

# Biometric Anti-theft and Tracking System for mobiles - BATS

**Lakxman Kumar C, Arunachalam P, Sandhya S**

B.E Final year (CSE), T J Institute of Technology, Chennai, India

**Abstract**— The accretion of mobile theft these days causes peril to people. Though we have facilities to recover, we need an eminent and rapid mode to recover the lost entity. To abrogate the larceny of mobiles, we have introduced a concept of integrating mobile phones with fingerprint reader which serves as a solution to this augmenting problem. Along with mobile tracking facility, we also need information security. Thus to overcome these challenges we have developed *BATS*. The basis of *BATS* is the *Fingerprint Reader integrated with other mobile applications* in Smart phones and PDAs. The outcome is the prevention of mobile theft and high information security. When the Fingerprint reader senses the illegitimate fingerprint through *image processing*, it immediately sends alert to the person whose contact number has been registered in the mobile security name field, at regular intervals. The alert contains the information of time and place the mobile has been used. This is done with such celerity that the Smart phones and PDAs can be tracked in no time. The information ceded is enough to recover the stolen article. Thus, the mobile can be recovered, thereby depleting mobile theft and also increasing information security in a rapid and profitable way.

**Keywords**— Antitheft, Biometrics, Fingerprint reader, Smart Phone

## I. INTRODUCTION

**P**HONE theft is on the rise all over the world. In this world of vast geographical distribution, the mobile phone has transformed from being a luxury to a bare necessity. And it is only since the past six months that an electronic network was established to monitor mobile theft. So, the actual number is probably higher. The poor recovery rate dissuades most victims from reporting the loss of a mobile phone. They can be sold off fast even before the victim knows that his phone has been snatched.

The network providers too are not willing to do their bit to tackle mobile theft and block the IMEI number of the stolen set. In fact they have a long set of excuses for not doing it. These have been compounded by police inaction in tracing lost phones.

How to secure your valuable, costly and your personnel phones from being lost? Here is the ultimate solution, **THE BATS!!!!**

## II. PURPOSE

- To abrogate the larceny of Smartphone and PDAs providing a thorough and covert security.
- To construct a recherché application that doesn't face any critics at any situation i.e. in emergency cases and gives a lissome performance.
- To provide an eminent, rapid and lissome way to recover the lost entity in no time.
- To provide the owner not only the product security but also the information security.
- Assuage the customers providing a copacetic authentication technique more efficient than a password based system.
- To give a flexible, easily manageable, less time consuming and perdurable application.
- To make the customers handle the application with ease and comfort.

## III. SCOPE

- Inefficient and delayed mobile tracking system using IMEI number.
- Failure of notification to customers regarding theft of the Smart Phones.
- Lack of good security application in Smart Phones, to provide antitheft facility.
- Deficiency of protection for the information inside the Smart Phone.
- Complex antitheft systems that do not reach customers.

This BATS is capable of winning all these challenges using biometrics.

## IV. LITERATURE REVIEW

The review brings out the best way of authenticating a Smartphone or PDA in a fast, secure and convenient manner, using **Biometric Authentication** technique, replacing the password based systems.

**Biometrics** is the science and technology of measuring and statistically analyzing biological data. **Biometrics** is used in cases to identify specific people by two characteristics namely,

- Physiological (fingerprint, face recognition, hand geometry and iris recognition) and
- Behavioral (signature, voice).

**Biometric Authentication** is the act of establishing or confirming something (or someone) as authentic. **BATS** makes use of the physiological characteristic, fingerprint.

Here, the fingerprint reader is integrated with other applications of the product featuring password protection that frees users from having to remember and type passwords. The biometric security capability prevents unauthorized users from turning on the phone or accessing private applications and data like phonebook records and SMS messages thus giving the consummate security possible to the proprietors.

## V. METHODOLOGY

The vital concept behind **BATS** is the **Biometrics**. The convenience of biometrics is obvious to anyone who accesses a secure computer or network on a regular basis. The ability to replace existing password based systems with a biometric (**fingerprint**) would allow for a more secure computing environment, while also reducing the very real and documented cost associated with maintaining a password system.

**BATS** is an integration of mobile services and Fingerprint Reader services. *Five Fingerprint Readers* are placed on the phone and its services are integrated with the mobile features, such that every service in the phone has to be accessed by the fingerprint of the user.

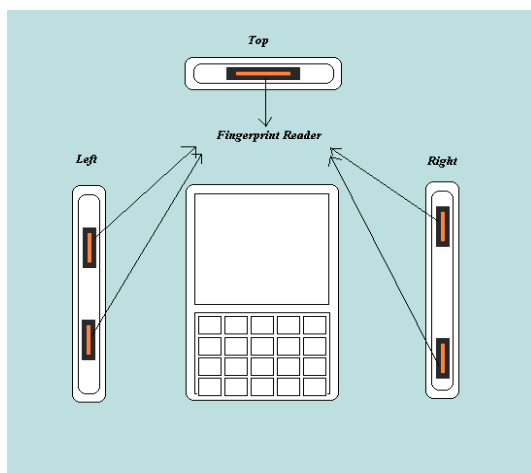


Figure 5.1 Five fingerprint readers on smart phone

### A. Work flow of BATS

The Owner will have the option to Enable or Disable the security application during his first use. When he/she **enables** it, the phone will ask to enroll the fingerprint. After enrollment, the Owner or Admin can continue using the gadget with high security. Suppose, he **disables** the application, he/she will receive a notification saying, '**The phone is Insecure**'.

Basically, **BATS** encounters three types of users, Registered User (Admin of the phone), Permitted Users (Other users permitted by Admin, with fettered services) and Anonymous Users. Registered User is the Admin of the phone, whose finger print is registered initially in the phone. Permitted Users are those, who are been registered by the Admin. Anonymous Users are those whose finger prints are not registered in the phone. **BATS** has four modes to work with.

- Registered Users work in **Admin mode** i.e. they can access all the services of phone. There is no time limit for the Admin to work in this mode.
- Permitted Users has two options to work in, **Guest mode** and **Protected mode**. Initially when the Fingerprint Reader scans the Permitted users, automatically the mode is switched to **Guest mode**, where the user can access only **few services** such as Messaging, Call and Gaming with a **time limit** of fifteen minutes which can be customized by the Admin. If he/she wants to access some more features, the mode is then switched to **protected mode**, by the Admin, where the services such as phonebook, MP3 can be accessed. This mode doesn't have any specific time limit, but can be customized by the Admin, if needed. Customization of the time limit and Modes are done only by the Admin. Hence, the Permitted User cannot work in protected mode without the Admin's permission.
- When the Fingerprint reader scans Anonymous Users, immediately the mode is switched to **unauthenticated mode**, where all the services are blocked.

At an instance, at least one Fingerprint Reader will be securing the device at specific time intervals. When the scan matches the Admin's fingerprint, then the user continues to consume the service. If the scan is invalid, then it tries to match it with the Permitted users and if it matches then the mode is switched to Guest mode. Later it can be customized to protected mode if needed, with the Admin's permission. Suppose, the scan doesn't match any of the registered users, then the unauthenticated mode is switched on, blocking all the services. Then a SMS alert is sent to the number saved already by the Admin. There are two more cases when the device is handled by an Anonymous user,

- When the battery is removed, the alert will be sent next time the battery is assembled and switched on.
- When the SIM card is detached, the Emergency Number will be called and the information about the

IMEI number, mobile number and an auto generated unique number will be ceded at the receiver.

Some facilities are provided for the Admin to overcome some inevitable cases mentioned below.

- When the Admin plans to sell his phone, he/she needs to erase all the registered fingerprint data. This can be done by the **Reset** option, where the data (fingerprints) stored is endowed to the other user. Reset option can be handled only with the proprietor's fingerprint to initiate the process.
- Suppose, the Admin gets his/her fingers damaged after enrollment, he/she can use the password protection as the substitute of fingerprint scanning, to access

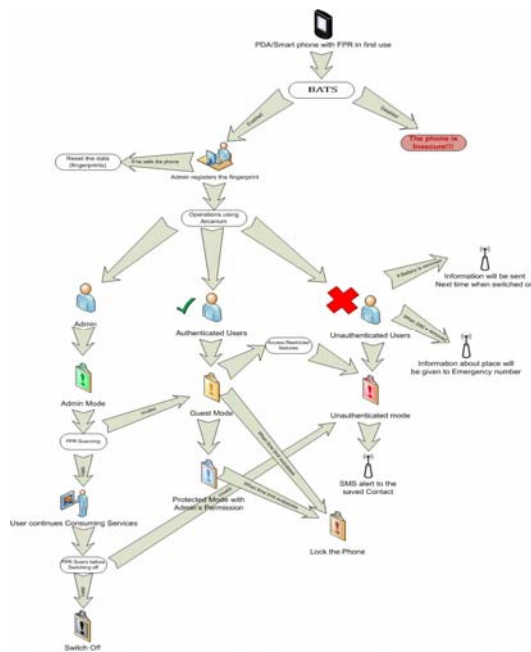


Figure 5.2 workflow of BATS

his/her phone. Persons other than the Admin are not allowed to use the password protection.

*B. How does the tracking process work?*

Today's smart phones and PDAs are provided with A-GPS receivers, which are the tracing devices, used for tracing the gadgets with the help of data from the satellite.

A normal GPS receiver spends about a minute (or even more) to receive the navigation data from the satellite. Also, it does not give the accurate location of the object every time, i.e. it locates the object 50 to 100m apart. These inaccurate data and time consuming process makes the tracing difficult.

Assisted GPS or A-GPS which has the assistance server and the network components, acts as a remedy for the above problems. A-GPS spends only 30 seconds at the maximum for decoding the navigation data from the satellites. It is also

capable of providing the required accuracy i.e. < 5m. A-GPS consumes less than 20mW of power per second, thereby improving the battery life. Surveys say that, having A-GPS alone active continuously, gives 5 days of battery life. A-GPS thereby serves as a good mobile tracker too.

When the fingerprint reader scans any unmatched data, first -the user will be notified thrice to stop the access. If he/she continues the access, the GPS service and the A-GPS receiver in the gadget will be enabled automatically. Then the A-GPS receiver starts extracting the decoded navigation data from assistance server through network; once received, a voice call to the corresponding emergency number with the information about the IMEI number and mobile number (only if the Admin enables) and an alert to the saved contacts with the information about the exact location of the gadget, the time of scan and IMEI number are sent.

The alert will be sent continuously at regular time interval, with the updation of location got from the A-GPS, until the fingerprint reader scans the Admin's fingerprint. This facilitates the tracking process to a great extent such that the phone can be traced even when it is out of hands, thereby avoiding E-wastage. The process will work even when the SIM card is removed since GPS traces the location using latitude/longitude/altitude measures got through satellites and not through the assistance of cell tower. When the battery is low, the A-GPS receiver will send a low battery alert to the saved contact.

An assistance data takes up to 3-4 messages to broadcast the complete data set. Each message is of 140 bytes in size. Hence, the maximum data charge per month will only be 10mb at the maximum which does not cost the user more.

VI. FINDINGS AND ANALYSIS

Smartphone have become the most wanted gizmo of this decade. These expensive devices with advanced technology, lacks proper security, resulting in continuous mobile theft.

Not just one instance, but many cases can be 'quoted' about gadget theft.

".... black with silver back 30G iPod was stolen at a house party in Taylorsville, UT on Christmas day 2007. Please if you've seen it or if it has been sold to you, contact me for a full refund of your money. It's engraved on the back with my name and e mail address."

"It's a RED BLACKBERRY CURVE WITH IMEI# \*\*\*\*\*. It was stolen at Oakdale High School on 1-30-08. @ 3:00 p.m."

All mobile users demand a technique for tracking the lost device using information about the tower's location where it was last seen. People await a more secure and pretentious technique than the password based system. BATS, a

Biometric Authentication technique assuages the customers in all these criteria.

*A. Why Fingerprint reader?*

There are many security applications and biometric techniques other than fingerprint recognition such as, Facial Recognition, Iris Scan, Hand Geometry, Signature Recognition, Keystroke Recognition, etc for security of the gadget. Of all these, Fingerprint system is more proficient with ease of use, good stability, low cost, good standard and high security level, as described in the statistics below.

	Security Level	Stability	Ease of Use	Cost	Hardware	Falses Positive Rate/100
Finger Print Reader	3	3	3	Low	Special, cheap	3
Facial Recognition	2	2	2	Low	Common, Cheap	1
Hand Geometry	2	2	3	High	Special, Mid-price	2
Iris Scan	3	3	2	High	Special, Expensive	2
Keystroke Recognition	2	1	3	Low	Common, Cheap	1
DNA	3	3	1	High	Special, Expensive	3

Fig 6.1 Statistics of Biometric Techniques

As an additional benefit, fingerprint reader consumes less power for scanning and recognizing, i.e. < 200mA during scanning and <400mA during recognizing, which does not affect the battery life to big extent.

*B. Fingerprint recognition*

A fingerprint is made up of a pattern of ridges and furrows as well as minutiae, which are discontinuities of ridges i.e. ridge bifurcation and ridge ending. Identification of a fingerprint is performed by recognizing the unique pattern in an individual.

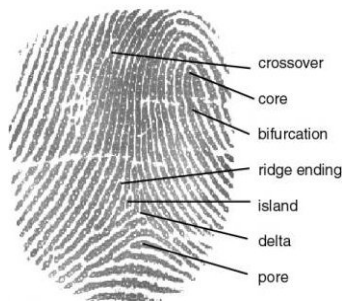


Figure 6.2 Characteristics of fingerprint

A fingerprint recognition system consists of three vital elements namely, the sensor, the processor and the matcher. The sensor is used to scan the finger; the processor is used for extracting the features in the finger and stores it in the

database and the matcher is used for matching the extracted features with the stored features.

*i. Fingerprint sensors*

There are two basic types of fingerprint sensors:

*Placement/Contact sensors:* the user places his finger over the sensor till it is scanned.

*Swipe sensors:* the user swipes his finger across the sensor maximum thrice allowing it to scan.

BATS uses the placement sensor to scan the fingerprint, making the gadget highly secure and trouble free.

*ii. Fingerprint matching technique*

The first step for the matching process is the *enrollment*. The user has to enroll his fingerprint with the user ID by swiping thrice over the sensor. The next step is *extraction*, where the fingerprint image is got as a result of scanning. During every swipe, the sensor scans the pattern elements of the fingerprint, encrypts them i.e. convert them into digital representation called the ‘template’ and stores them in the database. The template is smaller than a fingerprint image and thus can be processed at higher speed.

The next step in the matching process is the *identification*. Here one template is compared with N number of templates in the database. If it matches, the access is granted. Else the access is denied.

The matching process always uses only the fingerprint template and not the fingerprint image for comparison.

Fingerprint matching techniques are of two basic types: *graph-based matching* and *minutiae-based matching*. BATS uses the Minutiae-based matching technique, which is recommended for the modern embedded systems, as it uses a smaller template size, saving memory and thus producing higher processing speed than the graph-based matching

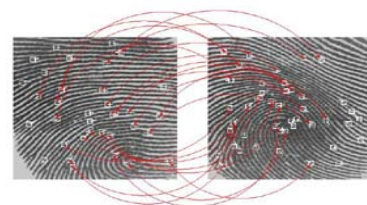


Figure 6.3 Minutiae-based matching

However, the matching is achieved only with the help of *image processing*, which uses the matching algorithms for computing the characteristics of ridges i.e. it calculates the relative position and angle between two minutiae of a single part in the input template, and compares it with the one in stored template. If they are similar, they are taken as ‘matched minutiae pair’.

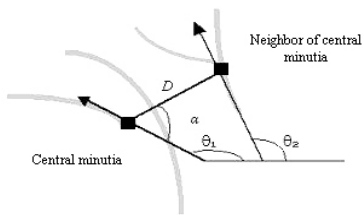


Figure 6.4 Calculation of angles and relative position

Likewise, every minutia in every part of the input template is checked and the total number of ‘matched minutiae pair’ is used to compute the final matching score.

C. How does fingerprint identification work in BATS?

Basically, a fingerprint template is stored as various parts. According to BATS, at an instance, at least one Fingerprint Reader will be securing the device at specific time intervals.

When a user holds the phone, at least one of his fingers will be touching the sensor. So, even when the sensor scans only a part of his/her finger, it encrypts the extracted feature and stores into a template with several parts.



Source: Precise Biometrics

Figure 6.5 Pattern stored as parts

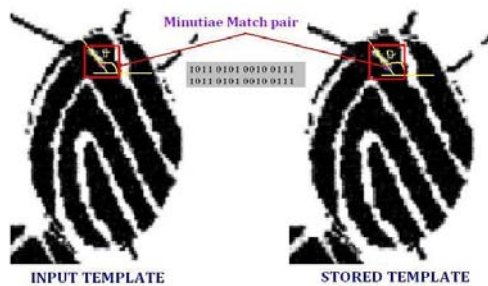


Figure 6.6 matching algorithm implemented on a single part

Then matching algorithm is implemented on each and every part of the input template, as explained in the section VI.B.ii.

VII. CONSTRAINTS

- When the proprietor uses the phone for the first time, he/she should **enable** the **BATS** to secure his gadget and confidential data. If he **disables**, his/her phone will be prone to an insecure state. Hence without proprietor’s cooperation the phone cannot be secured properly.
- BATS will work effectively only in the phones having GPS service.

- The user must be careful that he/she does not register any **‘latent fingerprint’** i.e. fingerprint made of sweat, sebum, dirt etc. Though the Fingerprint Reader works effectively, it is recommended to the Admins, not to register any latent fingerprints, as it may lead to malfunctioning in the device.
- The user must ensure that he/she does not enroll any affected finger such as psoriasis, scar etc which will definitely lead to authentication problem.
- The Permitted Users or the Secondary users cannot access all the features available in the Smartphone and PDA. He/she can access only very few fettered features such as Messaging, Making Call and Gaming.
- The Admin should be very cautious while handling his privacy features and customizing the Modes such that other users don’t access them at any cost.
- In spite of placing five Fingerprint Readers in the places, where the user holds the phone, there are very fewer chances for insecurity, that, none of the user’s finger touches any of the Fingerprint Reader.
- When the Admin plans to sell his phone, he/she should not forget to **reset** the stored data (fingerprints).

VIII. CONCLUSION

In every field in present days, biometrics is being used for authentication systems to eradicate the crime activities, such as confidential data theft. These biometric techniques work proficiently and succumbs a lissome performance of the device. Use of such a Biometric Authentication technique, like **BATS**, in mobile phones, especially Fingerprint systems, which is more pretentious, compared to any other security applications, will surely reveal a good dramatic change in the mobile arena, providing a secure and satisfactory environment.

REFERENCES

- [1] IDTeck, “Overview of Biometrics System”, White paper, <http://www.idteck.com>.
- [2] “An introduction to biometrics”, Biometric Consortium, <http://www.biometrics.org/html/introduction.html>.
- [3] <http://www.stolen911.com/>
- [4] Jim Bruene, “Identity Theft Statistics from Javelin Research”, Javelin Strategy & Research, January 26, 2005.
- [5] Shenglin Yang, Ingrid M. Verbauwhede, “A Secure Fingerprint Matching Technique”, UCLA dept. of EE, Los Angeles, CA 90095.
- [6] National Institute of Standards and Technology, “NIST Biometric Image Software(NBIS)”, <http://fingerprint.nist.gov/NBIS/index.html>
- [7] Hamilton Rocha, “How fingerprint recognition works”, A&H Software Ltda.
- [8] Nemerix, “Assisted GPS (A-GPS)”, [http://www.nemerix.com/CN/technology/about\\_agps.htm](http://www.nemerix.com/CN/technology/about_agps.htm)

- [9] Peter H.Dana, “*Global Positioning System Overview*”, Dept. of Geography, University of Texas, Austin, TX, September, 1994.
- [10] Chris Rizos, “*Principles and Practice of GPS Surveying*”, September, 1999.
- [11] Günther Heinrichs, Jinkel, Christian Drewes, Linus Maurer, Andreas Springer, Rainer Stuhlberger, Christian Wicpalek, “*GNSS/UMTS Prototype for Mass-Market Applications*”, GPS World, Jan1, 2006.
- [12] IDTeck, “*Fingerprint Recognition*”, White paper, <http://www.idteck.com>.
- [13] Alfredo C.Lopez, “*Fingerprint Recognition*”, EE Dept., Polytechnic university, 2004
- [14] R. Cappelli, D. Maio, D. Maltoni, “*Fingerprint classification by directional image partitioning*”, IEEE Trans. Pattern Anal. Mach. Intell, 1999
- [15] Digital Persona, “*Guide to Fingerprint Recognition*”, [www.digitalpersona.com](http://www.digitalpersona.com)
- [16] Zurich, “*AGPS Architecture*”, Los Angeles.
- [17] Brooks Shera, “*A-GPS based Frequency Standard*”, July, 1998, W50JM.
- [18] Recognition Systems Inc., “*Convenience vs. Security: How Well Do Biometrics Work*”.
- [19] Recognition Systems Inc., “*About Fingerprint scanning*”, [http://www.findbiometrics.com/Pages/fingerprint\\_articles/fingerprint\\_1.html#anchor3](http://www.findbiometrics.com/Pages/fingerprint_articles/fingerprint_1.html#anchor3)
- [20] Chao-Hsu Yao, “*Global Positioning System (GPS) Technology and Cars*”, April, 2002.
- [21] Beagle Software, “*Understanding GPS Technology*”, <http://www.beaglesoft.com/gpstechnology.htm>
- [22] Amy Zalman, “*Fingerprint Scanning*”, Ph.D., About.com.