# Information Provider via Biometrics Security

**Kulkarni Sahil Santosh[1] Gaikwad Rushikesh Narendra[2] Cheriyal Omkar Shrinivas[3]**
**Chavan Vijay Parshuram[4] Mr. Vijay Namdeorao Kukre[5]**
[1,2,3,4]Student [5]Head of the Dept.
[1,2,3,4,5]Department of Computer Engineering
[1,2,3,4,5]AISSMS's Polytechnic Pune-411001, India

*Abstract*— Over the last few years a we have observe a focus on engineering science has been established whose products are likely to create a large market in the near future. It has been known "biometrics". Nature has build every human beings with different characteristics which may vary from one person to another. This property is made use of by Biometric technology to perfectly identify each person Biometric technique is necessary to determine a pattern which determines a user pattern by determining the validity of a specific substantial or behavioral types influenced by the user. Individual major concern must be observed in making a practical biometric system. First, a user must be register in the system so that his biometric impression can be identified. This impression is securely stored in a central database or a smart card given to the user. The impression is fetched when an individual needs to be verified. Depending on the information, a biometric system can operate either in a verification (authentication) or a recognition mode.

***Keywords:*** Algorithms, Security, Authentication, Biometrics, Ridges, Valleys, Authorization, Arch, Whorl, Scanner, Database

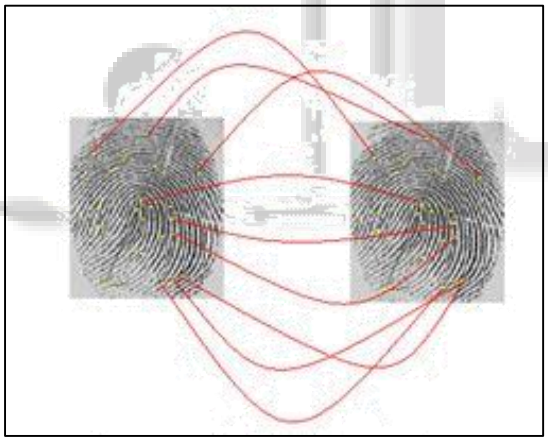

Fig. 1: Scanned Fingerprint Authentication.

## I. INTRODUCTION

Biometrics works in such a way that it recognizes the correct person by his physical aspects. Among the features measured are; face, fingerprint, hand geometry, iris, retinal, signature, and voice. Biometric has become the ideal mode of verify/authenticate a person. Now-a-days the security falls short to prevent from hacker and the level of increasing fraud is requesting for a great demand of high level security.

Biometric devices are the best and most demanded for high level security in transaction and data security and confidentiality. The need of biometrics is very crucial in fields like military, transaction and personal data security. Enterprise-wide network security infrastructures, government IDs, secure electronic banking, investing and other financial transactions, retail sales, law enforcement, and health and social services are already benefiting from these technologies.

Biometric-based verification applications contain workstation, network, and realm access, individual sign-on, application logon, data security, distant access to resources, transaction protection and Web protection. Faith in these electronic deal is essential to the good growth of the global wealth. Effective use of individual or grouped technologies such as smart cards, conceal keys and D.S, biometrics are set to fill nearly all aspects of the economy and our daily needs. Using biometrics for personal authentication is becoming easy and considerably more perfect than current methods (such as the using of passwords or PINs). This is because biometrics links the impression to a particular person (a password or token may be used by someone other than the authenticated user), is easy (nothing to carry or recall), perfect (it provides for possessive authentication), can provide an report stream and is becoming socially allowed and cheap.

The security field uses three different types of authentication:

- Something you know — a password, PIN, or piece of personal information (such as your mother's maiden name)
- Something you have — a card key, smart card, or token (like a Secure ID card)
- Something you are — a biometric.

Of these, a biometric is the most secure and convenient authentication tool. It can't be borrowed, stolen, or forgotten, and forging one is practically impossible. (Replacement part surgery, by the way, is outside the scope of this introduction.).

## II. DIFFERENT TYPES OF BIOMETRICS AUTHENTICATION

Biometric sensors or access control systems are classified into two types such as Physiological Biometrics and Behavioural Biometrics. The physiological biometrics mainly include face recognition, fingerprint, hand geometry, Iris recognition and DNA. Whereas behavioural biometrics include keystroke, signature and voice recognition. For better understanding of this concept, some of them are discussed below.

### *A. Fingerprint Recognition*

Fingerprint Recognition includes taking a fingerprint image of a person and records its features like arches, whorls, and loops along with the outlines of edges, minutiae and furrows. Matching of the Fingerprint can be attained in three ways, such as minutiae, correlation and ridge

- Minutiae based fingerprint matching stores a plane includes a set of points and the set of points are corresponding in the template and the i/p minutiae.
- Correlation based fingerprint matching overlays two fingerprint images and association between equivalent pixels is calculated.

 

– Ridge feature based fingerprint matching is an innovative method that captures ridges, as minutiae based fingerprint capturing of the fingerprint images is difficult in low quality.

### *B. Face Recognition*

Face recognition systems work by capturing data for the nodal points on a digital image of a person's face and resulting data can be stored as a face print. When the conditions are favorable, these systems use a face prints to identify accurately. Currently, these systems focus on smartphone applications which include personal marketing, social networking and image tagging purposes. Social sites like FB uses software for face recognition to tag the users in photographs. This software also increases marketing personalization. For instance, billboards have been designed with integrated software that recognizes the ethnicity, gender and estimated age of onlookers to deliver targeted marketing.

### *C. Iris Recognition*

Iris recognition is a one type of bio-metric method used to identify the people based on single patterns in the region of ring shaped surrounded the pupil of the eye. Generally, the iris has a blue, brown, gray or green color with difficult patterns which are noticeable upon close inspection. Please follow the below link to know more about iris recognition technology.

### *D. Voice Recognition*

Voice recognition technology is used to produce speech patterns by combining behavioral and physiological factors that can be captured by processing the speech technology. The most important properties used for speech authentication are nasal tone, fundamental frequency, inflection, and cadence. Voice recognition can be separated into different categories based on the kind of authentication domain, such as a fixed text method, in the text dependent method, the text independent method and conversational technique.

### *E. Signature Recognition*

Signature recognition is a one type of biometric method used to analyze and measure the physical activity of signing like the pressure applied, stroke order and the speed. Some biometrics are used to compare visual images of signatures.

## III. WORKING

Biometric Verification System resembles social systems such as finger-print machines. Iris scanner, voice authenticator, face recognition. Figure 2 represents working of a Finger-print Verification System. Finger-print verification consists of a Finger-print scanner that is used for both verification and authentication. Faster Finger-print detection algorithms like Jiang, Chen, and Minutia-Cylinder-Code (MCC).

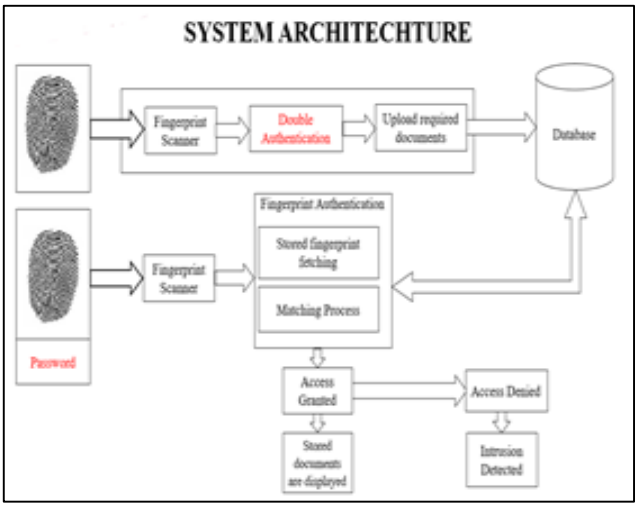


Fig. 2: Finger-print Authentication System

There are three types of Fingerprints

– Arch
– Loop
– Whorl

The Fingerprint Verification is based on the types of fingerprint. The Fingerprint Scanners are classified into two types mainly Optical and Capacitive.

### *A. Capacitive Fingerprint Scanner:*

A capacitance scanner uses electrical current to display the image processed. The principle of capacitance is used in this device. As shown in the figure 3, each sensor consists of arrays of cells. These cells have two conductor plates, which are covered with an insulating layer. Thus, they form a simple capacitor which is used to store the charge. The cells are so small that their actual size will be smaller than the width of a ridge from our finger. These sensors will then be connected to an integrator. The output of the integrator will be given to the input of an inverting operational amplifier. This op-amp will consist of hundreds of transistors, resistors and capacitors. This op-amp is alters the input voltage with respect to the reference voltage provided to the other input. The non-inverting input is connected to the ground. The inverting input is given to the reference voltage and then to the feedback circuit. This feedback circuit is given to the amplifier output and also includes the two conductor plates.

When the finger is placed for recognition, it acts as another capacitor plate. It is separated with the help of insulating layers. When moving the finger from one point to another, the capacitance changes due to the variation in distance between the capacitor plates. Thus, the output voltage is recorded with the change in output voltage according to the appearance of ridges and valleys. A perfect output image of the fingerprint is thus obtained.

This device is much better than an optical scanner as it is very compact and harder to trick. The device needs a real fingerprint shape to get the output. The optical scanner a dark and light pattern is more than enough to make an output image. Though an optical scanner needs CCD devices for sensing, a capacitance scanner needs only semi-conductor chips.

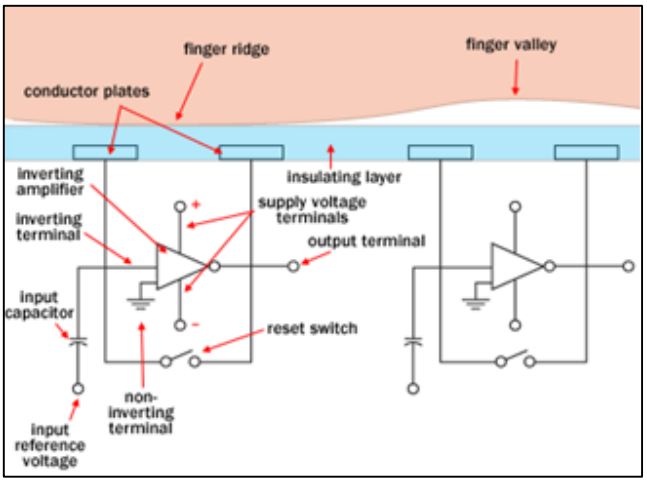


Fig. 3: Capacitive Fingerprint Scanner

The ridges and valleys of our fingerprint scanned by the fingerprint scanner is mapped and stored in the database in various formats that is .GIF, .JPEG, and etc.

The scanner does not actually scans the fingerprint but tries to match the key features that are ridges and valleys with our stored data.

After the keywords are matched successfully it grants the access to the documents or data that is stored in database secured by fingerprint.

### *B. Fetching and Displaying*

First of all we need to store our fingerprint in database. After successfully storing the fingerprint in the database there is option for uploading the required documents in the database. When the user want to fetch or to share the stored data he/she must verify the fingerprint stored in the database after successful verification the user will be redirected to his/her account page where data/documents are stored.

## IV. ADVANTAGES AND DISADVANTAGES

### *A. Benefits of Biometrics:*

An increasingly popular commercial security option, biometric security systems are able to provide strong security through accurate validation of personnel. This validation is based on a range of biometric qualities such as facial and iris recognition, fingerprint scans, and vascular pattern recognition. Biometric systems are an effective security system for public and private offices to keep track of authentication, attendance, access control time, and much more.

A TechSci Research report indicates that the global biometrics market is projected to grow to over $24.8 billion by 2021. As the industry continues to advance and develop, these systems have become much more reliable and cost effective. Below are some advantages to installing a biometric security system for your business.

### *B. Accurate Identification and Accountability*

Biometric systems provide more accurate identification, lowering your risk of unwanted breaches. With this type of security system, access is granted not by passwords or smart cards but by biological characteristics like iris scans or fingerprints which are difficult to duplicate or forge. This more accurate information helps with security as well as accountability. Logging activity through a biometric security system helps connect personnel with specific actions or events that can be referred to in the unfortunate case of a security breach.

### *C. Efficient*

Incorporating biometrics into your commercial security will save you time and money. Biometric security systems are designed with ease of use in mind and give you accurate results with minimal effort. With the right security system provider, installation of a biometric security system is easy and manageable with simple, straightforward training. Biometric identification functions very quickly, typically identifying an employee or visitor in a matter of seconds. This helps keep productivity steady while also keeping your business secure.

### *D. Accuracy*

Traditional security systems mess up regularly costing us a big amount of time, money and resources. The most common security systems are passwords, personal identification numbers (PINs) and smart cards that aren't always accurate. However, biometric works with your physical traits such as fingerprints, palm vein, retina amongst others that will always serve you accurately anywhere, anytime.

### *E. Accountability*

In other verification methods, anybody can use your password or security number to hack your personal information, which is highly risky and we are suffering from this problem continuously. But, in case of biometric security, it needs your direct interactions to login or pass the security system which allows 100% accountability for all your activities.

### *F. Convenient*

Imagine all the times when you forgot your passwords, quite nerve-wrecking, right? You are not alone. We all have gone through this process where it is hard to memorize or note down each and every password and we are more than likely to forget it at some sticky situations. There are some handy tools to do the job for you, but none of these can beat the convenience of biometric solutions which stands to be the most convenient solution ever. Your credentials are with you forever, so it doesn't require you to memorize or note down anything.

### *G. Scalability*

Unlike other solutions, biometrics are highly scalable solutions for all types of projects. Biometric technologies are used in many government projects, banking security systems, workforce management, etc. It is possible because of the scalability of its solutions.

### *H. ROI*

Biometric solutions will provide you the best ROI compared to other security systems. You can keep track of thousands of employees of a large company with just one biometric device and software. On the other hand, you would need to manage a huge resource to do the same job costing you more time than the appropriate biometric solution.

*I. Profitable*

The return on investment (ROI) on a biometric security system is very high. For one, it's much more effective at avoiding fraud than most security systems, protecting your business from potentially catastrophic breaches – according to IBM's 2017 Ponemon Cost of Data Breach Study, the global average cost of a data breach is almost $4 million. It also saves resources and money, as it reduces management time and helps keep policies consistent.

Biometric security systems are a long term commercial security solution for any business. Efficient, effective, and versatile, biometric security systems will keep your business secure while saving you time, money, and resources. However, your commercial security system is only as effective as the security system provider you partner with. At Veridin, we offer a comprehensive suite of services and support for facility biometric security systems in Toronto. We have over 25 years of experience in security management and have worked with a wide variety of businesses, always making sure their unique needs are met. Learn more about our security system solutions or contact us today to get started on protecting your business.

## V. CONCLUSION

Fig. 4: Biometric Systems

This paper summarizes Biometric representations of our data stored in database using biometric security. The active biometric learning module developed can be easily adapted and effectively used by the common peoples and which in terms also saves the environment through less use of paper.to survive in such a hack-able and fraud environment we need a strong security mechanism to secure our personal data which is only possible through biometrics which is unique identification of individual (even in case of twins).

## REFERENCES

[1] "IBM International Technical Support." Secure Fingerprint Devices on the Web in Theory and Practice. Jun 1997. http://www.redbooks.ibm.com/redbooks/pdfs/sg244978.pdf
[2] Bella, G. Massacci, F. and Paulson, L. "Verifying the SET Registration Protocols." Proceedings of IEEE Journal of Selected Areas in Communications 2003. http://www.cl.cam.ac.uk/~lp15/papers/Bella/registration.pdf
[3] Bella, G. Masaccio, F. and Paulson, L. "Verifying the SET Registration Protocols." Proceedings of IEEE Journal of Selected Areas in Communications 2003. http://www.cl.cam.ac.uk/~lp15/papers/Bella/registration.pdf
[4] https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-111-introductory-digital-systems-laboratory-spring-2006/projects/project4.pdf
[5] https://www.webopedia.com/TERM/F/fingerprint_template.html
[6] https://www.youtube.com/results?search_query=double+access+from+application

 