ACOUSAUTH: A SMARTPHONE EMPOWERED PERSONAL AUTHENTICATION SYSTEM EXPLOITING KEYLESS ACOUSTIC COMMUNICATION

REPORT FOR MOBICOM 2013 MOBILE APP COMPETITION

Team Member

Si Chen	schen23@buffalo.edu
Muyuan Li	muyuanli@buffalo.edu
Jun Wang	jwang39@buffalo.edu
Yujin Tu	yujintu@buffalo.edu
Chao Zhang	czhang28@buffalo.edu
Bingsheng Zhang	bzhang26@buffalo.edu
Zhan Qin	zhanqin@buffalo.edu
Junfei Wang	junfeiwa@buffalo.edu

Advisor

Dr. Kui Ren kuiren@buffalo.edu

Introduction

AcousAuth is a smartphone empowered system we designed for personal authentication. It features a seamless, faster, easier and safer user authentication process without the need for special infrastructure. Our system is intended to provide security assurances comparable to or greater than that of conventional authentication systems while offering the same user experience as inputing a password alone. Potentially, any mobile device or computer with microphone and speaker can use AcousAuth, regardless of the hardware and operating system. Our application provides a purely software-based solution to secure smartphone short-range communication without key agreement phase and it is potentially well suited for legacy mobile devices. Despite the computational restrictions and bandwidth of mobile device, our mobile application is able to maintain real-time performance.

Data confidentiality of existing short-range communication systems typically relies on key-exchange then encryption mechanism, which is inefficient. The state-of-the-art NFC-based short-range communication requires special hardware, i.e. NFC chips that are not common on most low-cost smartphones. AcousAuth incorporates keyless acoustic short-range communication techniques and an intuitive user interface. To the best of our knowledge, our mobile application demonstrates the first secure cloud-based approach chiefly on friendly jamming technique for acoustic short-range communication.

Our work leverages the following key insights. First, a mobile device can utilize acoustical channel to communicate directly with a cloud-based terminal automatically. Second, it is possible to provide a layered approach to security, whereby a web server can enact different policies depending on presence of the user's mobile device.

System Architecture

Our application is developed based on leading best practices in cloud based **software-as-a-service (SaaS)** and **mobile application** architecture.

It can be roughly divided into three main entities: a **data modulating system** running on user's smartphone, a **web-browser based GUI** running on a computer and a **cloud-based online acoustic signal-processing terminal** running on a virtual private machine (VPS).

The data modulating system is a mobile application that runs on legacy mobile devices. It is responsible to acquire user input and modulate data into acoustic signal. We employ frequency-shift keying (FSK) modulation scheme in our demonstration setup. There are two major components of this module:

(1) **Data modulator.** We construct a modulator to modulate encoded data into an acoustic signal data matrix. Specifically, we employ *frequency-shift keying* (FSK) modulation scheme in our demonstration setup for its smartphone friendly light-weight signal processing. Before FSK, the input string is first under crypto hash

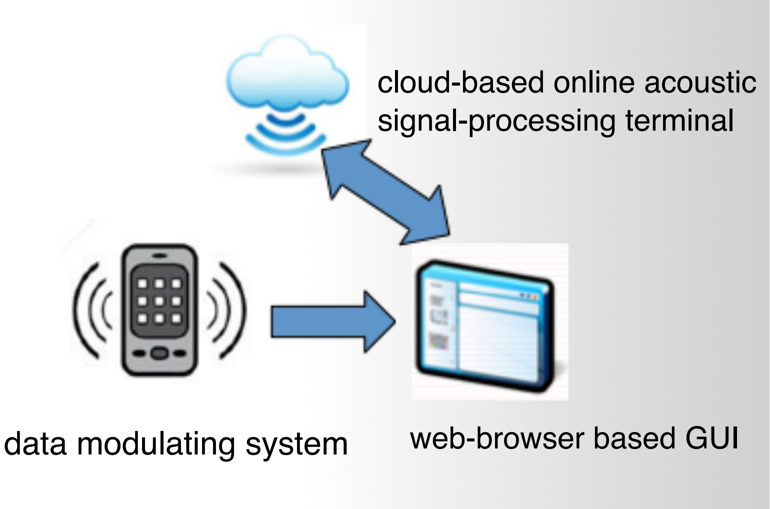


Figure 1. System Architecture

function(i.e. SHA-1) to ensure collision at negligible possibility for communication error tolerance.

(2) **Tone generator.** Due to the nature of the acoustic signal propagation and speaker characteristics, the gain of the speaker and microphone combination in smartphones is varied from different manufacturer and it is extremely non-uniform across the range of frequencies. In our system, we use tone generator to convert modulated acoustic signal data matrix into an optimal frequency, and thereby transmitting the acoustic signal from the sender's speaker.

The web-browser based GUI is responsible for broadcasting self-jamming signal while simultaneously performing acoustic data collection from the air medium via its microphone. Once finished, it pre-processed the data and upload them to the cloud.

Online graphic user interface (GUI) is intuitive and it is the main area for acquiring acoustic signal through a microphone and sending self-jamming signal through a speaker. During recording, the user sends a initial signal to wake up the recorder, then the web browser sends out jamming noise.

In order to achieve platform independent, we implement online GUI based on HTML5 technique, due to the fact that HTML5 has brought a surge of access to device hardware and its Web Audio API supports local microphone stream access and self-jamming signal broadcast.

Cloud-based online acoustic signal-processing module handles acoustic signal self-jamming and data recovery. It contains 5 main components.

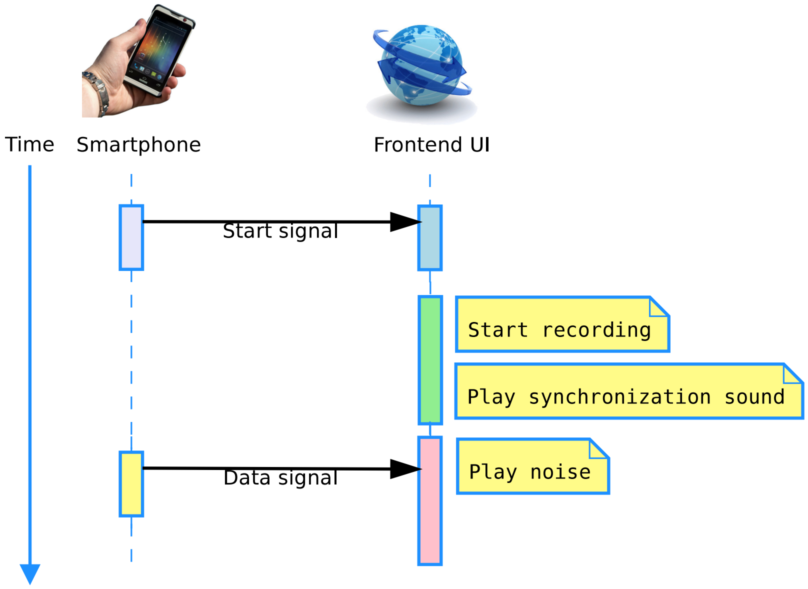


FIGURE 2. Sequence Diagram

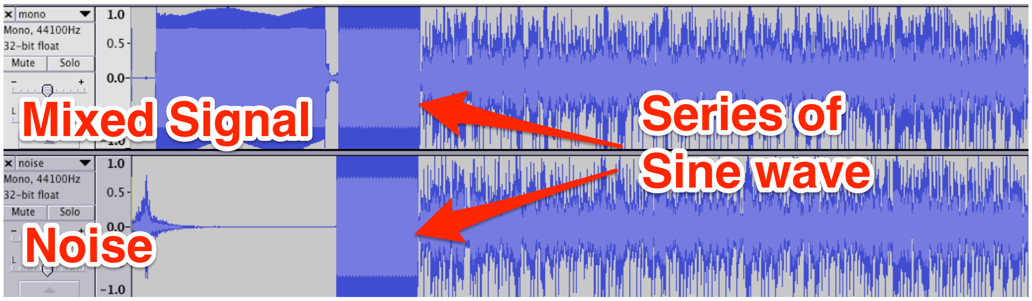


FIGURE 3. Synchronization Signal

(1) **Self-jamming components:** In our system, the terminal needs to generate and transmit the jamming signal to protect the sender data signal. The jamming should be random and strong enough that any eavesdroppers are unable to cancel out the jamming. This component generates a series of random noise signal at the same frequency interval as the data signal and amplifies it by 10dB. In order to assist jamming cancellation process, we pad a series of sine wave at its front as synchronization signal.

(2) **Self-jamming cancellation components (SCC):** When the mixed signal is received, we align the noise and the mixed signal via the sine wave. Then we

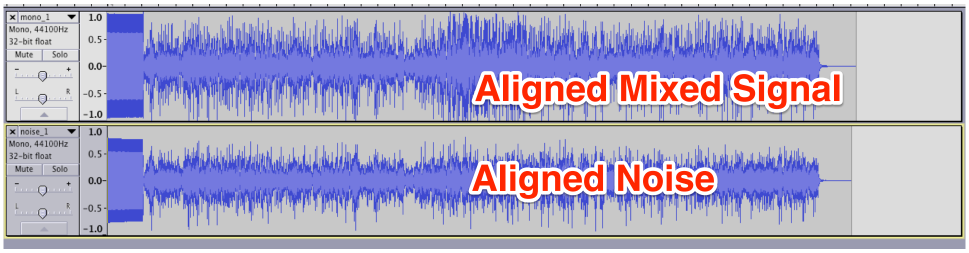
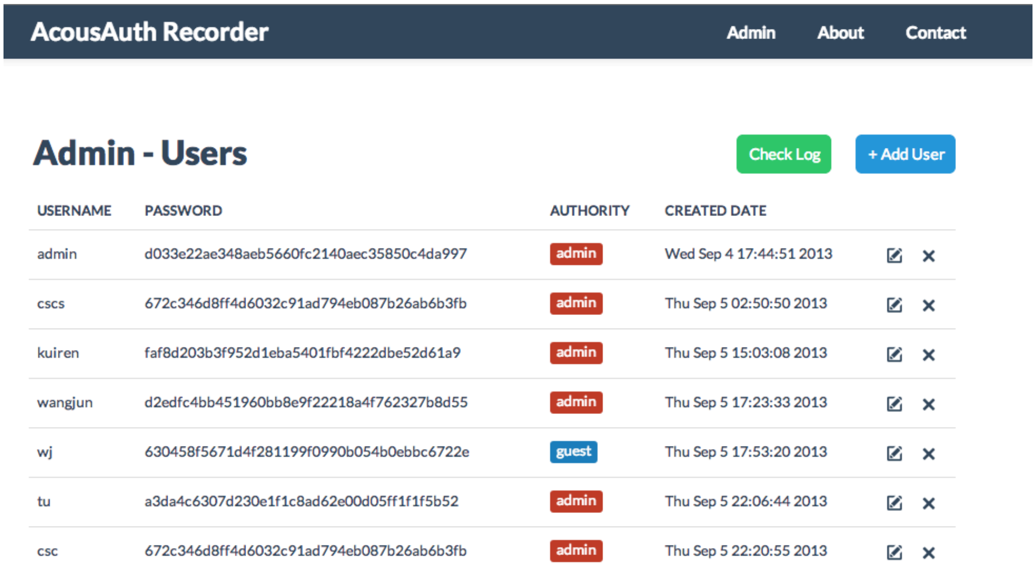


FIGURE 4. Aligned Signal

subtract the noise from the mixed sound track. The remaining part should only include the data signal and ambient noise with high signal to noise ratio.

(3) **Data demodulator:** Data demodulator module demodulate the recovered FSK signal at specified baud rate into encoded channel data. It acts like a software FSK modem.

(4) **Authentication:** We compare the pre-logged hashed passcode with our recovered data. When the similarity exceeds certain threshold(factoring in the negligible possibility of even partial hash collision), we authenticate the user.



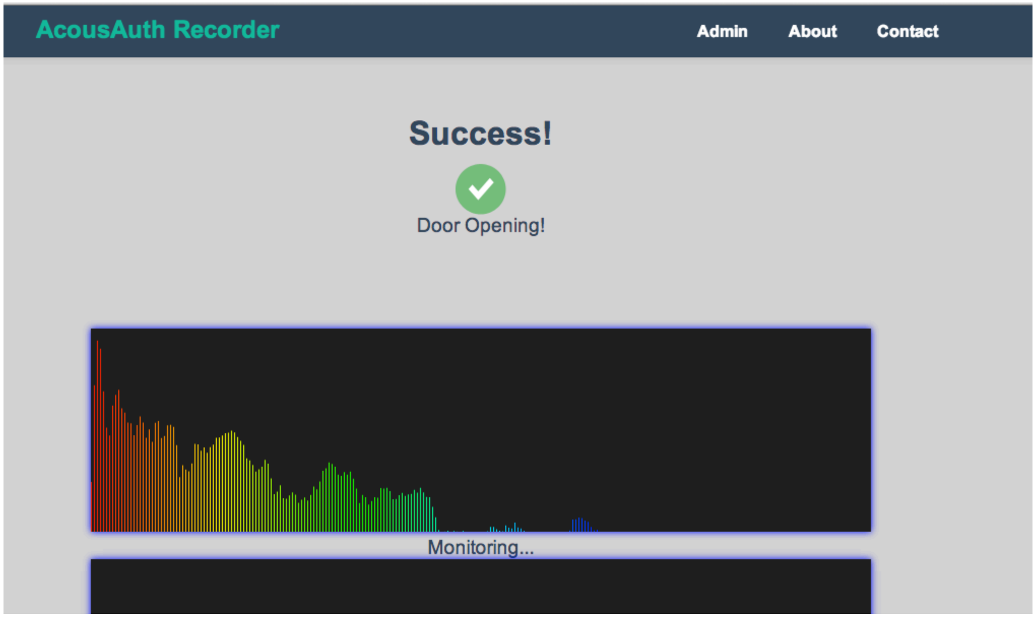
Admin - Users

USERNAME	PASSWORD	AUTHORITY	CREATED DATE		
admin	d033e22ae348aeb5660fc2140aec35850c4da997	admin	Wed Sep 4 17:44:51 2013	✎	✕
cscs	672c346d8ff4d6032c91ad794eb087b26ab6b3fb	admin	Thu Sep 5 02:50:50 2013	✎	✕
kuiren	faf8d203b3f952d1eba5401fbf4222dbe52d61a9	admin	Thu Sep 5 15:03:08 2013	✎	✕
wangjun	d2edfc4bb451960bb8e9f22218a4f762327b8d55	admin	Thu Sep 5 17:23:33 2013	✎	✕
wj	630458f5671d4f281199f0990b054b0ebbc6722e	guest	Thu Sep 5 17:53:20 2013	✎	✕
tu	a3da4c6307d230e1f1c8ad62e00d05ff1f1f5b52	admin	Thu Sep 5 22:06:44 2013	✎	✕
csc	672c346d8ff4d6032c91ad794eb087b26ab6b3fb	admin	Thu Sep 5 22:20:55 2013	✎	✕

FIGURE 5. Basic Access Authentication Subsystem

The authentication component receives a message and returns a Boolean value *TRUE* or *FALSE*. We also provide an application programming interface (API) to help developer implement AcousAuth into their project.

For demonstration purposes, one of the applications is keyless entry system. This mobile application lets you or those you trust to control your front-door lock by using your cellphone speaker to send modulated tone to the terminal. In our setup, the terminal is an electronic door lock combined with a cloud-based server; our application also provides an online GUI for all administration related functionality. Thus, users can easily grant access to their family, friends and guests nearly at anytime and anywhere. The user can interact with our system as follows. In the first step, user inputs their password to our mobile app. Then, our mobile application generates a modulate tone and broadcast it through cellphone speaker. At the same time, the terminal broadcast jamming signal and start collecting and decoding data. Final result shows on the terminal in the end to indicate whether the authentication process is succeed or not. Users can repeat the entire process again if necessary.



Success!

✓

Door Opening!

Monitoring...

FIGURE 6. Successfully Grant Access to a Guest

Originality & Innovation

(1) **Secure and Robust:** AcousAuth employs a purely software-based solution to secure smartphone short-range communication without the key agreement phase. In this system, we adopt the emerging friendly jamming technique from radio communication for data confidentiality. Therefore, the authentication process is very straightforward and fast. It makes our system robust and enables the short-range personal authentication functionalities without relying on complex supporting infrastructure. AcousAuth's security has been analytically and experimentally studied in our previous research paper. We proved that the acoustic-based short-range communication implement in this application is secure and can protect the confidentiality of the transmitted data against many passive attacks (e.g. passive blind signal segmentation attacks). Plus, our system is also naturally resistant to many active attacks, like data injection and jamming. This is due to the reason that the carrier frequencies of AcousAuth lie in the audible bandwidth, hence the short-range acoustic communication is noticeable by the users.

(2) **Cheap and Compatible:** Unlike other techniques such as Bluetooth or NFC, AcousAuth only depends on cellphone's speaker and microphone to accomplish the authentication process; it does not require any additional hardware. Therefore, the total cost for building up this system can be greatly decreased. In addition to this, the pervasive hardware that we used in our application makes AcousAuth compatible with majority of off-the-shelf mobile devices.

(3) **Tunable and Customizable:** The cloud-based architecture allows user to control AcousAuth through our incredibly simple online GUI. The tunability of this carrier frequency we used in AcousAuth creates the ability to design a customizable and tunable system.

(4) **User centric:** In spite of the state-of-the-art technique that we used, our team also focuses on adding user experience enhancing features into our application. We capture and represent essential demand of users which result in building a user centric application. The prototype for demonstration is well designed and we make it visually appealing to target market.

Other Products on the Market

Alipay sound wave mobile payment Alipay has launched a new payment system that makes user of sound waves for connecting smartphones to the ticketing machines in the Beijing Subway. The sound wave mobile payment system did not address the potential eavesdropping issue.

Lockitron (https://lockitron.com/) is a keyless entry system. It allows users to unlock their door directly from Internet. Users can also choose either use Bluetooth or NFC to trigger a command to toggle the state of their Lockitron when touched with a Bluetooth-enabled or NFC-enabled smartphone.

Kevo (UniKey) (http://www.unikey.com/) Kevo is pairs with UniKey, a Bluetooth-connected deadbolt door local. This app lets you send, receive and delete eKeys, see a log of lock activity or set up notifications and it is compatible with Apple iPhone 4s & 5.

NFCPorter (http://www.nfcporter.com/) is a system enabling users to control door, garage gates or attendance terminals with their mobile phones. Mobile phone therefore easily replaces all identification cards and unifies them under a mobile app. The application is designed for mobile phones with integrated NFC hardware. It allows the mobile phone to communicate with a contact-less reader and to identify the user.

GarageMate (http://BTmate.com/) is a secure garage door opener and takes advantage of Bluetooth security and user's phone's password protection. Only phones that have been previously "paired" to the receiver can open the door. The pairing process requires physical access to the receiver.

Seos (http://www.assaabloy.com/en/com/Products/seos-mobile-access/) Seos is an ecosystem of interoperable products and services for issuing, delivering and revoking digital keys on NFC mobile devices so that they can be used to open doors to homes, hotels, offices, hospitals, universities, industries and commercial buildings.

System Flow Chart & Screenshots

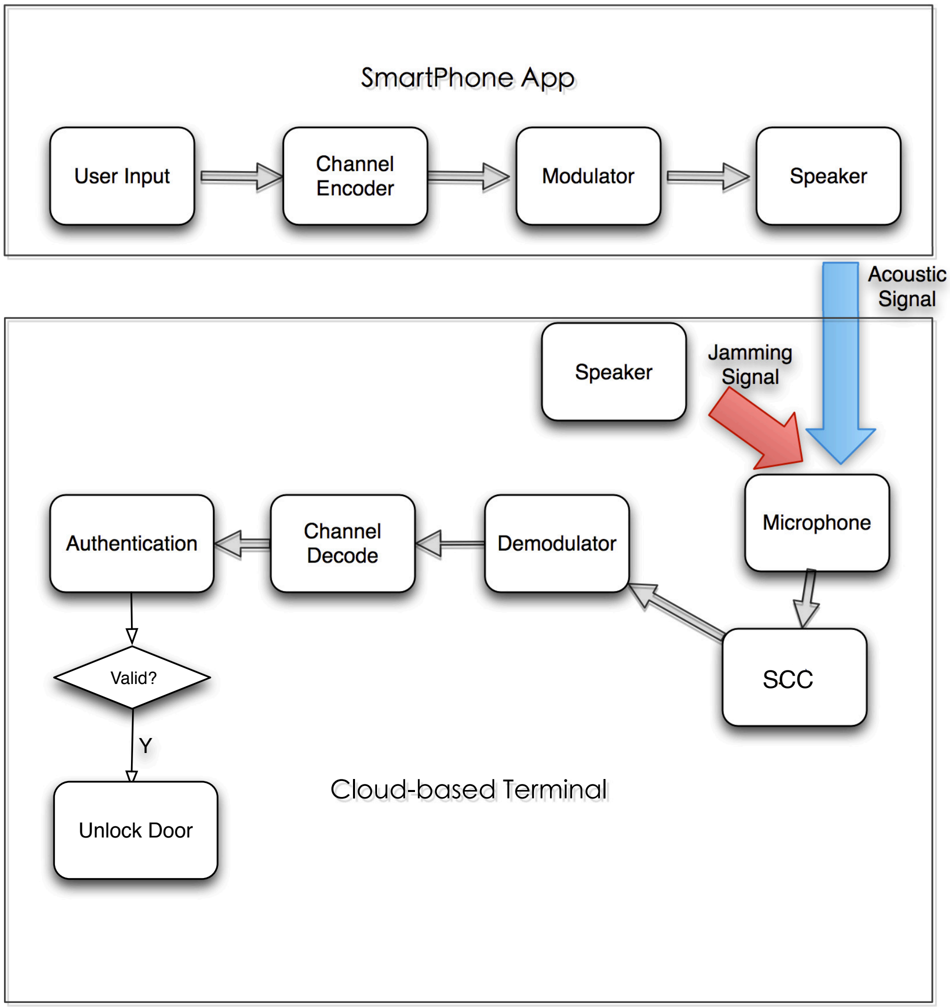


Figure 7. Flow chart of functionality

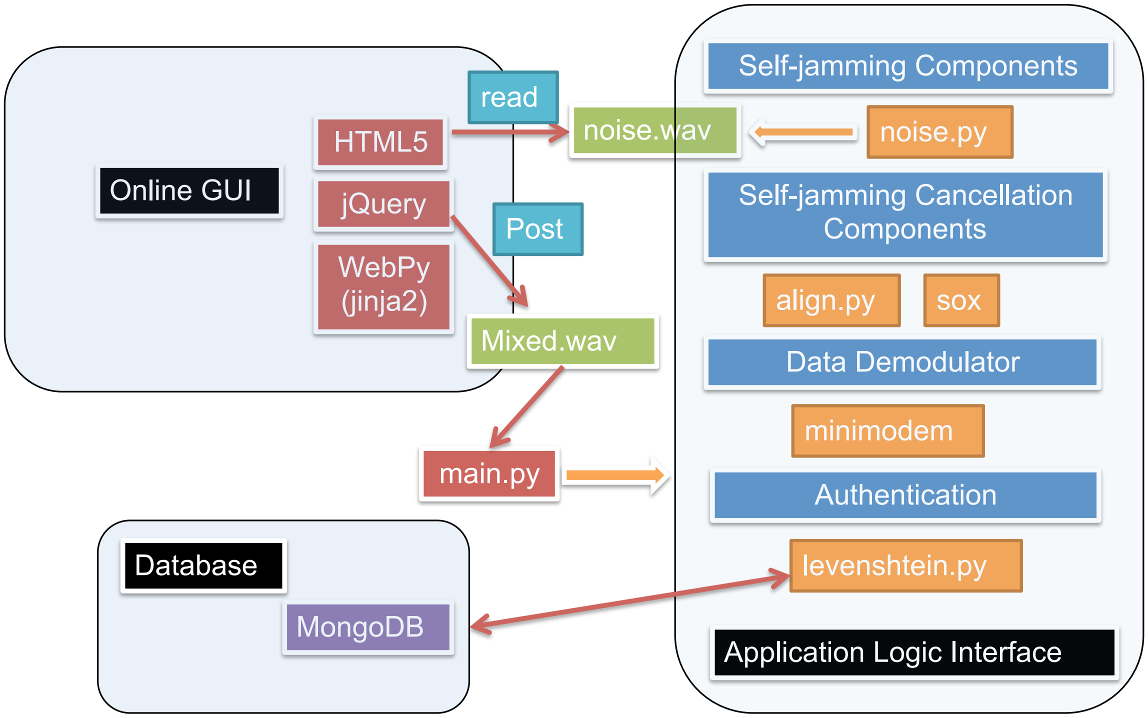


Figure 8. Server Side Component Graph

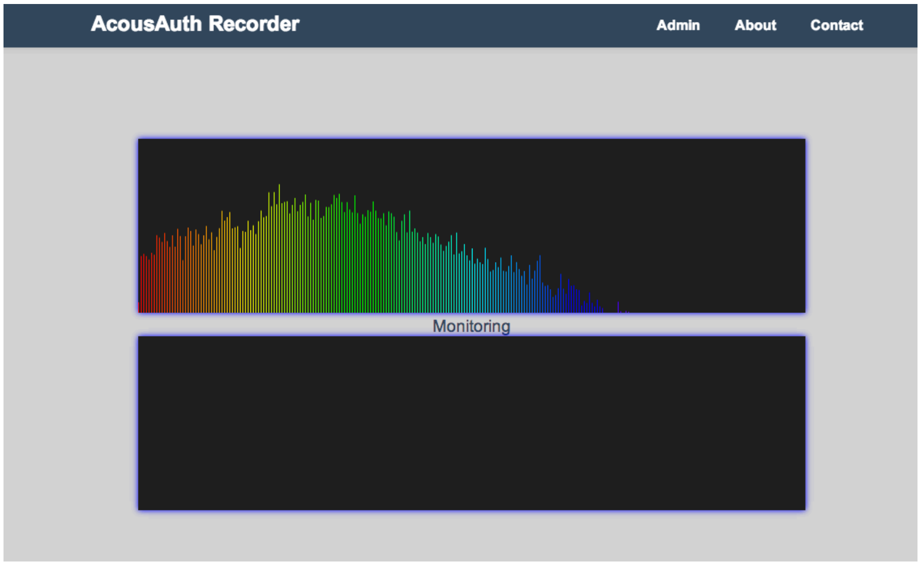


Figure 9. Front-End Graphic User Interface

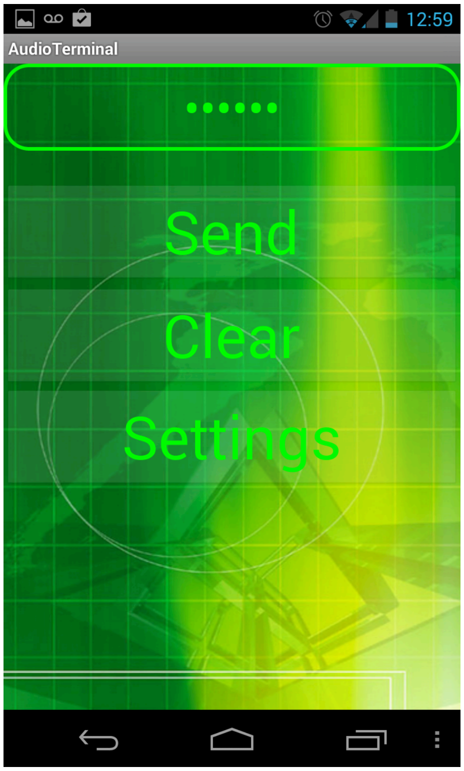


FIGURE 10. Mobile App Screen Shots