ISSN 2395-1621

Securing Personal Images using Image Encryption Technique

[#1]Swati Horgar, [#2]Shweta Gaikwad, [#3]Aboli Kolhe, [#4]Patil Gayatri,
[#5]Prof. V.B.Kadam

[1]swatihorgar@gmail.com,
[2]shwetagaikwad2214@gmail.com,
[3]abolikohle@gmail.com,
[4]patilgauri159@gmail.com

[#12345]Computer Engineering,
JSPM's Bhivarabai Sawant Institute Of Technology and Research (BSIOTR)
Savitiribai Phule Pune University India.

ABSTRACT

In this paper we identified Application problem, so users are constantly at risk of installing malicious apps that steal personal data or gain root access to their device. For example, while using such malicious application, the response from application provider may contain the hidden request to have control on different devices connected to our mobile such as camera, front or main no issues phone is been attacked. This paper implement new security threats are emerged for mobile devices. We implement secure communication using the encryption technique using the AES algorithm for user stored personal data (Images) on cloud server. We provide the two modes for storing the personal images on local cloud. First is normal mode another is secure mode. In Normal mode images stored without apply encryption process, and secure mode encryption process will generated. So advantages of the proposed system is securely stored camera captured images on local cloud server.

ARTICLE INFO

Article History

Received: 24th April 2017

Received in revised form :

24th April 2017

Accepted: 24th April 2017

Published online :

28th April 2017

Keywords: Secure Image Transfer, Encryption, Privacy.

I. INTRODUCTION

Mobile phones are becoming important part of our day to day life specially the smart phones, since they are involved in keeping in touch with friends and family, doing business, accessing the internet and other activities. Andy Rubin, Google's director of mobile platforms, has commented: "There should be nothing that users can access on their desktop that they can't access on their cell phone" [1]. Growth in smart phone sales is depicted in the figure below.

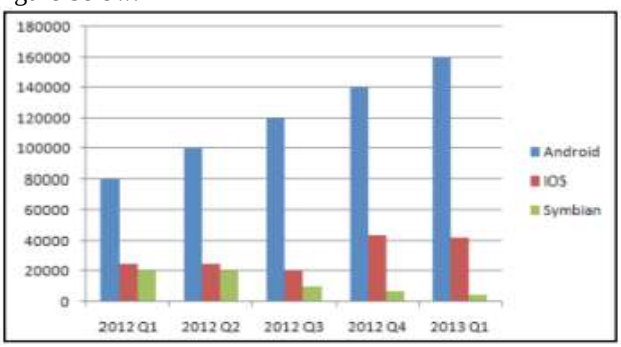

Fig. 1: Smartphone Sales Worldwide

It indicates that smart phone sales are continuously on rise and more and more people are becoming dependent on these devices. As these smart phones are going to outnumber the world's total population in 2014, securing these devices has assumed paramount importance. Owners use their smart phones to perform tasks ranging from everyday communication with friends and family to the management of banking accounts and accessing sensitive Work related data. These factors, combined with limitations in administrative device control through owners and security critical applications like the banking transactions, make Android-based Smart phones a very attractive target for hackers, attackers and malware authors with almost any kind of motivation. Smart phones retrieve apps from application markets and run them within a middleware environment.

Existing smart phone platforms rely on application markets and platform protection mechanisms for security. The fig. 2 shows the general architecture of smart phones.

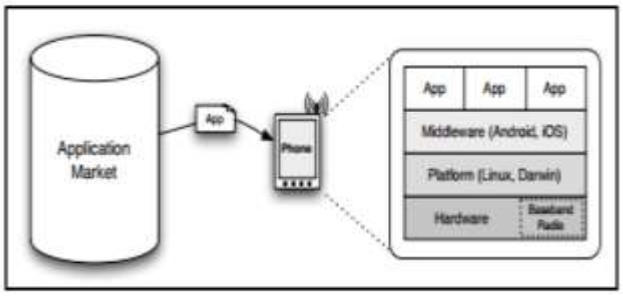

Fig. 2: General Smart Phone Architecture

The rest of the paper is organized as follows: Section 2 present problem statement, Section 3 presents our proposed system, Section 4 present our result analysis system and finally, Section 5 concludes the paper.

III. PROBLEM STATEMENT

Mobile devices implementing Android operating systems inherently encourage opportunities to create and implement malicious software. This opportunity increases as dissemination of the Android OS to standalone devices, such as cameras, increases. The problem intensifies when these devices utilize cloud storage service capabilities. Previous security and forensics research is focused on Android malware detection, data leakage and operating system modifications.

IV. PROPOSED SYSTEM

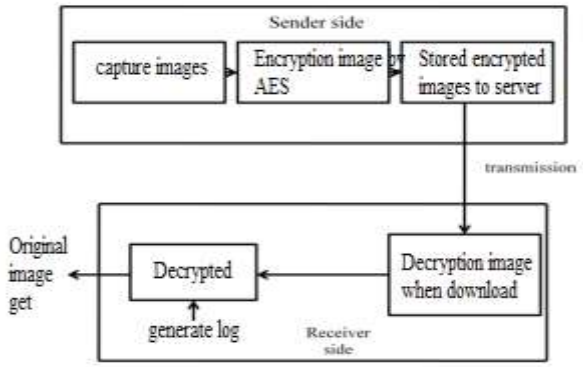

Fig 3. System process

Capture images:
Camera use is popular with several applications that encourage photo sharing; hackers are finding sneaky ways to exploit them. Camera technically requires a preview to be displayed on screen, but background services do not have associated visible activity.

Encryption AES Algorithm:

Encryption process has two inputs one image which is already converted into plain text and one encryption key.

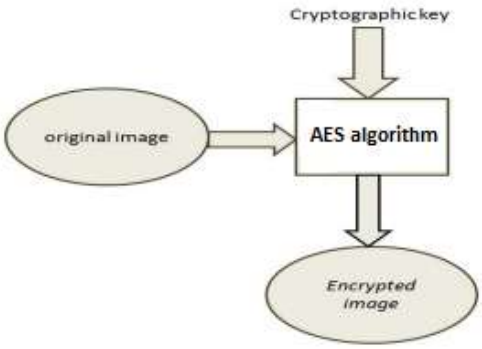

Fig 4. Encryption

The encrypted image is divided into same block length of DES algorithm. First block of 64 bit is entered into the function and same cryptographic key is used for decryption but this is used in the reverse order.

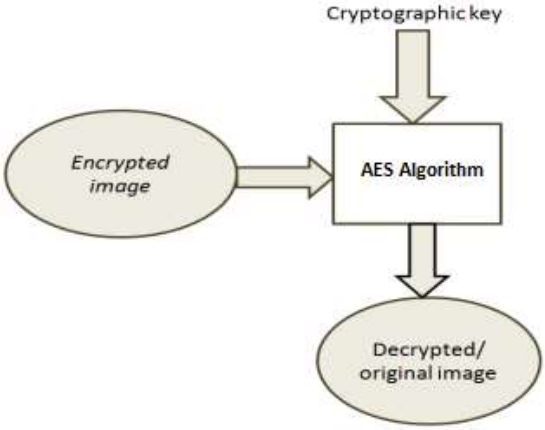

Fig 5. Decryption

Advantages:

1. The proposed system provides authencation.
2. It also prevents hacking.
3. It uses Encryption algorithm for image secure
4. The system prevents identity theft.
5. It also provides security to the user personal data.

V. MATHEMATICLA MODEL

Our system can be represented as a set
System S = {I, O, C}
Where,
I=set of inputs
O=set of outputs
C = set of constraints
Input
Input I = {Login, Request}
Login = {Username, Password}
Request = {Upload images, Search images, download images, Apply security, View History}
Users = {User, Service provider}
Username = {Username1, Username2… Username n}
Password = {Password1, Password2… password n}

Output
Output O = {Display uploaded images, Download start, Prevent hacking, Display history}
Constraint
C = "User should login to the system

VI. RESULT

Fig 6. System login

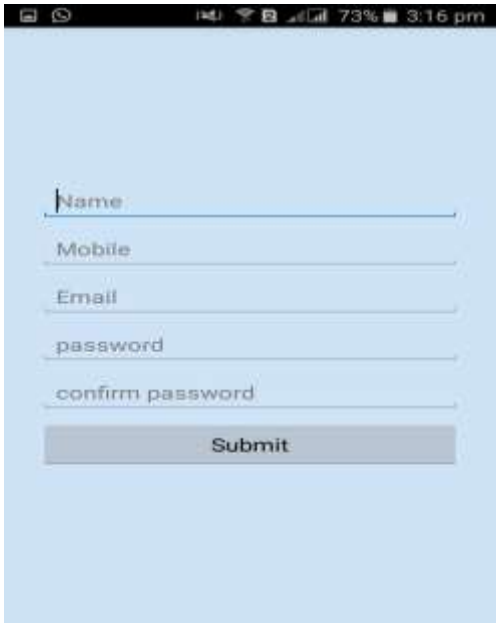

Fig 7. System registration

Fig 8. Capture images from camera

Fig 9. Images store secure or normal mode option

Fig 10. Download images

VII. ACKNOWLEDGEMENT

I wish to express my profound thanks to all who helped us directly or indirectly in making this paper. Finally I wish to thank to all our friends and well-wishers who supported us in completing this paper successfully I am especially grateful to our guide Prof. V.B.Kadam for time to time, very much needed, valuable guidance. Without the full support and cheerful encouragement of my guide, the paper would not have been completed on time.

VIII. CONCLUSION

In this paper, we presented the most challenging aspects in cloud are guaranteeing user privacy and the provision of mobile application security that uses cloud resources. We also provide security detected the owner's account information but did not display any information associated with the hacker's account.

REFERENCE

[1] McMillan, J., W.B. Glisson, and M. Bromby, Investigating the Increase in Mobile Phone Evidence in Criminal Activities, in Hawaii International Conference on System Sciences (HICSS-46). 2013, IEEE: Wailea, Hawaii.

[2] Berman, K., W.B. Glisson, and L.M. Glisson, Investigating the Impact of Global Positioning System (GPS) Evidence in Court Cases, in Hawaii International Conference on System Sciences (HICSS-48). 2015, IEEE Kauai, Hawaii.

[3] Zhang, X. and W. Du, Attacks on Android Clipboard,in Detection of Intrusions and Malware, and Vulnerability Assessment, S. Dietrich, Editor. 2014, Springer International Publishing. p. 72-91.

[4] Grace, M., et al., RiskRanker: scalable and accurate zero-day android malware detection, in Proceedings of the 10th international conference on Mobile systems, applications, and services. 2012, ACM: Low Wood Bay, Lake District, UK. p. 281-294.

[5] Biggs, S. and S. Vidalis. Cloud Computing: The impact on digital forensic investigations. in Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference for. 2009.

[6] Huang, J., et al., AsDroid: detecting stealthy behaviors in Android applications by user interface and program behavior contradiction, in Proceedings of the 36th International Conference on Software Engineering. 2014, ACM: Hyderabad, India. p. 1036-1046.

[7] Christos Kynigos, William Bradley Glisson, Todd McDonald: Utilizing the Cloud to Store Hijacked Camera Images, IEEE Computer Society, 49th Hawaii International Conference on System Sciences, 1530-1605/16, 2016.

