Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 5, May 2015, pg.683 – 688

RESEARCH ARTICLE

Secured Image Transmission over Cloud using Device Obscurity

Pratiksha
Department of Computer Science & Engineering, M.Tech, Punjab Technical University, India
pratikshasrivastav@hotmail.com

Abstract— In this paper, we present an encrypted image transmission system to secure the storage of data and ensure its authorized access at different levels so that its usability and integrity are maintained. We discover Encrypted image transmission over the cloud, to maintain the device obscurity. Hence it provides security to both the sender and receiver ends. It involves obscurity techniques which hide the data from hackers.

Keywords— Android, cloud computing, device obscurity, Mobile device, cloud

INTRODUCTION

The term “cloud”, is a network diagrams that represented the internet, or various parts of it, as schematic clouds .Cloud computing is mainly used for sharing computing resources. It is basically a internet based computing where different services like server, storage and applications to organization’s computer and devices through the internet Mobile devices are increasingly being used for capturing and spreading images of popular uprisings and civil disobedience. To keep such records hidden from authorities, deniable storage encryption may offer a viable technical solution. The users face problem to manage the security and integrity of their data because of the security issues wherein the data become extremely vulnerable to be hacked from any part of the world by any person and in order to avoid it we needed mechanisms that protect the data comprehensively. Security is the main issue to protect our transactions of files on the cloud.

Hence to protect our data we need of an application that implements a large scale of encoding mechanisms which also involve obscurity techniques because encoding and hiding of data from hackers are two very strong and significant aspects to protect our data. Cloud provides the following services:

Software as a Service (SaaS) — Consumers purchase the ability to access and use an application or service that is hosted in the cloud.

Platform as a Service (PaaS) — Consumers purchase access to the platforms, enabling them to deploy their own software and applications in the cloud.
Infrastructure as a Service (IaaS) — Consumers control and manage the systems in terms of the operating systems, applications, storage, and network connectivity, but do not themselves control the cloud infrastructure.

PROPOSED IMPLEMENTATION

In our proposed implementation, there would be two things of the project namely Android and Cloud. There will be a Sender & Receiver who will register themselves on a website called a cloud service for obtaining user id. Sender will login the Android application with user id and password of the account created on cloud. After login, sender shall capture the image through device camera using Image Capture feature of the Android application. Further it goes through following steps:

- The captured image will be encrypted by the Android application using AES algorithm.
- The encrypted image will further be secured by an encrypted password key, set by the sender through the Android application.
- The doubly-secured, encrypted image is saved by the Android application in only the external memory (SD card) of the device and not in the internal memory. This feature might behave differently in different handsets depending upon their file architecture.
- The image may not listed in the Picture Gallery of device and it also may not be viewed from the File Manager option of the handset
- The encoded image will also be displayed in the Android application till the time it is not transmitted to the sender
- Sender transmits the image to the recipient using Send Image feature of the Android application. In order to deliver the image the recipient's user id is required
- When the sender has completed the transmission, the image will get automatically omitted from the Android application as a security feature
- When the sender has sent the image, it gets saved on the cloud database in an encoded form which disallows it to be viewed even on the cloud
- The recipient shall be able to view the images using Received Images feature of the Android application using which all the images sent by different senders will be listed from cloud database
- In order to view the image, the recipient taps on the image icon of the received images and inputs the respective password in order to decode the image
- The decoded image is not saved anywhere in the recipient's device by the Android application.

Before working on this idea, we consulted the below research:

Mobile devices are increasingly being used for capturing and spreading images of popular uprisings and civil disobedience. To keep such records hidden from authorities, deniable storage encryption may offer a viable technical solution. Such PDE-enabled storage systems exist for mainstream desktop/laptop operating systems. With Mobiflage, we explore design and implementation challenges of PDE for mobile devices, which may be more useful to regular users and human rights activists. Mobiflage's design is partly based on the lessons learned from known attacks and weaknesses of desktop PDE solutions. We also consider unique challenges in the mobile environment (such as ISP or wireless carrier collusion with the adversary). To address some of these challenges, we need the user to comply with certain requirements. We compiled a list of rules the user must follow to prevent leakage of

information that may weaken deniability. Even if users follow all these guidelines, we do not claim that Mobiflage's design is completely safe against any leaks. We want to avoid giving any false sense of security. We present Mobiflage here to encourage further investigation of PDE-enabled mobile systems [1].

Portable file system encryption engine that uses NIST certified cryptographic algorithms for Android mobile devices. We offer a comparative performance analysis of our encryption engine under different operating conditions and for different loads including file and database (DB) operations. Our experimental results suggest a 20 times overhead for write operations on the internal storage. When increasing the cryptographic key-length from AES-128 to AES-256, we incurred an additional performance loss of 10% to 15%, depending upon the operation performed. Although file operations incurred a 20 times overhead, the database operations had a much more moderate overhead of 58% which accounts for sequential write and update DB operations. By optimizing the file system block-size and I/O mode, we were able to gain 20% to 57% performance. In addition, we then demonstrate that device-specific optimization methods can also provide performance boost. Despite the seemingly large overhead observed for I/O intensive applications, we were successful in running our encryption file system on a variety of Android devices and applications without significant user-perceived latency. Therefore, we conclude that our encryption engine is easily portable to any Android device and the overhead due to the encryption scheme is an acceptable trade-off for achieving the confidentiality requirement. The data has to be stored in an encrypted format using cryptography on biometric for the security reasons. The protocol is blind in the sense that it reveals only the identity, and no additional information about the user or the biometric to the authenticating server or vice-versa. As the protocol is based on asymmetric encryption of the biometric data, it captures the advantages of biometric authentication as well as the security of public key cryptography. The user initially enrols with the biometric system which is provided by a cloud, once the identity is registered his/her biometric authentication details are stored in cloud service provider database. The authorization details are also entered at the registration time which is also encrypted. Whenever the user wants to use any cloud service user first uses the biometric authentication service rather than a traditional password mechanism. Once authenticated, the user is redirected to the actual cloud service for which he is authorized to use. The Biometrics allow for increased security, convenience we can say that fused biometric authentication system will be novel solution for authenticating users on cloud computing ,which can be provided as service on cloud and can be used as a single sign on [2].

Deploying Android in security-critical environments is a complex task, as confidential data might get compromised when being accessed, processed, and stored by insecure mobile devices. To facilitate this task, we have systematically analyzed and assessed different encryption systems of the Android platform, which provide the opportunity to protect security critical and confidential data. From the obtained assessment results, potential attack scenarios have been derived. Finally, a workflow has been proposed, which assists in deploying and configuring Android devices in security-critical environments and applications. Obtained assessment results have also shown one of the main challenges of the Android platform: In contrast to other mobile platforms such as iOS, BlackBerry, or Windows Phone, Android features many more different versions and hence shows a much higher fragmentation. This heterogeneity is mainly caused by device manufactures, who supply their devices with customized versions of the Android OS. Due to this heterogeneity, the deployment of Android devices in security-critical scenarios is a challenging task that requires an in-depth security analysis of the envisaged platform. The main difficulties are the various sub-systems that depend on the specific device manufacturer's implementation, the

lack of MDM rules/restrictions to configure relevant aspects of the Android system, and the differences in the encryption systems. Due to the given heterogeneity, the proposed workflow has been defined on a rather abstract basis and does not consider manufacturer-dependent features or limitations. Still, the proposed workflow – and also the results obtained from the conducted assessments – represents a useful basis that facilitates a correct use of Android's encryption systems in security-critical applications. Manufacturer- or version-dependent refinements of the proposed workflow are regarded as future work [3].

After studying the prevalent researches, we discovered that:

Most of the studies were based on the fact that they developed their own product in order to secure one area but not the entire content transmission as a whole. All the studies focused on one idea only and they did not concentrate on eliminating its disadvantages whereas we attempt to balance the demerits of one with the merits of another technique. The studies mostly depend on the complicated calculations in order to secure the storage of data whereas we shall focus on simplistic calculations that not only use minimum resources but also produce efficient output in the minimum possible turnaround time. The studies clearly show that they do not protect the classified data of the user which might be consisting of extra sensitive information that is useful for some investigation purpose or some verification purpose, right from the point of its creation and delivery whereas in our research, we make a conscious attempt to protect the data at all the levels i.e. Device, Network & Cloud because we believe that data is protected comprehensively once it become non – accessible to the outside world from the different dimensions. The techniques do not discuss about the efficient resource utilization of the user's resources be it hardware or software whereas in our study we plug and bridge this gap through minimizing the consumption using simple yet efficient obscurity and encoding mechanisms that put minimum possible load.

Problem Formulation

We discover from the studies that:

There is large need of an application that protects user's data from geographically any coordinate and allows them to conveniently store and retrieve data from the cloud. The users face problem to manage the security and integrity of their data because of the security issues wherein the data become extremely vulnerable to be hacked from any part of the world by any person and in order to avoid it we needed mechanisms that protect the data comprehensively. There is a large need of an application that implements a large scale of encoding mechanisms which also involve obscurity techniques because encoding and hiding of data are two very strong and significant aspects to protect data. There is a large need of a simple system that does not involve much user interaction and is able to perform the tasks on its own. Users nowadays want convenience that their data should protected wherever it is, be it handset, network, cloud, data centre or anywhere and our application shall ensure that it is done and the users do not have to concern themselves for manual intervention regarding protection of their sensitive data. They want that the data should be protected automatically, conveniently and efficiently so they do not think about decoding or hacking by any unauthorised authority. Furthermore, large number of systems involves very complex mathematical calculations and procedures during facial recognition for ex: that occupy huge memory resources, calculation overheads due to processor loads and thereby slow turnaround times eventually leading to downtimes. There is a large need of a system that simplifies all that, that enables the user to access a simple application while on-the-go and facilitates him/her to save as well securely retrieve data using simplified yet very robust encoding and obscurity mechanisms.

Comparison and contrast:-

How is our application different from the other applications already exist in this domain?

1. Device Obscurity: This feature distinguishes our application from others in a way that it stores the captured multimedia images only in the memory card of the user's mobile handset unlike other applications which (also) save the images inside the Picture Gallery of the phone.
2. Cloud Security: By the virtue of this feature, the transmitted multimedia images by the sender users will be stored on the cloud database in an encoded numeric format so that not even the authorized user is able to view. This feature is implemented with a view that if any user's cloud account is accidentally compromised, his/her confidential stored images are not leaked. These (encoded) password-protected images are decoded only once they are delivered to some recipient's phone and the decoding shall happen on the device itself during runtime by our application. Unlike the existing cloud services which store the (confidential) images as is, leaving them vulnerable to be compromised, our application largely differs from them from this security perspective.

Conclusion & Future Scope

This application will help the users to exchange multimedia images, effectively, in a secured manner, ensuring the confidentiality of communication. It may be utilized in classified communications like criminal investigations, business communications, and the like. The communication and data is not just encoded over the transmission channels and cloud but the exclusive feature of Device Obscurity ensures the content security at the user's device / handset level also. The reliable and fail-safe cloud service shall not only guarantee the integrity of the stored information but also its security because the multimedia content shall be stored in an encoded manner plus every user's data is enveloped in his/her own individual user account on the cloud.

Future Scope: This idea is extendable towards delivering a wide range of encrypted content like audio, video and text (apart from images) with handset/device obscurity. The ease-of-use for this application could be further improved through inclusion of speech synthesis while selecting the recipients to whom the content is to be sent. The security features of the application could be further fortified through implementation of additional, multi-layer encryption algorithms along with more device and user level authentications like OTP, IRIS Recognition, etc. The addition of Data Mining and Artificial Intelligence concepts is another futuristic scope within this application for the improvement of its user friendliness and intelligent analysis of data being exchanged through it.

REFERENCES

[1] Adam Skillen and Mohammad Mannan "On Implementing Deniable Storage Encryption for Mobile" Concordia Institute for Information Systems Engineering Concordia University, Montreal, Canada ISSN No. 3324 – 6965, Vol – 1, ISS – 3 (2012)

[2] Zhaohui Wang, Rahul Murmuria, Angelos Stavrou "Implementing and Optimizing an Encryption Filesystem on Android" Department of Computer Science George Mason University Fairfax, VA 22030, USA (2013)

[3] Peter Teufl, Andreas Fitzek, Daniel Hein, Alexander Marsalek,Alexander Oprisnik, Thomas Zefferer "Android Encryption Systems" Institute for Applied Information

Processing and Communications Graz University of Technology Inffeldgasse 16a 8010 Graz, Austria (2012)

[4] Cong Wang, Student Member, IEEE, Ning Cao, Student Member, IEEE, Kui Ren, Senior Member, IEEE, Wenjing Lou, Senior Member, IEEE "Enabling Secure and Efficient Ranked Keyword Search over Outsourced Cloud Data". IEEE Journals, Volume 23, Issue 8 (2012)

[5] Daniele Grasso "Authentication and secure data storage in cloud based mobile data collection". 265743 Corso di Laurea Magistrale in Ingegneria Informatica (2013)

[6] Cong Wang, Student Member, IEEE, Qian Wang, Student Member, IEEE, Kui Ren, Member, IEEE, Ning Cao, Student Member, IEEE, and Wenjing Lou, Senior Member, IEEE "Towards Secure and Dependable Storage Services in Cloud Computing". IEEE Journals (2013)

[7] Varsha S.Agme, Prof. Archana C.Lomte "Cloud Data Storage Security Enhancement Using Identity Based Encryption", IJAIEM, ISSN 2319 – 4847, Volume 3, Issue 4, April (2014)

[8] Saurabh Prabhune, Indrajeet Sharma, Sachin Bayas, Prof. T.B.Mane "Application for Data Transmission using Encryption Methods via Information Security" IJESC, ISSN-2321 -3361 © (2014)

