# A COMPREHENSIVE REVIEW ON DEVELOPMENTS IN BIOMETRIC AUTHENTICATION SYSTEMS

**Malvinder Singh**

Assistant Professor (Comp. Sc.), Miri Piri Khalsa College, Bhadur, Punjab, India.

**ABSTRACT**

The measuring and statistical analysis of an individual's distinct physical and behavioral traits is referred to as biometrics. These traits can include voiceprints, iris patterns, fingerprints, facial features, or even patterns in a person's gait or handwriting. These traits are used by biometric systems to identify and verify people. These traits are employed to authenticate and recognize people. Modern security solutions now stand on the foundation of biometric authentication systems, which provide a strong and dependable way to identify people based on their distinctive physiological or behavioral traits. This study offers a thorough analysis of the developments and difficulties encountered in biometric identification systems, including a range of modalities such as iris patterns, fingerprints, facial recognition, and behavioral biometrics. The review starts with an outline of the basic ideas behind biometric authentication, emphasizing the distinctiveness, consistency, and applicability of biometric characteristics. These developments could lead to future improvements in biometric systems' security, precision, and usability, opening the door to a more linked and safe digital environment.

**Keywords:** authentication, biometrics, facial features, fingerprints, iris.

## I. INTRODUCTION

Because biometric technologies provide a more dependable and secure means of confirming identity than more conventional techniques like passwords or PINs, they are becoming more and more popular for authentication and security applications. Generally, the procedure entails gathering biometric data using sensors or other equipment, identifying important characteristics from the data, contrasting these characteristics with templates that have been saved in a database, and determining the person's identity based on the comparison findings.

Applications for biometric systems include border control, law enforcement, time and attendance monitoring, security access management, and identity verification for online or financial transactions. They do, however, also bring up issues with data security, privacy, and possible openings to spoofing or hacker assaults. Two primary categories of biometric traits exist:

***Physiological biometrics:*** The measurement and examination of an individual's bodily attributes for identification or authentication is known as physiological biometrics [1]. Fingerprints, iris patterns, facial traits, hand geometry, and DNA are a few examples. Every individual has these distinct physical traits, which don't change much over time. Physiological biometrics are widely employed in several fields, including law enforcement, healthcare, border security, and access control. Physiological biometric features include, for example:

- *Fingerprints:* Each person has a distinct pattern of ridges and valleys on their fingertips. For identification, fingerprint recognition systems record and examine these patterns [2].
- *Facial Features:* To identify people, facial recognition algorithms examine their distinctive facial features, such as the separation between their eyes, the contour of their jawline, and the shape of their nose.
- *Iris Patterns:* Iris recognition systems may identify and authenticate users by capturing and analyzing their very distinctive patterns on the colored portion of the eye, the iris.
- *Hand Geometry:* For identification purposes, measurements and analyses of a person's hand's size, shape, finger lengths and widths, and joint locations can be made.
- *DNA:* Deoxyribonucleic acid, or DNA, is the genetic material that makes up each person's unique genetic makeup. Identification can be accomplished using DNA analysis, especially in forensic investigations.
- *Vein Patterns:* Each person has a distinct pattern of veins beneath the skin, especially in the hands and fingers. This pattern can be photographed and examined for biometric identification.

Physiological biometrics have several benefits, such as great precision, resistance against theft or forgery, and simplicity of use. They do, however, also give rise to worries about data security, privacy, and possible rights abuses. Therefore, to guarantee the moral and responsible use of physiological biometric data, appropriate protections and restrictions are required.

***Behavioral biometrics:*** These are patterns derived from each person's distinct behavior. The measurement and examination of distinctive behavioral patterns for identification or authentication is known as behavioral biometrics [3]. In contrast to physiological biometrics, which concentrate on an individual's bodily attributes, behavioral biometrics emphasize acts or behaviors that may be unique to each person. Voice patterns, typing rhythm, gait analysis, and signature dynamics are a few examples. Applications like fraud detection, continuous authentication, and user profiling frequently employ behavioral biometrics. These behaviors can be recorded and examined with a variety of sensors and equipment, and they are frequently constant. Behavioral biometric features include, for example:

- *Typing Rhythm:* Everybody types on a keyboard differently, with variations in pace, rhythm, and force used on the keys. Analysis of typing rhythms can be applied to user authentication.
- *Voice Patterns:* Voice recognition and authentication can be performed by analyzing a speaker's tone, pitch, cadence, and word pronunciation.

- *Gait Analysis:* Every person has a distinctive gait that can be examined for identification reasons. This gait includes elements like stride length, walking speed, and foot placement angle.
- *Signature Dynamics:* To verify a signature, one can examine the speed, pressure, and stroke order of an individual's signature.
- *Mouse Movement:* For user verification, the movement and clicking patterns made with a computer mouse or trackpad can be examined.
- *Keystroke Dynamics:* For user authentication, the rhythm and timing of keystrokes made while typing on a keyboard can be examined.

Behavioral biometrics have several benefits, such as continuous authentication capabilities, resistance to fraud or impersonation, and the capacity to passively gather data without requiring explicit user input [4]. However since they might entail tracking or recording user behavior, they also give rise to privacy problems. As a result, it's critical to deploy behavioral biometric technologies in an open, accountable manner that includes the necessary safeguards for user permission and data protection.

## II. STAGES INVOLVED IN BIOMETRICS

There are various phases to the study of biometrics, and each is essential to comprehending, applying, and developing the discipline. The standard steps in a biometric study are as follows:

- *Fundamental Research:* To comprehend the underlying principles of biometric features, including their uniqueness, variability, and stability throughout time, theoretical and experimental study must be conducted at this stage. In addition to examining the technological difficulties and constraints involved in gathering, processing, and interpreting biometric data, researchers also look at the physiological and behavioral traits that can be utilized for biometric identification [5].
- *Algorithm Development:* During this phase, scientists create methods and algorithms for gathering, handling, and interpreting biometric information. This covers machine learning models that are specifically designed for biometric modalities like voice, iris, fingerprint, facial, and behavioral biometrics; additionally, it includes signal processing techniques, feature extraction methods, and pattern recognition algorithms [6].
- *System Design and Implementation:* Algorithms must be incorporated into workable biometric systems after they are created. In this phase, biometric systems that can collect biometric information from people, extract pertinent features, compare data to templates that have been recorded, and decide whether to verify or authenticate identity are designed and put into place. Hardware selection, sensor technologies, data storage, encryption, and user interface design are all factors to be taken into account while designing a system.
- *Evaluation and Performance Assessment:* To determine a biometric system's accuracy, dependability, performance, and usability, a thorough evaluation is required. To quantify important metrics including equal error rate (EER), false rejection rate (FRR), false acceptance rate (FAR), and receiver operating characteristic (ROC) curves, this stage comprises doing experiments and benchmarking tests [7]. Controlled laboratory tests, field trials, and standardization initiatives are some of the evaluation approaches used to guarantee uniformity and comparability among various biometric systems.
- *Application and Deployment:* Biometric technologies are used in consumer electronics, healthcare, banking, law enforcement, border security, and access control, among other real-world applications. In this phase, biometric systems are implemented in real-world scenarios, and integrated into the current infrastructure, and practical issues like interoperability, scalability, privacy, security, and regulatory compliance are addressed.
- *Innovation and Constant Improvement:* The subject of biometrics is always changing due to developments in science, technology, and practical applications. In this stage, continuous efforts are made to enhance sensor technology, algorithm development, data fusion methods, multimodal biometrics, adaptive authentication tactics, and overall accuracy, resilience, efficiency, and usability of biometric systems.

During these phases, addressing the technological, moral, legal, and societal ramifications of biometric technologies and guaranteeing their responsible and moral application requires interdisciplinary cooperation between researchers, engineers, practitioners, policymakers, and stakeholders.

## III. STEPS INVOLVED IN BIOMETRIC SYSTEMS

Several steps that are involved in biometric systems are listed below.

- Enrollment: In this step, the individual's biometric data is captured for the first time and stored securely in the system's database. During enrollment, the biometric trait (such as fingerprint, iris scan, or facial features) is captured using a sensor or device, and a template representing the unique characteristics of that trait is created. The template is then securely stored in the system's database along with associated identity information.
- Capture: A sensor or other device is used to record the biometric feature. For instance, a fingerprint scanner records each individual's distinct fingerprint patterns.
- Extraction: The distinct characteristics or templates that can be compared are taken out of the biometric data that has been collected.
- Comparison: The features that were extracted are compared to the templates that were saved in the database. The person's identification is confirmed or validated if there is a match.
- Decision: A determination of the individual's identity is made in light of the comparison findings. If the biometric matches the stored template, the decision could be accepted; if not, it could be rejected.
- Feedback: Finally, feedback is provided to the user regarding the outcome of the authentication process. This could involve displaying a message indicating whether access was granted or denied or providing additional instructions if further action is required.

The flowchart in Fig. 1 illustrates the various biometric operations processes, which are followed by the detailed algorithm.

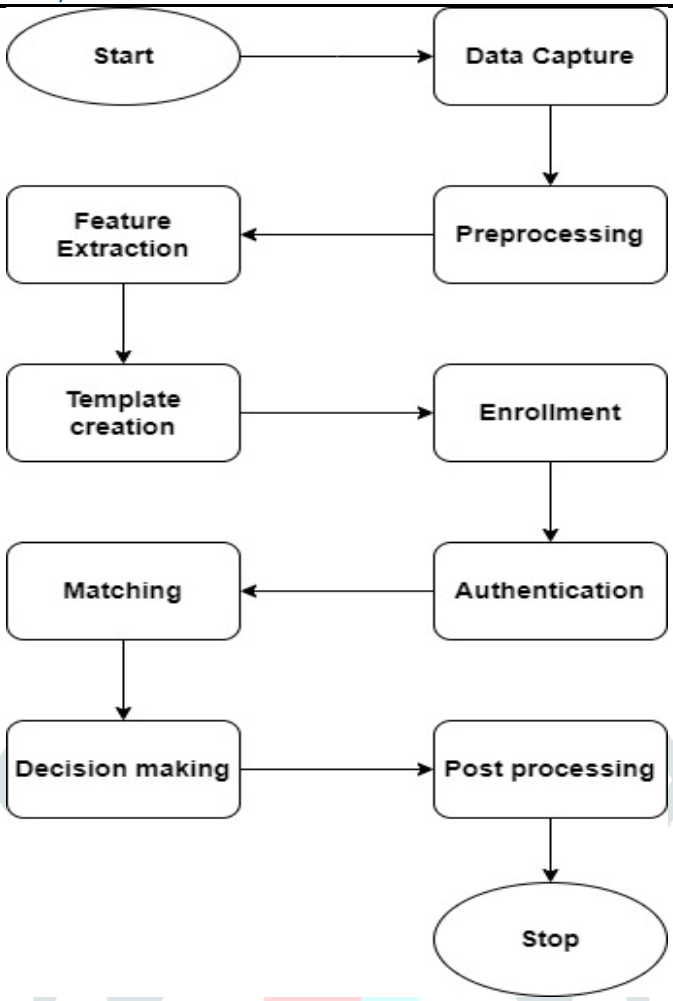


Fig. 1 Steps involved in biometric operations

**Algorithm**

Start

1. Data Capture:
   - Capture biometric data using sensors or devices
   - Choose the appropriate biometric modality (e.g., fingerprint, facial recognition, iris scan)
2. Preprocessing:
   - Cleanse and preprocess raw biometric data
   - Normalize data to ensure consistency and comparability
3. Feature Extraction:
   - Extract distinctive features from biometric data
   - Reduce dimensionality and extract relevant information
4. Template Creation:
   - Create a unique template or representation of biometric features
   - Store the template securely in a database
5. Enrollment:
   - Enroll individuals by capturing their biometric data
   - Extract features and create templates
   - Store templates in a database with associated identity information
6. Authentication:
   - Capture biometric data from a person seeking authentication
   - Extract features and create a template
   - Compare the template with stored templates in the database
7. Matching:
   - Match the extracted template with stored templates
   - Perform comparison using similarity metrics or algorithms
   - Determine the degree of similarity or dissimilarity
8. Decision Making:
   - Based on the comparison result, make a decision:
     - If similarity exceeds a threshold, authenticate the individual
     - If similarity does not exceed the threshold, reject the individual
9. Post-Processing:
   - Update system records/logs
   - Provide feedback to the user (e.g., access granted or denied)

End

## IV. FINGERPRINTS AS BIOMETRIC

One of the most popular types of biometric identification is the fingerprint. The following are some benefits and features of fingerprints as a biometric:

- Originality: The distinctiveness of fingerprints is one of its main benefits. Even identical twins have different ridges, valleys, and minute patterns on their fingertips. Because of their individuality, fingerprints are a highly effective biometric identifier for individual identification [8].
- Stability: Throughout an individual's life, their fingerprint patterns are largely unchanged from those that are generated during fetal development. Even though injuries, surgeries, and some medical conditions can change a fingerprint, fingerprints usually hold over time, making them trustworthy for long-term identification.
- Ease of Capture: Fingerprints are non-invasive and generally simple to capture. Convenient and seamless authentication is made possible by the integration of fingerprint sensors into a wide range of devices, including laptops, tablets, smartphones, and access control systems [9].
- Extremely Accurate: Fingerprint recognition software is capable of identifying people with a high degree of precision. Sophisticated algorithms examine the distinct arrangements of ridges, valleys, and small spots on the fingerprint to generate a template, or mathematical representation, for comparison.
- Quick and Effective: Fingerprint authentication is quick and effective, usually requiring a few seconds for verification. Because of this, fingerprints are perfect for applications that need fast and easy access, such as unlocking cell phones, entering secure spaces, or approving purchases.
- Resistance to Forgery: Fingerprint patterns offer a high degree of security against fraud and identity theft since they are hard to copy or fake. It is difficult and requires advanced techniques to attempt to spoof fingerprint identification systems using counterfeit or replica fingerprints.
- Privacy Protection: Fingerprints are not intrinsically connected to a person's identity, unlike some other biometric modalities like face recognition or iris scanning. An extra degree of privacy protection is offered by the fact that fingerprint templates are kept in a database apart from actual personal data.
- Versatility: A wide range of industries, including banking, healthcare, law enforcement, border and access control, time and attendance tracking, and access control, can use fingerprint biometrics. Fingerprints are widely used in many different businesses and sectors for identity verification due to their adaptability and efficiency [10]. All things considered, fingerprints provide a dependable, accurate, and practical biometric modality for person identification and authentication, improving security and user experience across a wide range of applications.

## V. FACIAL FEATURES AS BIOMETRIC

Facial features are another commonly used biometric identification method. Below is a summary of the benefits and traits of using facial features as a biometric:

- *Universal Nature:* Humans all share the same facial traits, which makes it simple to photograph them without making direct physical contact. Because of their universality, facial recognition technologies can be widely used and adopted by users.

  *Non-Intrusive:* Without requiring direct physical contact with sensors or devices, facial recognition is a non-intrusive biometric method. It is convenient and easy to use since users may authenticate themselves by just looking into a camera.
- *Natural and Intuitive:* Facial recognition is a well-known and natural biometric modality because humans are inherently skilled at identifying and interpreting facial features. For users to operate facial recognition systems efficiently, no specific training is required.
- *Highly Accurate:* Sophisticated facial recognition algorithms are capable of recognizing people with a high degree of accuracy. These algorithms generate a distinct biometric template for comparison by analyzing a variety of facial features, including the size and shape of the eyes, nose, mouth, and jawline [11].
- *Dynamic Authentication:* By continuously monitoring and confirming the user's identification in real-time, facial recognition systems can do dynamic authentication. This makes capabilities like dynamic surveillance systems and facial unlock on cell phones possible.
- *Contactless Authentication:* Applications requiring contactless authentication, like office buildings, stadiums, and airports, are ideally suited for facial recognition technology. By enabling remote authentication, users can minimize in-person contact and lower their chance of spreading infections.
- *Versatility:* There are many uses for facial recognition technology, including identity verification, access management, security and surveillance, attendance monitoring, and customized user interfaces for consumer electronics [12].
- *Integration with Current Infrastructure:* To leverage current infrastructure for authentication, facial recognition systems can be integrated with surveillance cameras, cellphones, tablets, and other devices that have built-in cameras.

Facial recognition brings up issues with privacy, security, and potential biases in algorithmic decision-making even with these benefits. To allay these worries and guarantee the morally and responsibly applied use of facial recognition technology, appropriate safeguards and restrictions are required.

## VI. IRIS AS BIOMETRIC

A very reliable and safe method of biometric identification is through iris patterns. An outline of the benefits and features of using iris patterns as a biometric is provided below:

- *Distinctive and Robust:* Similar to fingerprints, iris patterns are extremely distinctive to each person and don't change over time. Iris recognition is quite reliable for identification because the complex patterns that arise during fatal development are different even in identical twins [13].

- *Extremely precise:* Iris recognition technologies are capable of recognizing people with remarkably high accuracy. A multitude of distinctive characteristics are included in the intricate and exquisite patterns of the iris, making authentication accurate and trustworthy.
- *Resistance to Forgery:* Iris patterns are hard to copy or spoof, which makes iris recognition systems very secure against fraud and identity theft. It is difficult and requires advanced technology to fool iris identification systems using replicas or fake irises.
- *Non-Invasive:* The biometric modality of iris recognition does not necessitate direct physical contact with sensors or devices. Conveniently, users may authenticate themselves by merely glancing into a camera.
- *Speed and Efficiency:* Iris recognition is quick and easy to use; it usually takes a few seconds to authenticate [14]. Applications needing speedy and seamless access, such as border control, airport security, or secure facility access, are well suited for this rapid authentication process.
- *Contactless Authentication:* Iris recognition systems can perform contactless authentication, allowing users to be identified from a distance. This feature is particularly valuable in environments where hygiene and social distancing are important, such as during the COVID-19 pandemic.
- *Versatility:* A wide range of applications, including banking, healthcare, law enforcement, access control, border control, and mobile device identification, can make use of iris recognition. Iris identification is a widely used method for identity verification in a variety of sectors and industries due to its efficacy and versatility [15].
- *Privacy Protection:* Iris recognition does not take or store pictures of people's faces, in contrast to several other biometric modalities like facial recognition. Iris recognition systems, on the other hand, provide another degree of privacy protection by using mathematical representations, or templates, of iris patterns.

Overall, iris recognition contributes to improved security and user experience by providing a highly accurate, safe, and effective biometric modality for person identification and authentication in a variety of applications.

## VII. ADVANTAGES OF BIOMETRIC

Comparing biometric technologies to conventional methods of identification and authentication reveals several benefits. Here are a few main benefits:

- *Enhanced Security:* Since biometric features are specific to each person and hard to copy or steal, they increase security. Because of this, biometric systems are extremely safe against unwanted access. Biometric characteristics are difficult for others to recreate, in contrast to passwords or PINs, which are readily forgotten, exchanged, or stolen.
- *Accuracy:* Extremely accurate identification and verification can be achieved with biometric technology. Reliable authentication is ensured by the uniqueness and stability of biometric features, which lowers the possibility of false positives—the improper acceptance of an unauthorized person—or false negatives—the incorrect rejection of an authorized person [16].
- *Convenience:* Biometric verification is easy to use and convenient. Passwords and tangible tokens like ID cards or keys are not necessary for users to remember. Rather, individuals can gain access to protected locations, gadgets, or services by merely using their biometric characteristics, including fingerprints or facial features [17].
- *Identity Theft Prevention:* By making sure that only people with permission may access sensitive data or carry out certain tasks, biometric systems aid in the prevention of identity theft and fraud. Biometric characteristics offer a trustworthy means of confirming an individual's identity because they are difficult to copy or mimic [18].
- *Time and Money Savings:* Biometric solutions can reduce the time and money spent on manual identity verification procedures like ID checks and password entry. Organizations may increase productivity and streamline operations with the help of automated biometric authentication methods, which are quicker and more effective.
- *Audit Trails and Accountability:* By logging biometric authentication events, biometric systems can offer thorough audit trails and accountability. Tracking who accessed what, when, and where, aids companies in improving security and adhering to legal obligations [19, 20].
- *Accessibility:* For people with impairments or disabilities, biometric technologies can increase accessibility. For instance, compared to conventional verification techniques, fingerprint or iris recognition may be simpler for people with vision or movement problems.
- *Scalability:* A large number of users or devices can be simply added to biometric systems through scalability. Biometric technology may be effectively scaled to fulfill different needs, whether they are used in large-scale deployments such as national ID systems or small-scale applications like cell phones [21, 22].

In general, biometric systems provide increased security, simplicity, and dependability by offering a strong and adaptable solution for identity verification and identification across a broad range of applications.

## VIII. CONCLUSION

To sum up, this research study has examined the diverse topic of biometrics, emphasizing its uses, difficulties, and potential future possibilities. The research have demonstrated the important role that biometrics plays in identity verification, authentication, and security across a variety of sectors through an examination of various biometric modalities, including physiological and behavioral traits like fingerprints, facial features, and iris patterns.

The benefits of biometric systems, such as their superior accuracy, dependability, and ease of use in comparison to conventional authentication techniques, have been highlighted by our analysis. In a variety of industries, including banking, healthcare, consumer electronics, law enforcement, and border security, biometrics provides a potent answer for security issues and expedites access control procedures.

Future developments in biometrics seem promising in terms of ongoing innovation and progress. Emerging technologies that have the potential to improve security, and user experience, and solve current limitations include biometric fusion approaches, continuous authentication, and multimodal biometrics. Furthermore, current research initiatives in fields like biometric

encryption, deep learning, and artificial intelligence have the potential to significantly improve the reliability and efficacy of biometric systems.

In conclusion, by shedding light on the field's applications, difficulties, and potential prospects, this study adds to the expanding corpus of knowledge in biometrics. We can create a more safe, effective, and inclusive digital society by tackling the opportunities and challenges presented by biometric technologies.

**REFERENCES**


[1]. Angulo, J., and Wastlund, E. Exploring Touch-Screen ¨ Biometrics for User Identification on Smart Phones. Privacy and Identity Management for Life 375 (2012), 130–143.

[2]. Aviv, A., Gibson, K., Mossop, E., Blaze, M., and Smith, J. Smudge Attacks on Smartphone Touch Screens. In WOOT (2010), 1–7.

[3]. Azenkot, S., and Zhai, S. Touch Behavior with Different Postures on Soft Smartphone Keyboards. In MobileHCI 2012 (2012), 251–260.

[4]. Baldwin, T., and Chai, J. Towards Online Adaptation and Personalization of Key-Target Resizing for Mobile Devices. In IUI 2012 (2012), 11–20.

[5]. Banerjee, S., and Woodard, D. Biometric Authentication and Identification using Keystroke Dynamics: A Survey. Journal of Pattern Recognition Research 7 (2012), 116–139.

[6]. Baudisch, P., and Chu, G. Back-of-Device Interaction Allows Creating Very Small Touch Devices. In CHI 2009 (2009), 1923–1932.

[7]. Beton, M., Marie, V., and Rosenberger, C. Biometric Secret Path for Mobile User Authentication: A Preliminary Study. In WCCIT 2013, Ieee (June 2013), 1–6.

[8]. Bohmer, M., Hecht, B., Sch ¨ oning, J., Kr ¨ uger, A., and ¨ Bauer, G. Falling Asleep with Angry Birds, Facebook and Kindle - A Large Scale Study on Mobile Application Usage. MobileHCI 2011 (2011), 47–56.

[9]. Bours, P., and Barghouthi, H. Continuous Authentication Using Biometric Keystroke Dynamics. In NISK (2009), 1–12.

[10]. Buchoux, A., and Clarke, N. L. Deployment of Keystroke Analysis on a Smartphone. In Australian Information Security Management Conference (2008).

[11]. Burgbacher, U., and Hinrichs, K. An Implicit Author Verification System for Text Messages Based on Gesture Typing Biometrics. In CHI 2014 (2014), 2951–2954.

[12]. Buschek, D., Rogers, S., and Murray-Smith, R. User-Specific Touch Models in a Cross-Device Context. In MobileHCI 2013 (2013), 382–391.

[13]. Buschek, D., Schoenleben, O., and Oulasvirta, A. Improving Accuracy in Back-of-Device Multitouch Typing: A Clustering-based Approach to Keyboard Updating. In IUI 2014 (2014), 57–66.

[14]. Campisi, P., Maiorana, E., Lo Bosco, M., and Neri, A. User authentication using keystroke dynamics for cellular phones. IET Signal Processing 3, 4 (2009), 333–341.

[15]. Clarke, N. L., and Furnell, S. M. Authenticating mobile phone users using keystroke analysis. International Journal of Information Security 6, 1 (Aug. 2006), 1–14.

[16]. Crawford, H. Keystroke Dynamics: Characteristics and Opportunities. In 8th International Conference on Privacy, Security and Trust (2010), 205–212.

[17]. Jagdev, G., Singh, S., Singh, T., & Joshi, D. S. (2015). *Constraints of 2D Face Recognition Crafts Way for 3D Face Recognition Technique*. *1*(3), 41–46.

[18]. Bansal, S., & Jagdev, G. (2017). Analyzing Working of DES and AES Algorithms in Cloud Security. *International Journal of Research Studies in Computer Science and Engineering*, *4*(3), 1–9. https://doi.org/10.20431/2349-4859.0403001

[19]. Bansal, S., & Jagdev, G. (2018a). Comparative Analysis and Implementation of Cryptographic Algorithms in Cloud Computing. *International Journal of Research Studies in Computer Science and Engineering*, *5*(1), 17–25. https://doi.org/10.20431/2349-4859.0501003

[20]. Jagdev, G., & Kumar, A. (2016). International Journal of Scientific and Technical Advancements Analyzing 2D & 3D Fingerprint Recognition Techniques as Secure Biometric. *International Journal of Scientific and Technical Advancements*, *2*(4), 119–124.

[21]. Jagdev, G., & Singh, T. (n.d.). *ANALYZING AND IMPLEMENTATION OF SPEECH RECOGNITION AS ADVANCED BIOMETRIC*. 229–235.

[22]. Kaur, P., & Jagdev, G. (2017). Reconnoitering and Instigating Fingerprints as Secure Biometric Technique. *International Journal of Research Studies in Computer Science and Engineering*, *4*(4), 81–89. https://doi.org/10.20431/2349-4859.0404010


**ABOUT THE AUTHOR**

Mr. Malvinder Singh completed his Master of Computer Application from Maharishi Dayanand University, Rohtak in 2009. He is currently working in the capacity of an Assistant Professor in the Department of Computer Science, at Miri Piri Khalsa College, Bhadaur since 2009. He has published more than 4 research papers at National and International Conferences. His areas of interest are Network Security and Cloud Security.