# A BioCapsule Based Authentication System with Secured Intrusive user Authentication

Swathy. G. S
Student, CSE
Toc H Institute of Science and Technology
Arakkunnam, Kerala, India, pin: 682313

Rasmi. P. S
Associate Professor, IT
Toc H Institute of Science and Technology
Arakkunnam, Kerala, India, pin: 682313

***Abstract:*** **A large portion of system breaches are caused by authentication failure. These failures are themselves related to the limitations associated with existing authentication methods. The current proxy based or biometrics based authentication, are not user-centric or endanger users security and privacy. A central theme of authentication is to authenticate users using characteristics intrinsically linked with human users rather than some external factors. A central theme of authentication is to authenticate users using characteristics intrinsically linked with human users rather than some external factors. But current authentication methods, whether proxy based or biometrics based, are not user-centric and/or endanger users' security and privacy. A promising direction emerging from this effort is biometrics. This work proposes a biometrics based user-centric authentication approach. The proposed method securely fuses the extracted user biometrics feature with the user data forming a BioCapsule(BC) and enabling these BCs for authentication. This BC is then encrypted using AES algorithm to provide high security to the data. The user data used in this approach consist of user name, date of birth, address and account number which combines together forming a Reference Byte (RB). Such an approach is user friendly, secure, identity bearing yet privacy-preserving, resilient, and revocable once a BC is compromised. The proposed model can be applied for biometric ATMs which replaces card system by biometric technology for operating ATMs. During authentication, the user is required to provide another sample of the users biometric characteristics. This is matched with the one in the database, and if the two samples are the same, then the user is considered to be a valid user. Proposed model provides high security in authentication which also protects service user from unauthorized access for authentication. Such an approach is secure, privacy-preserving, user friendly, and revocable. By fusing the users biometrics with a distinct user details makes the reference subject different among different users.**

***Keywords: Biometric Authentication, Biometric Cryptosystems,Kernel Principal Component Analysis.***

## I.INTRODUCTION

Identification and authentication are two terms that describe the initial phases of the process of allowing access to a system. The terms are often used, but authentication is typically a more involved process than identification. Identification is the process of possessing an identity to a system. Identification is done in the initial stages of gaining access to the system and is what happens when you claim to be a particular system user. The claim is verified by providing your username during the login process; placing your finger on a scanner; giving your name on a guest list or any other format in which you claim an identity with the aim of gaining access. Authentication is the process of validating an identity provided to a system. This includes checking the validity of the identity prior to the authorization phase. The primary difference between them is that identification relates to the provision of an identity, while authentication relates to the checks made to ensure the validity of the claimed identity. Authentication is considered one of the great ideas in computer security. Authentication is a process which a user gains the right to identify himself. Techniques to authenticate a user can be passwords, biometrics, smart cards, certificates, etc. If a user has rights to identify himself in several different organizations or systems, it may cause problems. Immigration cards holding both passport number and measures of the user's hand; fingerprints taken as a legal requirement for a driver license, that is not stored anywhere on the license ; automatic facial recognition systems searching for known card cheats in a casino; season tickets to an amusement park linked to the shape of the purchaser's fingers; home incarceration programs supervised by automatic voice recognition systems; and confidential delivery of health care through iris recognition: these systems seem completely different in terms of technologies and usage, but each uses biometric authentication in some way. Biometric technologies are automated methods of verifying or recognizing the identity of a living person based on a physiological or behavioral characteristic. There are two key words in this definition: "automated" and "person". The word "automated" differentiates biometrics from the larger field of human identification. Biometric authentication techniques are done completely by machine. Forensic laboratory techniques, such as latent fingerprint, hair and fiber analysis, are not included in this type of biometric authentication. The second key word is "person". Particularly statistical techniques using fingerprint patterns have been used to differentiate or to probabilistically link persons to groups, but biometrics is interested only in recognizing people as individuals. All of the measures used contain both physiological and behavioral characteristics, both of which can differ or can posses similarity across a population of individuals. So biometrics uses computers to recognize people, by avoiding individual similarities and within individual variations. Determining true identity is beyond the scope of any biometric technology. Biometric

technology can only link an individual to a biometric pattern and any identity data (common name) and personal attributes (age, gender, profession, residence, nationality) presented at the time of enrolment in the system. Biometric systems inherently require no personal data, thus allowing anonymous recognition. Ultimately, the performance of a biometric authentication system, depends upon the interaction of individuals with the automated mechanism. This interaction of technology with human characteristics features that makes “biometrics” such a fascinating subject.

## II.RELATED WORKS

Emerging techniques for user authentication involve traditional biometric authentication, cognitive authentication, BCS, CB and the hybrid approach. Traditional biometrics binds users to their biological traits, either physiological traits (e.g., iris, palm print, sclera ) or behavior traits (e.g., mouse dynamics , gait ). As indicated previously, a limitation of traditional biometrics is security, user privacy risk and irreplaceability.

### *A.Biometric Technology*

Biometric technology is used for automatic personal recognition based on biological traits fingerprint, iris, face, palm print, hand geometry, vascular pattern, voice or behavioral characteristics gait, signature, typing pattern. Fingerprinting is the oldest of these methods and has been utilized for over a century by law enforcement officials who use these distinctive characteristics to keep track of criminals. A typical biometric system is comprised of five integrated components: A sensor is used to collect the data and convert the information to a digital format. Signal processing algorithms are used to perform quality control activities and develop the biometric template. A data storage component stores information that new biometric templates will be compared to. A matching algorithm compares the new biometric template to one or more templates kept in data storage. Finally, a decision process uses the results from the matching component to make a level decision. Biometric Encryption [3] is a group of emerging technologies that securely bind a digital key to a biometric or generate a digital key from the biometric, and a biometrically encrypted key or helper data is stored. With BE the digital key is recreated only if the accurate biometric sample is presented on verification. The outcome of BE verification is either a digital key or a failure message. BE technologies exemplify the fundamental privacy and data protection principles that are endorsed around the world. Although introducing biometrics into information systems may result in considerable benefits, it also introduces many new security and privacy issues, risks, and challenges.

### *B.Biometric Authentication*

Personal identity refers to a set of attributes (e.g., name, social security number, etc.) that are associated with a person. Identity management is the process of creating, maintaining and destroying identities of individuals in a population. One of the critical tasks in identity management is person authentication, where the goal is to either determine the previously established identity of an individual or verify an individual's identity claim. Identity theft and the loss or disclosure of data and related intellectual property are growing problems in this computer driven era. We all will be having multiple accounts and use multiple passwords on an ever-increasing number of computers and Web sites. Maintaining and managing access while protecting both the user's identity and the computer's data and systems has become increasingly difficult. Central to all security is the concept of authentication verifying that the user is who he claims to be. Biometrics based authentication offers several advantages over other authentication methods. It is important that such biometrics-based authentication systems be designed to withstand attacks when employed in security critical applications, especially in unattended remote applications such as e-commerce.

Although, for illustration purposes, fingerprints authentication is used throughout [8] analysis extends to other biometrics-based methods. Biometrics based authentication has many usability advantages over traditional systems such as passwords. Specifically, users can never lose their biometrics, and the biometric signal is difficult to steal or forge. It is shown that the intrinsic bit strength of a biometric signal can be quite good, especially for fingerprints, when compared to conventional passwords. Any system, including a biometric system, is vulnerable when attacked by determined hackers. A challenge/response method has been proposed to check the liveliness of the signal acquired from an intelligent sensor. The greatest strength of biometrics is the fact that the biometrics does not change over time, is at the same time its greatest liability. Once a set of biometric data has been compromised, it is compromised forever. Human authentication is the security task whose job is to limit access to physical locations or computer network only to those with authorisation. This is done by [2] using equipped authorized users with passwords, tokens or using their biometrics. Unfortunately, the first two suffer a lack of security as they are easy being forgotten and stolen; even biometrics also suffers from some inherent limitation and specific security threats. A more practical approach is to combine two or more factor authenticator to reap benefits in security or convenient or both. A novel two factor authenticator based on iterate dinner products between tokenized pseudo-random number and the user specific fingerprint feature, which generated from the integrated wave let and Fourier–Mellin transform, and hence produce a set of user specific compact code that coined as Bio Hashing. Bio Hashing highly tolerant of data capture offsets, with same user fingerprint data resulting in highly correlated bit strings.

### *C.Biometric Systems*

A biometric system provides automatic identification of an individual based on a unique feature or characteristic possessed by the individual. Iris recognition is regarded as the most reliable and accurate biometric identification system available. Most commercial iris recognition systems use patented algorithms, and these algorithms are able to

produce perfect recognition rates. The work [7] presented involved developing an open-source iris recognition system inorder to verify both the uniqueness of the human iris and also its performance as a biometric. For determining the recognition performance of the system two databases of digitised greyscale eye images were used. The iris recognition system consists of an automatic segmentation system that is based on the Hough transform, and is able to localise the circular iris and pupil region, occluding eye lids and eyelashes, and reflections. The extracted iris region was then normalised into a rectangular block with constant dimensions to account for imaging inconsistencies. This thesis has presented an iris recognition system, which was tested using two databases of grayscale eye images inorder to verify the claimed performance of iris recognition technology. Multibiometric systems combine the information presented by multiple biometric sensors, algorithms, samples, units, or traits. Besides enhancing matching performance, these systems are expected to improve population coverage, deter spoofing and impart fault tolerance to biometric applications. This introductory paper enumerates the various sources of biometric information that can be consolidated as well as the different levels of fusion in a biometric system. The role of using ancillary information such as biometric data quality and soft biometric traits (e.g., height) to enhance the performance of these systems is also included. Multibiometric systems are expected to enhance the recognition accuracy of a personal authentication system by reconciling the evidence presented by multiple sources of information. In [3] the different sources of biometric information as well as the type of information that can be consolidated was presented. Typically, early integration strategies (e.g., feature-level) are expected to result in better performance than late integration (e.g., score-level) strategies. However, it is difficult to predict the performance gain due to each of these strategies prior to invoking the fusion methodology. In paper [6] summarizes noncontact biometrics such as face and iris have additional benefits over contact based biometrics such as fingerprint and hand geometry. However, three important challenges need to be addressed in a noncontact biometrics based authentication system: ability to handle unconstrained acquisition, robust and accurate matching and privacy enhancement without compromising security. In this paper, a unified framework based on random projections and sparse representations that can simultaneously address all the three issues mentioned above in relation to iris biometrics was proposed.

*D. Biometric Cryptosystem*

Biometric cryptosystems can be used for user authentication by matching the exactness of the outputted keys. The majority of BCSs require some biometric dependent public information (known as helper data), which is not supposed to reveal much information about the biometrics; with the helper data, the cryptographic key is retrieved or extracted from the query biometrics. The helper data are either obtained by binding a chosen key to biometrics or derived only from biometrics. BCSs use different techniques to deal with biometric variance; for example, some schemes apply error correction codes, while some others apply quantization. The introduction of helper data, in some circumstances (e.g., when multiple copy of helper data extracted from the single biometrics are obtained) may create vulnerabilities. The work [14] provided formal definitions and efficient secure techniques for turning biometric information into keys usable for any cryptographic application, and reliably and securely authenticating biometric data. The authors proposed two primitives: a fuzzy extractor extracts nearly uniform randomness R from its biometric input; the extraction is error tolerant in the sense that R will be the same even if the input changes, as long as it remains reasonably close to the original. Thus, R can be used as a key in any cryptographic application. The first practical and secure way to integrate the iris biometric into cryptographic applications is proposed by [5]. A repeatable binary string, which is a biometric key, is generated reliably from genuine iris codes. A well-known difficulty has been how to cope with the 10 to 20 percent of error bits within an iris code and derive an error-free key. A form of robust for biometrics and presents experiments showing that when applied per class they can dramatically improve the accuracy of face recognition. Unlike passwords, biometric signatures cannot be changed or revoked. The paper [12] shows how the robust distance measures introduce can be use for secure robust revocable biometrics. The technique produces what we call Biotopes which provide public key cryptographic security, supports matching in encoded form, cannot be linked across different databases and are revocable. A minutiae-based template is a very compact representation of a fingerprint image, and for a long time, it has been assumed that it did not contain enough information to allow there construction of the original fingerprint. The paper [11] proposes a novel approach or construct fingerprint images from standard templates and investigates to what extent there constructed images are similar to the original ones. In order to increase security in common key management systems, the majority of so called Biometric Cryptosystems aim at coupling cryptographic systems with biometric recognition systems. As a result these systems produce cryptographic keys, dependent on biometric information, denoted Biometric Keys. In a generic approach [4] to producing cryptographic keys out of biometric data is presented, by applying so called Interval Mapping techniques.

## III.PROBLEM STATEMENT

Inorder to prevent the users from identity fabrication and other security and privacy attacks more advanced biometric system has to be developed. The Biometric systems are compromised due to lack of security. Due to this security lack the privacy of user is revealed and thus causes identity fabrication. Also the time taken for other biometric authentication is more.

*A.Design Objectives*

Biometrics has been widely used and adopted as a promising authentication method due to its advantages over some existing methods, particularly, its resistance to losses incurred by theft of passwords and smart cards. The proposed mechanism is based on iris biometrics and form a concrete construction of iris based authentication. The proposed approach aims at user's privacy, security and prevent from identity theft.Inorder to prevent the users from identity fabrication and other security and privacy attacks more advanced biometric system has to be developed. The Biometric systems are compromised due to lack of security. Due to this security lack the privacy of user is revealed and thus causes identity fabrication. Thus the main objective of the proposed work is to design a iris biometric system which reduces the time for authentication with high user-friendliness, security, privacy preserving and revocable authentication model. System security refers to the required effort to be accepted by a biometric system as a certain individual without having access to the biometrics of this individual, which is also known as the brute force attack. Biometric privacy refers to the required effort to obtain the biometric information of an individual. One critical property of biometric systems is diversity and cross-matching resistance. It is likely that the user utilizes the same biometrics across systems, thus it should be possible to build different versions of biometric credentials based on the same biometrics. The revocability is closely related to the diversity and cross-matching resistance of the system; based on the same biometrics a new credential can be generated, and the compromised biometric credential cannot be matched against the new one. Usability is the ease of use. Here usability refers to the necessity to require external factors (e.g., password, token) from users for authentication.

## IV.PROPOSED SYSTEM

A unique BioCapsule (BC) generation method based on secure fusion of the user biometrics and the user data is proposed. The biometric used here is iris. The iris of the eye has been described as the ideal part of the human body for biometric identification for several reasons: It is an internal organ that is well protected against damage and wear by a highly transparent and sensitive membrane. This distinguishes it from fingerprints, which can be difficult to recognize after years of certain types of manual labour. The fusion based BC construction is more usable and flexible, while also secure, resilient to different attacks, and tolerant to the disclosure of both the RB and BC. In the registration part the iris captured, preprocessed and extracted. After pre-processing, the key features of iris are extracted using Kernel Principal Component Analysis (KPCA). Then the extracted feature is then combined with the user Reference Byte (RB) forming a BioCapsule. This BC will be encrypted using AES algorithm and it will be stored in the database for further verification process.

This proposed model can be applied in the field of ATM authentication. The current ATM authentication technologies like a credit card are small, lightweight and can be easily lost if the person is irresponsible. Also anyone else other than the user knew about the PIN number and he/she holds the credit card, they could easily fool the original user by withdrawing the money from the user's account. Thus the current ATM authentication has lots of flaws. So by adopting the BioCapsule based authentication in the field of ATM authentication yields more security and privacy to the users. In practical application during the registration phase, the user's biometrics is captured via camera of the authentication client, extracted, encrypted and stored in Bank database. The captured iris image undergoes Kernel Principal Component Analysis (KPCA) to extract the iris features. The extracted feature is then combined with the reference byte (RB) forming a BioCapsule(BC). This BC is then encrypted using AES algorithm for providing high security to the BC.

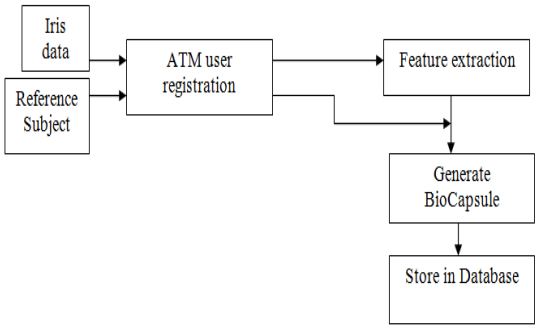


Fig.1 User Registration

For getting fast experimental results the iris dataset is chosen as input to this work. The dataset is taken from various iris data collection websites. This collected set of iris images are then given as the user biometric input to the system. The dataset are converted to the database engine and the attributes are stored. The datasets were tested on the ICE database which is provided by National Institute of Standards and Technology (NIST) for the Iris Challenge Evaluation (ICE) 2005. The ICE database contains 1,426 images from the right eye from 132 subjects, and 1,527 images from the left eye from 132 subjects. These images were collected with the LG EOU 2200 and intentionally represent a broader range of quality than the camera would normally acquire. Hence the need of an Identity provider is further reduced. Also, this key is directly generated from user biometrics and is user intrinsic, making its compromise significantly more difficult when compared to factors artificially bound to a user. All these data are bundled to build a BioCapsule object. Every user, after registering to the banking system will get a BioCapsule model and that is stored on the database. This may be reference on other transactions sections of the banking application.

The key extraction is applied on the preprocessed images. The algorithm used for key extraction is Kernel Principal Component Analysis (KPCA). Kernel principal component analysis (kernel PCA) is an extension of principal component analysis (PCA) using techniques of kernel methods. Using a kernel, the originally linear operations of PCA are done in a

reproducing kernel Hilbert space with a non-linear mapping. KPCA is an extension of Principal Component Analysis (PCA) to non-linear distributions.

The goal of fusion aims to increase the security of the biometrics. Through the fusion, the RB hides the user data, thus providing security and preserving privacy. This fusion equally treats the user biometrics and RB. The security also consolidates the contribution of designing equal treatment of the user biometrics and the RB. One user iris image and user details are used to illustrate the fusion process. The proposed fusion mechanism is a general procedure, which can be integrated with existing biometric processes to generate Biometric Cryptosystems. And to show how the fusion fits into the biometric system. After the generation of the BC , it is encrpyted using AES algorithm and it will be stored in the bank database for further verification.

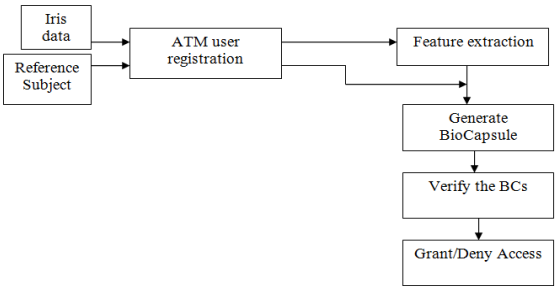


Fig.2 User Authentication

During the verification part the BC's are compared. The BioCapsule formed during the registration part is compared with the Biocapsule formed during the verification part. The iris extraction techniques used during the registration phase is also used in the verification process. The Kernel Principal component analysis and AES decryption is used here inorder to gain the same features of iris, that was obtained during the registration part. The biometrics dataset should also be fed to the system as part of verification. In practical implementation the iris of every customer is to be captured during both registration and verification phases. The images of the iris will undergo a KPCA algorithm and features will be extracted, which can be used to fuse with Reference Byte to form BioCapsule. This BC will be compared with the BC that is stored in the bank database, by AES decryption on the BC generated during the registration part. The authentication request is given by the user during the time of cash withdrawal. If the user wants to get the money, then the user has to cross the proposed authentication criterias. The admin then checks it with the BioCapsule already stored in Bank database . If there is no difference with the BioCapsule already stored and that formed during request, then the user will be given the access permission. If the BioCapsule formed during this phase is different then the user access will be denied.

## V.CONCLUSION

In this proposed work a user-friendly, secure, privacy-preserving and revocable secure-fusion based biometric authentication method is designed. The proposed approach involves key extraction: the extracted feature is used in a "secure fusion" for mixing the user's biometrics and user details, and the fused biometrics is encrypted to generate a BioCapsule for authentication. The proposed BC mechanism has many desired features: The approach is secure and able to defeat various attacks, thus the security of the user biometrics is guaranteed and the user privacy is preserved. Comparisons with existing approaches show comparable performance to traditional approaches and other Biometric Cryptosystem and Canceleble biometric systems. The system does not require user training, and is both easy to use and transparent to end-users since they are not required to remember a password or carry a token. These features make the proposed BC mechanism a user-centric authentication approach.

## REFERENCES

[1] Yan Sui and Eliza Y Du, *"Design and Analysis of Highly User Friendly, Secure, Privacy-Preserving and Revocable Authentication Method"*, IEEE Transaction on Computers, vol. 63, NO.4, April 2014.

[2] A. Jin, D Ling, and A. Goh, *"Biohashing: Two Factor Authentication Featuring Fingerprint Data and Tokenized Random Number"*, Elsevier Pattern Recognition, vol. 37, pp. 2245-2255, 2004.

[3] A. Ross, K. Nandakumar, and A. Jain, *"Introduction to Multi-biometrics"*, Handbook of Biometrics, pp. 271-292, Springer, 2008.

[4] Cavoukian and A. Stoianov, *"Biometric Encryption"*, Encyclopedia of Biometrics. Springer, 2009.

[5] C. Rathgeb and A. Uhl, *"An Iris-Based Interval-Mapping Scheme for Biometric Key Generation"*, Proc. Sixth Intl Symp. Image and Signal Processing and Analysis, pp. 511-516, Sept. 2009.

[6] F. Hao, R. Anderson, and J. Daugman, *"Combining Crypto with Biomet-rics Effectively"*, IEEE Trans. Computers, vol. 55, no. 9, pp. 1081-1088, Sept. 2006.

[7] J. Pillai, V. Patel, R. Chellappa, and N. Ratha, *"Secure and Robust Iris Recognition Using Random Projections and Sparse Representations"*, IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 33, no. 9, pp. 1877-1893, Sept. 2011.

[8] L. Masek, *"Recognition of Human Iris Patterns for Biometric Identification"*, technical report, Univ. of Western Australia, 2003.

[9] N. Ratha, J. Connell, and R. Bolle, *"Enhancing Security and Privacy in Biometrics-Based Authentication Systems"*, IBM Systems J., vol. 40, pp. 614-634, 2001.

[10] O. Ouda, N. Tsumura, and T. Nakaguchi, *"BioEncoding: A Reliable Tokenless Cancelable Biometrics Scheme for Protecting Iriscodes"*, IEICE Trans. Information and Systems, vol. E93-D, no. 7, pp. 1878-1888, July 2010.

[11] O. Ouda, N. Tsumura, and T. Nakaguchi, *"Tokenless Cancelable Bio-metrics Scheme for Protecting Iris Codes"*, Proc. 20th Intl Conf. Pattern Recognition (ICPR), pp. 882-885, Aug. 2010.

[12] R. Cappelli, A. Lumini, D. Maio, and D. Maltoni, *"Fingerprint Image Reconstruction from Standard Templates"*, IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 29, no. 9, pp. 1489-1503, Sept. 2007.

[13] T. Boult, *"Robust Distance Measures for Face-Recognition Supporting Revocable Biometric Tokens"*, Proc. Seventh Intl Conf. Automatic Face and Gesture Recognition, pp. 560-566, Apr. 2006.

[14] U. Uludag, S. Pankanti, S. Prabhakar, and A. Jain, *"Biometric Cryptosys-tems: Issues and Challenges"*, Proc. IEEE, vol. 92, no. 6, pp. 948-960, June 2004.

[15] Y. Dodis, L. Reyzin, and A. Smith, *"Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data"*,Proc. Advances in Cryptology (Eurocrypt), vol. 3027, pp. 523-540, 2004.

[16] Y. Sui, X. Zou, and E. Du, *"Biometrics-Based Authentication: A New Approach"*, Proc. 20th Intl Conf. Computer Comm. and Networks (ICCCN), pp. 1-6, Aug. 2011.