# A Survey on Biometric Identification Scheme in Cloud Computing and Blockchain Technology

[1]Jyothsna Sarah, [2]Aashreya Reddy, [3]Latha NR
[1]Computer Science & Engineering,
[1]BMS College of Engineering, Bangalore, India

***Abstract:*** With the birth of electronic banking, e-commerce, and smartcards and an increased emphasis on the privacy and security of information stored in various databases, automatic personal identification has become a very important topic. The traditional methods of identification [password or personal identification number (PIN)] and token-based (passport, driver license, and ID card) which are knowledge-based are prone to fraud because PIN's may be forgotten or guessed by a hacker and the could be replicated, lost or stolen. Therefore, the need for biometrics showed up. Biometrics tend to be more convenient than other methods of identity authentication. This is because of the uniqueness and permanence of it.

***IndexTerms* - biometric, blockchain, identification, cloud computing**

## I. INTRODUCTION

Accurate personal identification is now needed in a wide range of civilian applications involving the use of passports, cellular telephones, automatic teller machines, and driver licenses. The traditional methods of identification password or personal identification number and token-based (passport, driver license, and ID card) which are knowledge-based are prone to fraud because PIN's may be forgotten or guessed by a hacker and the could be replicated, lost or stolen. Therefore, the need for biometrics showed up. Biometrics is a more resourceful method than other methods of identity authentication. This is because of the uniqueness and permanence of it. You might forget your ID at home when you head out the door, but you'll still be able to use biometric devices. Imagine verifying your identity while at the store by swiping your finger across a sensor.

Traditionally, in cybersecurity anyone wanting to store, share or process information must own it. Creating, borrowing or buying that information, obtaining permission to use it (if necessary) and then making sure everyone is aware of any changes. The earlier methods in verifying & identifying was to gain permission from a user and then subjugate it to different methods of security. All of this would be centralized. Blockchain technology has been around for just under a decade, initially introduced to store and/or send the first cryptocurrency, Bitcoin. However, as the technology has gradually spread worldwide, people have begun using it in a variety of ways in numerous industries, including to increase cybersecurity.

Biometric technology works by capturing anatomical or behavioral patterns found in human beings. Everyone's biometric patterns are different and biometric technology can find this minute difference in these patterns using technological, mathematical and statistical means. Biometric recognition technology has proved its superiority over traditional and other recognition methods; however, permanence of human biometric patterns becomes the strength as well as the weakness of this technology. Your fingerprints or iris patterns are unique as well as permanent, it is a good thing when your biometric data is secure, and a very bad thing when it is not.

The survey done in this paper is to integrate biometric identification storage in cloud computing and secure it with block chain technology.

## II. BIOMETRIC IDENTIFCATION SCHEME

The previous works of privacy preserving biometric identification scheme in cloud computing by Anil K Jain [6] shows a traditional approach to biometrics which only include the fingerprints of the individual. Fingerprint verification & identification is one of the first biometric approaches that came into existence. These finger print schemes are either based on predominantly local landmarks (e.g., minutiae-based fingerprint matching systems) or exclusively global information (fingerprint classification based on the Henry system). The minutiae-based automatic identification techniques first locate the minutiae points and then match their relative placement in each finger and the stored template.

Joaquim de Mira Jr., Hugo Vieira Neto, Eduardo B. Neves, F´abio K. Schneider introduced a [2] new method for biometric identification of human irises is proposed in this paper. The method is based on morphological image processing and identified the unique skeletons of iris structures, which are then used for feature extraction. In this approach, local iris features are represented by the most stable nodes, branches and endpoints extracted from the identified skeletons.

### 2.1 Fingerprint Identification

[1] Arun Rossa and Rohin Govindarajan, Multibiometric systems utilize the evidence presented by multiple biometric sources (e.g., face and fingerprint, multiple fingers of a user, multiple matchers, etc.) to determine or verify the identity of an individual. Information from multiple sources can be combined in several distinct levels, including the feature extraction level, match score level and decision level. While fusion at the match score and decision levels have been studied in the literature, fusion at the feature level is a relatively understudied problem. In this paper the fusion at the feature levels is discussed in 3 different scenarios: (i) fusion

of PCA and LDA coefficients of face; (ii) fusion of LDA coefficients corresponding to the R,G,B channels of a face image; (iii) fusion of face and hand modalities.

[5] Anil K. Jain, Fellow, Salil Prabhakar, Lin Hong, and Sharath Pankanti, with identity fraud in our society reaching new proportions with an increasing stress on the rising automatic personal identification applications, biometrics-based verification, particularly fingerprint-based identification, is receiving plenty of attention. There are two major shortcomings of the normal approaches to fingerprint illustration. For a substantial fraction of population, the representations supported specific detection of complete ridge structures within the fingerprint are tough to extract automatically. The wide used minutiae-based representation doesn't utilize a big component of the rich discriminatory data obtainable in the fingerprints. Local ridge structures cannot be completely characterized by minutiae. Further, minutiae-based matching has issue in quickly matching two fingerprint images containing totally different variety of unregistered minutiae points. The planned filter-based algorithm uses a bank of Gabor filters to capture each native and global details in an exceedingly fingerprint as a compact fixed length FingerCode. The fingerprint matching is predicated on the Euclidean distance between the two corresponding FingerCodes and thus is extraordinarily quick. This was achieved by a verification accuracy which is only marginally inferior to the best results of minutiae-based algorithms published in the open literature.

### 2.2 Iris Identification

[2] Joaquim de Mira Jr., Hugo Vieira Neto, Eduardo B. Neves, F´abio K. Schneider, introduced a new method for biometric identification of human irises is proposed in this paper. The method is based on morphological image processing for the identification of unique skeletons of iris structures, which are then used for feature extraction. In this approach, local iris features are represented by the most stable nodes, branches and endpoints extracted from the identified skeletons. Assessment of the proposed method was done using subsets of images from the University of Bath Iris Image Database (1000 images) and the CASIA Iris Image Database (500 images). Compelling experimental results demonstrate the viability of using the proposed morphological approach for iris recognition when compared to a state-of-the-art algorithm that uses a global feature extraction approach.

[3] Sami Romdhani, Volker Blanz, and Thomas Vetter, presented an innovative algorithm aimed at analyzing and identifying faces viewed from different poses and illumination conditions. In an analysis-by-synthesis fashion, face analysis from a single image is performed by recovering the shape and textures parameters of a 3D Morphable Model was done. The shape parameters are computed from a shape error estimated by optical flow and the texture parameters are obtained from a texture error. The algorithm uses linear equations to recover the form and texture parameters no matter the pose cause and lighting conditions of the face image. Identification experiments are reported on more than 5000 images from the publicly available database.

[4] Jiawei Yuan and Shucheng Yu, Biometric identification is a reliable and convenient way of identifying individuals. The widespread adoption of biometric identification requires solid privacy protection against possible misuse, loss, or theft of biometric data. Existing techniques for privacy-preserving biometric identification primarily admit standard cryptography primitives like homomorphic encryption and oblivious transfer, that inevitably introduce tremendous value to the system and are not applicable to practical large-scale applications. In this paper, they propose a unique privacy conserving biometric identification scheme that achieves potency by exploiting the facility of cloud computing. In the proposed scheme, the biometric database is encrypted and outsourced to the cloud servers. To perform a biometric identification, the owner generates a credential for the candidate biometric trait and submits it to the cloud.

The cloud servers perform identification over the encrypted information using the credential and return the result to the owner. During the identification, cloud learns nothing regarding the original private biometric information. Because the identification operations are securely outsourced to the cloud, the real time computational/communication costs at the owner side are minimal. Thorough analysis shows that their proposed scheme is secure and offers a higher level of privacy protection than related solutions such as kNN search in encrypted databases. Real experiments on Amazon cloud, over databases of different sizes, show that their computational/communication costs at the owner side are several magnitudes lower than the existing biometric identification schemes.

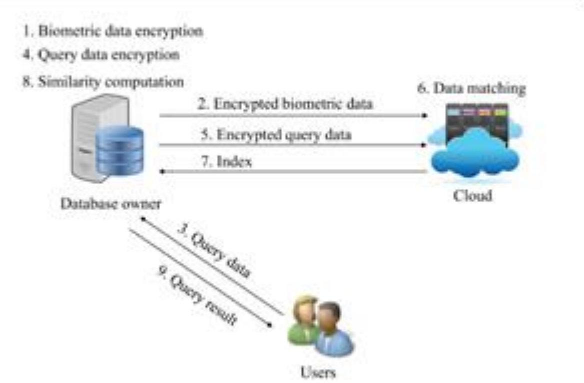

**Fig. 1** Proposed Model

### IV. Blockchain Technology

Asem Othman and John Callahan [9] explored blockchain technology in mobile systems. The idea behind it was to propose BlockID, a novel framework for people identity management that leverages biometric authentication and trusted computing technology. A prototype that explained the feasibility of the project was also designed. A recent paper proposed by Montes D. Juan, Rincón P. Andrés, Páez M. Rafael, Ramírez E. Gustavo, and Pérez C. Manuel I [11] expressed a security model for a national electronic Identity Document (e-ID) in Colombia, based on blockchain network concept using smart cards and taking advantage of the traditional authentication methods as biometry (citizen authentication) and physical security (document authentication), in order to reduce the security issues of the currently used Identity Document. In a research done by Anthony M. Butler, Ghada Dulaim, Victor Usobiaga [13] a digital identity including a private key is created. The private key was encrypted on a mobile device via use of captured biometric data. This includes a decentralized approach to the system.

[6] J.S. Hammudoglu, J. Sparreboom, J.I. Rauhamaa, J.K. Faber, L.C. Guerchi, I.P. Samiotis, S.P. Rao and J.A. Pouwelse introduced a mobile biometric-based authentication system was devised only relying on local processing. The android open source solution explores the potential of current smartphones to accumulate, process and match fingerprints using solely its built-in hardware. The architecture is specifically designed to run fully locally and autonomously, not requiring any cloud service, server, or permissioned access to fingerprint reader hardware. It involves three main stages, beginning with the fingerprint acquisition using the smartphone camera, followed by a processing pipeline to get minutiae options and a final step for matching against other locally stored fingerprints, A mean matching accuracy of 55%, with the highest value of 67% for thumb fingers. The ability to capture and process a finger fingerprint in only seconds using a smartphone makes this work usable during a wide range of situations, for instance, offline remote regions. This work is specifically designed to be a key building block for a self-sovereign identity solution and integrate with the permission less blockchain for identity and key attestation.

[7] In Arthi Manohar's paper, it shows that since the invention of internet, Identity has become a significant aspect for nearly every interaction that occurs online. In this position paper, they demonstrated and discussed current limitations of centralized IdM systems by drawing from the cases of two of world's largest biometric ID systems India's Unique Identification System Aadhar and China's Social Credit System Sesame Credit. This paper explores self-sovereign identity through innovative application from blockchain 3.0. Some few key characteristics of blockchain technologies is explored to deal with the challenges centralized IdM services face and present opportunities for furthering HCI analysis around de-centralized IdM services to provoke workshop discussion.

[8] Karen Lewison and Francisco Corella, is the second of a series of papers describing the results of a project whose goal was to identify five remote identity proofing solutions that may be used as alternatives to knowledge-based verification. This paper describes the Second Solution, that makes use of an upscale credential tailored for use on a blockchain and backed by a blockchain PKI. A rich credential, additionally utilized in solution one, permits the subject to identify him/herself to a far-off friend with which the subject has no previous relationship by presenting verification factors including possession of a private key, information of a password, and possession of one or more biometric features, with selective disclosure of attributes and selective presentation of verification factors. In Solution 2 the issuer could be a bank and the biometric verification factor is speaker recognition, which might be combined with face recognition to defeat voice morphing. The paper describes intimately the idea of a blockchain PKI and shows that it has remarkable advantages over a traditional PKI, notably the fact that revocation checking is performed on the verifier's native copy of the blockchain while not requiring CRLs or OCSP.

[9] Asem Othman and John Callahan, most user authentication methods and identity proving systems rely on a centralized database. Such data storage presents one purpose of compromise from a security perspective. If this technique is compromised, it poses an immediate threat to users' digital identities. This paper proposes a decentralized authentication methodology, referred to as the Horcrux1 protocol, within which there's no such single point of compromise. The protocol relies on decentralized identifiers (DIDs) under development by the W3C Verifiable Claims Community Group and the concept of sovereign identity.

[10] Zhimin Gao, Lei Xu, Glenn Turner, Brijesh Patel, Nour Diallo, Lin Chen, Weidong Shi, Blockchain is a powerful and distributed platform for transactions which require a unified, resilient, transparent and consensus-based record keeping system. It has been applied to scenarios like smart city, supply chain, medical data storing and sharing. Many works are done on improving the performance and security of such systems. However, there's an absence of the mechanism of identity binding when an individual's being is involved in corresponding physical world, i.e., if one is involved in an activity, his/her identity within the world should be correctly reflected within the blockchain system. To mitigate this gap, they proposed BlockID, an innovative framework for people identity management that leverages biometric authentication and trusted computing technology. They additionally develop a model to demonstrate its practicability in practice.

[11] Montes D. Juan, Rincón P. Andrés, Páez M. Rafael, Ramírez E. Gustavo, and Pérez C. Manuel I, This paper proposes a security model for a national electronic Identity Document (e-ID) in Colombia, based on blockchain network concept using smart cards and taking advantage of the traditional authentication methods as biometry (citizen authentication) and physical security (document authentication), to reduce the security issues of the currently used Identity Document. The proposed model uses smart cards to store information of the citizen, such as the encrypted template of their biometric features to perform user authentication, fingerprint and iris recognition technologies. In addition, the well-known benefits of a private blockchain network are exploited to verify the authenticity of the document and validate the legality of the user transactions.

The blockchain network architecture are bestowed shaping the block structure, the kind of transactions and the blockchain approach for the e-ID.

[12] Shih Hsiung Lee and Chu Sing Yang, Human nails have a high degree of uniqueness, and it can be used for biometric recognition. In this work, microscope sensor was used to capture the clear image and segment the lunula and nail plate effectively through image processing. Fingernails' image is managed as the identity authentication. Histogram of oriented gradients and local binary patterns are accustomed capture the characteristic value. It uses support vector machine and random forest tree for classification. The performance of each feature extraction algorithm was analyzed for the two classifiers and the deep neural network algorithm was used comparatively. Furthermore, the security and privacy of the Internet of Things is still a challenge. This work uses the extremely anonymous blockchain technology to effectively shield data privacy and manage every user's data through the

blockchain, in which any change or manipulation can be recorded and tracked, and the data security is improved. Therefore, this article presents a nail analysis management system with the employment of research sensor and blockchain.

[13] Anthony M. Butler, Ghada Dulaim, Victor Usobiaga, A method and system for decentralized biometric signing of a digital contract. A digital identity that includes a private key is created. The private key was encrypted on a mobile device via use of captured biometric data. A digital hash of the digital contract is generated. A user using biometric data is authenticated. Usage of the biometric data is authorized. Responsive to the usage of the biometric data being authorized, the encrypted private key is decrypted. The digital hash is signed with the decrypted private key. The signed digital hash is stored in a blockchain.

## III. CONCLUSION

The conventional cryptographic techniques for privacy-preserving biometric identification such as homomorphic encryption and oblivious transfer, which inevitably introduce tremendous cost to the system and are not applicable to practical large-scale applications. Yuan and Yu [6] introduced a novel privacy-preserving biometric identification scheme which achieves efficiency by exploiting the power of cloud computing. Here the biometric database is encrypted and outsourced to the cloud servers. This is the idea of stepping up the traditional method and introducing blockchain technology to it. The idea behind blockchain being simple. It is designed to be immutable, tamper-proof and democratic. IT achieves this through three defining characteristics Decentralization, Cryptography and Consensus. Blockchain is still an emerging technology and evolving with each passing day. Most security vulnerabilities are patched up quickly, and in extreme cases, they can result in a new version of that blockchain known as a hard fork. Since the blockchain database is managed autonomously using a peer-to-peer network and a distributed time stamping server it allows the participants to verify and audit transactions It's also more secure because the data cannot be altered without the alteration of all subsequent blocks and the consensus of the network. Also, title rights can be assigned through blockchain and since all this is happening in real time, this cannot be altered without knowledge either. Since it's decentralized, in a p2p network files can be shared directly between systems on the network without the need of a central server. Blockchain is a much better solution to storing and exchanging digital value than anything that has come before it.

### REFERENCES

**[1]** Arun Rossa and Rohin Govindarajanb, Feature Level Fusion Using Hand and Face Biometrics
**[2]** Joaquim de Mira Jr., Hugo Vieira Neto, Eduardo B. Neves, F´abio K. Schneider, Biometric-oriented Iris Identification Based on Mathematical Morphology
**[3]** Sami Romdhani, Volker Blanz, and Thomas Vetter, University of Freiburg, Germany, Face Identification by Fitting a 3D Morphable Model using Linear Shape and Texture Error Functions
**[4]** Jiawei Yuan and Shucheng Yu, University of Arkansas at Little Rock, USA, Efficient Privacy-Preserving Biometric Identification in Cloud Computing
**[5]** Anil K. Jain, Fellow, IEEE, Salil Prabhakar, Lin Hong, and Sharath Pankanti, Filterbank-Based Fingerprint Matching. IEEE 2000
**[6]** J.S. Hammudoglu, J. Sparreboom, J.I. Rauhamaa, J.K. Faber, L.C. Guerchi, I.P. Samiotis, S.P. Rao and J.A. Pouwelse (course supervisor), Biometric-based authentication and blockchain storage for self-sovereign identity systems, Computer Science department, Delft University of Technology, The Netherlands., 2017
**[7]** Arthi Manohar, Identity Management in the Age of Blockchain 3.0
**[8]** Karen Lewison and Francisco Corella October 24, 2016, Backing Rich Credentials with a Blockchain PKI∗
**[9]** Asem Othman and John Callahan, A Method for Decentralized Biometric-based Self-sovereign Identity, 2017