Document (DOC). No encryption calculation was utilized as a part of the wiping strategy proposed by Kang et al. It utilized Endless overwriting a couple of bytes of a document to wipe and after that avoiding a settled interval. On the off chance that there are escape clauses in their approach. One of them is that, to upgrade the productivity some measure of security is surrendered. It is a keen way to deal with help the customers to wipe their data in light of their honest to goodness needs instead of settling on a decision by the procedure itself.

While discussing the removal of ordinary records, A.M. Braga [1] has talked about in three stages, they are depicted as:

With standard erasure remove directed file logically.

All free space must be involved by composing a brief file of randomized information.

Logically expel that file when there is no free space any longer. Along these lines no basic information is behind as it cleanses all free memory.

While examining about all means, this technique has two shortcomings. To begin with, it requires some opportunity to quantify the free space to be cleaned and the speed of memory composing. Besides, this system can diminish the lifetime of memories, if used with high recurrence.

III. EXISTING ANDROID MOBILE APPLICATIONS

Top applications related to our work available on Google Play Store are:

A) Secure Delete

Most popular application available on the play store for secure deletion of data is Secure Delete [4]. This application is used to delete data securely from your device. It does provide multiple languages.

B) SDelete - File Shredder

SDelete is the popular application available on the play store for secure deletion of data [14]. A user can delete more than one files and folder at the same time. It follows overwrite Zeros (1 Pass) deletion standard.

C) Shreddit - Data Eraser

SHREDDIT is a popular application available on the play store for secure deletion of data [13]. It follows quick shredding algorithm. It shreds image or videos media files from gallery completely.

Considering difficulties for standard erasure of record, in this paper secure information removal procedure is proposed. It is hypothetical based encryption arrangement, constrained for pictures just and actualized by means of programming based android application named as Secure Wipe Application (SWipe-App).

IV. PROPOSED SYSTEM

In the wake of concentrate a couple of examines on secure erasure, we have characterized architecture that can empower client to eradicate his information totally from the gadget. It demonstrates a thorough examination and broad elaboration of every single part of the structure clarifying the major working and sole reason. The Proposed arrangement is involved both hypothetical and programming based arrangement. To begin with the product based arrangement essential architecture of the framework is given in Fig. 1.

The proposed design contains four sections. They joined team up all together to get required outcomes.

A) Source of Data

Source of data can be utilized to gather information for interpretation and after that, you can gain final consequences of information. In our situation, the source of data is a programming based application which is created in android. To perform secure cancellation of information our framework is made out of an application, almost

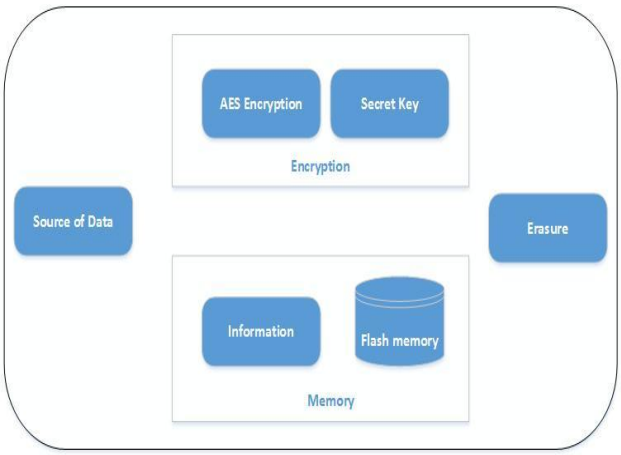

Fig. 1. Proposed System Architecture

certainly we can get to information from the advanced mobile phone specifically, however, getting to information exhaustive application empowers client to perform deletion tasks simply.

B) Memory

It included two sections, Flash memory, and information. As we realize that Android utilizes Flash memory, which is utilized as default memory for Android gadgets. The path toward securing new or eradicating existing data by an application generally occurs over various layers of the OSI model as appeared in Fig. 2.

Rundown of given model can be portrayed as, a client puts new or deletes data by an application, which changes data by utilizing Application Programming Interface (API) which additionally interfaces with the File System to deal with the given data. File System utilizes partition map that determines space apportioned or how much space is detracted from that point. At that point, data is passed to the File Translation Layer (FTL) which is utilized to remap logical block address and stores data to the physical address in flash storage.

Data is speaking to the information which is recovered from the flash memory of the gadget to perform the deletion. Our concentration in this work is just on pictures so for this situation data is just speaking to the picture that is accessible in the inside memory of gadget. A picture can be in any organization that could be Joint Photographic Experts Group (JPEG), Portable Network Graphics (PNG) and so forth. Assist this data is utilized to perform secure erasure.

C) Encryption

Third module of architecture is Encryption. The reason for encryption is to utilize it for concealing the first picture into some scrambled shape so that if there should be an occurrence of recuperation it can't be conceivable to get it in its original form impostor will get just the encoded picture. It comprises of two sections which join together to

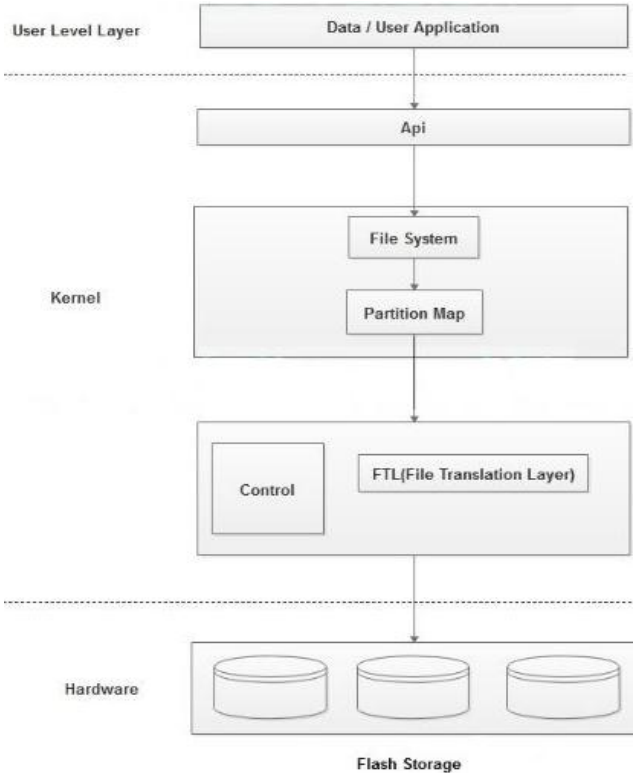

Fig. 2: Overview of OSI Model for Data Storage

perform encryption. They can be portrayed as:

AES Encryption: To encrypt the information, we have utilized Advanced Encryption Standards (AES). There are three square figures which involve the Advanced Encryption Standard (AES), they are AES-128, AES-192, and AES-256. The motivation behind this encryption procedure is to give quick, secure and solid encryption of the data. It is exceptionally challenging for an interloper to decipher encryption procedure and plain content from encoded data in light of the fact that during encryption, there is a great deal of perplexity and dissemination of information. It is likewise impervious to pattern assaults and Brute force assaults for the data which is scrambled by the created application.

Secret Key: With the utilization of AES encryption which has settled piece size of 128 and key size is 128, on the grounds that 128 bits are all that could possibly be needed for security. Longer keys suggest a slight computational overhead and furthermore, as to portable phone productivity, a 128-piece key is favored. Default elements of Android are utilized for encryption. Encryption method and method to create generate key are given in Fig. 3. While coding encryption and mystery key benchmarks characterized by [12] are obeyed.

The logic behind the erase order is that, as we probably aware pictures are made out of pixels. We have bit estimations of picture when we get to picture in our application. AES encryption is utilized here to scramble the picture. It requires the 128-bit secret key which is created

```
private static byte[] encrypt(byte[] raw, byte[] clear) throws Exception {
    SecretKeySpec skeySpec = new SecretKeySpec(raw, "AES");
    Cipher cipher = Cipher.getInstance("AES/CBC/PKCS5Padding");
    cipher.init(Cipher.ENCRYPT_MODE, skeySpec);
    byte[] cipherImage = cipher.doFinal(clear);

    return cipherImage;
}


public static SecretKey generateKey() throws NoSuchAlgorithmException {

    final int KeyLength = 128;

    SecureRandom secureRandom = new SecureRandom();
    KeyGenerator keyGenerator = KeyGenerator.getInstance("AES");
    keyGenerator.init(KeyLength, secureRandom);
    SecretKey key = keyGenerator.generateKey();
    return key;
}
```

Fig. 3: Encryption and Secret Key Function

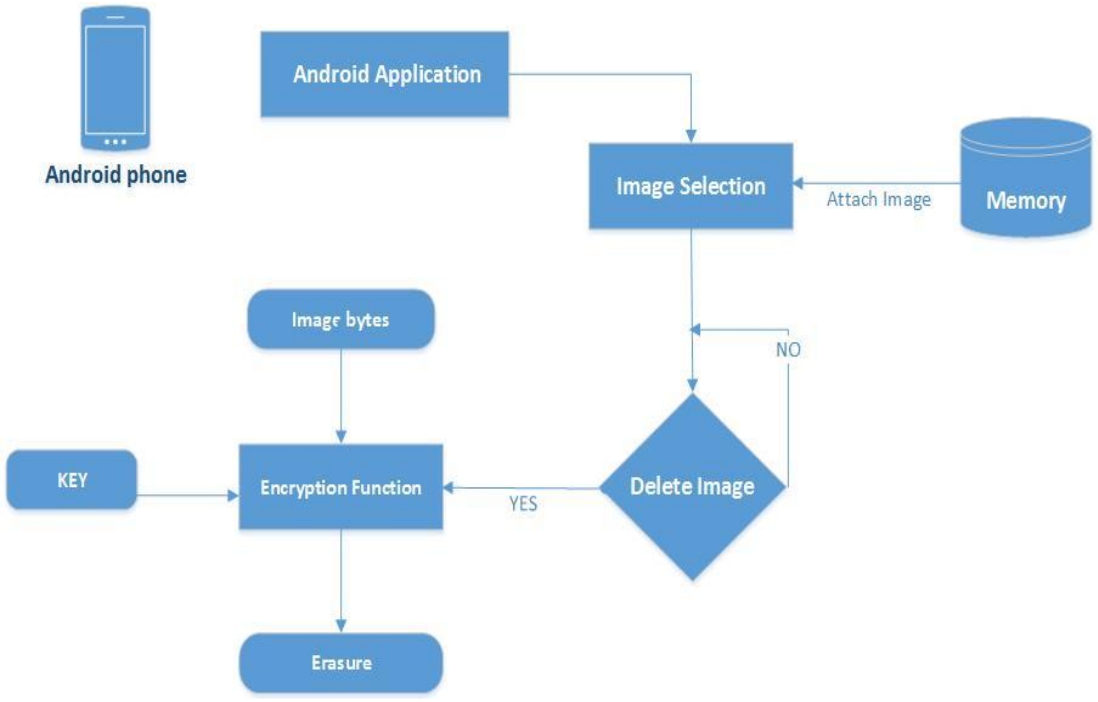

Fig. 4: Work Flow of Proposed Architecture

arbitrarily by another worked in technique for android programming. Both AES encryption technique and 128-bit secret key consolidates to encode the picture. All things considered picture are put away in the byte frame in the android memory.

As we realize that "When a record is erased, the operating system just erases the relating pointers in the document table and denotes the space that is involved by the record as free. Actually the document isn't erased and the information it contained still stays on the memory. Henceforth document isn't noticeable just in the index, all things considered it is available there until the point that the earlier area involved by erased records are over composed by more current substance. This is the purpose behind why most documents can be promptly recuperated even in the wake of erasing the records [8]".

When erase charge is given by the client, chose picture's bytes are encoded with the encryption key and afterward picture is erased from the memory the picture as well as secret symmetric key that is utilized to scramble the picture will likewise be erased for security reasons.

As portrayed when we erase a picture it just overlooks the

pointer of the picture that is stored in address memory however unique image information consequently moved and stored in the past block from where the data has been caught to be noticeable for the client, so as we have scrambled the picture with AES-128 bit encryption calculation, encoded picture will store in the block. Each time when you will erase a picture each time another secret key will be produced with the arbitrary capacity and toward the end when the picture will be erased the key will likewise be erased. When it is secure erasure there is no need of key to store as key is just used to decode the figure picture and contaminate it is secure when it can't be recouped in its unique shape.

On the off chance that we scramble picture before erasure the picture will be reestablished on the memory in encoded form. On the off chance that, if any invader recoups the picture that will be in a scrambled form it will require a similar key to decode the picture and to see it in the first original shape. That will enable us to keep our information to save in the sense that our information can't be recouped once erased.

To verify that our proposed software-based system (SWipe-App) gave desired results, we have examined it by passing through the data recovery tool. For this purpose android recovery application named Dumpster: Undelete & Restore Pictures and Videos was used. It has more than 10 Million users all with 4.1 rating on play store. Image with name test.jpg was tried. After deletion from our programmed application, it was recovered using Dumpster app. The image recovered is given in Figure 5. As it can be seen that recovered image is not in its original form. Hence we can say that our proposed system is working efficiently.

Table I provides the limitations of current applications available at Google Play Store that are used to delete data securely. None of the limitation is the part of our proposed system.

An examination of our method with the past system is given in Table II, which expounds likenesses and contrast between the two frameworks.

V. CONCLUSION

In this work, we introduced the review of information protection issues in cell phones that client needs to confront particularly in the event that when the gadget is sold by the client, he evacuates every one of his information into trusting that record have been eradicated, while that is ordinarily not the circumstance. Furthermore erased information can likewise be recovered utilizing distinctive systems. As per given circumstance, we have talked about the design of secure erasure of information from Android with its detail work process. We examined contextual analysis of our proposed framework which guides a client to erase their basic information with easy and proficient way utilizing a product based application having basic user interface and named as SWipe-App. With it, the client doesn't need to roll out improvements at the system level. Just client level cancellation drives the client to eradicate his information securely and it is confined to pictures as it were. Our future work is to quantify the security appraisal to genuine extend the solution, and furthermore upgrade this work to other information writes too like audios, documents, messages, and videos etc.

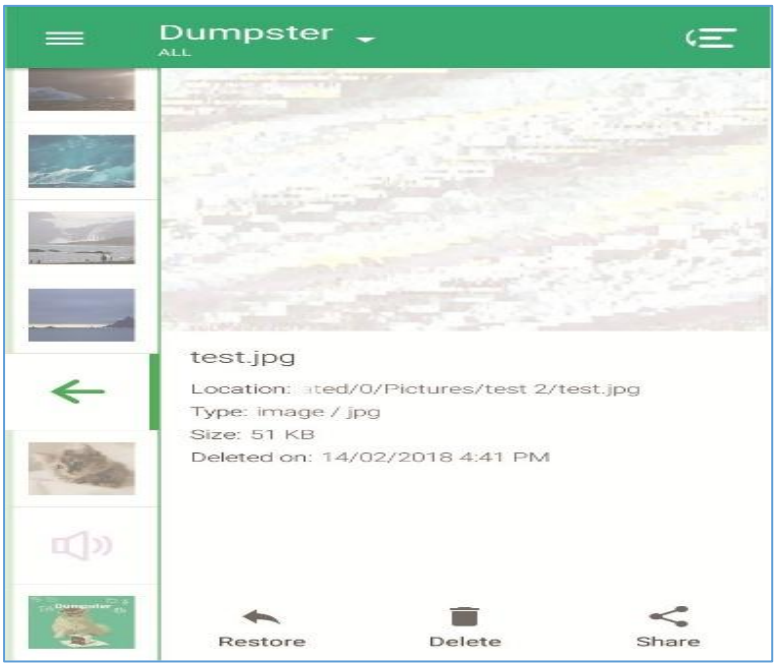

Fig. 5: Dumpster: Recovered Image

Table I: Limitations of existing applications on play store

Technique	Limitations
Secure Delete [4]	User needs to check wipe memory option otherwise data can be recovered using deep scan technique. Wiping takes more time and not efficient as well.
SDelete-File Shredder [14]	User has to delete thumbnails manually and also need to check wipe memory which is not efficient and it is time taking.
Shreddit-Data Eraser [13]	Required super rights of user i.e. user's device must be rooted.

Table II. Comparison of our system with existing technique

Technique	Encryption	User Level Deletion	Deletion Time	OS Modification	Memory Lifetime	Disadvantage	Efficiency
SWipe-App	Yes, image encrypted before deletion	Yes, as a common mobile app	Shorter erasure time	No, OS modification require	Long term as no need to occupy all free space	Limited data type (images only)	More efficient
A.M. Brag et al. [1]	No encryption for deletion	Yes, as a common mobile app	Longer erasure time	No, OS modification require	Shorten as uses high frequency	Additional operations like purging	Less as requires occupy and deletion of free space

REFERENCES

[1] A. Braga, A. Colito, "Adding Secure Deletion to an Encrypted File System on Android Smartphones," The 8th Inter Conf. on Emerging Security Information Systems and Technologies, pp. 106-110, Nov. 2014.

[2] E. S. Høgset, "Investigating the Security Issues Surrounding Usage of Ephemeral Data within Android Environments," UiT Norges arktiske universitet, 2015.

[3] J. Reardon, D. Basin, and S. Capkun, "Sok: Secure data deletion," in Security and Privacy (SP), 2013 IEEE Symposium on, pp. 301-315, IEEE, 2013

[4] "Secure Delete" December, 2017. [Online]. Available: https://play. google.com/store/apps/details?id=com.peterhohsy.securedelete &hl=en. [Accessed: February 19, 2018].

[5] N. Joukov, H. Papaxenopoulos, and E. Zadok, "Secure Deletion Myths, Issues, and Solutions," ACM Workshop on Storage Security and Survivability, pp. 61-66, 2006.

[6] P. Gutmann, "Secure Deletion of Data from Magnetic and Solid-State Memory," in Proceedings of the Sixth USENIX Security Symposium. pp. 77-89, 1996.

[7] S.-H. Kang, K.-Y. Park, and J. Kim, "Cost Effective Data Wiping Methods for Mobile Phone," Multimedia tools and applications, vol. 71, pp. 643-655, 2014.

[8] J. Shu, Y. Zhang, J. Li, B. Li, and D. Gu, "Why Data Deletion Fails? A Study on Deletion Flaws and Data Remanence in Android Systems," ACM Transactions on Embedded Computing Systems (TECS), vol. 16, p. 61, 2017.

[9] "Exclusive Media for Future," [Online]. Available: http://www. trffcmedia.com/topics/why-are-smartphones-so-important-in-daily-life/. [Accessed: December 28, 2017].

[10] "Analyze the Future," [Online]. Available: https://www.idc.com /promo/smartphone-market-share/os. [Accessed: January 3, 2018].

[11] "Android is for everyone," [Online]. Available: https://www. android.com/. [Accessed: November 27, 2017].

[12] "Developers," [Online]. Available: https://developer.android.com /reference/javax/crypto/Cipher.html. [Accessed: December 2, 2017].

[13] "Shredit," March 2, 2018. [Online]. Available: https://play. google.com/store/apps/details?id=com.palmtronix.shreddit.v1. [Accessed: March 8, 2018].

[14] "SDelete," September 15, 2017. [Online]. Available: https://play. google.com/store/apps/details?id=com.vb2labs.android.sdelete &hl=en. [Accessed: Feb. 19, 2018].