ISSN 2395-1621

Utilizing the Cloud Attacks on Personal Images

[#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

Data over the cloud is transferred or transmitted between servers and users. Privacy of that data is very important as it belongs to personal information. If data get hacked by the hacker, can be used to defame a person's social images. Sometimes delays are observed during data transmission. i.e. Mobile communication, bandwidth is low. Hence compression algorithms are proposed for fast and efficient transmission, encryption is used for security purposes and blurring is used by providing additional layers of security. These algorithms are hybridized for having a robust and efficient security and transmission over cloud storage system.

Keywords: Secure Image Transfer, Encryption, Privacy.

ARTICLE INFO

Article History

Received: 8th October 2016

Received in revised form :

8th October 2016

Accepted: 12th October 2016

Published online :

19th October 2016

I. INTRODUCTION

Every user require secure storage and safe data transmission. Several trends are there in cloud computing, which are an internet based deployment. The more powerful processors together with the (SaaS) software as a service computing architecture, transforming data centers into pools of service on large scale. To subscribe high quality services we have to increase network bandwidth, yet flexible connections can be made. As we know that data security is an important term of (QOS) quality of service, cloud computing has to invent new challenging security threats for number of reasons. firstly, traditional cryptographic primitives are the most basic blocks which are used to build cryptographic protocols and security. various kind of user's data is stored on cloud and demand for secure and safe data for long term and verifying the correctness of that data in the cloud becomes even more challenging. Secondly, cloud computing is not just a third party data warehouse. The data stored in the cloud is continuously changing by including insertions, deletion , modification , appending, recording . basically the stored data is frequently updated by users. It is the paramount important to ensure the correctness of data under such dynamic data updates. However, this dynamic feature also makes the traditional integrity insurance technique futile and entails new solutions.

User's data is redundantly stored on multiple physical locations to further reduce the data integrity threads. Last, but not the least, deployment of cloud computing is powered by data centers running in the cooperated, simultaneous and distributed manner. Here, distributed are used to ensure the correctness of data in cloud for achieving the secure and robust cloud data storage system in real world.

In this paper, we focus on number of techniques available for preventing attacks on cloud.

The rest of the paper is organized as follows: literature survey is presented in Section 2. Section 3 presents overview of existing system techniques, Section 4 present problem statement, Section 5 present our proposed system and finally, Section 6 concludes the paper.

II. LITERATURE SURVEY

In the last few years, due to advancements in technologies, mobile communication devices and Personal Digital Assistants (PDAs), such as the iPhone and Blackberry, are now not limited to making voice calls only, instead they are used for browsing the Internet and accessing emails in plethora, and as the technology is progressing, it is becoming cheaper, thereby easily available and accessible to more and more people. Although the amount of data stored in such devices is much less as compared to the amount of data stored in computers, In this section we presented, survey of previously proposed system on different attacks on cloud data.

McMillan, J., W.B. Glisson, and M. Bromby,[1], The research identified the magnification of mobile devices in everyday life prompts the idea that these devices will increasingly have evidential value in criminal cases. While this may have been assumed in digital forensics communities, there has been no empirical evidence to support this idea. This research investigates the extent to which mobile phones are being used in criminal proceedings in the United Kingdom thorough the examination of appeal judgments retrieved from the Westlaw, Lexis Nexis and British and Irish Legal Information Institute (BAILII) legal databases. The research identified 537 relevant appeal cases from a dataset of 12,763 criminal cases referring to mobile phones for a period ranging from 1st of January, 2006 to 31st of July, 2011. The empirical analysis indicates that mobile phone evidence is rising over time with some correlations to particular crimes.

Berman, K., W.B. Glisson, and L.M. Glisson,[2], This study investigates the continued amalgamation of Global Positioning Systems (GPS) into everyday activities stimulates the idea that these devices will increasingly contribute evidential importance in digital forensics cases. This study investigates the extent to which GPS devices are being used in criminal and civil court cases in the United Kingdom through the inspection of Lexis Nexis, Westlaw, and the British and Irish Legal Information Institute (BAILII) legal databases. The research identified 83 cases which involved GPS evidence from within the United Kingdom and Europe for the time period from 01 June 1993 to 01 June 2013. The initial empirical analysis indicates that GPS evidence in court cases is rising over time and the majority of those court cases are criminal cases.

Zhang, X. and W. Du,[3], He perform a thorough study on the risks imposed by the globally accessible Android Clipboard. Based on the risk assessment, we formulate a series of attacks and categorize them into two groups, i.e., manipulation and stealing. Clipboard data manipulation may lead to common code injection attacks, like JavaScript injection and command injection. Furthermore, it can also cause phishing attacks, including web phishing and app phishing. Data stealing happens when sensitive data copied into the clipboard is accessed by malicious applications. For each category of attack, we analyze a large number of candidate apps and show multiple case studies to demonstrate its feasibility. Also, app analysis process is formulated to benefit future app development and vulnerability detection. After a comprehensive exposure of the risk, he briefly discuss some potential solutions.

Grace, M., et al.,[4], He propose a proactive scheme to spot zero-day Android malware. Without relying on malware samples and their signatures, our scheme is motivated to assess potential security risks posed by these untrusted apps. Specifically, we have developed an automated system called RiskRanker to scalably analyze whether a particular app exhibits dangerous behavior (e.g., launching a root exploit or sending background SMS messages). The output is then used to produce a prioritized list of reduced apps that merit further investigation. When applied to examine 118,318 total apps collected from various Android markets over September and October 2011, our system takes less than four days to process all of them and effectively reports 3281 risky apps. Among these reported apps, we successfully uncovered 718 malware samples (in 29 families) and 322 of them are zero-day (in 11 families). These results demonstrate the efficacy and scalability of RiskRanker to police Android markets of all stripes.

Biggs, S. and S. Vidalis,[5], The magnification of mobile devices in everyday life prompts the idea that these devices will increasingly have evidential value in criminal cases. While this may have been assumed in digital forensics communities, there has been no empirical evidence to support this idea. This research investigates the extent to which mobile phones are being used in criminal proceedings in the United Kingdom thorough the examination of appeal judgments retrieved from the Westlaw, Lexis Nexis and British and Irish Legal Information Institute (BAILII) legal databases. The research identified 537 relevant appeal cases from a dataset of 12,763 criminal cases referring to mobile phones for a period ranging from 1st of January, 2006 to 31st of July, 2011. The empirical analysis indicates that mobile phone evidence is rising over time with some correlations to particular crimes.

Huang, J., et al, [6] he propose a novel technique to detect such stealthy behaviour. In this model stealthy behaviour as the program behavior that mismatches with user interface, which denotes the user's expectation of program behavior. he use static program analysis to attribute a top level function that is usually a user interaction function with the behavior it performs. Then he analyze the text extracted from the user interface component associated with the top level function. Semantic mismatch of the two indicates stealthy behavior. To evaluate AsDroid, we download a pool of 182 apps that are potentially problematic by looking at their

permissions. Among the 182 apps, AsDroid reports stealthy behaviors in 113 apps, with 28 false positives and 11 false negatives.

Christos Kynigos, William Bradley Glisson, Todd McDonald, [7], The 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.

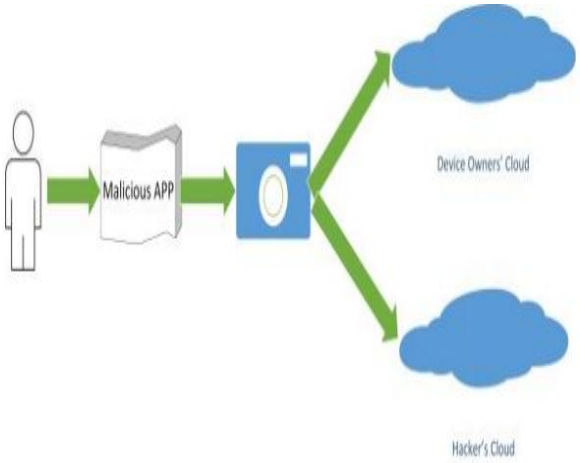

Fig 1. Existing System

III. PROBLEM STATEMENT

In this existing research paper, aims to investigate the plausibility of developing malware for an Android Operating System (OS) installed on a camera and utilize the cloud for storage capture. The approach used in this research utilizes a first complete pass at an iterative implementation of a design science methodology that follows the general activities as defined by existing system. The high-level problem statement focuses on the utilization of the cloud to store hijacked data.

IV. PROPOSED SYSTEM

We study there are appears to be a growing interest in the mobile phone area. Specifically, research has examined the social impact mobile phone technology has made on mainstream culture. We examined user behaviour when a mobile phone is lost. This study looks at ways in which users cope when they lose their mobile device, personal data, and access to social networks. This research does not mention the legal implications of the loss, nor does it examine the legal position where the device could be used to prosecute for theft or fraud. So our system provide the security policy when any hacker access user account and check all data then we maintain the security that situation explain module section.

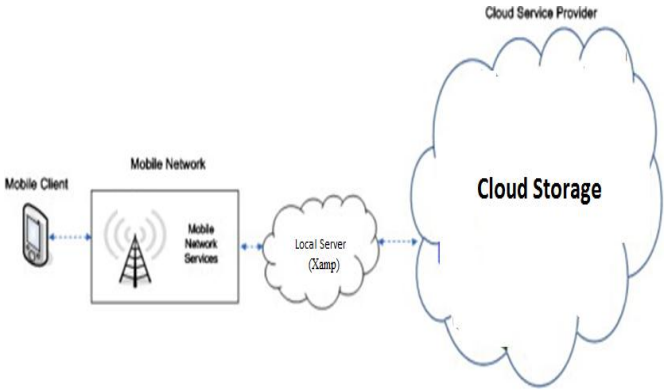

Fig 2. System architecture

Module Explanation:

User Module:

User can authorize login access. He can update all personal images. He also cans authority to generated secure encryption process. We achieve the security, on storing personal images on cloud.

Upload Image:
User uploaded image while account creation. That image is encrypted.

Admin Module:

Admin is the authorized person, he check all the user activity records as well as profile. Admin have also authority block particular user account if any user can perform any malicious activity.

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. 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.

