Role of Mathematical Modelling and Learning Techniques for Privacy Preservation: A Systematic Review

Santosh Kumar[1], Sunil Kumar[2], Mithilesh Kumar Chaube[3], Sachin Kumar Gupta[4], and R. K. Saket[5,*]

ARTICLEINFO

Article history:
Received: 28 June 2021
Revised: 13 August 2021
Accepted: 16 Sepember 2021

Keywords:
Privacy
Preservation
Biometrics
Attacks
Machine Learning
Cryptography
Blockchain

ABSTRACT

Recent advancements in disruptive technology have gathered extensive data from various sectors, including healthcare, transportation, retail, market prediction, surveillance, finance, and telecommunication. Quantifiable information has been obtained from the massive amount of shared consumer data to achieve valuable insights into each of these sectors. Moreover, augmented mobile spectrum usage has paved the way for tracing consumers' activities and interests via numerous working prototype systems and commerce apps. For protecting the sensitive information and maintaining its integrity of stored data, it has upheld the necessity to mathematical modeling paradigm design and learning frameworks for protection of user data where all the storage and operations are supported out without unveiling any details. For protecting these details containing one's confidential evidences, classical privacy-preserving based on other techniques and methods developed over the few decades. However, classical models/ techniques have severe problems with data preservation of individual information. This paper provides a comprehensive review of the existing mathematical modelling and learning techniques and framework for privacy preservation along with significant challenges of privacy-preserving biometric schemes and highlight the future research pathways in preserving biometric schemes are discussed.

1. INTRODUCTION

Recent advancements in disruptive technology have gathered extensive data from various sectors, including healthcare, transportation, retail, market prediction, surveillance, finance, and telecommunication. Quantifiable information has been obtained from the massive amount of shared consumer data to achieve valuable insights into each of these sectors [1]. Moreover, augmented mobile spectrum usage has paved the way for tracing consumers' activities and interests via numerous working prototype systems and commerce apps [1] [2] [3].

Privacy preservation of individual health data has been a fundamental concern for the data owners who submit their health data for analysis in this modern times. However, interdisciplinary researchers and scientists have proposed systems to solve privacy preservation problems. They proposed a unimodal learning framework to enable a security mechanism for preserving data.

Several researchers proposed multimodal systems, algorithms and biometrics-based recognition systems to match the individual's identity based on similarity matching of individual biometric features.

A multimodal system is highly used to extract several multiple features for identification of individual.

The extracted features are used for better representations. The better representations of features are achieved by selecting optimal features from biometric data. The selected optimal features can be projected in feature spaces using linear projection methods for matching of query biometric template for verification and identification of individual. The biometric features can be extracted from different biometric datasets such as face biometric, fingerprint biometrics, ear biometric and other biometric modality database using different feature extractors and multiple matching schemes and algorithms. These algorithms are operating on a single feature set of datasets for verification of different identity.

Lu et al., 2003 proposed a mathematical framework for the identification of individual faces. They are extracted features from face image database for face recognition. They used the dimensional reduction techniques such as Principal

[1]*Department of Computer Science and Engineering, IIIT Naya Raipur, India.*
[2]*V Ship Company, India.*
[3]*Department of Mathematical Sciences, IIIT Naya Raipur, India.*
[4]*School of Electronics and Communication Engineering, Shri Mata Vaishno Devi University, Katra-182320, Jammu & Kashmir, India.*
[5]*Department of Electrical Engineering, IIT (BHU), Varanasi, (Uttar Pradesh), India.*
**Corresponding author:* R. K. Saket; Email: rksaket.eee@iitbhu.ac.in.

Component Analysis (PCA), Independent Component Analysis (ICA), and Linear Discriminant Analysis (LDA) technique for extraction of facial features from the face images. The extracted features are encoded in Eigen face values (i.e., represent) a single face image for accurate matching.

Moreover, in multi-algorithm systems, the same biometric data is processed using various algorithms.

The existing feature descriptor and extraction-based algorithms are used to verify individual based on minutiae features. Researchers employed texture feature extraction methods to extract features from the fingerprint image and they, improved the system's performance (Ross et al., 2003). It does not require the use of new data sensors, and, therefore, it is cost-effective. Furthermore, the consumers are not needed to

Interact with multiple data acquisition-based sensors by enhancing user applications and convenience. However, it requires mathematical modeling and machine learning paradigms for novel feature extractors and matcher modules, increasing the system's computational requirements. Multi-instance systems use the same medical record and the human body. The multiple instances of these features from the same body or identical medical records are multi-unit systems.

For example, scanned images of an individual's left and right index fingers or the left and right irises may be used to verify an individual's identity. Multi-instance systems usually do not require new sensors, nor do they necessitate developing new machine learning techniques for feature extraction and matching algorithms, and are. Therefore, these are cost-efficient. However, in some cases, a new sensor deployment might be required to facilitate the various unit's/instances' simultaneous capture.

One or many sensors are integrated into multi-sample systems; these integrated sensors are utilized to acquire one or multiple biometric samples of individuals with the same health data and biometric traits. It accounts for the changes in the traitor to get a complete representation of the underlying trait. The individual face can be captured from multiple cameras or sensors for identification in a face recognition system. The face images may be captured from the frontal profile of a person's face, with the left and right profiles to account for variations in an individual's facial pose. There is a need to perform better integration among captured multiple features from individual faces for better accuracy.

Multimodal systems use the process for the integration of multiple features from captured health data evidence of individuals. The system combines this information or evidence presented by various body traits or information to establish identity.

For example, the earliest multimodal biometric systems employed face and voice features to establish an individual's identity.

Chang et al., 2005 proposed a system for integrating one or more modal or extracted information into one system, known as a hybrid system. The hybrid systems can combine homogeneous features or instances or multiple heterogeneous features or instances for the complete model using different algorithms, multi-algorithm, multi-instance-based systems, and Multimodal systems.

The multiple features are extracted from one or many biometric traits to obtain the hybrid features using hybrid systems. The significant advantages of the hybrid system are to cater better performances on the heterogeneous database; it performs robust feature representation for complete matching with a stored database, (3) multiple representations of extracted features in different feature spaces, and extracting multiple features by multiple or multimodal systems.

The hybrid system-based privacy preservation techniques provide the concerns to alleviate the user conveniences. The unimodal system generally hinders patients' usage of the several integrated unimodal systems and enables devices such as electronic healthcare systems to submit their essential healthcare data and their credentials for analysis. Privacy perseveration is an open, challenging problem of shared data due to the unregulated open system where anyone can access patients' records in analyzing them on the centralized shared platform. Patients' apprehensions include leakage of personal health information for medical insurance fraud or identity theft [2].

With the significant progress of biometric-enabled senor technology, the automatic verification system and smart-enabled framework have been implemented for its tremendous and comprehensive utilization. The primary aspect is to provide a better system to protect privacy in biometric data. It also includes access to many shared computers connected. It also caters to personal information at airports and allows the right to use in shielded zones such as nuclear facility stations, across border transfer, individual identity.

The computation and sharing of data are extensively high because of the exponential increase in internet usage; thus, measuring of biometric data identity and authentication here turn out to play a vital role in web-based applications such as online banking, online verification of an individual, and online shopping and other applications [1]-[4]. The passwords, passcodes, i-cards, and PINs are applied to verify an individual's identity. This information and passcode-based systems and frameworks do have some cons. For example, one's PIN could be made accessible to many people, and an identity card could be misused if stolen by someone. The attackers can access an authentication system by trial-and-error method to get access or disable the systems by providing the fraudulent data many times.

To breathe significant issues in customary privacy and preservation systems and frameworks and verification methods. The fundamental characteristics of human biotic

features are now being subjugated in order to create biometric systems [1] [2] [3], which include biometric of the finger, handprints, palm recognition, face, voice, iris, and keystroke biometric feature patterns.

The biometric has primal characteristics that it can neither be stolen nor shared in identity verification. In addition, biometric-based authentication schemes cater to high ease of access without remembering or carrying any extra identification kit [3].

Though these frameworks and systems have distinct pros over the customary systems, they can still risk privacy maintenance if not immediately [4] [5]. The literature review is given in Table 1. It includes different techniques to encrypt data for providing privacy preservation of the individual.

The biometric-based authentication system and frameworks may store the finger, handprints, face biometrics, ear image, or iris data.

Suppose the stored biometric data is uncovered to any unauthorized agents, which they could use either as a masquerader or impersonator. Since the stored biometric sensitive information is derived from the biotic appearances of humans, this discriminatory biometric information is unique and immutable. They cannot be altered. The biometric is sensitive data. Therefore, the attacks and breaching the sensitive data might cause significant severe dangers to the individual's privacy.

Table 1: Comparative study of existing methods for privacy preservation of individual

Reference	Method	Used database	Accuracy	Remarks
Amiri et al. [1]	Soft computing	KDD database	NA	It provides survey of privacy preservation using different machine learning techniques.
Jia et al. [8]	Stochastic gradient descent (SGD) method	MNIST and CIFAR-10 dataset	MNIST (90%), 99% (CIFAR)	The proposed system takes 839 milliseconds to encrypt all training data samples. It can be minimized.
Kumar et al. [35]	PCA+Eigen face Paillier encryption Elliptic curve-based encryption algorithm	FERET face database	96.89%	Deep learning-based methods can be used to provide security at different level.
Mohammad Haghighat [36]	Gabor feature method, + LDA, +PCA	Face image	Classification accuracy 95%	Requirement to valid model based on different setting and benchmark setting.
Li Ping et al. [36] [37]	SIFT key point descriptor, BCP double encryption algorithm	Face image	Decryption time 55s, Feature detection 95s	Huge database requirement for classification of face images
Jegede et al. [38]	Facial images (200 face images)	LBP feature extractors	FAR=0.47% FRR= 1.56%	Accuracy can be improved based on validation and trading of model at different features.
Huang et al. [39]	No database	Block chain techniques	verify a zero-knowledge proof (0.614s vs.0.062s) and the verification key size (125.4KB vs. 31KB	It needs to validate the system performance based on different attacks and benchmark settings.
Chenthara et al. [40]	No database used	Block chain technique Hyper ledger fabric and Hyper ledger composer method	NA	Data needs more preservation mechanism over cloud.

Abbreviation: LDA= Linear Discriminant Analysis, PCA= Principal Component Analysis, LBP= Local Binary Pattern method, FAR=False Acceptance Rate, FRR= False Rejection Rate.

The privacy preservation of biometric data also can be breached and altered over the stored cloud servers. Therefore, the biometric data should be secured to remain uncompromised even if the unauthorized users cannot collect the relevant data, which might rupture one's privacy. Besides, some authenticated users should be unable to log in to authorized systems as unpretentious users [6] [7].

2. TYPES OF PRIVACY PRESERVING SYSTEM

In literature, for protecting the individual information that consists of private data such as health records, biometric identity information using encryption mechanisms and systems in current years [8] [9]. The privacy-preserving systems can be divided into the following groups: (1) biometric features-based encryption systems, (2) the cancellable biometric-based features schemes, (3) multimodal-based biometric systems, and (4) hybrid-features-based schemes, and (5) secure computation (SC) based privacy preservation systems.

Biometric features-based encryption systems are presented for coupling biometric data with digital keys to maintain data privacy, and authorized users can access shared data. The encryption of biometric data could be done by using a binding key with the biometric data. Creating the key from data provides the security mechanism to protect the privacy of individuals [10] [11].

Cryptography-based encryption and key generation methods are applied in biometric security [9] [10] [11]. Key-based cryptographic encryption methods are chosen for assuring the security of biometric in Wireless Body Sensor Network (WBSNs).

A. The cancellable biometric-based features schemes involve usage and purposefully storage of inaccurate or altered biometric features mined from biometric signals. The usage of intentionally reformed signals decreases the threat of revealing the details of the original biometric data [12] [13].

B. Multi or Cross-Modal Biometrics-based systems use one or more biometric characteristics (e.g., facial features, ear biometric features, iris biometrics, fingerprints, and voice-based signals) for verification. Hybrid system combines multiple features from multiple modalities and provides the better privacy-preserving of extracted biometric frameworks. These features are encrypted using the encryption-based framework.

C. Concerning the secure communication (SC) based framework and methods, the high level of privacy of biometric information by applying the cryptography-based encryption and key generation methods encryption techniques that guaranteed mechanism to protect data. The encryption techniques include a homomorphic encryption-based framework for encrypting the stored biometric data and garbled circuits.

D. Currently, privacy-preserving systems using biometric information have been reported and studied [14] [15] in the current literature. However, this study has provided a coherent set of ideas and mathematical formulation and simulation conception of preserving privacy biometrics from various computing paradigms and aspects. However, their scopes are limited.

E. In the current literature, the establishment of different privacy preservation systems for cloud computing paradigms is used to access shared data and leverage accessing the big data, cybersecurity, and IoT-sensor data need security constraints against unauthorized people. In the traditional privacy preservation systems and frameworks, there are no such methods and procedures to provide reliable solutions for the privacy preservation of the individual. Therefore, there is a need to design efficient systems for protecting the privacy of biometric data. Moreover, it has provided a better paradigm for computing biometric data. Also endorsed the necessity to cultivate biometric data protection methods and frameworks where all the information is stored, and retrieval processes are performed without linkage of any biometric data and disclosing any sensitive information.

F. Following these research trends, the current state-of-the-art-based framework or systems emphasizes novel algorithms to compute and efficiently compare the uneven-length biometric data in the encrypted field and new coming domain by using homomorphic encryption technique, garble circuits-based techniques, and other cryptographic methods. Only encrypted biometric data is stored or exchanged in the encryption mechanism to provide a better privacy method for preserving the individual's identity.

The uneven-length biometric database frameworks and algorithms are bonded with current fixed-length frameworks or techniques to gather the modified system to perform the comparison for getting better accuracy. For assessing the soundness of privacy, preservation-based systems and frameworks can be evaluated on different applications. The particular application needs a privacy preservation system by incorporating different parameters. For example, a multiple algorithm-based biometric pattern protection system can be used for protecting the privacy in biometric data, such as dynamic signatures of individuals. It obeys the needs as defined by the ISO/IEC 24745 standard on biometric information protection paillier cryptosystem and other techniques. It ensures pro-creditability and affinity to another schema.

In a similar direction, the author [4] has not conferred any of the famous privacy-preserving biometric-based authentication systems and schemes nor conferred a complete description of cancellable biometrics. The author

[5] did not indicate the robustness and effectiveness of systems against various attacks on biometrics-based privacy preservation systems.

In [16], the author suggested a system to preserve the biometric information of individual humans to protect the system and stated the potential attacks and performance assessment. However, few essential privacy-preserving biometric schemes such as hybrid privacy-preserving biometric schemes were not included. Similarly, the author [7] not provided details about working prototypes systems under the pattern protection grouping and secure computation (SC) based framework and schemes. Further, Table 1 shows methods for privacy-preserving of individuals.

In the comparison of [7] – [15], it was noticed that the possibilities of [8] – [15] are even tighter. The authors have focused on significant issues and challenges in privacy preservation based biometrics authentication systems. These systems include privacy preserving-based by using multimodal biometric systems [8], secure computation (SC) based systems [9], error control mechanisms and methods related to privacy-preserving biometric schemes [10], adversarial machine learning techniques and frameworks [11], biometrics-based feature extraction and pre-processing systems [12], spoofing attack-based privacy preservation systems [13], the cancellable biometric features [14] and biometric signal and its processing in encrypted domain [15]. Moreover, calibration is essential in privacy-preservation biometrics, not stated in [4-15].

The standardization protocols and frameworks for providing privacy preservation are mentioned in [6]. However, the significant difficulties and defies that came across in standardization were also not mentioned. The papers [4] – [6], [8] – [11], and [15] did not demonstrate the fundamental ideas and coherent set of formulation, the core idea, and solutions about the current need and significant challenges and future research directions.

In [7] and [12–14], the authors have studied that the significant challenges and research directions, However, they did not mention in several specific sub-areas, for example, significant issues and challenges in preservation of extracted set of biometric features, privacy preservation of the individual, linkage of biometric features, attacks over systems [12] and robustness enhancement of cancellable biometrics, and efficient solutions for privacy-preserving biometric schemes [14].

2.1 Research Contributions

The primary research contributions are illustrated as follows:

1. In this paper, a comprehensive survey is provided with significant motivations and efficient solutions of privacy preservation of individuals based on biometric information. It also presents efficient algorithms and frameworks to protect the privacy and preservation of individual identity. The detailed and updated outline of the modern privacy preservation methods is presented using a generic framework.
2. The primary objectives of this work are to provide an exhaustive assessment of the research performed in these areas since the inception of the term and to motive the various researchers in this research domain. The significant challenges and the potential future research directions are also highlighted to motive the research in these directions. We will also suggest possible techniques and proposed frameworks and tools to deal with these challenges and control future demands.
3. The paper concludes with a broad discussion on the significant emerging research fields that require to address in the coming years to see the promise of biometrics features-based privacy preservation system or frameworks.

The remaining part of the paper is given as: Section 3 illustrates proposed system and its major components for privacy preservation. Section 4 provides the privacy-preserving based biometric authentication systems. In Section 6, the major challenges in privacy preservation system are discussed. Section 6 shows prospective application an opportunity. Finally, conclusion and future direction are provided in Section 7.

3. PROPOSED SYSTEM

The proposed system architecture comprising of several modules: (1) patients user (PU) module, (2) collection and pre-processing of health data, (3) encryption phase (EP), (4) decryption phase (DP), (5) administrator, (6) health worker (HW), and (7) data storage. The brief description of each module are illustrated in next subsections.

3.1 Patients User (PU) and Encryption Module

It is the requirement first to submit information of PU for registration. Every user can receive a unique code that is assigned to the PU for verification. The user authentication can be done by performing an identification process based on submitted biometric data (face, fingerprint, and others). Then PU is granted entry into the medical diagnosis and treatment process based on submitted health records or information for the analysis. Upon receiving the unique code, patient user can now send their health data, which will be encrypted to preserve the PU's privacy.

The individual is registered into the proposed biometric base recognition systems using face images. During enrollment, facial images are captured and stored in the cloud face template database. The query (test) face images are encrypted using the homomorphic public-key Paillier [63] encryption algorithm to provide the security, confidentiality, and integrality of sensitive biometric face data in the cloud.

The motive behind choosing the Paillier encryption technique is that it is homomorphic, efficient, and straightforward. Paillier encryption technique is based on the determined additively homomorphic public encryption scheme to encrypt the message.

The homomorphic public-key encryption schemes are applied to match encrypted biometric feature templates for user identification using the Elliptic encryption technique. The distributed computation is done for better security when users interact with cloud computing. Because the group protocol using Elliptic encryption system enables cloud and user's communication for data secure, credible, and complete when in an insecure, open network communication environment. The Elliptic encryption algorithm is illustrated in the following steps:

1. **Step 1:** Patient/user (A) selects an elliptic curve method Ep (a, b), y2=x2+ax+b (mod p) n and finds a point on the Elliptic curve known as point Q.
2. **Step2:** User (A) chooses a private key (k) and creates a public key K=kQ.
3. **Step3:** User (A) sent the Ep (a, b) and generated point K, Q to the server-side cloud (B).
4. **Step 4:** When cloud (B) accepted the completed information from the (A), the accepted message b is to be encoded and transmitted to the point J on Ep(a, b) and generates random integer r (r<n)
5. **Step 5:** Cloud B decides the points C1=J+rK; C2=r.
6. **Step 6:** Cloud B passes C1, C2 to the user registration process.
7. **Step7:** After receiving the information, (A) determines C1k C2; point J results. Because C1-k C2=J+rK-k (rG) =J+rK-r (kG) =J, then the point M can be explicitly decoding.

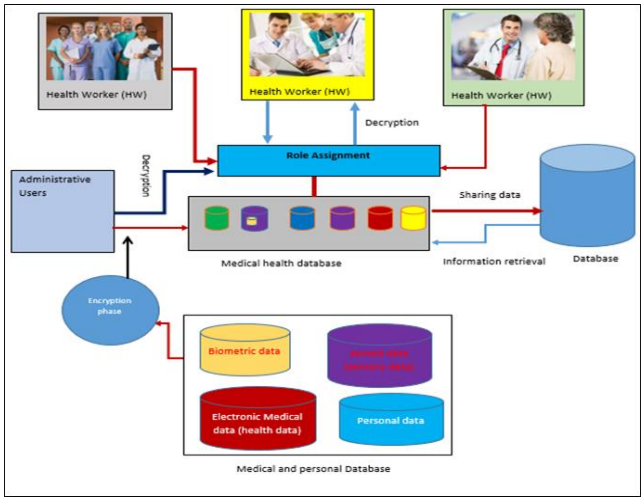

Fig. 1. Working system for health monitoring.

The encryption module encrypts the shared data of an individual. It involves comparing the patient's unique code to the key generated for the health data to be submitted for analysis. The identification of patients is performed based on matching their biometric credentials with the stored database. It prevents the disclosure of the identity of the patient-user with his health data submitting for analysis if interceded by an attacker. It secures the health data on the EMR system to be accessed by the administrator.

We used a biometric-based verification system to verify the identity of an individual based on captured biometric characteristics. The captured face biometric feature is encrypted, and the secret key (SK) and the encrypted biometric features are used at the verification stage.

At this stage, (X0) and (V0) acquired the biometric feature set and stored data, respectively. We calculated similarity matching scores between partner (V0) and (V) to determine whether a genuine user or an attacker is present.

In the validation mode, h (SK) and its complement h'(SK) have code values compared and matched.

In the literature, three metrics are used to compute and compare the similarity between two binary vectors. These similarity-based matching techniques include hamming distance-based similarity metrics, set difference-based similarity-metric, and edit-difference-based similarity metric methods.

3.2 Decryption Module

Based on stored biometric information on the system, the system performs encryption and decryption using homomorphic public-key encryption schemes. The encryption phase performs encryption of health data and allows the encrypted health data using pillar encryption method. It. has been submitted to be decrypted and released for analysis. At this stage, only the health data is released for analysis without attaching the patient user's personal information or the unique code assigned to the patient-user.

The encrypted biometric data was decrypt performed using homomorphic public-key encryption schemes based on measured minimum distances between the query image template and stored biometric template of the individual.

Minimum Distance Finding

After measuring distances between input biometric images (face images) and stored face templates, the system computes minimum distances computed among M encrypted distances.

The k-d tree structure technique is employed in this experiment; the calculated M distances are initially categorized into even and odd neighboring with M/2 groups.

Each group cannot take the smaller one, reject the bigger one, and remain M/2 distances. This method is taken into consideration to find the minimum distances between store templates and biometric query templates. In other words, to compare the two encrypted numbers and solve the primary problem, the matching algorithm is illustrated (Algorithms-1) as follows:

Algorithm: 1 Encryption steps

Step 1: We used the cloud server (B) to generate a random number r, encrypted to [r].

Step 2: Cloud sever (B) passes following encrypted data to User (A).

$$[a+\gamma] = [a].[\gamma]$$
$$[b+\gamma] = [\mathrm{b}].[\gamma]$$

Step3: User (A) decrypt using private key and obtain $[a+\gamma]$ and $[b+\gamma]$, and subtract the two numbers, if result is negative, then $\gamma = 1$, otherwise $\gamma = 0$;

Step 4: A passes $[\gamma]$ to B;

Step 5: B brings $[\gamma]$ to the following formula:

$$[m] = [\gamma]^{\left\lceil [a] \,/\, [b] \right\rceil}.[b] = [(a < b).(a-b)+b]$$

In the equation, obtained result $[m]$ is the smaller one of *a* and cipher text of *b*. It presents the credible, efficient result of comparing the two encrypted numbers.

Finally, Elliptical encryption technique encrypts the achieved the smaller number calculated from above method. Achieve encrypted $[[m]]$, and then transfer the $[[m]]$ back to A which applies the private-key scheme to perform the decryption of encrypted message $[[m]]$.

3.3 Data Storage and Protocol Execution

Data Storage is used for synchronous analytics. Also, it helps the proposed system share the analyzed data for future references and research usage. It is by preserving the privacy of the various patient users for diagnosis of acute disease. The system protocol is used for designing the models. It consists of (1) a health data submission phase and (2) a decryption phase.

3.4 Health Data Submission Module

At the initial stage for submission stage, all the PU are requested to submit all medical data related to their health problems through the login portal. It provides a login into the medical system for submission of health to the user based on the authorization of individual users based on the biometric data enrollment process. This process is achieved by deploying a biometric-enabled system known as the electronic biometric and medical data record system.

After stored biometric data and health data, the system performs the encryption and decryption process to encode and decode data during transfer from user system/devices to the server using encryption method.

Based on the available literature, privacy preservation techniques are used to protect the privacy of individuals based on different biometric characteristics. The privacy preservation techniques are discussed in the following subsections.

3.5 Privacy Preservation Techniques

The privacy-preserving-based biometric framework or schemes are used to protect the biometric information for the individual. These schemes can be broadly categorized as (1) biometric encryption-based schemes, (2) cancellable biometric schemes, (3) multimodal fusion, (4) hybrid-based schemes, and secure computing-based schemes. The brief description about biometric encryption based privacy preservation techniques is illustrated in next subsections.

3.5.1 Biometric Schemes on Encryption Technique

Biometric encryptions shield the biometric signal from attackers using cryptanalysis algorithms and techniques. It has a low false accept rate; therefore, the biometric signals are more secure from attackers. Due to the invariantly vague structure of cryptanalysis and biometric extraction and matching algorithms, the exact matching of biometrics is always flawed and impractical in reality. Hence, it is not feasible to use classic cryptographic algorithms with biometric approaches uprightly. To solve said significant problem, fuzzy techniques were brought to light to secure the system against various attacks over biometric systems. In the initial process of the biometric verification system, a diverse feature set is extorted from original biometric data, which is combined with some wrapper algorithm to generate a secret key. In this processing, the foresaid output and hashed secret keys are saved in databases. Wrapping and binding agreements are secured so that once data is stored, it cannot be breached. In the biometrics-based verification process, if the biometric input data is relatively similar to the data stored, then generated primary secret key could be used again and retrieved later. Actual users are authenticated depending upon its similarity matching. The accuracy level will now depend upon the secret key and cryptographic algorithm [18]. The biometrics-based authentication systems could be categorized into (1) critical binding mode and (2) critical generating mode. A brief description is given as follows:

3.5.2 Key Binding Mode Based Schemes

A secret key is produced randomly, and the biometric features are combined monolithically with generated keys using the cryptographic framework or algorithms in the keybinding mode. The critical binding process provides help to encrypt the extracted biometric features with the secret key generation. The encrypted biometric information with generated hashed secret keys are kept in the stored data. The secret key is retrieved from the biometric data stored, and the received biometric signal for verifying individuals at the verification end, where the retrieved and secret keys are evaluated [19]–[35].

3.5.3 Key Binding Mode Based Privacy-Preserving Biometric Schemes

The fuzzy vault framework was initially stated [20] and formulated to knead with unordered sets and manage classed variation generally encountered in biometric data. Figure 1 and Figure 2 show the fundamental key binding privacy-preserving biometric schemes (mode-based). Biometric feature set X is extorted from the input(for ex: finger/palm prints). Then from the secret key SK, resulting polynomial (p) coefficients are generated. These set [X] values are protrusion on polynomial by which the values not directly lying on the polynomial(shreds) are now added as produced points. These points are depicted as V.

In a fuzzy-based privacy-preserving biometric scheme, the partner data is popularly known as the vault. The shreds points are added to avoid attackers getting knowledge about polynomial. At the verification stage, acquired secret keys and stored secret keys are compared. To acquire the secret key, feature set X0 must overlie on polynomial, which enables to locate the points V lying on p. Operative model of the fuzzy vault and key binding mode [21] supposed pre allineated feature sets. Due to this supposition, the prudency got restricted. To overcome this restriction, [22] proposed employing the high warp values acquired from the assimilated area of biometrics [23-28].

Many amendments were suggested for fuzzy commitment in privacy preservation biometric schemes for performance improvement. 2D iterative and binary Reed-Muller codes are used to enhance the effectiveness of the decrypting procedure [30]. In [31] proposed a mechanism for extorting iris details using the context-based decent component. Similarly, dynamic quantization random transformation was used to extort fingerprint features, and the Reed-Solomon algorithm is being used to enhance the decoding performance.

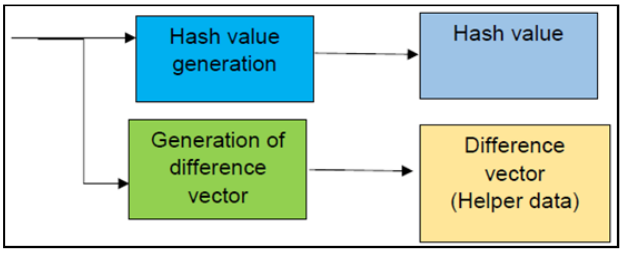

Fig. 2. Illustrates key binding mode based fuzzy commitment.

The focused data values of high curve areas for gaining coalition with biometric features had binary fixed-length feature representation [33]. This idea was also tested on face biometrics [34] and online signatures [35]. Since this method used wee-sized code phrases hence, they are more susceptible to brute force attacks.

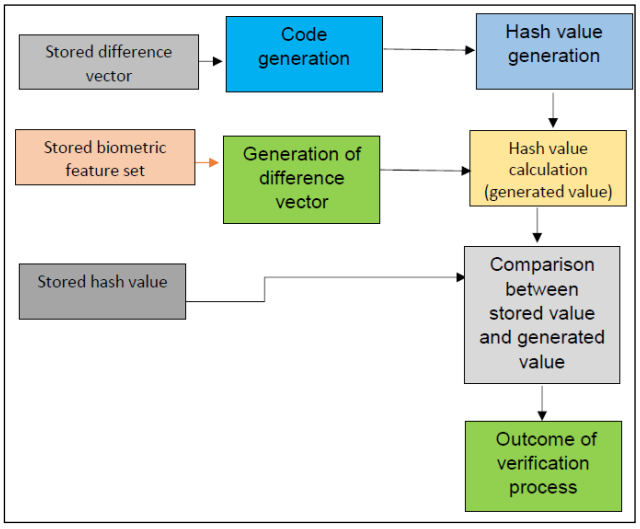

Fig. 3. Block diagram for fuzzy commitment in basic key binding mode.

3.5.4 Scheme Depending upon Secret Key Generation

In the critical generation mode, keys are produced from the feature set promptly, but this process is onerous as it needs key equity and mortification, which always might seem an easy task. Key equity meant the capability of recursively producing similar keys from input signals, and key mortification meant the probable keys which might be produced. With the noise factors in signals, it is somewhat arduous to retain key quit. Key equity and mortification are inversely propositional; hence managing both is troublesome. One type of key generating mode uses the notions of user-related quantization methods [36]. A method is used in [37] for the steady generation of keys from input feature signals. In order to register the user, his biometrics are used and later transformed in a specific way. These transformed biometrics of actual users are stored, which helps in differentiating from attackers. All biometrics features are helpful in data bits in encrypting the key process. Thus, durable and long-lasting keys are generated. These keys are moreover generated in user-specific ways using biometric schemes quantization methods [38-40].

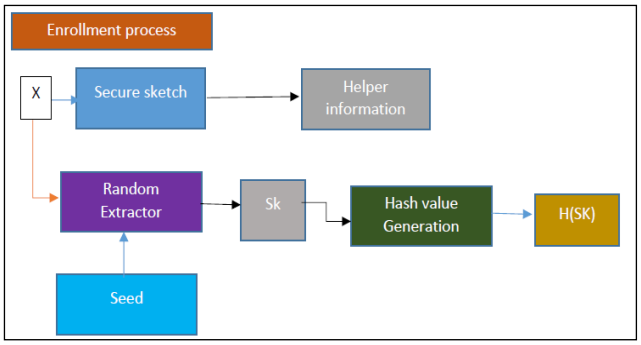

Fig. 3a: Block diagram of key production by fuzzy extraction.

Another type of key generation for biometric schemes utilized fuzzy extractor [17], as shown in Figure 3a. From input seed and biometric feature set (X), the partner data are generated by methods of the secure sketch. This method engages the random extractor, seed, and projections of X to correct the error is detected. These details are used to generate a uniform secret key (SK) randomly.

By X0 extracted at the initial stage and v are used to restore the feature set X. In [17], the combination of hamming distance, set difference, and edit distance metrics created a fuzzy extraction mechanism. Being more storage efficient, it has few disadvantages, too, fuzzy extractors being used repeatedly for the same input signal loses their mortification and reusability [41] [42]. There exists a doubt of exposure and de-positioning [43]. Lastly, there might be chances of data leakage [44].

4. CANCELLABLE BIOMETRIC SCHEMES

The primary role of cancellable biometric systems is to preserve the privacy of the registered users. The preserved biometric information is created by employing a parameterized transformation function to the original biometric information. Although cancellable biometric schemes obtain high-level security, however, they may diminish the recognition accuracy.

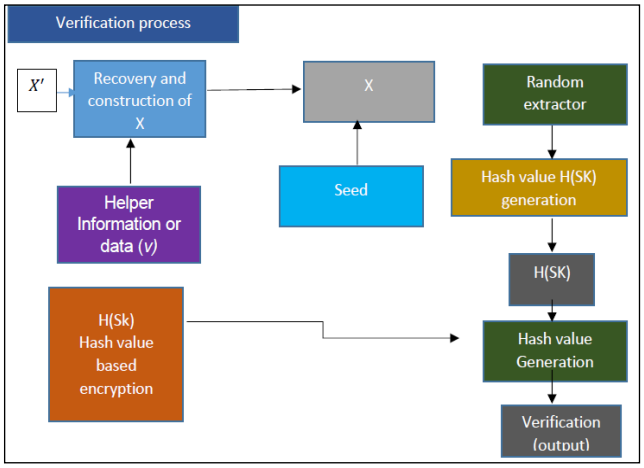

Fig. 3b. Illustrates the verification process.

Cancellable biometric scheme adds a reiterated deformity in the input signal correctly and purposefully to safeguard user privacy [3]. The deformity is regulated by conditions from a secret key generated by random numbers or passcodes.

The partner data *v* is composed by employing deformity onto feature set (X.) Figure 3b shows the verification process by devising (*v0*) from the input signal biometrics set (*x0*) and correlating the *v0* with the stored partner data (*v*). If the partner data (*v*) is imperiled, the deformed parameters can be altered to get a new bunch of partner data. The deformed operations are devised that it is computationally challenging to recover the original signal for an attacker. The brief description is given in next section.

4.1 Cancellable Biometric Based Privacy-Preserving using Bio hashing Technique

A bio-hashing has two steps, as shown in Figure 4. In the first step, image pre-processing is performed on the biometric images to make them proportional even to minute deviation in the input signal. Then an explicit secret key is produced by a random vector.

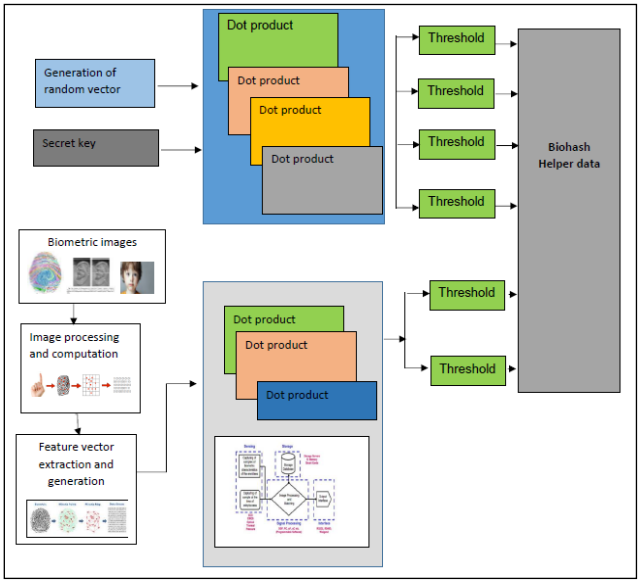

Fig. 4. Block diagram of generating bio hash value.

Then, a bio-hash value is produced by comparing the product value of the random vector and feature vector extorted. Verification is done by checking the similarity between the new bio hash value and already stored hash value [45]–[47]. In a privacy-preserving biometric scheme using hashing, the specific secret key enhances the mortification of the feature set. It is not possible to regenerate the main input feature set lacking the knowledge of the key. It is mainly because of using dot product and the threshold mechanisms [48]. Though some schemes are good for preserving privacy using the bio hash technique, they still have a significant constraint of getting keys stolen and thus compromising the system's security.

As stated in [49], the hashing performed under the assumptions that key might be stolen, the system's performance in terms of FAR increases from 7.3% to 10.3%. To highlight such a problem, [50] proposed some solutions for considering the length of the secret key as a protective shield. Also, [51] used the precise local binary pattern operator for biometrics to improve verification accuracy [51], but all these mechanisms result in more minor privacy issues.

4.2 Cancellable Biometric Using Non-Invertible Transform Technique

In cancellable biometric privacy preservation schemes using a non-invertible transform, the feature sets are preserved by implementing non invertible transformation, which refers to a unidirectional function F(x), accessible in computation but challenging to invert [52]. The central aspect of this approach is that, for an attacker using a brute force attack to recover signals, it is still not possible to breach the key due to the high complexity of the algorithm. In the initial process itself, the partner data v is saved. Noninvertible transformation and verification accuracy are district necessities for privacy preservation in biometric schemes [53].

- Various other transformations are explored for privacy preservation schemes in biometric with their effects on authentication accuracy [52]. It is shown that the original input biometric signal can be remarked if feature set x and secret key are well noted.
- Cancellable formulation on feature set/vector disrupts the signal, later re-invoked by non-invertible transform [55]. This disrupted vector is cast upon random subparts as a key by using a random number for a particular user. In performance, three disparate scenes could be assumed; common, stolen key and compromised key.
- Amongst all the other transformations investigated [56], the random level of transformations has given a better level of privacy. Adaptive bloom filters were employed for providing adaptive and proportional sequences with respect to comparison of feature set [57].

5. MULTIMODAL FUSED BIOMETRIC SCHEMES

The main intention of biometric privacy schemes is to gain better accuracy. Using more than one biometric scheme to increase privacy preservation accuracy can be hybrid and multi-modal schemes.

5.2 Multi-Modal Privacy-Preserving Biometric Schemes

As stated in [58], amalgamating two different biometric facets such as iris+face, finger print+face, voice+palm, etc., overcomes the defects of variability and similarity within classes, quality, and noise subtlety. Fixing the defects can eventually increase accuracy. By amalgamating different facets of biometrics, new approaches and schemes were proposed.

The preserving privacy issues in the biometric scheme [59] has merged fingerprint and users' voice signal using fuzzy logic. In [60], face and online handwritten signatures were merged using Linear Discriminant Analysis (LDA) feature extraction and representation techniques. In [61], the Independent Component Analysis (ICA) technique are used to extract biometric characteristics from the multimodal biometrics modality. The multimodal biometric modality includes Ear+iris, and face+fingerprint, palmprint+face biometrics. Few multimodal approach-based biometric schemes [62] and [63] can be found to secure sensitive biometric information over cloud servers.

5.2 Hybrid Based Privacy-Preserving Biometric Schemes

In privacy-preserving biometric schemes, as stated above about encrypting biometrics and cancellable biometrics both have their benefits and detriment. The ground concept of a hybrid-based multimodal framework and approach is to mix various biometric schemes properly to gain maximum benefits from each in terms of its strengths. On the other side, this approach's detriment is that it is likely to break the feature structure in the process of transmutation, sometimes decreasing the accuracy level. In order to extract the most delicate parts of both approaches, implementation of error correction techniques within fuzzy extractor and cancellable schemes may give better efficacy in verification and targeting to get more out of the strengths it possesses [63-67].

6. SECURE COMMUNICATION SCHEMES

As per the above discussions, encrypted biometrics and cancellable schemes preserve privacy at the cost of decreased verification accuracy levels. In contrast, secure communication-based privacy-preserving biometric schemes shield biometric feature sets at higher time and space complexity. Higher complexity is gained when computations are performed directly in the encryption area.

In comparing this scheme with biometric encryption and cancellable biometric-based privacy-preserving biometric schemes, secure communication (SC)-based privacy-preserving biometric schemes attains high secrecy and verification accuracy levels by using highly complex algorithms. The main application of this approach is in client-server-based massive computational systems and workstation systems where they exchange biometric data without revealing it for verification. However, they are not practically used due to high complexity and massive computations.

6.1 SC Based Privacy Preserving Using Homomorphic Encryption Method

Homomorphic encryption was first brought in in 1978 [68]. In this approach, homomorphic encryption is done on a feature set by the public key. While performing verification, encryption is implied using a public key once the feature set is extracted.

Verification is performed amid encrypted feature set and stored set. A comparison protocol will conclude that the distance value is above or below the threshold of the verification system. By implementing homomorphic

encryption, encryption is projected with the likeness amid biometric input feature in enrolment and verification part as these parts are distinct in noise parameters. There are few applications where complete partial homomorphic encryption methods are discussed/used [69]-[72]. Partially homomorphic encryption implements either additive or multiplicative homomorphism [69]. The famous system of partially homomorphic encryption is known as the Paillier cryptosystem, implementing additive homomorphism. To increase the precision, this system merges with multiparty computation techniques [73] [74].

6.2 SC based Privacy Preserving Schemes

As for large biometric systems, partner data is stored within the system. Whenever a user accesses the system via biometrics, the store's data system can track the user's corresponding verification activities. For example, suppose a user tries to get him verified at a bank of a different place. The system then traces his location and grants access, if feasible. The garbled circuit introduced in 1986 are widely used to manage such issues [75]. It incorporates the AND gate and OR gate circuits for computations. The fundamental essence of the garbled circuit hides the partner data from the verification system. Thus, the system is unaware of the verification process. The concept of garbled circuits was rigorously used in iris and fingerprint matching [76], authentication [77], however the results have shown have more time complexity and are unsatisfactory.

6.2.1 Major Problems in Existing Privacy-Preserving System

Although the above-discussed schemes have their strengths, still their snags cannot be ignored.

- ***A. Robustness:*** Preservation of privacy in biometric schemes is a critical task to be performed as it is constantly under the danger of getting attacked in all possible ways [78]-[92]. To avoid this, many schemes are developed to confront attacks as much as possible. Following are the attacks that might be possible on biometric systems:
- ***B. False Acceptance Rate (FAR) Attack***: It is an inadmissible event under security in biometric systems where the attacker gets verified as a real user by mistake. FAR is stated as the probability of erroneous acceptance amongst all verification cases.
- ***C. Linkage Attack:*** an attacker can trace a user connected to the distributed system (for example, an online platform) via biometrics security. Attackers will trace a user and gather supportive details in parts, which can be brought together to get complete details against the user, helping the attacker intrude into the system.
- ***D. Hill-Climbing Attacks:*** The hill-climbing attack is performed by exposing the similarity level amid feature set and partner data. Once the details are exposed, it is enough for the attacker to reconstruct the original input signal/image [81]-[93].
- ***E. Brute Force Attack:*** Brute force attack intensely exploits the keys and passcodes by trying all probable sequences to breach the system. This attack needs enormous computing power [82]-[89].

6.2.2 Level of Privacy versus False Acceptance Rate

The primary motive of privacy-preserving biometric schemes is to shield users' privacy while assuring the lowest chances of FAR. The research was rigorously conducted to understand the FAR against privacy mechanism [83] – [85]. Thus, research showed that using the long-sized secret key. There are chances to avoid the attack as it is now challenging for an attacker to breach the system [86] [87]. However, this idea of using long key size again had a glitch, as partner data will now have more details about an original signal.

7. FUTURISTIC APPLICATION

Although researches are carried out on schemes that provide better accuracy, their benefits and demerits still exist challenges that cannot be ignored. Thus, we have discussed the existing challenges and future scope in which research needs to be performed.

7.1 Optimum Privacy-Preserving Biometric Schemes Selection

It is complicated; it is impossible to surmount these issues by developing a privacy-preserving biometric scheme that accomplishes the evaluation constraints stated in the above sections. However, hinging on the operation scenario, few parameters might be more necessary to fulfil than other parameters. Thus, it is necessary to have an optimal and generalized scheme for execution plots. This scheme should also consider the objective cost measure of the parameters required.

7.2 Biometric Features Calibration

Execution of privacy-preserving biometric schemes depends upon the calibration features set in some ways. As discussed, whenever a new feature set is generated, it is stored as partner data, and the old feature set gets replaced by the new one. Sometimes partner data requires additional details for verification and calibration. The author [91] proposed a fuzzy vault-based hashed mechanism for fingerprint feature calibration. To overcome this issue, either feature calibration should be assured, or the system should perform well autonomously without correlation of feature calibration.

7.3 Fulfilment of Unconventional Biometric Attributes

Today people are relying more on interactive devices using biometrics. With the development of technology, it is also essential to aid interactive devices with un-conventional biometric attributes such as palm, eye, voice, body

recognition [1]. At the same time incorporating such attributes, it is also necessary to consider robustness, unanimity, persistence.

7.2 Measurement of Attack Tolerance of the System

Various attacks were discussed in previous sections; however, new types of attacks will come into existence with time. So, the system should be sustainable enough against possible attacks. Hence new methods should be evaluated for persistence. A concord amid various disparate schemes and methods is necessary to work together in the biometric system. Allied mechanisms are required in such systems to assure compatibility [28] [90].

7.2 Scalable Schemes for Privacy-Preservation

With the advancements in cloud computing, business giants have shifted their business onto clouds. Many applications are being executed via the cloud. For security purposes, methods that are scalable and accessible distributed are required. Biometrics security systems could add as a security feature in clouds. Implementation of biometrics in business is a challenging task to ensure secure data exchange [92]. This is a need to use adjustable privacy-preserving biometric schemes. Depending upon the usability and platform on which it may be used, biometric schemes should be adaptable and adjustable with the platform. Moreover, it should satisfy the requirements of platforms too [93] - [100].

8. CONCLUSION AND FUTURE DIRECTIONS

In this paper, a comprehensive review is provided for the privacy preservation of individuals. The privacy preservation mechanism used mathematical simulation and encryption techniques to encode and decode the extract information such as biometric features or other confidential information from individual data or their biometric traits. The biometric data includes the face images, fingerprint, palm, and other behavioural biometric features.

In this paper, we have provided biometric-based privacy preservation systems and encryption for protecting stored biometric templates. The paper has summarised various biometric schemes and their structure and evaluation norms. It has provided a detailed discussion on the current privacy-preserving schemes, including encrypted biometric, cancellable, multimodal, and hybrid-based and SC schemes. The complications correlated by the current privacy-preserving biometric schemes were also outlined and conferred. Problems and its futuristic scope of privacy-preserving biometric schemes are also highlighted. Based on overall observation, we conclude that a comprehensive survey will provide a better learning paradigm for several interdisciplinary researchers, scientists, and other newcomers to learn encryption methods.

It is expected that the survey analysis portrayed in the paper might encourage other researchers to advance and expand the existing biometric schemes to provide better accuracy and efficacy.

REFERENCES

[1] Amiri, F. and Quirchmayr, G., 2017, October. A comparative study on innovative approaches for privacy-preservation in knowledge discovery. In Proceedings of the 9th International Conference on Information Management and Engineering (pp. 120-127).

[2] A. K. Jain, P. Flynn, and A. A. Ross, Handbook of Biometrics. New York, NY, USA: Springer, 2008.

[3] Gumaei, A., Sammouda, R., Al-Salman, A.M.S. and Alsanad, A., 2019. Anti-spoofing cloud-based multi-spectral biometric identification system for enterprise security and privacy-preservation. Journal of Parallel and Distributed Computing, 124, pp.27-40.

[4] Kumar, S., Datta, D., Singh, S.K. and Sangaiah, A.K., 2018. An intelligent decision computing paradigm for crowd monitoring in the smart city. Journal of Parallel and Distributed Computing, 118, pp.344-358.

[5] R. Song, H., Luo, T., Wang, X. and Li, J., 2019. Multiple Sensitive Values-Oriented Personalized Privacy Preservation Based on Randomized Response. IEEE Transactions on Information Forensics and Security, 15, pp.2209-2224.

[6] T. Liu, B. Di, P. An and L. Song, "Privacy-Preserving Incentive Mechanism Design for Federated Cloud-Edge Learning," in IEEE Transactions on Network Science and Engineering, doi: 10.1109/TNSE.2021.3100096.

[7] P. Kumar et al., "PPSF: A Privacy-Preserving and Secure Framework using Blockchain-based Machine-Learning for IoT-driven Smart Cities," in IEEE Transactions on Network Science and Engineering, doi: 10.1109/TNSE.2021.3089435.

[8] S. Rane, Y. Wang, S. C. Draper, and P. Ishwar, ‘‘Secure biometrics: Concepts, authentication architectures, and challenges,’’ IEEE Signal Process. Mag., vol. 30, no. 5, pp. 51–64, Sep. 2013.

[9] Jia, Q., Guo, L., Jin, Z. and Fang, Y., 2018. Preserving model privacy for machine learning in distributed systems. IEEE Transactions on Parallel and Distributed Systems, 29(8), pp.1808-1822.

[10] C. Rathgeb and C. Busch, Multi-Biometric Template Protection: Issues and Challenges. Rijeka, Croatia: InTech, 2012.

[11] J. Bringer, H. Chabanne, and A. Patey, ‘‘Privacy-preserving biometric identification using secure multiparty computation: An overview and recent trends,’’ IEEE Signal Process. Mag., vol. 30, no. 2, pp. 42–52, Mar. 2013.

[12] H. S. G. Pussewalage, J. Hu, and J. Pieprzyk, ‘‘A survey: Error control methods used in bio-cryptography,’’ in Proc. 10th Int. Conf. Natural Comput., Aug. 2014, pp. 956–962.

[13] B. Biggio, G. Fumera, P. Russu, L. Didaci, and F. Roli, ‘‘Adversarial biometric recognition: A review on biometric system security from the adversarial machine-learning perspective,’’ IEEE Signal Process. Mag., vol. 32, no. 5, pp. 31–41, Sep. 2015.

[14] M. Lim, A.-B. Teoh, and J. Kim, ‘‘Biometric feature-type transformation: Making templates compatible for secret protection,’’ IEEE Signal Process. Mag., vol. 32, no. 5, pp. 77–87, Sep. 2015.

[15] A. Hadid, N. Evans, S. Marcel, and J. Fierrez, ''Biometrics systems under spoofing attack: An evaluation methodology and lessons learned,'' IEEE Signal Process. Mag., vol. 32, no. 5, pp. 20–30, Sep. 2015.
[16] V. M. Patel, N. K. Ratha, and R. Chellappa, ''Cancelable biometrics: A review,'' IEEE Signal Process. Mag., vol. 32, no. 5, pp. 54–65, Sep. 2015.
[17] M. Barni, G. Droandi, and R. Lazzeretti, ''Privacy protection in biometric-based recognition systems: A marriage between cryptography and signal processing,'' IEEE Signal Process. Mag., vol. 32, no. 5, pp. 66–76, Sep. 2015.
[18] Y. Wang, S. Rane, S. C. Draper, and P. Ishwar, ''A theoretical analysis of authentication, privacy, and reusability across secure biometric systems,'' IEEE Trans. Inf. Forensics Security, vol. 7, no. 6, pp. 1825–1840, Dec. 2012.
[19] Y. Dodis, L. Reyzin, and A. Smith, ''Fuzzy extractors: How to generate strong keys from biometrics and other noisy data,'' in Proc. EUROCRYPT, 2004, pp. 523–540.
[20] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography. Boca Raton, FL, USA: CRC Press, 1996.
[21] C. Soutar, G. J. Tomko, and G. J. Schmidt, ''Fingerprint controlled public key cryptographic system,'' U.S. Patent 5 541 994, Jul. 30, 1996.
[22] A. Juels and M. Sudan, ''A fuzzy vault scheme,'' in Proc. IEEE Int. Symp. Inf. Theory, Jul. 2002, p. 408.
[23] T. C. Clancy, N. Kiyavash, and D. L. Lin, ''Secure smartcard based fingerprint authentication,'' in Proc. ACM SIGMM Workshop Biometrics Methods Appl., 2003, pp. 45–52.
[24] K. Nandakumar, A. K. Jain, and S. Pankanti, ''Fingerprint-based fuzzy vault: Implementation and performance,'' IEEE Trans. Inf. Forensics Security, vol. 2, no. 4, pp. 744–757, Dec. 2007.
[25] P. Li, X. Yang, K. Cao, X. Tao, R. Wang, and J. Tian, ''An alignment-free fingerprint cryptosystem based on fuzzy vault scheme,'' J. Netw. Comput. Appl., vol. 33, no. 3, pp. 207–220, 2010.
[26] A. Nagar, K. Nandakumar, and A. K. Jain, ''Securing fingerprint template: Fuzzy vault with minutiae descriptors,'' in Proc. IEEE 19th Int. Conf. Pattern Recognit., Dec. 2008, pp. 1–4.
[27] T. H. Nguyen, Y. Wang, Y. Ha, and R. Li, ''Improved chaff point generation for vault scheme in bio-cryptosystems,'' IET Biometrics, vol. 2, no. 2, pp. 48–55, Jun. 2013.
[28] X. Wu, N. Qi, K. Wang, and D. Zhang, ''A novel cryptosystem based on iris key generation,'' in Proc. 4th Int. Conf. Natural Comput., 2008, pp. 53–56.
[29] X. Wu, K. Wang, and D. Zhang, ''A cryptosystem based on palmprint feature,'' in Proc. 19th Int. Conf. Pattern Recognit., 2008, pp. 1–4.
[30] Y. Wu and B. Qiu, ''Transforming a pattern identifier into biometric key generators,'' in Proc. IEEE Int. Conf. Multimedia Expo, Jul. 2010, pp. 78–82. 890 VOLUME 4, 2016 I. Natgunanathan et al.: Protection of Privacy in Biometric Data
[31] A. Juels and M. Wattenberg, ''A fuzzy commitment scheme,'' in Proc. 6th ACM Conf. Comput. Commun. Secur., 1999, pp. 28–36.
[32] J. Bringer, H. Chabanne, G. Cohen, and B. Kindarji, ''Theoretical and practical boundaries of binary secure sketches,'' IEEE Trans. Inf. Forensics Security, vol. 3, no. 4, pp. 673–683, Dec. 2008.
[33] C. Rathgeb and A. Uhl, ''Context-based texture analysis for secure revocable iris-biometric key generation,'' in Proc. 3rd Int. Conf. Imag. Crime Detect. Prevent., 2009, pp. 1–6.
[34] A. Teoh and J. Kim, ''Secure biometric template protection in fuzzy commitment scheme,'' IEICE Electron. Exp., vol. 4, no. 23, pp. 724–730, Dec. 2007.
[35] Kumar, S., Singh, S.K., Singh, A.K., Tiwari, S. and Singh, R.S., 2018. Privacy preserving security using biometrics in cloud computing. Multimedia Tools and Applications, 77(9), pp.11017-11039.
[36] Haghighata M, Zonouzb S, Abdel-Mottaleba M (2015) CloudID: trustworthy cloud-based and crossenterprise biometric identification. Expert Syst Appl 42(21):7905–7916
[37] Li, P., Li, T., Yao, Z.A., Tang, C.M. and Li, J., 2017. Privacy-preserving outsourcing of image feature extraction in cloud computing. Soft Computing, 21(15), pp.4349-4359.
[38] Jegede A, Udzir NI, Abdullah A, Mahmod R (2015) Face Recognition and Template Protection with
[39] Shielding Function. International Journal of Security and Its Applications 9(12):149–164.
[40] Huang, H., Zhu, P., Xiao, F., Sun, X. and Huang, Q., 2020. A block chain-based scheme for privacy-preserving and secure sharing of medical data. Computers & Security, 99, p.102010.
[41] Chenthara, S., Ahmed, K., Wang, H., Whittaker, F. and Chen, Z., 2020. Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology. Plos one, 15(12), p.e0243043.
[42] Firoozjaei, M.D., Lu, R. and Ghorbani, A.A., 2020. An evaluation framework for privacy-preserving solutions applicable for blockchain-based internet-of-things platforms. Security and Privacy, 3(6), p.e131.
[43] Y.-J. Chang, W. Zhang, and T. Chen, ''Biometrics-based cryptographic key generation,'' in Proc. IEEE Int. Conf. Multimedia Expo, Jun. 2004, pp. 2203–2206.
[44] T. Scheidat, C. Vielhauer, and J. Dittmann, ''An iris-based intervalmapping scheme for a biometric key generation,'' in Proc. 6th Int. Symp. Image Signal Process. Anal., 2009, pp. 511–516.
[45] S. Hoque, M. Fairhurst, and G. Howells, ''Evaluating biometric encryption key generation using handwritten signatures,'' in Proc. IEEE Symp. Bio-Inspired Learn. Intell. Syst.Secur. Aug. 2008, pp. 17–22.
[46] Y. Sutcu, H. T. Sencar, and N. Memon, ''A secure biometric authentication scheme based on robust hashing,'' in Proc. 7th Workshop MultimediaSecur., 2005, pp. 111–116.
[47] X. Boyen, ''Reusable cryptographic fuzzy extractors,'' in Proc. 11th ACM Conf. Comput. Commun. Secur. 2004, pp. 82–91.
[48] M. Blanton and M. Aliasgari, ''Analysis of reusability of secure sketches and fuzzy extractors,'' IEEE Trans. Inf. Forensics Security, vol. 8, no. 9, pp. 1433–1445, Sep. 2013.
[49] W. Yang, J. Hu, and S. Wang, ''A Delaunay triangle-based fuzzy extractor for fingerprint authentication,'' in Proc. IEEE 11th Int. Conf. Trust, Secure. Privacy Comput. Commun. Jun. 2012, pp. 66–70.
[50] Q. Li, M. Guo, and E.-C. Chang, ''Fuzzy extractors for asymmetric biometric representations,'' in Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit.

Workshops, Jun. 2008, pp. 1–6.
[51] A. T. B. Jin, D. N. C. Ling, and A. Goh, ''BioHashing: Two-factor authentication featuring fingerprint data and tokenized random number,'' Pattern Recognit., vol. 37, no. 11, pp. 2245–2255, Apr. 2004.
[52] T. Connie, A. Teoh, M. Goh, and D. Ngo, ''PalmHashing: A novel approach for dual-factor authentication,'' Pattern Anal. Appl., vol. 7, no. 3, pp. 255–268, Aug. 2004.
[53] S. C. Chong, A. B. J. Teoh, and D. C. L. Ngo, ''Iris authentication using privatized advanced correlation filter,'' in Proc. Int. Conf. Biometrics, 2006, pp. 382–388.
[54] A. B. J. Teoh, Y. W. Kuan, and S. Lee, ''Cancellable biometrics and annotations on BioHash,'' Pattern Recognit., vol. 41, no. 6, pp. 2034–2044, 2008.
[55] L. Nanni and A. Lumini, ''Empirical tests on BioHashing,'' Neurocomputing, vol. 69, nos. 16–18, pp. 2390–2395, Oct. 2006.
[56] R. Lumini and L. Nanni, ''An improved Bio-Hashing for human authentication,'' Pattern Recognit., vol. 40, no. 3, pp. 1057–1065, Mar. 2007.
[57] L. Nanni and A. Lumini, ''Local binary patterns for a hybrid fingerprint matcher,'' Pattern Recognit., vol. 41, no. 11, pp. 3461–3466, Nov. 2008.
[58] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, ''Generating cancelable fingerprint templates,'' IEEE Trans. Pattern Anal. Mach. Intell., vol. 29, no. 4, pp. 561–572, Apr. 2007.
[59] S. G. Kanade, D. Petrovska-Delacrétaz, and B. Dorizzi Enhancing Information Security and Privacy: Combining Biometrics & Cryptography (Synthesis Lectures on Information Security, Privacy, and Trust). New York, NY, USA: Morgan & Claypool Publishers, 2012.
[60] Q. Feng, F. Su, A. Cai, and F. Zhao, ''Cracking cancelable fingerprint template of Ratha,'' in Proc. Int. Symp. Comput. Sci. Comput. Technol., 2008, pp. 572–575.
[61] A. B. J. Teoh and C. T. Yuang, ''Cancelable biometrics realization with multispace random projections,'' IEEE Trans. Syst., Man, Cybern. B, Cybern, vol. 37, no. 5, pp. 1096–1106, Oct. 2007.
[62] Y. Wang and D. Hatzinakos, ''On random transformations for changeable face verification,'' IEEE Trans. Syst., Man, Cybern. B, Cybern., vol. 41, no. 3, pp. 840–854, Jun. 2011.
[63] C. Rathgeb, F. Breitinger, and C. Busch, ''Alignment-free cancelable iris biometric templates based on adaptive bloom filters,'' in Proc. IEEE Int. Conf. Biometrics, Jun. 2013, pp. 1–8.
[64] P. P. Paul and M. Gavrilova, ''Multimodal cancelable biometrics,'' in Proc. IEEE 11th Int. Conf. Cognit. Inform. Cognit.Comput., Aug. 2012, pp. 43–49.
[65] S. Vasuhi, V. Vaidehi, N. T. N. Babu, and T. M. Teresa, ''An efficient multimodal biometric person authentication system using fuzzy logic,'' in Proc. IEEE Int. Conf. Adv.Comput., Dec. 2010, pp. 74–81.
[66] S. Awang, R. Yusof, M. F. Zamzuri, and R. Arfa, ''Feature level fusion of face and signature using a modified feature selection technique,'' in Proc. Int. Conf. Signal-Image Technol. Internet-Based Syst., 2013, pp. 706–713.
[67] M. F. Nadheen and S. Poornima, ''Fusion in multimodal biometric using iris and ear,'' in Proc. IEEE Int. Conf. Inf. Commun. Technol., Apr. 2013, pp. 83–87.
[68] P. P. Paul and M. Gavrilova, ''Rank level fusion of multimodal cancelable biometrics,'' in Proc. IEEE 13th Int. Conf. Cognit. Inform. Cognit.Comput. Aug. 2014, pp. 80–87.
[69] L. Yuan, ''Multimodal cryptosystem based on fuzzy commitment,'' in Proc. IEEE 17th Int. Conf. Comput. Sci. Eng., Dec. 2014, pp. 1545–1549.
[70] J. Bringer, H. Chabanne, and B. Kindarji,''The best of both worlds: Applying secure sketches to cancelable biometrics,'' Sci. Comput. Program. vol. 74, nos. 1–2, pp. 43–51, Dec. 2008.
[71] W. J. Wong, M. L. D. Wong, and A. B. J. Teoh, ''A security- and privacydriven hybrid biometric template protection technique,'' in Proc. Int. Conf. Electron., Inf. Commun., 2014, pp. 1–5.
[72] M. M. Monwar and M. L. Gavrilova, ''Enhancing security through a hybrid multibiometric system,'' in Proc. IEEE Int. Conf. Comput. Intell. Biometrics, Theory, Algorithms, Appl., Mar./Apr. 2009, pp. 84–91.
[73] H.-H. Zhu, Q.-H. He, and Y.-X. Li, ''A two -step hybrid approach for voiceprint-biometric template protection,'' in Proc. IEEE Int. Conf. Mach. Learn., Jul. 2012, pp. 560–565.
[74] R. L. Rivest, L. Adleman, and M. L. Dertouzos, ''On data banks and privacy homomorphisms,'' Found. Secure Comput., vol. 4, no. 11, pp. 169–180, 1978.
[75] C. Gentry, ''Fully homomorphic encryption using ideal lattices,'' in Proc. 41st Annu. ACM Symp. Theory Comput., 2009, pp. 169–178.
[76] C. Gentry and S. Halevi, ''Implementing Gentry's fully-homomorphic encryption scheme,'' in Proc. 30th Annu. Int. Conf. EUROCRYPT, 2011, pp. 129–148.
[77] T. Plantard, W. Susilo, and Z. Zhang, ''Fully homomorphic encryption using hidden ideal lattice,'' IEEE Trans. Inf. Forensics Security, vol. 8, no. 12, pp. 2127–2137, Dec. 2013.
[78] P. Paillier, ''Public-key cryptosystems based on composite degree residuosity classes,'' in Proc. EUROCRYPT, 1999, pp. 223–238.
[79] M. Osadchy, B. Pinkas, A. Jarrous, and B. Moskovich, ''SCiFI—A system for secure face identification,'' in Proc. IEEE Int. Conf. Secur. Privacy, May 2010, pp. 239–254.
[80] M. O. Rabin, ''How to exchange secrets with oblivious transfer,'' Aiken Comput. Lab, Harvard Univ., Cambridge, MA, USA, Tech. Rep. TR-81, 1981.
[81] A. C.-C. Yao, ''How to generate and exchange secrets (extended abstract),'' in Proc. 27th Annu. Symp. Found. Comput. Sci., 1986, pp. 162–167.
[82] M. Blanton and P. Gasti, ''Secure and efficient protocols for iris and fingerprint identification,'' in Proc. 16th Eur. Conf. Res. Comput. Secur., 2011, pp. 190–209.
[83] H. Chun, Y. Elmehdwi, F. Li, P. Bhattacharya, and W. Jiang, ''Outsourceable two-party privacy-preserving biometric authentication,'' in Proc. 9th ACM Symp. Inf., Comput. Commun. Secur, 2014, pp. 401–412.
[84] P. Bogetoft et al., ''Secure multiparty computation goes live,'' in Financial Cryptography and Data Security (Lecture Notes in Computer Science). New York, NY, USA: Springer, 2009, pp. 325–343.
[85] K. Simoens, J. Bringer, H. Chabanne, and S. Seys, ''A framework for analyzing template security and privacy in biometric authentication systems,'' IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 833–841, Apr. 2012.
[86] W. J. Scheirer and T. E. Boult, ''Cracking fuzzy vaults and

biometric encryption,'' in Proc. IEEE Int. Conf. Biometrics, Sep. 2007, pp. 1–6. VOLUME 4, 2016 891 I. Natgunanathan et al.: Protection of Privacy in Biometric Data.

[87] A. Adler, ''Reconstruction of source images from quantized biometric match score data,'' in Proc. Int. Conf. Biometrics, Sep. 2004, pp. 43–98.

[88] P. Mihăilescu, A. Munk, and B. Tams, ''The fuzzy vault for fingerprints is vulnerable to brute force attack,'' in Proc. BIOSIG, vol. 155. 2009, pp. 43–54.

[89] L. Lai, S.-W. Ho, and H. V. Poor, ''Privacy–security trade-offs in biometric security systems—Part II: Multiple use case,'' IEEE Trans. Inf. Forensics Security, vol. 6, no. 1, pp. 140–151, Mar. 2011.

[90] J. Bringer, H. Chabanne, and C. Morel, ''Shuffling is not sufficient: Security analysis of cancelableiriscodes based on a secret permutation,'' in Proc. IEEE Int. Conf. Biometrics, Sep./Oct. 2014, pp. 1–8.

[91] A. Nagar and A. K. Jain, ''On the security of non-invertible fingerprint template transforms,'' in Proc. 1st IEEE Int. Workshop Inf. Forensics Secur., Dec. 2009, pp. 81–85.

[92] R. Ahlswede and I. Csiszàr, ''Common randomness in information theory and cryptography—Part I: Secret sharing,'' IEEE Trans. Inf. Theory, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

[93] R. Ahlswede and I. Csiszàr, ''Common randomness in information theory and cryptography—Part II: CR capacity,'' IEEE Trans. Inf. Theory, vol. 44, no. 1, pp. 225–240, Jan. 1998.

[94] JTC1 SC27 IT Security Techniques: Biometric Information Protection, document ISO/IEC 24745, Intl Organization for Standardization, 2011.

[95] JTC1 SC37 Biometrics, Parts 1-7: Biometric Performance Testing and Reporting, document ISO/IEC 19795, Intl Organization for Standardization, 2012.

[96] Performance Testing of Biometric Template Protection Schemes, document WD 30136, ISO/IEC working draft, 2014.

[97] F. Enbo, H. Caiyun, and L. Jiayong, ''Auto-aligned sharing fuzzy fingerprint vault,'' China Commun., vol. 10, no. 10, pp. 145–154, Oct. 2013.

[98] Spooren, J., Vissers, T., Janssen, P., Joosen, W. and Desmet, L., 2019, December. Premadoma: An operational solution for DNS registries to prevent malicious domain registrations. In Proceedings of the 35th Annual Computer Security Applications Conference (pp. 557-567).

[99] DASH, P., KARIMIBIUKI, M. and PATTABIRAMAN, K., Stealthy Attacks Against Robotic Vehicles Protected by Control-based Intrusion Detection Techniques. January 2021, Article No.: 7, pp 1–25https://doi.org/10.1145/3419474

[100] Toshinori Usui, Yuto Otsuki, Tomonori Ikuse, Yuhei Kawakoya, Makoto Iwamura, Jun Miyoshi, Kanta Matsuura, Automatic Reverse Engineering of Script Engine Binaries for Building Script API Tracers.