Perspectives in Communication, Embedded-Systems and Signal-Processing (PiCES) – An International Journal
ISSN: 2566-932X, Vol. 2, Issue 9, December 2018
Proceedings of National Conference on Knowledge Discovery in Information Technology and Communication Engineering (KITE 18), May 2018

GPS- Finger Print System

K Murali
ISE Dept,4thSem, Brindavan College of Engineering, Bangalore, India,km16952@gmail.com

Adarsh Gowda
ISE Dept,4thSem, Brindavan College of Engineering, Bangalore, India,adarshss00004@gmail.com

Abstract: The biometric sensors are highly secured (example: fingerprint retina scanners, heartbeat, sweat, sound pattern, and face ID). Most of the security system widely use fingerprint based systems only .GPS software system is also one of the security system for military purpose. Many secret data transfer through this GPS line .By developing an application of GPS fingerprint system we can improve highly secured data. This GPs fingerprint system works on the basis of fetching GPS location and fingerprint access , it means that whenever the fingerprint is accessed in our system it can also fetch the information of that person with the present location . Many applications can be built under this system, example: banking data security, police tracking, hospital treatment, military, transaction.

Keywords: Global Positioning System; User; Client

I. INTRODUCTION

At the present age, safety has becomes a necessary issue for most of the people mainly in the rural and urban areas. Some people are more concern about their safety for their expensive thing like jewellery, money, property etc. So the bank lockers are the safest place to accumulate them but the conventional security system is not providing the higher security because in conventional security system a user can open the lockers using keys, can make a transaction with non-secure or some about loans are approved on illegal property. Sometimes the keys could be stolen, if password will be published, some loans are non-renewable on duplicate documents. Then the user will apply for original keys, temporary blocking our account, or re-verification of documents on loans but the time period is longer to get new keys or password or approval letter for applied loans, so in its place of using this security system we have implemented. In this present age, safety has becomes an necessary issue for

Biometric (FINGERPRINT) and GSM/GPRS based security system which provide more security then conventional system. In this paper we have implemented security of the money in the bank locker, house or other documents by using Fingerprint and GSM/GPRS technology which will be more protected than other systems.

In this paper, we also explained that, a particular person can be traced out with the exact location where ever that person accessed his fingerprint, by merging of both GPS tracker & fingerprint sensor device.

II. RELATED WORK

The Global Positioning System, also called Navistar, that we use was built by the US military and has been fully operational since 1995. Many modern GPS receivers use a combination of both GPS and the Russian GLONASS satellites for improved coverage and accuracy.

The term “biometrics” refers to the collection and use of biological data and behavioural characteristics. As more global financial activity becomes digitally-based, many banks are utilizing new technologies to develop next-generation identification controls to combat fraud, make transactions more secure, and enhance the customer experience. Fingerprint liveness detection methods have been developed as an attempt to overcome the vulnerability of fingerprint biometric systems to spoofing attacks. Traditional approaches have been quite optimistic about the behaviour of the intruder assuming the use of a previously known material. This assumption has led to the use of supervised techniques to estimate the performance of the methods, using both live and spoof samples to train the predictive models and evaluate each type of fake samples individually. Additionally, the background was often included in the sample representation, completely distorting the decision process. Therefore, we propose that an automatic segmentation step should be performed to isolate the fingerprint from the background and truly decide on the liveness of the fingerprint and not on the characteristics of the background. Also, we argue that one cannot aim to model the fake samples completely since the material used by the intruder is unknown beforehand. We approach the design by modelling the distribution of the live samples and predicting as fake the samples very unlikely according to that model. Our experiments compare the performance of the supervised approaches with the semi-supervised ones that rely solely on the live samples. The results obtained differ from the ones obtained by the more standard approaches which reinforces our conviction that the results in the literature are misleadingly estimating the true vulnerability of the biometric system

Relatively in this paper we explained that by using both GPS & FINGERPRINT technology we can get the exact location of the particular person. This will done by the team work of both by considering the flow chart (fig. 1)

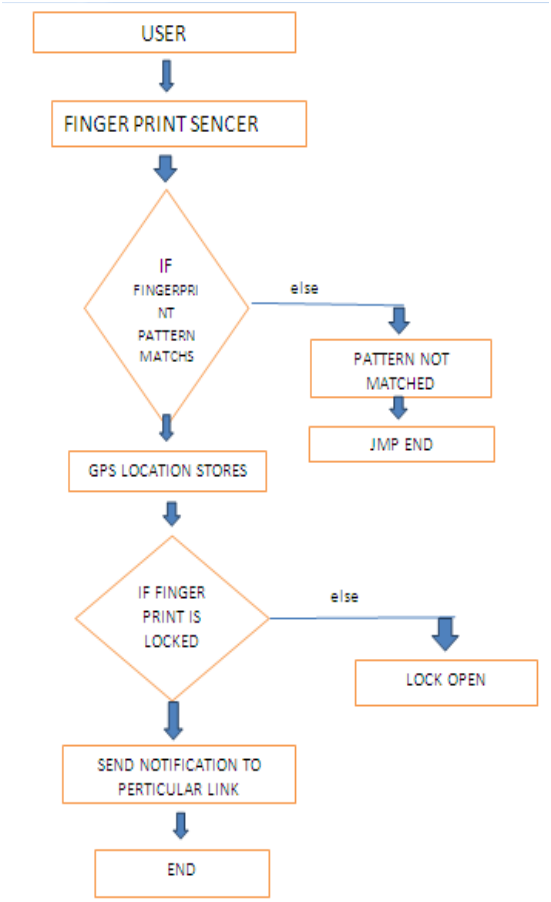

Fig 1. Flowchart

A. GPS Fingerprint Sensor

Step 1: User can access his fingerprint in any device

Step 2: Fingerprint of the user will be scanned by the sensor

Step 3: After fingerprint scanned by the sensor, the process starts matching that with already stored data

If the user fingerprint is matches that will moved on to the next step, otherwise it displays the message as “pattern not match” and jump to end

Step 4: If the fingerprint is matches location of that access will be stored on cloud

Step 5: After storing the location it can check whether that fingerprint is locked by some or not.

If that fingerprint didn’t locked by any of them, then that will opens the lock and moved on to the next process whatever the user needs.

If his fingerprint is locked by someone, the system sends the notification to that particular link, who locked his fingerprint with the exact location of that user

Step 6: Without opening the lock, process will be ends

III. APPLICATION

A. Banking

In this paper, we can explain about the banking security based on THE GPS-FINGERPRINT of the user .We mainly concentrate on the approval order of the loan by the bank .The present condition is that ,if the bank customer is applied for the loan bank will check only the client property details ,but not his background whether he has taken any other loan in any different bank and his transaction is cleared or not.

By example Mr .VIJAY MALLYA is a great business man ,he has taken crores of money from great nationalized banks ,but till now he have not yet cleared his due to the banks .It may cause loss to those banks ,If the banks can know about his background then ,they can reject his approval but it is not yet happened .If that crores of money can be used for other rural areas or some agricultural fields ,the middleclass families or backward families can improve their life needs from those bank money

If we use the GPS-FINGERPRINT system we can know all about the client and also his background ,whether he has taken a loan in other bank or not ,whether he has cleared the loan or not ,and also his fingerprint is blocked or not .If he cheat’s the bank ,his fingerprint can be locked through that bank. Wherever he tries to access his fingerprint that location can be fetched, and that location is sends to the bank and also tothe nearest police station, by this we can easily catch hold of the criminal and also most of the illegal crimes can be caught by this system. This system is easily under-stood by the below flow chart.

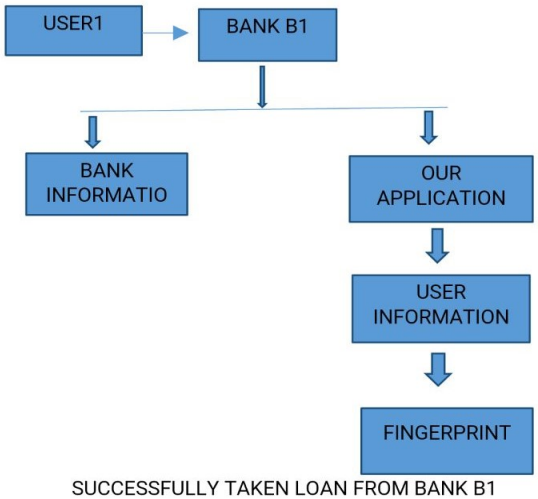

Fig 2. Flowchart for issuing loan

Banks have their own system, which is maintained very secretly about their client which cannot be known by the public .But bank can save only some details about the

client and his reference ID about his loan documents whichever he has submitted (it can be help-full for spot civil verification), in this GPS-FINGERPRINT SYSTEM, all these information are to be stored and locked by his FINGER-PRINT.

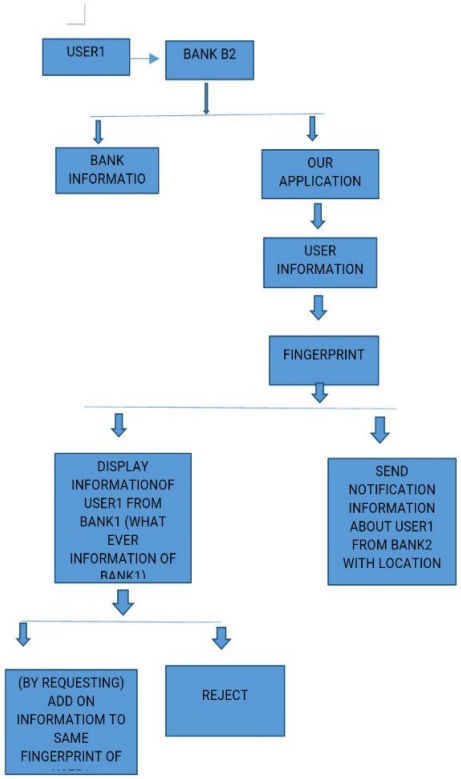

Fig 3. BANKER 2 finding out whether the customer has taken loan from any other source

If the same client requires more money from other bank then he goes to some other bank rather than going to the same bank which he received previously then he will apply for the loan, as similar what we explained in the above paragraph for the Bank-1 even this bank also consist of same security system .As same process will be followed as fig. 2.

After the GPS-FINGERPRINT access in this system, it will display the information of that client in the previous bank, soon after it sends notification with all the information of the client from Bank-2 with exact location with the help of this information both the banks can stay in contact with each other and share the information about the loan.

Bank-2 have an additional power, if the client request is approved by the bank-2. He will receive the loan amount then the amount received information about the second loan will be added to the same finger print.

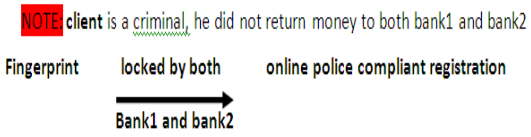

Fig 4. Notification

After the given duration of time he will not return the loan amount and the client will cheat both the banks, bank-1 and bank-2 then the bank will register the case on the client through online police complaint, and will launch the FIR against the client. As soon as the FIR is registered the client's finger print automatically gets blocked.

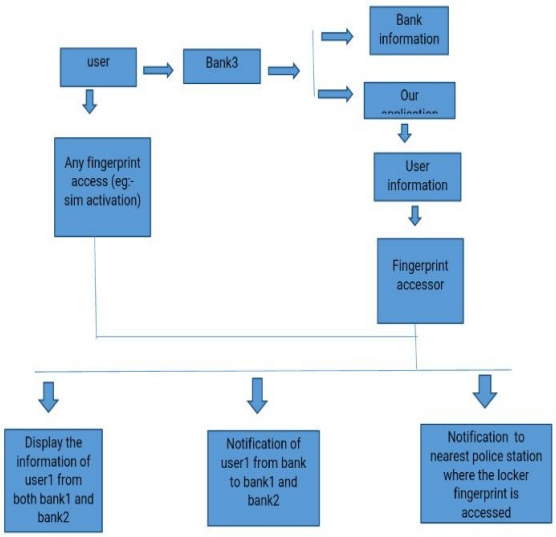

Fig 5. BANKER 3 finding out whether the customer has taken loan from any other source

In fig. 5 it shows that, if the client goes to Bank -3 and applies for the loan as in the fig.2 and the process will continue .After the client FINGERPRINT is access in the system of Bank-3 .Then the FINGERPRINT blocked notification will be displayed.

As soon as the notification is received the location of the Bank-3 will be fetched & stored and all the information about the client in the Bank-1 & Bank-2 is displayed in bank-3 system .Then the information about Bank-3 is sent to Bank-1 and Bank-2 and also to the FIR registered police station with the exact location of the client and Bank-3 .Then all the information about Bank-1,Bank-2,Bank-3,FIR information is sent to the nearest police station of the Bank-3.

By this system we catch hold of the criminal very easily.

B. Police Investigation

For example, in the murder case police investigation. The murder is occurred, the police investigator does not know any clues about the criminal and the murdered person. By the forensic - report the police investigator will get the FINGERPRINT of the criminal, then they will block that particular FINGERPRINT so that if the criminal access his FINGERPRINT the location can be fetched and detected by the police system.

For the further investigation by keeping as a reference of that FINGERPRINT , police compares all the FINGERPRINT which is stored in the cloud (example: police records, bank records, airports , hospitals) with the reference of the obtained criminal FINGERPRINT , if any FINGERPRINT in cloud matches with the criminal FINGERPRINT then it is easy to find out the criminal. This process is represented using the block diagram as shown in the fig.6

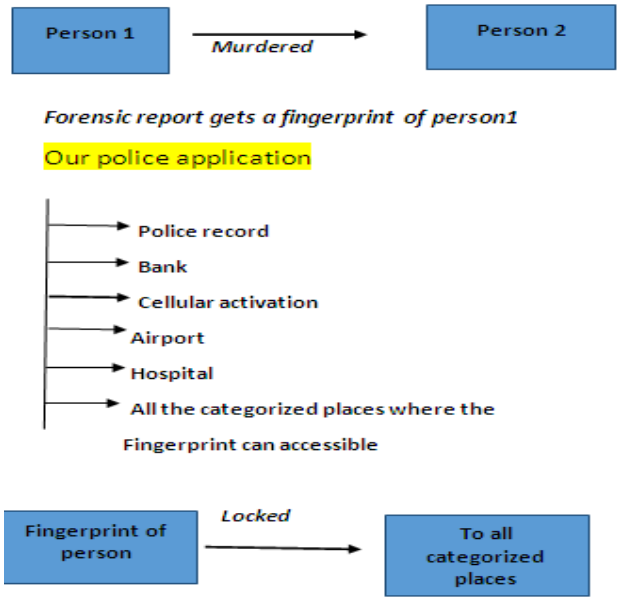

Fig 6. System assisting to solve murder case

Example

If the criminal tries to escape through the air- lines, the criminal undergoes some rules and regulations in airport such as passport verification and FINGERPRINT access. If the FINGERPRINT is blocked then the information of that location is fetched and stored, then the notification of the criminal's information is displayed in the police station of the airlines and also in the police head –quarters.

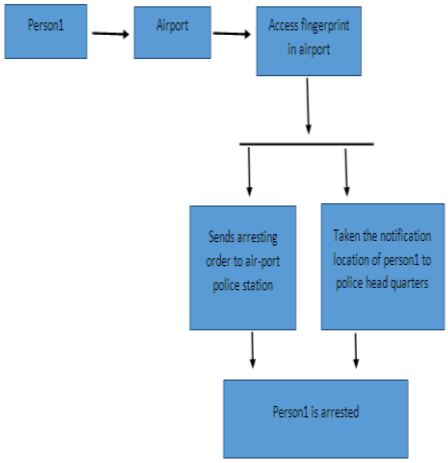

Fig 7. Scenario: Person escaping through airport

C. Hospital

In this case the person is met with an accident and that person is been hospitalized and the hospital staff doesn't know any information regarding that person ,but it's their responsibility of that hospital to inform about the patient to their family and also to complain for the police station ,so that they can proceed with the further treatment. This process is structurally explained in the below fig.8

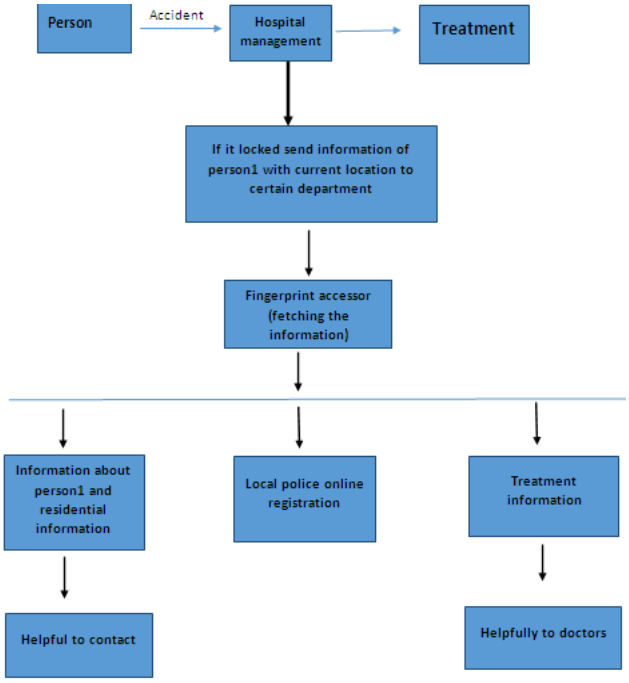

Fig 8. Scenario: Hospital

IV. OVERCOME DISADVANTAGE

1. Till now we have used only particular servers based on each accessories systems, but by this system we can access our job from any of our location with the help of any server.

2. In forensic report we get unknown FINGERPRINT, that pattern can be matched globally (worldwide cloud) by this system.
3. In network abounded area so many soldier's loss their lives due to communication problem but by this system we can overcome this by fetching the previously loaded GPS location of the particular soldier.
4. If an unknown injured patient is hospitalized the staff members will not be having any information regarding patient. In that situation the hospital management can get the information about that patient by accessing patient FINGERPRINT and this system is helpful to inform to the patient guardian
5. We can also block someone's FINGERPRINT by the help of police, if that person is a criminal and if he tries to escape

V. DISADVANTAGES

1. This system is comparatively costly to install.
2. It takes more time to get implemented all over the servers.
3. There are some complicated steps to be undertaken in this system.
4. Merging of both FINGERPRINT and GPS is difficult.

VI. CONCLUSION

Developing each and every application is highly secured and useful, those applications change our life style and needs .Every application is part of technology and hence improves the present technology. Our application also develops the technology and improves the life style and changes the needs accordingly.

REFERENCES

[1] https://en.wikipedia.org/wiki/Global_Positioning_System

[2] https://en.wikipedia.org/wiki/GLONASS