IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-7, Issue-7, July 2019 E-ISSN: 2347-2693

An Overview of Biometric Technologies and Its Benefits

D. Gayathri[1*], R. Uma Rani[2]

[1]Department of Computer Science, Periyar University College of Arts & Science,Tamilnadu, India
[2]Department of Computer Science, Sri Sarada College for Women,Tamilnadu, India

Corresponding Author: dgayathri78@rediffmail.com, Tel.: +00-94437-10117

DOI: https://doi.org/10.26438/ijcse/v7i7.207213 | Available online at: www.ijcseonline.org

Accepted: 18/Jul/2019, Published: 31/Jul/2019

***Abstract*—**Biometric technology is becoming a standard security feature in large businesses. In the modern networked society, there is an ever growing need to determine or verify the identity of a person. Where authorization is necessary for any action, be it collecting a child from child-care facilities or boarding an aircraft, authorization is almost always vested in a single individual or a class of individuals. There are a number of existing methods, used by society or automated systems to verify identity. Traditional existing methods can be grouped into three classes: (i) possessions; (ii) knowledge and (iii) biometrics. Biometrics is the science of identifying or verifying the identity of a person based on physiological or behavioral characteristics. It provides additional layer of security via its strong authentication process. This innovation allows compromised premises to quickly identify intruders. As the technology world is evolving there are more and more trends and demand in the field of identity management. All these trends and demands are generated from one basic need – the need for a more accurate and secure way of identifying an individual. The intelligent ones are already learning to adopt with these trends in order to gain competitive advantage. This Paper brings about the recent trends in Biometric Technologies and its applications.

Keywords— Wi-Fi, SSO, Cryptography, Cloud-Biometrics etc.,

I. INTRODUCTION

Biometrics is the science of identifying or verifying the identity of a person based on physiological or behavioral characteristics. Physiological characteristics include fingerprints and facial image [1]. With the pace of rapid innovation in today's biometric technology field, new uses are appearing to make the process of authentication more convenient and secure. These innovative and useful processes of human identification are increasing in frequency with every year. As these uses are increasing, they are also creating some trends and reshaping the way to identify humans. Of all the trends in the field of biometric technology, most are focused on finding a better and more efficient way of authenticating a person based on "Who they are." Of course, there are still the traditional ways of identifying a person including personal identification numbers (PINs), ID cards, and passwords but these methods identify a person based on "what they have" or "what they know." None of them identifies a person with the most important factor, which is "Who they are" [7]. As biometric traits are personal and unique, this is perhaps the most accurate way of identifying a person. This paper indicates how biometric technology is evolving to make authentication more convenient and secured. The identification technologies are given in below 'Table 1'.

Table :1 Identification Technologies

Method	Examples	Comments
What they know	userid, password, PIN	Forgotten Shared Many passwords are easy to guess
What they have	Cards, badges, keys	Lost or stolen Shared Can be duplicated
Who you are	Fingerprint, face.....	Non-repudiable authentication

Biometrics systems has three primary components such as [10],

- ✓ Automated mechanism that scans or photographs (video or still) and captures a digital or analog image of a living biometric characteristic.
- ✓ Another mechanism that handles compression, storage, processing, and comparison of the captured data with the stored data (enrollment template).
- ✓ Interface with the application system

The organization of this paper is to study advanced biometric technologies to improve security with the help of biometric systems and devices across the globe.

II. LITERATURE REVIEW

Biometric identification systems are widely spread since the reliability of these systems has been proven. They exhibit a large number of advantages when compared to other traditional identification systems such as key and password that are subject to falsification and loss. Although biometric techniques seem to be very powerful, they are incapable of currently guaranteeing a high recognition rate with unimodal biometric systems based on a unique biometric signature or on a unique resource. In addition, these systems are often affected by the following problems [8]: noise generated by the sensor, non-universality, lack of individuality, lack of invariant representation and sensitivity to attacks. To prevent these problems, several biometric modalities within a same system can be utilized. Multimodality consists of a multitude of possibilities, such as the multi-sensor, multi-instance, multi-algorithms, multi-samples, and multi-biometrics.

The unimodal biometric systems have to contend with a variety of problems, namely, noisy data, intra-class variations, restricted degrees of freedom, non-universality and spoof attacks [4]. Many of these limitations can be addressed by deploying multimodal biometric systems that integrate the evidences presented by multiple sources of information.

Further, multimodal biometric systems provide anti-spoofing measures by making it difficult for an intruder to simultaneously spoof the multiple biometric traits of a legitimate user. Thus a challenge-response type of authentication can be made possible by the use of multimodal biometric systems [2].

Early automated authorization relied on possessions and knowledge, but there are several well-known problems associated with these methods, which restrict their use and the trust that can be placed in them. These methods verify attributes which are usually assumed to imply the presence of a given person. The most important drawbacks of these methods are (i) possessions can be lost, forged or easily duplicated; (ii) knowledge can be forgotten; (iii) both knowledge and possessions can be shared or stolen. Consequently (iv) repudiation is easy (it is easy to deny that a given person carried out an action, because only the possessions or knowledge are checked, and these are only loosely coupled to the person's identity). Such drawbacks are not tolerable in applications such as high security physical access control, bank account access and credit card authentication [7]. The science of biometrics provides an elegant solution to these problems by truly verifying the identity of the individual.

Multimodal modality can significantly improve the recognition accuracy of a verification/identification system. In this fusion at the score level is most important and widely used because it offers the best tradeoff between information content and ease of fusion. It give better performance, reduce failure and provide more security against fraud [6].

III. BIOMETRIC TECHNOLOGIES

There are several biometric technologies are available today. They are

- Mobile Biometric Technology
- Multimodal Biometric Authentication Systems
- Cloud Based Biometric Solutions
- Vertical Specialized Biometric Solutions
- Biometric Single Sign on (SSO)

A. Mobile Biometric Technology

Both governments and the private industry are turning to mobile biometrics to speed up processing of human identification. Mobile biometrics simply means achieving individual biometric identification on a mobile device with the portability to be easily moved or shifted from one place to another. Biometric functionality can be achieved on a mobile device either through its built in biometric sensors or by attaching portable biometric hardware to it via a USB cable or through a Wi-Fi connection.

1) Biometrics on Smartphones

There are nearly 7 billion mobile subscriptions worldwide, estimates The International Telecommunication Union which is equivalent to 95.5 percent of the world population. The world is more connected than ever before and every Smartphone user wants to be sure about personal data security in the digital age. For years, the password was the only secured way of authentication, but times have changed and passwords are now much easier to hack and harder to remember as they increase in complexity. Mobile phones and biometrics are a winning combination in the mass market, allowing the technology to become much more widely accepted.

A recent report shows that at least 30% companies from all over the world will use biometrics on mobile devices by 2016. In addition, several Smartphone manufacturers have already started to embed biometric sensors on their devices with fingerprints, facial recognition and voice biometrics the most popular modalities of choice. Once upon a time a fingerprint scanner was used only by governments, the military, and law enforcement, but in the past 5 – 10 years, biometric identification has exploded and rapidly spread to the commercial sector, permeating virtually every corner of our lives as a more secure method of proving individual identification. It plays important roles in

a) Security
b) Payments
c) Data Access

a) Security

Already, a larger number of people are getting used to using Smartphone for daily activities, often storing highly sensitive information. However, most people are reasonably concerned about the security protection of using passwords. A multi-factor security system using biometric recognition offers Smartphone users higher security and convenience.

It is almost a certainty that within the next few years, biometric identification will become a standard feature in every new phone. Specifically, three biometric modalities will be key players: fingerprint scanners built into the screen, facial recognition powered by high-definition cameras, and voice recognition based off a large collection of vocal samples.

b) Payments

Biometric payments are a Point of Sale (POS) technology which uses biometric authentication system to identify a person by their unique traits such as a fingerprint, iris or palm vein pattern, or facial recognition. The rising use of biometric identification for financial service transactions has already begun to spread rapidly around the globe. In fact, in addition to banks and other financial institutions, companies like Apple and PayPal already showed their interest to implement biometric based payment solutions. Biometric payments have some remarkable benefits too – no need to carry cash, checks or credit cards, they offer stronger security, transactions can be processed faster, and banks don't charge any extra fees.

c) Data access

Our PCs are full of personal data and generally the passwords are used to protect them. More specifically, people use passwords to gain access in to the computer, laptop, and mobile devices. The interesting fact is most of those three gadgets have a camera that can be used to verify individual identities through biometric technologies such as facial recognition. Another gadgets that had seen is fingerprint biometrics, however due to problems like poor skin integrity that inhibits the effective use of this modality, it is more likely that we will see a rise in the use of alternative biometric modalities such as facial and voice recognition for individual identification. Apple integrates biometric technology on their products and Microsoft has integrated fingerprints and IRIS recognition system in Windows 10.

This trend is triggered by the fact that, biometric human identification can't always be performed in a controlled office environment. At times biometric identification might be required to go where people go, perhaps in public venues. Under these situations mobile biometrics can be effective and speed up the identification process. One great example of this can be the border control system to protect the borders from insurgents and terrorists.

B. Multimodal Biometric Authentication Systems

A single form of biometrics for authentication is no longer an effective option for many companies. The next trend in biometrics is the use of multiple biometric authentication systems for human identification. Multimodal Biometric Authentication systems take input from a single or multiple biometric devices for measurement of two or more different biometric characteristics to ensure authentication accuracy.

A unimodal biometric system captures and matches only one biometric trait resulting in an absence of sustainable ways to solve limitations like noisy data, intra-class variations, non-universality, and spoof attacks. Multimodal biometric authentication systems are expected to be more reliable against these issues due to the presence of multiple, independent biometric traits. Multimodal biometric authentication systems are expected to be used more in the future due to their effectiveness in providing more accurate results and stronger security [3].

There are five types of multimodal systems which are capable of reducing several problems encountered in unimodal systems. The multi-sensor, multi-instance, multi-algorithm, multi-sample systems combine the information resulting from a single modality able to improve the performances of the recognition by reducing the effect of intra-class variability. However these systems are not able to deal with the problem of the non-universality of certain biometrics as well as resistance to the frauds. In contrary to the multi-biometrics systems which use several biometrics, they are able to build a more flexible system. In case of any failure in any method, the system can rest on the other methods in order to provide an acceptable recognition rate [9].

C. Cloud Based Biometric Solutions

This trend is mainly driven by mobile biometric technology. In mobile biometric technology, pairing that mobile biometric device with a cloud based biometric solution can speed up the identification process even more. Instead of saving the biometric data locally, sending it to the cloud is a safer solution.

In addition, when government and enterprises are calculating the overhead cost they have to bear for maintaining a physical server, moving to the cloud seems like a wise choice. Another fact behind the rising trend of using cloud based biometric solutions is the scalability of the cloud. Cloud computing allows the business to easily upscale or downscale their IT requirements as required. For example, they can quickly increase their existing resources to accommodate increased business needs or changes. This allows them to accommodate their business growth without expensive changes to existing IT systems.

D. *Vertical Specialized Biometric Solutions*

Having a vertical specialized biometric solution for identity management is becoming a popular choice for many industries. These kinds of solutions are designed to meet the unique demand of their respective industries. They are also customized by keeping in mind the local and international industrial laws and standards. For instance, in the vertical specialized biometric solution for the financial services industry, it is designed to provide security, and reduce fraud and waste providing a complete audit trail for both customer and employee activity. For the healthcare industry, the smart health platform that facilitates a higher accuracy level for patient identification and unifies big data and clinical knowledge in healthcare in an unprecedented way to drive personalized health, decision support, and predictive analytics.

When seeking biometric identification management solutions, businesses are very conscious about their unique requirements and are opting to deploy a customized solution designed specifically for their verticals. These solutions will provide higher efficiency and control.

E. Biometric Single Sign on (SSO)

Perhaps one of the most popular debates at this point is whether biometrics will replace passwords**.** This debate came to light due to the fact that many companies are adopting biometric **single sign on (SSO)** over traditional passwords to secure their networks from data breaches and to minimize password management costs. The passwords are weak because of multiple reasons: they can be guessed, forgotten, shared or swapped. Conversely, biometrics is unique, hard to spoof, and a person cannot lose or share them.

In some cases where employees must log into multiple databases and have different passwords for each of them, it can be very frustrating. This was not only making employees frustrated but also decreasing productivity. Many companies where choose to implement Enterprise B**iometric suite**, a complete biometric single SSO. The employees no longer have to remember passwords and their networks were secured too.

IV. BIOMETRICS TECHNOLOGY IN HOME SECURITY

Technology is enabling criminals to boost their operations, even making it possible to conduct massive heists off-site. For a household, installing a home alarm system is not the end of the security. It's imperative to do regular assessments, customizations, and upgrades to ensure the infallibility of home security. The introduction of biometrics technology was a game-changer in the security system industry. Over the past decade, companies are boosting their product lines that incorporate biometrics into various devices. The various biometric trends are:

- Two-factor authentication
- Public-Key Cryptography
- Cloud Biometrics
- Out-of-Band biometric login

A. Two-factor authentication

The strong authentication capability of biometrics is the primary reason why more businesses opt to shift to this security technology. Mary Chaney, a security specialist at GE Capital Americas, said: "If you use dynamic/behavioral biometric measure, like keystroke dynamics, you can gain advantage of two-factor authentication."

The two-factor authentication combines password and physiological characteristics. This security tool is being used by governments in authenticating voters and licensed drivers. Banks are also embracing this biometric trend by providing corporate clients with a hardware that produces unique codes every 20 to 30 seconds. Before a company representative is able to perform wire transfers, he/she has to input a password and the unique codes displayed on the hardware.

B. Public key cryptography

Biometrics technology is coming to homes as demand for heightened home security continues to rise. The home security systems with biometrics that are gaining popularity include biometric locks and physical access systems secured via Bluetooth or Wi-Fi. One problem, however, is the risk of a server storing user credentials getting compromised. Public key cryptography is an innovative solution. This decentralized security protocol allows users to choose their own biometric authenticators with their biometric data remaining encrypted and protected against malware.

C. Cloud biometrics

To improve the security system in your home, it's not enough to add hardware. You need to boost your security software and integrate new technologies to protect your personal data. Explore cloud biometrics that use cloud services via a web browser or mobile application. This innovation allows real-time and parallel processing. Cloud biometrics can be used on a personal computer or Smartphone. Most users of cloud biometrics are businesses, though the technology will likely be accessible to households soon.

D. Out-of-Band biometric login

Out-of-band login is a type of two-factor authentication that requires a secondary verification method through a separate communication channel along with the typical ID and password. Today, more families are installing home surveillance cameras that can be monitored wherever they may be. This is used not only to protect against burglars but also to watch over little kids. Security systems that have biometric features ensure that data such as videos do not fall into the hands of the wrong people. People can integrate an out-of-band login in all their electronic devices.

One challenge of integrating biometrics technology in residential spaces is the cost. In weighing down the costs and benefits of a biometric technology in home, people should always keep in mind that criminals are more equipped now than ever. Simple alarm systems don't stand a chance against sophisticated burglars. People can start by securing physical access to their home via biometrics technology—no need for keys or access cards.

V. BIOMETRIC TECHNOLOGY IN E-COMMERCE

Biometric Technology has a particular significance in Ecommerce of the future. Ecommerce has successfully penetrated into the daily routine of the common man for getting them access to reliable and cost effective products in comparison to those available in the local markets. The ease and comfort of online shopping has facilitated people to get products at home, whereas merchants have also explored these channels to endorse their products to revenue maximization. Despite the benefits, the eCommerce industry has brought several insecurities to the table regarding the personal and confidential information of customers. The buyers are interested in placing orders online, but the fear of fraud often prevents them from doing so.

Traditional security methods like remembering a username, password, and a secret question are now outdated because hackers can easily break them and get access to user accounts. In such cases, the systems do not recognize the true identity of a user and allow anyone to sign in to an account whoever has a password.

For preventing identity misuse, biometric technology is proposed to be implemented on eCommerce websites because a biometric identification system uses physical and behavioral characteristics of an individual to grant account access. For example, it includes the use of fingerprints, iris patterns, facial recognition, voice, and palm vein patterns to match it with a database to verify a user's identity.

A. Significance of Biometric Technology in E-commerce

Every online business wants to strengthen their platform to provide a safe shopping experience to the end consumer, so they have altered or defined new strategies with the passage of time. The ability to pay from the comfort of home through credit cards or any other payment gateways has made the eCommerce world more vulnerable to fraud and identity theft. Hackers gather personal and financial information of consumers, breaking passwords, getting illegal access to accounts and forging identities which discourage people from paying for goods and serves online.

To lower the risks associated with an online store, biometric technology has replaced conventional identity verification in favor of behavioral and physiological attributes. The most commonly used biometric is fingerprinting that needs the installation of a fingerprint and a database to capture and record the biometrics of users. The system reads fingerprints of a user and grants access only if it matches with the records, or else access is denied. This strengthens security checks of people frequently logging in to the web site and offers a secure alternate.

B. Implementing biometrics for a strategic move

Customer security and comfort is the ultimate priority of an online store. The implementation of biometrics on eCommerce website is also among the strategic moves that are performed to lead the market. The addition of a fingerprint reader in iPhone 6S, 5S and other branded cell phones has set new identity verification standards for online buyers.

Online store owners who have made their website mobile friendly to facilitate the majority of online users can easily turn users into loyal customers by allowing them to sign up for an account through fingerprints and get rid of entering passwords and personal details again and again. It will facilitate them to quickly select products, proceed to checkout, and confirm identity by tapping their finger and nothing else.

The use of biometrics with mobile commerce will further maximize the revenue of online stores as it sets customers free from remembering complicated passwords and ensures that their financial details are kept confidential.

C. Working of Biometric Technology In Ecommerce

The effectiveness of biometric technology has compelled experts to adopt it for online shops so users from different localities and regions can enjoy shopping without worrying about fraud. A merchant can add biometrics by following these steps:

- Selecting a type of biometric
- Enrollment and verification system
- Retrieving fingerprints

1) Selecting a type of biometric

Select a behavioral or physical aspect of a user to set as identity verification. It can be fingerprints, palm print, iris, palm veins, face, voice, ECG, DNA or a signature that is unique to each individual. By nature, we have a distinct body and personality, and no one can forge it exactly the same.

2) Enrollment and verification system

The selection of a biometric shall be based on consumer ease of entering the details. For example, if we set fingerprint scanning as the primary identity check, we will need to take a record of every customer registered. After a biometric enrollment template is created, users can be authenticated by scanning the fingerprints again and testing the system.

3) Retrieving fingerprints

Fingerprints are stored in binary code (no images are ever stored) on a server with the ecommerce web site and then retrieved in the matching process when a customer tries to access their account. Mobile users can easily tap the screen and get access to their accounts rather than configuring their social accounts or remembering complicated passwords that are made unbreakable with special characters and capital letters.

VI. USES OF BIOMETRICS ACROSS THE GLOBE

Over the years, we have seen steady upward growth of biometric technology across the globe for myriad reasons but mostly due to the fact that personal identification and authentication is considered more and more important. From border and immigration control to identifying criminals, time and attendance in working places, the practical uses of biometrics are growing rapidly [5]. Many businesses consider biometrics to be applicable for government use only but they are quickly learning that the applications of biometrics extend far beyond the government use exclusively. They are listed as follows:

- Airport Security
- Time and Attendance
- Law Enforcement
- Access Control and Single Sign On (SSO)
- Banking Transaction Authentication

A. Airport Security

Making the journey through airport terminals more seamless for passengers is a goal shared by airports around the world. Biometric technology to verify passenger identities has been used in several large international airports for a number of years and the technology is quickly spreading to other locations across the globe.

In many airports, the top biometric modality choice for immigration control is iris recognition. In order to use iris recognition, travelers are first enrolled by having a photo of their iris and face captured by a camera. Then, their unique details are stored in an international database for fast, accurate identification at ports of entry and exit that use iris recognition for traveler identity verification. When travelling, instead of waiting in long queues to be processed, passengers simply walk into a booth and look into an iris camera. The camera then photographs the iris and a software program then matches the details with the information stored on the database.

Biometrics simplifies the airport experience for millions of passengers travelling every day. Use of the technology also ensures the highest level of security and safety.

B. Time and Attendance

Fraudulent employee time and attendance activities are a common phenomenon in organizations throughout the world. According to an **American Payroll Association Study,** the average employee reportedly steals approximately 4 and half hours per week, which is equivalent to 6 weeks' vacation if extrapolated over a year. To solve this issue, companies are implementing biometric time clocks on their work sites.

A biometric time and attendance system is the automated method of recognizing an employee based on a physiological or behavioral characteristic. The most common biometric features used for employee identification are faces, fingerprints, finger veins, palm veins, irises, and voice patterns. When an employee attempts identification by their biological traits, a biometric hardware device compares the new scan to all available templates in order to find an exact match. Even government organizations now rely on biometrics for ensuring timely attendance of staff and accurate payroll calculations.

C. Law Enforcement

One of the most fascinating uses of biometrics is in crime solving. Organizations like the Federal Bureau of Investigations (FBI) and Interpol have been using biometrics in criminal investigations for years. Today, biometrics is widely used by law enforcement agencies across the world for the identification of criminals. Biometrics is also widely used for jail and prison management. Biometrics provides a modern solution by which the Jail Authority, Public Safety Departments, and Governments can safely and securely manage prisoner identities.

D. Access Control & Single Sign On (SSO)

The primary reason behind more and more organizations and personnel across the globe adopting biometric technology for access control and Single Sign On (SSO) is because traditional authentication tactics like passwords are insufficient for personal identification. Passwords only provide evidence or proof of knowledge whereas biometrics provides unique advantages because it relies on identifying someone by "who they are" compared to "what you know "or "what you have." Today, biometrics is widely used around the world for home access control, mobile phone access, vehicle authentication and single sign on (SSO).

E. Banking – Transaction Authentication

Biometrics in banking has increased a great deal in the last few years and is being implemented by banks throughout the world. As global financial entities become more digitally-based, banks are implementing biometric technology to improve customer and employee identity management in an effort to combat **fraud, increase transaction security, and enhance customer convenience [4].** Customers are also fed-up with identity theft and the inconveniences associated with constantly having to prove their identities. As a result, more and more customers are looking for banks that have biometric authentication in place prompting banks to more closely research the technology for implementation.

VII. CONCLUSION

Different biometric technologies offer varying features and benefits, which should be analyzed based on how and why they will be used. They all vary in performance. capabilities, infrastructure requirements, and cost, and all have their unique limitations and operating methodologies. While individual biometric devices and systems each have their own operating methodology, there are some generalizations that can be made as to what typically happens within a biometric system implementation. As the technology world is evolving there are more and more trends and demand in the field of identity management.

All these trends and demands are generated from one basic need- the need for a more accurate and secure way of identifying an individual. Biometric technology is supported by the addition of fingerprint scanning on mobile devices, making it easier for website owners to implement biometrics. Biometric identification management systems offer higher security, convenience, accountability, and accurate audit trails – all attributes that motivate businesses to research and implement the technology for their own use. Smartphones are now treated as all-in-one device, suitable for every purpose and its small wonder that they will become the next big market for biometric identification. The combination of biometrics and Smartphone is bound to fundamentally change access control, financial transaction authentication, personal data security, and many other areas of our lives.

Thus we must use advanced technologies to improve the security level in every organizations to save our data and to avoid many problems caused by misuse and theft of information.

REFERENCES

[1]. B.Miller, "Vital Signs of Identity". *IEEE Sectrum* , 22-30, 1994.

[2]. D.Gayathri, R.Uma Rani, "*A Prototype for Secure Web Access Model using Multimodal Biometric System based on Fingerprint and Face Recognition"*, International Journal of Computer Science and Information Technologies ,vol. **3**,issue. **3**,pp. **3985-3988, 2012**.

[3]. D.Gayathri, R.Uma Rani," *An Efficient Multimodal Biometric System Using Adaptive Gabor Filtering based Feature Extraction*", European Journal of Scientific Research ,vol. **141**,issue. **4**,pp. **463-475**, **2016**.

[4]. D.Gayathri, R.Uma Rani," *Multimodal Biometric System: An Overview"*, International Journal of Advanced Research in Computer and Communication Engineering ,vol**.2**,issue **1**,pp. **898-902**, **2013**.

[5]. K.Modi, S. "*Biometrics in Identity Management Concepts to Applications*".

[6]. Meenakshi Gupta, Adti Grover, "*Survey on Technique of Multimodal Biometric System*", International Journal of Innovative Research in Computer and Communication Engineering , 1-7, **2016**..

[7]. Nalini K. Ratha, Andrew Senior and Ruud M.Bolle. "*Automated Biometrics*", pp. 1-11.

[8]. S.Khellat-Kihel," *Finger Vein recognition using Gabor filter and support vector Machine in :IPAS*", **2014**.

[9]. S.Khellat-Kihel, R.Abrishambaf," *Multimodal Fusion of the finger Vein, fingerprint and the finger-knuckle-print using kernel fisher analysis*", *Elsevier*,439-447,**2016**.

[10]. Amandeep Kaur Bhatia and Harjinder Kaur, "*Security and Privacy in Biometrics: A Review",* International Journal of Scientific Research in Computer Science and Engineering ,vol **1**, issue **2**, pp. **33 – 35, 2013.**

Authors Profile

D. Gayathri has completed her M.C.A from J.K.K Nataraja College of Arts and Science, Komarapalayam, affiliated with Periyar University. She received her M.Phil Degree from Periyar University in June 2005. Now pursuing her Part time Ph.D., research in Periyar University, Salem. Now she is working as Asst. Professor, Department of Computer Science in Periyar University College of Arts and Science, Mettur Dam, Salem Dt. Her research area is of Information security.

Dr. R. Uma Rani has completed her M.C.A. from NIT, Trichy in 1989. She did her M.Phil. From Mother Teresa University, Kodaikanal. She received her Ph.D., from Periyar University, Salem in the year 2006. She has published around 121 papers in reputed journals and National and International Conferences. She has received the best paper award from VIT, Vellore, and Tamil Nadu in an International conference. She was the PI for MRP funded by UGC. She has acted as resource person in various National and International conferences and workshops. Her area of interest includes Information Security, Data Mining, Fuzzy Logic and Mobile Computing. She is working as Principal, Sri Sarada College for women, Salem.