IJESRT
INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

# SECURE MULTIMEDIA DATA STORAGE IN CLOUD COMPUTING

**Dipti Rao*, Muzammil Hasan**
[*] Dept. of Computer science and engineering M.M.M.U.T, Gorakhpur 273010
Dept. of Computer science and engineering M.M.M.U.T, Gorakhpur 273010

**DOI**: 10.5281/zenodo.581553

## ABSTRACT

Data is the most significant entity to every being. It is the sole ingredient of human and non – human communication in all forms, be it electronic, digital, verbal or written. And because of its importance, we adopt stringent measures to secure the storage of data and ensure its authorized access at different levels so that its usability and integrity are maintained. Security of any data deals both with its storage and retrieval. We may apply robust cryptographic algorithms in order to encode the data and/or implement several authentication checks to verify the genuineness of user attempting to access it. Here we develop an application that enables the users to exchange classified multimedia content, securely from any geographical coordinate. We aspire to apply security at all levels, in order to shield the data, right from the point of its creation to delivery. Our intention is to be different from the existent applications under this domain, in the form of latest technology, ease-of-use and scalability. In this paper we propose to provide convenience to the user through simple, understandable yet secure communication interfaces. Our goal is to shield date at all checkpoints through which it travels i.e. Sender Device Device → Network → Cloud → Recipient Device.

In this world of advanced communication, people prefer mechanisms through which data can be saved or retrieved quickly, easily and securely from any geographical coordinate. To facilitate this objective, smart phones and mobile cloud computing play an integral role. They fortify the user to use techniques for smart storage and retrieval of data using infrastructure, platform and software as a service being provided by 3rd party. Here we shall make use of the newest technologies, i.e. Android and Cloud Computing.

**KEYWORDS**: Android, Privacy, Authentication, Integrity, Data storage, Data Security.

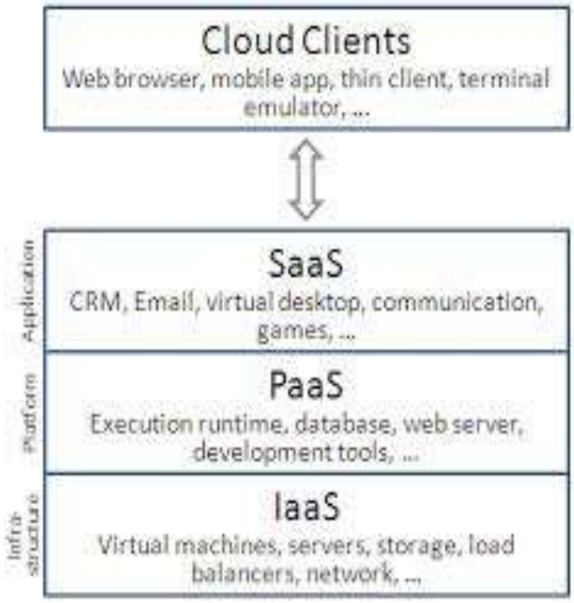
## INTRODUCTION

In our proposed work, we shall primarily be making use of Android platform along with application of AES algorithm for data security and obscurity. Android is a software stack for mobile devices that includes an operating system, middleware and key applications. By providing an open development platform, Android offers developers the ability to build extremely rich and innovative applications. The Android SDK provides the tools and APIs necessary to begin developing applications on the Android platform using the Java programming language. Whereas, the term Cloud computing refers to the many different types of services and applications being delivered in the internet cloud, and the fact that, in many cases, the devices used to access these services and applications do not require any special applications. Once a cloud is established, how its cloud computing services are deployed in terms of business models can differ depending on requirements. The primary service models being deployed are commonly known as:

**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.

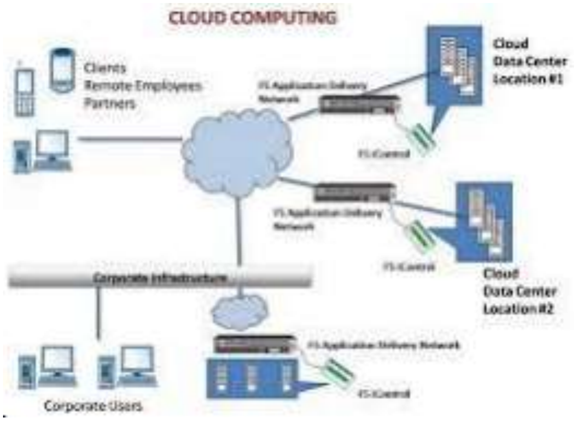

Cloud Clients
Web browser, mobile app, thin client, terminal emulator, ...
Application
SaaS
CRM, Email, virtual desktop, communication, games, ...
Platform
PaaS
Execution runtime, database, web server, development tools, ...
Infra-structure
IaaS
Virtual machines, servers, storage, load balancers, network, ...

## PROBLEM STATEMENT

Data was prone to hacking  hence  needed a robust solution to protect it from different angles such as sender, receiver, device/handset, network and cloud and so wanted a more sophisticated encryption technique that is not single but combination or mix of different techniques hence we use an existing algorithm i.e. AES with cipher(modified AES).

## MULTIMEDIA DATA SECURITY

Due to the current development in computer network technology, giving out of digital multimedia pleased through the internet is massive. Though, the augmented number of digital documents, compact disk processing tools, and the international ease of use of Internet access has created a very appropriate medium for exclusive rights fraud and disobedient distribution of multimedia content. A major condition now is to protect the scholar possessions of multimedia content in compact disk networks. There are figure of data types that can be characterize as multimediadatatypes



These are typically basics for the building blocks of general multimedia environments, platform, or integrate tools The essential type can be described as text, images, audio, video and Graphic objects. Multimedia finds its purpose in various areas counting, but not limited to, advertisements, art, education, entertainment, engineering, medicine, mathematics, business, scientific research and spatial temporal applications.

## SECURITY LEVELS

Here the idea involves multimedia image data transfer using multi-layered security mechanisms. It would enable users across the globe to share encrypted multimedia images (captured through the integrated phone's camera from within the application) wirelessly, independent of their geographical coordinates through HTTP.

**Security Layer-1**

As soon as the image is captured, it will automatically get encrypted using "modified" AES algorithm inside the Android device along with the merged encrypted password that will by default be the sender's cloud account password.

**Security Layer-2**

The picture captured from camera via this application will be stored in the internal and/or external memory in the encoded fashion too. Storage of the encoded images shall vary from handset to handset depending upon their respective internal file architecture. This feature will be called as Device Data Obscurity which will shield the (confidential) images clicked through our application from the external world. The sender will be able to send the encrypted picture via the application to the receiver.

**Security Layer-3**

Once the receiver receives the encrypted picture, in order to open it, he/she will have to input the password. Only upon entry of the correct password will the receiver be able to view the image.

**Security Layer-4**

Once the downloaded image from the cloud gets decoded on the receiver's device through our application, it will also not be stored or saved anywhere on the recipient's device thereby ensuring another level of highly secured transmission. In other words, they will always be downloaded from the cloud database in a secured manner.

**Security Layer-5**

The images which are stored on the cloud are also not viewable by the administrator as they shall be in an encoded format.

## RELATED WORK

Adam Skillen and Mohammad Mannan [1] described 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, here 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. here also consider unique challenges in the mobile environment (such as ISP or wireless carrier collusion with the adversary). To address some of these challenges, the user to comply with certain requirements. a list of rules the user must follow to prevent leakage of information that may weaken deniability. Even if users follow all these guidelines, and 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.

Zhaohui Wang, Rahul Murmuria, Angelos Stavrou[2] ,works on 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. this 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.

Peter Teufl, Andreas Fitzek, Daniel Hein, Alexander Marsalek[3] suggests 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.

## CONCLUSION

In this paper, we investigate the problem of data security in cloud data storage, which is essentially a distributed storage system. To achieve the assurances of cloud data integrity and availability and enforce the quality of dependable cloud storage service for users, we propose a work which helps 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.

## REFERENCES

[1] Adam Skillen and Mohammad Mannan ,On Implementing Deniable Storage Encryption for Mobile Devices, June 2014. IEEE Transactions on Dependable and Secure Computing

[2] Zhaohui Wang, Rahul Murmuria,Angelos Stavrou, Implementing & Optimizing an Encryption Filesystem on Android Mobile Data Management (MDM), 2012 IEEE.

[3] Peter Teufl, Andreas Fitzek, Daniel Hein, Alexander Marsalek, Alexander Oprisnik, Thomas Zefferer,Android Encryption Systems , 2014 IEEE .

[4] Ms. Minal G. Kumbharkhane ,Prof. V. S. Gulhan, Encryption of file system using android. January2015, IJFEAT.

[5] Geetanjali R. Kshirsagar, Savita Kulkarni, Real Time Implementation of Secured Multimedia Messaging Service System using Android IJSRP, Volume 3, Issue 3, March 2013.

[6] A.P. Fabien, R.J. Anderson, M.G. Kuhn, “Information hiding: A survey”, IEEE Special Issue on Protection of Multimedia Content, vol. 87, 1999.

[7] N.-I. Wu, M.-S. Hwang, “Data hiding: Current status and key issues”, International Journal on Network Security 2007.

[8] William Stallings, "Cryptography And Network Security Principles And Practice", Prentice Hall, 5th edition, 2011.

[9] Cong Wang and Kui Ren, Wenjing Lou, Jin Li, “Toward Publicly Auditable Secure Cloud Data Storage Services”, Network, IEEE, vol. 24 , issue 4, 2010.

## CITE AN ARTICLE

**Rao, D., & Hasan, M. (2017). SECURE MULTIMEDIA DATA STORAGE IN CLOUD COMPUTING. *INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY, 6*(5), 391-395. doi:10.5281/zenodo.581553**