ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

Face Recognition using Cloud Based Security in Mobile Devices

Deepak S[1], Sai Goutham N[2]

Programmer Analyst, Cognizant Technology Solutions, India[1]

Market Analyst, GoFrugal Technologies, India[2]

ABSTRACT: Face recognitions plays a major role in biometrics research which helps to identify the users based on various parameters. In this fast developing technological world face recognition is increasingly used to distinguish the users in mobile. Breach of mobile security is common in this fast paced world which is seriously something to look upon. Cloud gives us significant security as far as data is concerned. Cloud-based storage can assure a certain level of privacy to the end-users.

The goal of the paper is to provide mobile users to safeguard their device when some Intruder tries to access the device. This is done by means of image capture which is supplanted by Face-Detection and Recognition. The captured image is then sent to cloud based Storage for retrieval. The user initially registers himself using his Authenticated mail-id. The authorised mail-box receives the image from the cloud database which in turn helps to Track the intruder, thereby providing a certain extent of safety to the end-users.

KEYWORDS: Image Capturing, Cloud Transfer, Registration, Authentication, Data Privacy, Face Detection, Face Recognition

I. INTRODUCTION

World is contracting with the growth of mobile phone technology. As the number of users is increasing day by day, facilities are also increasing. Starting with simple regular handsets which were used just for making phone calls, mobiles have changed our lives and have become part of it. Now they are not used just for making calls but they have innumerable uses and can be used as a Camera, Music player, Tablet PC, T.V., Web browser etc. And with the new technologies, new software and operating systems are required. This concept is based is based on an application which can be used to track the Intruder and the operations performed by the intruder in our android device as this supports the functionality of recording a video of on-screen activity and also capturing the image of the person accessing it. The captured image is sent to cloud. After the image is received the image captured is then sent to configured users mail boxes which helps the person to track the intruder. This helps the owner of the device to continuously monitor the operations performed in their device hence leading to a secure usage of devices and also putting an end to the unauthorized access of devices. The entire process is confidentially monitored and every user operations is recorded and stored in a specific location for further viewing. The video recording is performed by converting a series of screenshot into a complete video.

II. RELATED WORK

This is an era of wireless (mobile) communication and computing where mobile devices such as personal digital assistants, smartphones, etc., are being used in place of traditional computers. The off-premises computing paradigm that comes with cloud computing has incurred great concerns on the security of data, especially the integrity and confidentiality of data, as cloud service providers may have complete control on the computing infrastructure that underpins the services. This makes it difficult to share data via cloud providers where data should be confidential to the providers and only authorized users should be allowed to access the data. This work aims to construct a system for trusted data sharing through untrusted cloud providers, to address the above mentioned issue.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

As one of the most successful applications of image analysis and understanding, face recognition has recently received significant attention, especially during the past several years. At least two reasons account for this trend: the first is the wide range of commercial and law enforcement applications, and the second is the availability of feasible technologies after 30 years of research. Even though current machine recognition systems have reached a certain level of maturity, their success is limited by the conditions imposed by many real applications. For example, recognition of face images acquired in an outdoor environment with changes in illumination and/or pose remains a largely unsolved problem. In other words, current systems are still far away from the capability of the human perception system. This paper provides an up-to-date critical implementation of image-based face recognition research there by providing the security over the cloud. There are two underlying motivations for us to write this survey paper: the first is to provide an up-to-date review of the existing literature, and the second is to offer some insights into the studies of secured transmission over cloud architecture. To provide a comprehensive survey, we not only categorize existing recognition techniques but providing detailed descriptions of a particular method using which Images intruders face is recognized and detected followed by transfer of images to cloud to provide the insight to the end user using the system. In addition, we are adding an enhancement of screen recording feature in order to trap the activities done on the phone to have a clear picture of the intruders activities.

III. OVERALL SYSTEM

- Registration of Users:

1. Downloads the application
2. Provides his name and mail box id's
3. Authentication of Mail box ids
4. Storage of entered information in Local Cloud for further use

- Face Capture:

1. Intruder touches the screen
2. Camera is switched on
3. Face is captured

- Face Detection and Face Recognition:

1. Face captured is identified
2. Face is then recognized based on feature extraction mechanism
3. Intruder's face is then matched with User's face

- Cloud Transfer:

1. Image is transferred to another cloud
2. Image is then transferred to user registered mail boxes after the reception

- Screen Recording

1. After user activates the application the recording starts
2. Once the application is deactivated the screen recording stops
3. The files will be saved in local memory

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

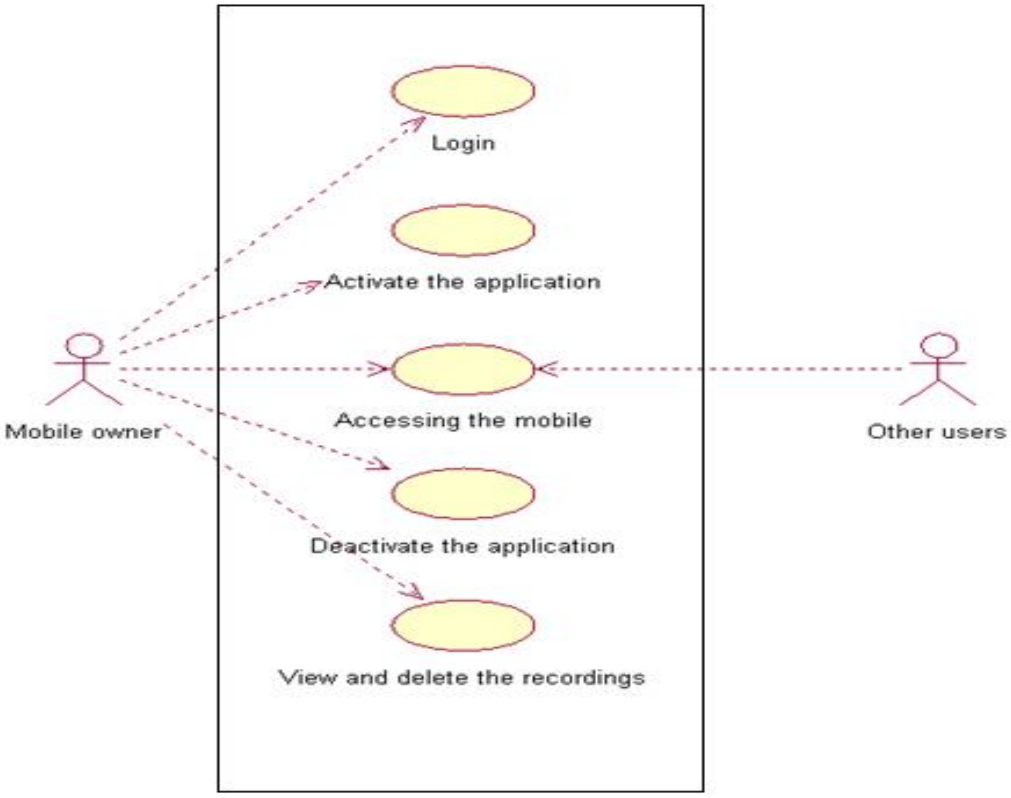

Fig 1. System Use Case Diagram

IV. FACE CAPTURE

Face capture is an essential feature in smart phones. In our implementation we use this technique to detect and recognize the individual who accesses the smart phone. The moments someone switches on the smart phone, the front camera application gets activated and the users face is captured. For example, when a mobile device is switched on by user A, face of user A is captured and it is sent for detection and recognition.

The major advantage of this feature is that the user who is accessing the mobile will not be aware of his face getting captured And it is the responsibility of the owner of the device to make sure the device contains enough space to hold the image. This is the initial phase of our implementation.

The front camera application is automatically triggered when the phone is switched on. But this feature is activated only when the app is activated by the owner. This feature doesn't work if the app is not activated.

Fig 2. Mechanism for Face Capture

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

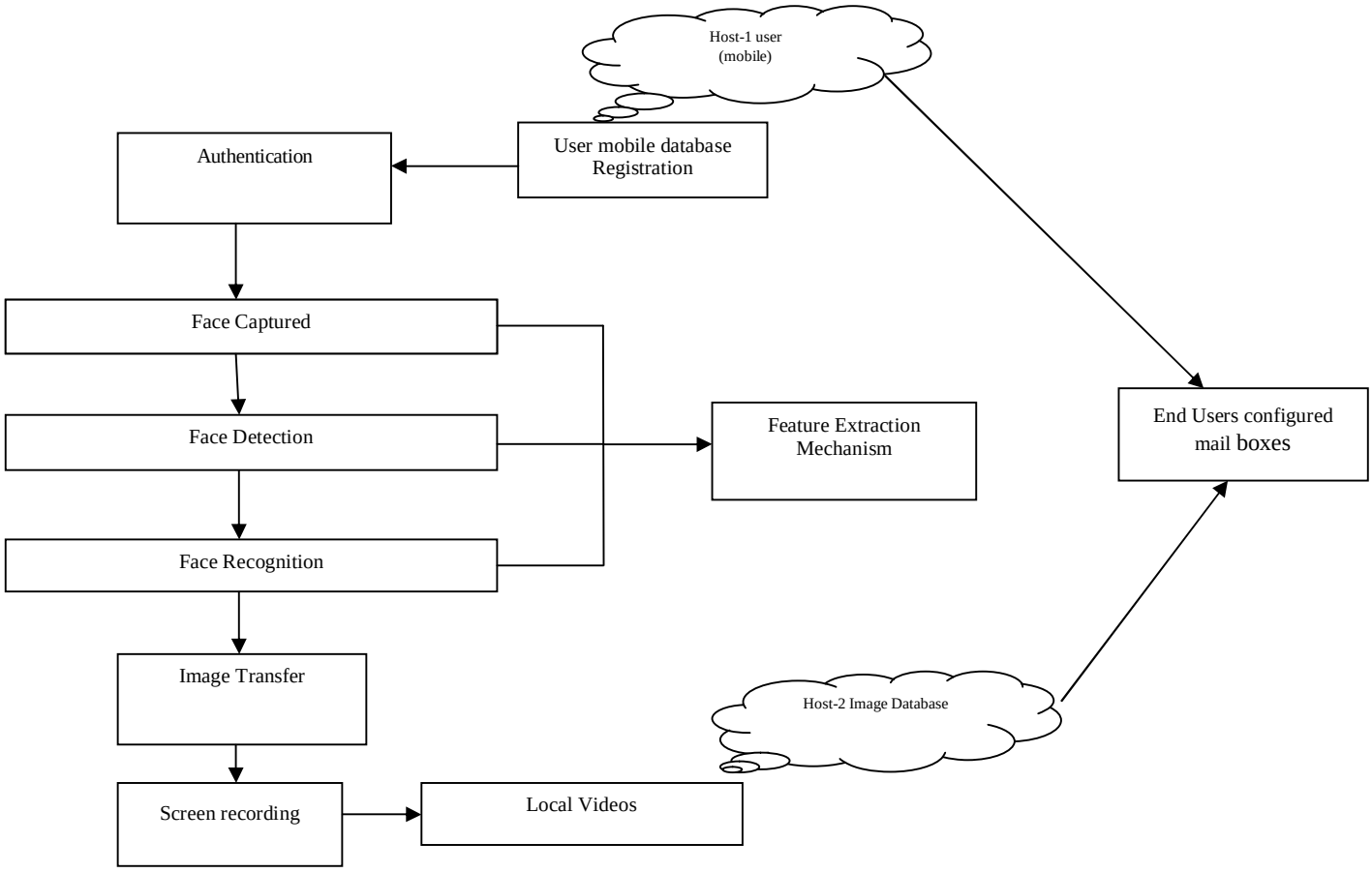

Fig. 3. Overall System

V. FACE DETECTION

Face detection is a computer technology which is used to detect a facial structure and recognize it by comparing it with the images available in the database.

After the image or the video is acquired by the mobile it is important that the image is segregated form the background. This phase is called the face detection phase. After the face is detected different kinds of analysis like skin texture analysis and nodal analysis, template creation is done. This part is called the face recognition. A comparison happens between a database of stored images and the image acquired is done and the final output is provided.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

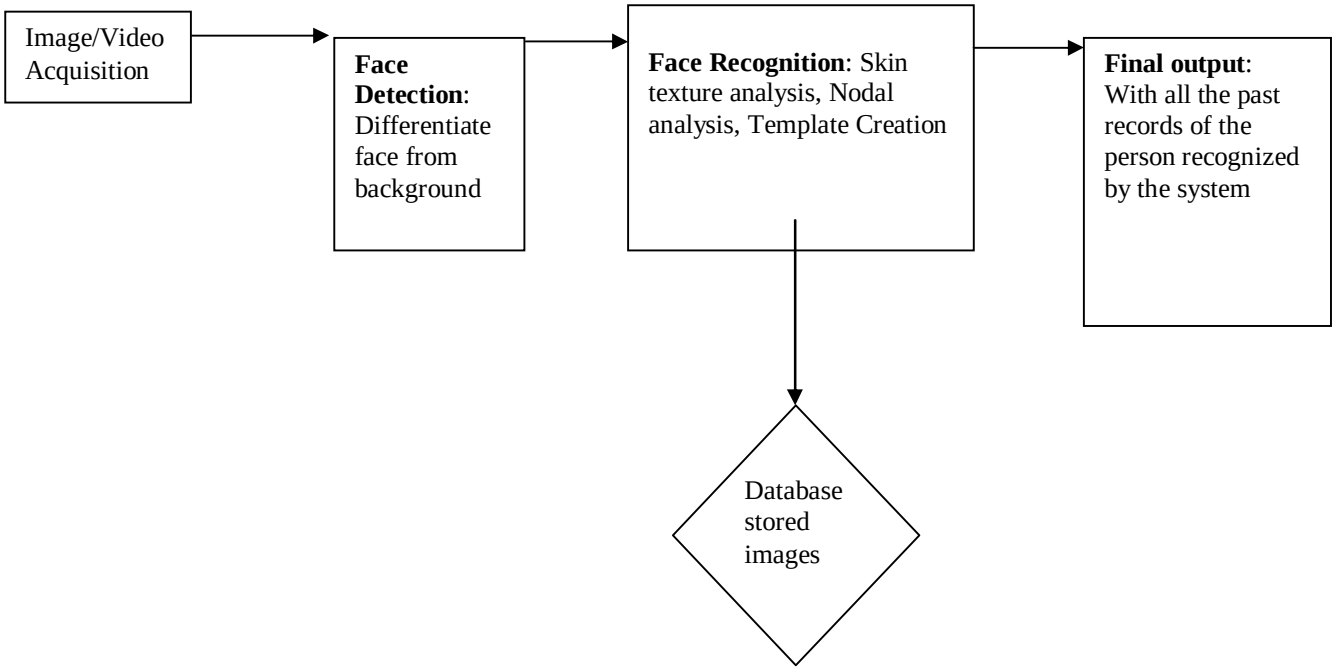

Fig. 4. Mechanism for Face Detection

VI. FACE RECOGNITION

A facial recognition system is a computer application for automatically identifying or verifying a person from a digital image or a video frame from a video source. It is typically used in security systems and can be compared to other biometrics such as fingerprint or eye iris recognition systems. Face recognition can be both used for verification and identification.

Face Recognition is another important feature in this application. After the image is captured, it is compared with authenticated image that is stored in the database. If the captured image does not match with the authenticated image present in the database then image is transferred to a Cloud storage system.

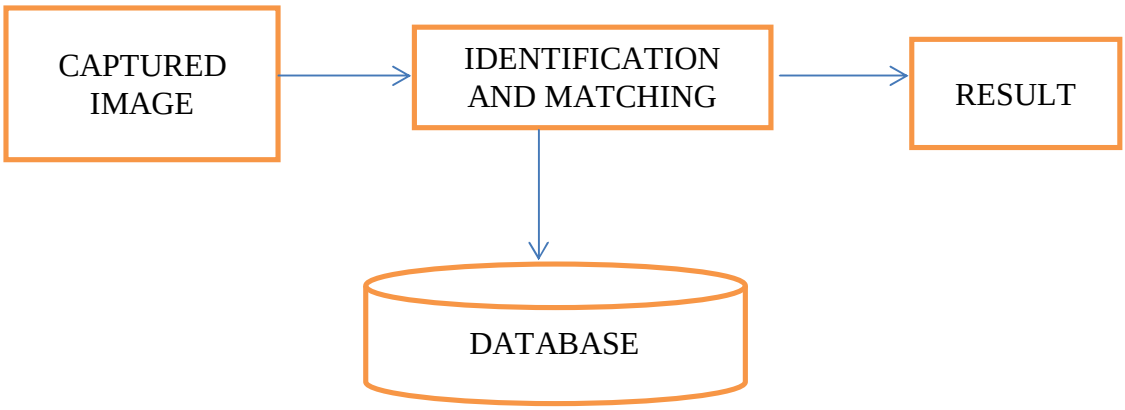

Fig. 5. Mechanism for Face Recognition

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

VII. CLOUD TRANSFER

Cloud computing mainly aims at collective usage of resources like hardware and software over any network which is specifically internet in our case study It also provides application programming interface that facilitates the programmers to employ programming concepts over the data by creating interaction with cloud software. Cloud also enables virtualization which brings about virtual devices, objectively to store information. These also enable various types of clouds like public, private, hybrid which are made use of according to the medical requirement. The services offered over cloud:
IAAS: Hardware (system), core connectivity

PAAS: Platform Integration and middleware (VMware)

SAAS: Services, API (java), Data, Fuzzy, applications

The image once taken is stored in the local storage and is also sent to the registered mail-id.
The Cloud database is created on VMware platform. The captured-image is transferred to the registered mail box through cloud. As we can see in the above image, the captured-mail is saved in HOST1(local storage) and another copy of it is sent to the registered mail box through cloud.

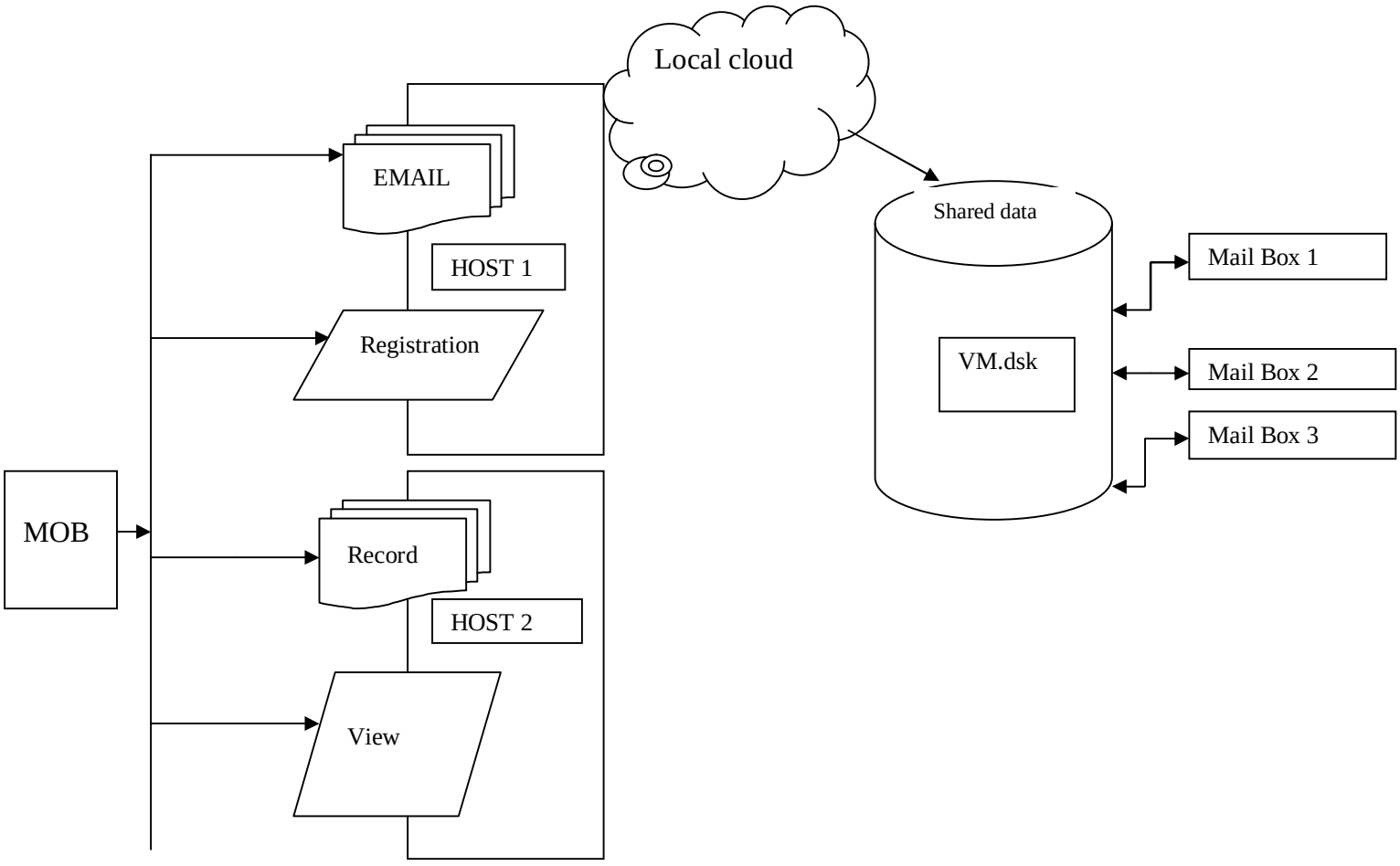

Fig. 6. Implementation of Cloud Transfer

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

VII. SCREEN RECORDING

Another important feature is in this utility application is the screen recording.
The moment the phone is switched on, the activities on the screen gets recorded automatically and the recordings are saved to the local database, But this feature must activated by the owner and once the owner wishes to deactivate the application, he may do so by selecting the deactivate option in the application. He can view the recordings in the specified folder.

Sequence of steps:

- Owner logins to the Application
- Activates the screen recording feature.
- Intruder access the mobile
- The recording feature gets activated
- Intruders activities are recorded
- Owner access the recording and deactivates the feature.

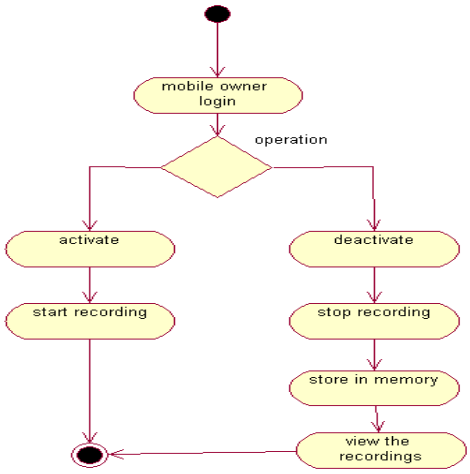

Fig. 7. Flow for Screen Recording

VIII. IMPLEMENTATION

Hardware

The main hardware platform for Android is the 32-bit ARMv7 architecture. The Android-x86 project provides support for the x86 architecture, and Google TV uses a special x86 version of Android. In 2012, Intel processors began to appear on more mainstream Android platforms, such as phones. In 2013, Free scale announced support for Android on its i.MX processor, specifically the i.MX5X and i.MX6X series.

Android devices incorporate many optional hardware components, including still or video cameras, GPS, hardware orientation sensors, dedicated gaming controls, accelerometers, gyroscopes, barometers, magnetometers, proximity sensors, pressure sensors, thermometers and touch screens. Some hardware components are not required, but became standard in certain classes of devices, such as smart phones, and additional requirements apply if they are present.

Some other hardware was initially required, but those requirements have been relaxed or eliminated altogether. For example, as Android was developed initially as a phone OS, hardware such as microphones were required, while over time the phone function became optional. Android used to require an autofocus camera, which was relaxed to a fixed-

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

focus camera if it is even present at all, since the camera was dropped as a requirement entirely when Android started to be used on set-top boxes.

Software Stack

On top of the Linux kernel, there are the middleware, libraries and APIs written in C, and application software running on an application framework which includes Java-compatible libraries based on Apache Harmony. Android uses the Dalvik virtual machine with just-in-time compilation to run Dalvik "dex-code" (Dalvik Executable), which is usually translated from the Java bytecode. Android 4.4 also supports new experimental runtime virtual machine, ART, which is not enabled by default.

Android uses Bionic in place of a standard C library, originally developed by Google specifically for Android, as a derivation of the BSD's standard C library code. Bionic has several major features specific to the Linux kernel, and its development continues independently of other Android's source code bases. The main benefits of using Bionic instead of the GNUC Library (glibc) or uClibc are its different licensing model, smaller runtime footprint, and optimization for low-frequency CPUs.

Android does not have a native X Window System by default nor does it support the full set of standard GNU libraries, and this makes it difficult to port existing Linux applications or libraries to Android. Support for simple C and SDL applications is possible by injection of a small Java shim and usage of the JNI like, for example, in the Jagged Alliance 2 port for Android.

SOFTWARE AND HARDWARE REQUIREMENTS

11.1 IDE: Eclipse

Eclipse is an open source IDE available to support a variety of languages.

Version: Eclipse 3.5

It is released under the license of **ECLIPSE PUBLIC LICENSE**

Eclipse is a free and open-source software.

11.2 ANDROID VERSION:

Android 2.0 éclair to Android 4.3 jelly bean

OS: Windows XP and above

REFERENCES

1. Grace Walker, IT Consultant, Walker Automated Services, Cloud Computing Fundamentals, A different way to deliver computer resources.
2. Developer.android.com/tools/help/index.html
3. Foster, C., Uchitel, C., Magee, J. and Kramer J. (2003) Model-based verication of web service compositions, In proc. of ASE03, pp. 152-163.
4. P. K. Tysowski and M. A. Hasan. (2011) Towards Secure Commu- nication for highly Scalable Mobile Applications in Cloud Computing Systems, Centre for Applied Cryptographic Research (CACR), University of Waterloo, Tech. Rep. 33.
5. M. Kirby, L. Sirovich, Application of the Karhunen-Loeve Procedure for the Characterization of Human Faces, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 12, No. 1, January 1990, pp.
6. L. Sirovich, M. Kirby, Low-dimensional Procedure for the Characterization of Human Faces, Journal of the Optical Society of America A - Optics, Image Science and Vision, Vol. 4, No. 3, March 1987, pp. 519-524
7. R. Brunelli, T. Poggio, Face Recognition: Features versus Templates, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 15, No. 10, October 1993, pp. 1042-1052
8. Suhas Holla, Mahima M Katti, Android Based Mobile Application Development and its Security, International Journal of Computer Trends and Technology, Vol. 3, Issue. 3-2012

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

9. https://www.microsoft.com/industry/government/guides/cloud_computing/4-SaaS.aspx
10. Gonzales D, Kaplan J, Saltzman E, Winkelman Z, Woods D, Cloud-Trust – a Security Assessment Model for Infrastructure as a Service (IaaS) Clouds, IEEE Xplore

BIOGRAPHY

Deepak S. The author was born in Chennai on 2nd august 1992. The author did his Schooling in Hindu Senior Secondary school, followed by Sri Sankara Senior Secondary School and passed out in flying colours with distinctions in X and XII standard. He completed his B.Tech Information technology Under Graduation at S.S.N College of Engineering Chennai in the year 2014. The author has done various contributions to the field of cloud computing by publishing his research ideas in IEEE, Lecture Notes on Software engineering, International Journal of Advanced Research in Computer and Communication Engineering. He has subsequently published his patent work for deducing a fuzzy model was disease diagnostics. He is also awarded as Student Researcher during his Under Graduate studies.

Sai Goutham N. The author was born in Chennai on 28th October 1992. The author did his Schooling in Hindu Senior Secondary school, followed by DAV Matriculation School and passed out with distinction in X and XII standard. He completed his B. Tech Information technology Under Graduation at S.S.N College of Engineering Chennai in the year 2014. The author was involved in various android projects and in order to name a few he was associated with Pesudo labs for android projects. The author currently works as an Market and Research analyst in GoFrugal Technologies, Chennai.