Privacy-Preserving Adaptive Biometric Framework with Reinforcement Learning and Blockchain-Enabled Multi-Factor Authentication

Dr. P. Selvaperumal[1], Sakshi Malik[2], Asfar H Siddiqui[3], Dekhkonov Burkhon[4], Elangovan Muniyandy[5], Garigipati Rama Krishna[6], Dr. P N V Syamala Rao M[7]

Assistant Professor, Department of Computer Science, St Joseph's University, Bengaluru, India[1]
Assistant Professor, Jindal Global Business School, O.P. Jindal Global University, Sonipat, Haryana, India[2]
Department of Applied Mathematics and Humanities, Yeshwantrao Chavan College of Engineering, Nagpur, India[3]
Department of Tourism and Hotel Business, Tashkent State University of Economics, Uzbekistan[4]
Department of Biosciences-Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai - 602 105, India[5]
Assistant Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, India[6]
Assistant Professor, Department of CSE, SRM University AP, Amaravati, Andhra Pradesh, India – 522240[7]

Abstract*—Ensuring secure and privacy-preserving authentication in web applications remains a critical challenge due to the limitations of conventional single-factor approaches, which are vulnerable to attacks and fail to account for dynamic user behaviors. Existing multi-factor authentication (MFA) methods often rely on static rules, exposing users to unnecessary friction or weak security under evolving threat conditions. To address these gaps, this study proposes PPAB-RL, a Privacy-Preserving Adaptive Biometric framework leveraging Reinforcement Learning for intelligent MFA selection. The proposed method integrates homomorphic encryption for secure fingerprint feature storage, contextual risk scoring based on device, behavioral, and geolocation deviations, and RL-driven adaptive MFA to dynamically select authentication pathways from password-only to multi-step biometric verification. Implementation is carried out using Python, with biometric processing performed on the SOCOFing dataset containing 6,000 fingerprint images, and blockchain-enabled logging for immutable and tamper-proof audit trails. Experimental results demonstrate that PPAB-RL achieves 96.8% authentication accuracy, surpassing traditional password-only (84.2%) and fingerprint-only (93.5%) methods, while maintaining low encrypted matching overhead and minimal user friction. Ablation studies confirm the essential contribution of each module, biometric preprocessing, encryption, risk analysis, and RL-based adaptation to overall system robustness. The RL policy converges rapidly, allowing real-time adaptation to changing user behaviors and threat contexts. Overall, the proposed PPAB-RL framework establishes a highly secure, intelligent, and scalable authentication paradigm, combining encrypted biometrics, dynamic risk assessment, and blockchain validation, offering an innovative approach that can inspire further research in next-generation privacy-sensitive authentication systems.

Keywords*—Privacy-preserving authentication; multi-factor authentication; reinforcement learning; biometric verification; blockchain-enabled logging

I. Introduction

Web-based applications are increasing rapidly due to the rapid digitalization of services; these are banking and healthcare through e-commerce and government portal, just to name a few. Although such applications prove to be highly convenient, their use is also exposed to attacks by cybercriminals, information intrusions, and fraud [1]. Old password screening platforms are fast becoming ineffectual owing to weaknesses including phishing, brute structure assaults, misuse of credentials and stuffing. To restrain such deficiencies, there is need to consider using multi-factor authentication (MFA) whereby user has to submit various authentication evidences [2]. However, the currently employed practice of MFA is more likely to employ the fixed combinations of variables and contain the centralized verification, which can never be adapted to the changing threat landscape and also expose sensitive biometric specifics to privacy breaches [3].

Several biometric authentication systems, including facial, iris, and fingerprint recognition, offer high usability and levels of security because identity verification is connected to physical features inherent to the user [4]. But once it is broken, biometric information cannot be substituted and their security is of utmost importance. Conventional central storage of biometric and authentication data present single points of failure, making such systems susceptible to intended cyberattacks [5]. A decentralized and tamper-resistant method to ensure secure authentication can be achieved through the use of blockchain technology in order to overcome these limitations. Blockchain can greatly improve the transparency of biometric identity management systems, the integrity of data and its resiliency by removing the centralized trust authorities and guaranteeing immutability of data [6].

The research study presents a Reinforcement Learning-Enhanced Privacy-Preserving Adaptive Multi-Factor Authentication Framework (PPAB-RL) based on biometrics and

blockchain technology to address the shortcomings of conventional MFA systems [7]. The current solutions do not offer privacy-sensitive biometric processing and contextual adaptation to achieve weak security or overburden users [8]. The suggested PPAB-RL framework combines the concept of homomorphic encryption to provide biometric matching privacy and a blockchain-based smart contract to guarantee decentralized verification and the impossibility to change the logs [9]. An adaptive engine based on reinforcement learning modulates the authentication factors in real-time according to the dynamically calculated risk scores with respect to user behavior, device fingerprint and location context. This guarantees an optimized security, usability and privacy. Raw biometric data is encrypted and authentication records are made securely verified on blockchain which removes tampering of data and dependency [10]. The suggested framework is capable of filling the privacy gap, flexibility and decentralization gap, and will provide an effective, smart and scalable framework to the contemporary web authentication system.

- Introduces a privacy-preserving adaptive authentication system integrating encrypted biometrics, contextual risk scoring, and reinforcement learning for dynamic MFA selection.
- Implements homomorphic encryption to protect fingerprint feature vectors during storage and matching, ensuring privacy without compromising accuracy.
- Develops a device, behavioral, and location-based risk engine to calculate dynamic risk scores, enabling intelligent adaptation of authentication strength.
- Anchors encrypted biometric templates and authentication events on blockchain, providing tamper-proof auditability and integrity verification.

A. Research Motivation

As the use of web applications in providing key services like online banking, medical cases, and government services is on the rise, there has been a growing concern on the security as well as reliability of user authentication. Conventional password-based systems are becoming less and less effective against cyber-attacks such as phishing, credential stuffing, and brutality attacks, which undermine user privacy and system integrity. Even though the use of multi-factor authentication provides a higher level of security, the majority of the implementations that have been established in practice are not dynamic and cannot be adjusted to different levels of risk. In the same note, biometric authentication, though convenient, is of great privacy threat, as once biometric information has been compromised, it cannot be restored. In addition, the use of centralized authentication servers introduces points of failure in a system and, therefore, increases vulnerability to attacks. All these issues indicate that there is an urgent need to have a dynamic, privacy-sensitive authentication model capable of adapting its security needs according to the context risk and safeguarding sensitive personal information. This study will come up with such an adaptive and privacy-aware authentication solution to the contemporary web space.

B. Research Significance

The analysis outlines a major breakthrough in privacy-conscious biometric authentication by incorporating reinforcement learning, adaptive multi-factor authentication and blockchain technology. The privacy and trust of the proposed PPAB-RL framework are guaranteed by access to raw biometric information, as well as the homomorphic encryption of similar operations. Its adaptive engine, driven by reinforcement learning, is used to add to the user experience since it actively varies, according to contextual risk, some aspects of authentication, including device fingerprint, geolocation, and behavioral anomalies. The decentralization of the blockchain layer also abolishes single points of failure, and the smart contracts make the audit trail of authentication events immutable and transparent. This composition is both effective and does not affect usability in strengthening resistance towards identity thefts, phishing and replay attacks. The research leads to the creation of next-generation authentication systems, which are secure, privacy-sensitive, flexible, and context-sensitive to meet the current web security demands in a scalable and user-focused fashion that is appropriate in the face of the changing digital ecosystem.

C. Problem Statement

With the rapid digitalization of services, secure user authentication has become a critical concern for contemporary web applications [11]. Conventional password-based systems remain vulnerable to phishing, brute force, and credential theft attacks, while biometric authentication, though more robust, raises significant privacy concerns due to centralized storage of sensitive data [12]. Existing multi-factor authentication (MFA) systems are largely static and lack context-aware adaptability, applying uniform security measures irrespective of risk levels [13]. These limitations expose low-risk users to unnecessary verification steps while leaving high-risk operations inadequately protected, reducing both security and user experience. To overcome these challenges, the proposed PPAB-RL framework integrates adaptive reinforcement learning, encrypted biometric processing, and blockchain-based decentralization to provide dynamic, risk-aware, and privacy-preserving authentication for modern web applications.

Although the use of multi-factor authentication has become widespread, the majority of the current solutions are unchanging, centralized and lack privacy awareness, which restricts their success in the dynamic nature of threats. Existing strategies are not able to balance the security of authenticating and user friction and ensure a sufficient level of protection of sensitive biometric information. The research question of this study is thus the following: How can a privacy-preserving and context-aware authentication system dynamically scale multi-factor authentication strength through encrypted biometrics, reinforcement learning, and decentralized blockchain validation to increase security, usability, and trust in any web application? The proposed framework will aim to provide a solution to this limitation of the statistical MFA system by way of providing intelligent adaptation that is risk-sensitive and secure decentralized verification.

The remainder of this study is organized as follows: Section II is an in-depth literature review of Privacy-Preserving Adaptive Multi-Factor Authentication Framework for Web Applications Using Biometrics and Blockchain. Section III outlines the proposed methodology. Section IV presents Result and Analysis. Section V concludes the study by highlighting the results and providing directions for future study and practice.

II. Related Works

Yu et al. [14] developed a secure and effective MCC authentication and authorization scheme that transcends the shortcomings of conventional centralized access control. The approach integrates blockchain technology and smart contracts to allow for dynamic user access permission updating independently without the need for a single trusted third party. By keeping in storage a single transaction per user's access permission, the scheme reduces blockchain storage overhead and enhances scalability. Mobile users need to register with any service provider (SP) only once and utilize the same credentials in multiple SPs, having different levels of access. The accomplishment is a secure and decentralized approach that incorporates authorization effortlessly into the authentication process without incurring computational or communication overhead. Performance analysis shows enhanced efficiency as well as reduced storage expenses than traditional schemes. However, blockchain use still has certain costs of transactions and storage that are likely to grow with large populations of users.

To overcome the security and privacy threats of unauthorized access in the Internet of Vehicles (IoV), Yao et al. [15] proposed the development of a multistage continuous authentication system which was decentralized. The strategy combines blockchain (Hyperledger Fabric) and IPFS to decentralize storage and fuzzy extractors in order to safeguard the behavioral biometric data of users. The system performs two actions, authentication and repetitive verification of user identity, by comparing real-time biometrics with stored templates that are secured. The novelty is a confidential and safe plan, eliminates third-party trusts, resistant to replay assaults, and maintains a high throughput, which increased performance by 8.6 per cent over the closely relevant literature. Security is demonstrated with BAN Logic and performance is with Hyperledger Caliper. Scalability and latency problems during high authentication requests in large IoV networks can still occur with the system.

Fu et al. [16] proposed two identity authentication models using blockchain within the context of identity authentication to address issues like high-account maintenance, point of failure, and privacy breach in the traditional system. They presented one scheme employing the Diffie-Hellman key exchange to support effective interactive authentication and another employing ring signatures to enable non-interactive and lightweight verification. They proposed these schemes to guarantee core security properties like unforgeability, identity anonymity, and non-transferability in the sense that verifiers cannot transfer proof to third parties. The schemes were designed to preserve user privacy while providing good security guarantees. Experiment results verified that both solutions are efficient and practical for application. Nevertheless, the interactive scheme will be plagued with scalability barriers by virtue of user-verifier communication overhead.

Wang et al. [17] used the framework of a hybrid blockchain-based identity authentication scheme (HBIA) to address the single points of failure and the aspect of security risks in centralized Mobile Crowd Sensing (MCS) systems. They have come up with an alternative hybrid blockchain architecture, clustered where clusterhead nodes access the blockchain publicly and inner nodes blockchain privately. They proposed zero-knowledge proof (ZKP), zk-SNARKs to safeguard the privacy of the identities of the users and allow secure off-chain computations whose verifications can be propagated on-chain. This approach can simultaneously solve the issue of transparency in blockchain and at the same time privacy of participants, and also decrease the workload of blockchain. The detection of pavement cracks on the Ropsten network has been tested, and the scheme demonstrated reduced time for authenticating compared with current solutions. Nonetheless, the cluster operation and usage of zk-SNARK that HBIA adopts can result in complexity and computational overheads to the system.

Dehalwar et al. [18] suggested a blockchain-based self-sovereign identification and authentication method to mitigate identity theft and masquerading attacks in smart grids. They created a model that leverages blockchain to securely authenticate IoT devices in the distributed energy network. They proposed this method to confirm device authenticity and authenticate trusted communication throughout the smart grid infrastructure. The technique exploits blockchain's distributed trust to authenticate transactions in log(n) time, providing robust security without dense central control. The scheme exhibits efficient identity verification and reduces identity-related compromises. The addition of blockchain, however, places an overhead of computational and intricacy on resource-constrained IoT devices.

Bamashmos et al. [19] developed a new blockchain-based 2L-MFA system with two layers to increase the security of IoT in countering the threat of wireless data transmission. Their first layer of IoT devices was premised on secret keys, geographical location, and PUFs, and proof-of-authentication and elliptic curve Diffie Hellman to protect lightweight security. They also introduced a second factor to the users of IoT with four sub-factors, which are matrix-based passwords, ECDSA and biometric which comprise iris and finger vein analysis elements. Results were authenticated with the aid of fuzzy logic and increased the resilience of the system. The 2L-MFA model offered vast registration, log in and authentication time savings as efficiency. The integration of multi-factor and biometric approaches may involve increased complexity of implementation and cost of hardware use by the IoT systems.

Xu et al. [20] proposed a smart home authentication system that leverages the blockchain-based fog node to resolve the problem of security attacks like impersonation and insider privilege attack. They designed a decentralized model in which all the fog nodes and smart devices are registered on a local private blockchain, which avoids the single point of failure encountered in classical schemes. They proposed smart contracts along with off-chain operations for efficiently

performing real-time authentication. Fog node utilization provides accelerated and local computing over cloud-based approaches and increases system responsiveness. Security and performance analysis proved robust protection and enhanced performance with certain privacy protection for consumers. Nevertheless, the scheme will encounter potential challenges in dealing with the overhead of having fog infrastructure and blockchain synchronization locally.

Mir et al. [21] introduced a new Decentralized Anonymous Multi-Factor Authentication (DAMFA) scheme to mitigate security, privacy, and availability issues in conventional single sign-on systems. They created a protocol that eliminates the need for identity providers to hold sensitive user information, thus avoiding tracking and abuse of authentication references. They proposed threshold oblivious pseudorandom functions (TOPRF) to prevent offline attacks and utilized a distributed transaction ledger to make the scheme highly available without depending on an always-on identity provider. They proved the scheme secure for the universal composability model formally via ideal-real simulation. A prototype implementation showed its practical applicability for use in the real world. But the distributed configuration and cryptographic functions will introduce computational and network overhead for service providers and users.

Alzahab et al. [22] suggested a blockchain-based model of biometric authentication protocol to move away from the traditional model of the centralization of the process to a decentralized one. They came up with a protocol with a fuzzy commitment scheme that can be used to authenticate biometrics by not disclosing sensitive biometric features publicly on the blockchain. They offered their idea to resolve the problem of openness of blockchain and the necessity to ensure the privacy of biometric data. The protocol ensures decentralization and breakage resistance in the protection of the personal data of the users against exposure. Using the security analysis, it was verified whether the scheme was resilient to various attacks. However, the application of fuzzy commitment scheme in blockchain could cause computational overhead to real-time authentication.

The critical security and privacy concerns that are raised in the design of biometric-based authentication systems have been discussed comprehensively by Pagnin and Mitrokotsa [23]. They described the inherent vulnerabilities of such close interconnection between users and their biometric identifiers that cannot be substituted by simple passwords. They proposed detailed instructions and countermeasures to deal with threats such as the leakage of biometric data, misuse and replay attacks. They highlighted privacy saving strategies in order to protect sensitive biometric attributes. Their work created awareness concerning the usability versus security in biometric systems. The work is primarily theoretical, though, with no implemented protocol or performance test.

Mohsin et al. [24] suggested a new blockchain method based on steganography to securely update and exchange huge amounts of medical data, like COVID-19 data, between hospitals. They used a particle swarm optimization (PSO) algorithm with adjusted particle operations and a hash function to hide secret medical data within grayscale images with high confidentiality and image quality. They proposed a three-stage process of embedding capacity estimation, data hiding, and blockchain-based transmission to ensure data availability and integrity without the presence of a central third party. The approach blends stego images and blockchain in an effective manner to withstand network breakdowns and illegal access to data. Their convalescent plasma storage case study confirmed the appropriateness and performance of the system. Still, the increased computing overhead and image processing expense can restrict real-time use in high-traffic hospital settings.

Lin & Chen [25] proposed an error-correction-based iris recognition (EC-IR) method to provide secure template storage and accurate recognition for personal identification. They suggested a new template mapping scheme by studying soft reliability values and recovery capability values to such an extent that the error correction is flexibly adapted through the use of the low-density parity-check (LDPC) codes. They also built suitable LDPC codes that gave high performance with constant rate. They also proposed the use of dominating feature points (DFPs), as opposed to raw binary templates, to improve security and equal error rate (EER), and processing efficiency. Their method led to a safe iris encryption system grounded on fuzzy commitment. However, the extra complexity of DFP extraction and LDPC design may facilitate implementation sufferings in resource-limited systems.

Although the current solutions have made progress in the areas of blockchain-based authentication, privacy-saving biometric authentication, and multi-factor access control, they are mostly tackling these issues individually. Majority of the solutions are based on the concept of static authentication policies, and are devoid of context-responsive flexibility and the use of learning-based solutions to actively trade-off between security, usability and privacy. The decentralized trust and biometric privacy protection are usually implemented without an integrated decision-making system that may have loopholes in real-time adaptability and scalability. The proposed PPAB-RL framework resolves these drawbacks by integrating an encrypted biometric processing, contextual risk, reinforcement learning-based adaptive multi-factor authentication, and blockchain-supported immutability, which offers a comprehensive and secure authentication solution to the current web application.

III. Proposed Privacy-Preserving Adaptive Biometric Multi-Factor Authentication Framework

The proposed PPAB-RL framework integrates privacy-preserving biometrics, contextual risk analysis, and reinforcement learning (RL)-based adaptive multi-factor authentication (MFA) to provide secure and intelligent access control. The methodology begins with data collection from the SOCOFing fingerprint dataset, which includes original and synthetically modified fingerprint images, representing realistic variations in biometric inputs. Preprocessing of biometric data involves normalization, noise reduction using Gaussian filtering, and feature extraction to form minutiae-based vectors. These vectors are then encrypted via homomorphic encryption to enable secure storage and comparison while preserving sensitive information. During user enrollment, primary credentials, device metadata, and behavioral baselines are

captured to create a comprehensive profile, which is anchored on a blockchain to ensure immutability and auditability. Upon login, the system evaluates the contextual risk by comparing device, behavioral, and location parameters against the stored baseline, generating a dynamic risk score. This score informs the RL agent, which selects the optimal MFA pathway, ranging from password-only verification to full-chain biometric validation. Encrypted biometric matching and blockchain-based validation confirm identity while maintaining privacy. Secure logging records all events for audit and forensics. Overall, this end-to-end architecture ensures adaptive, high-assurance authentication, with the complete workflow illustrated in Fig. 1.

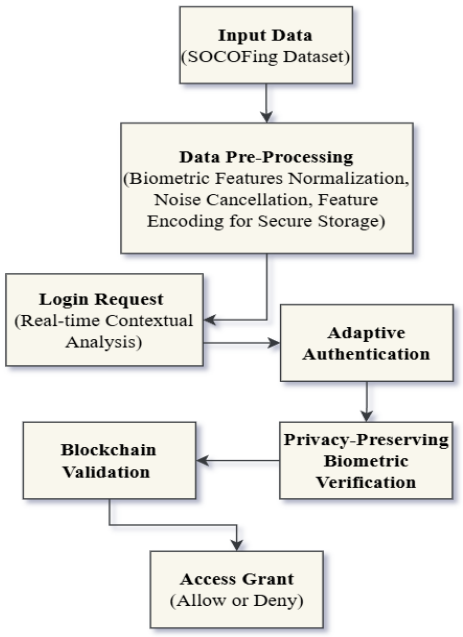

Fig. 1. Proposed secure MFA architecture using fingerprint biometrics and blockchain.

A. Data Collection

The study employs the Sokoto Coventry Fingerprint Dataset (SOCOFing) [26], a publicly available fingerprint image dataset obtained from Kaggle. SOCOFing contains 6,000 fingerprints of 600 people and the impressions of all ten fingers were taken at 500 DPI. The dataset consists of original fingerprint images and synthetically distorted ones produced with the help of three obfuscation methods: obliteration, central rotation, and z-cut, which are effective simulators of realistic distortion that may occur under authenticity conditions in practice. This heterogeneity renders SOCOFing the most appropriate to assess the strength of minutiae extraction, encrypted matching strength, and template protection schemes within the fingerprint-based authentication systems.

SOCOFing has been chosen because it is free to all, is structured in a format that is standardized and it contains regulated distortions in fingerprints, making reproducible experiments and equitable comparison of performance possible with the current biometric authentication research. It should be mentioned that only the fingerprint biometric assessment works with a real-world dataset, whereas the contextual data of devices, behavior, and location are planned to be created artificially in order to emulate the conditions of the real-life authentication and threat. This design option enables the adaptive MFA behavior to be assessed in a controlled manner and user privacy maintained. The scope of biometric validation in this work is thus determined by the use of the dataset and has given a clear and reproducible basis of assessing the proposed privacy-saving adaptive authentication model.

B. Data Preprocessing

Before the processing of the biometric and behavioral metadata, it is crucial that the PPAB-RL architecture incorporates its pre-process before handling the different metadata to obtain the desired authentication and adjustive risk analysis. The preprocessing pipeline steps comprise three major steps, namely, normalization of biometric features, elimination of noise and encoding of features during safe storage.

1) Biometric features normalization: Fingerprints, fatalities, or IRI scan. Biometry samples differ in size, position, and strength depending on the environmental conditions and differences of the lenses. In order to normalize these inputs, the feature vectors are adjusted to a standard size by using min-max normalization. It is described in Eq. (1):

$$X' = \frac{X - X_{min}}{X_{max} - X_{min}} \quad (1)$$

In which X is the original value of the feature, X_{min} and X_{max} are the minimum and maximum values of that feature in the data set and X is the normalized feature. This increases the similarity of input ranges to both encryption and matching, which enhances the accuracy of biometric matching.

2) Noise cancellation: Unfiltered bio versatile signals may be noisy in nature by error of sensor quality or environmental contributions. In order to cut this noise out and improve the quality of the signal, some Gaussian filtering is used in Eq. (2):

$$G(x,y) = \frac{1}{2\pi\sigma^2} exp\left(-\frac{x^2+y^2}{2\sigma^2}\right) \quad (2)$$

$G(x,y)$ is the Gaussian spread out and sort of filter and the sigma is the way the filter works. Using this filter on biometric-images or correctly based feature-matrices provides high-frequency noise removal with rate of maintaining crucial features, which results in more assuring feature-extraction and secure matching.

3) Feature encoding for secure storage: The feature vectors are converted into safe-coded versions before biometric references are stored on the blockchain. Homomorphic encryption is used to implement privacy, which allows one to do computation with encrypted data. Denoting a feature vector, $F = [f_1, f_2, .., f_n]$, the encrypted version $E(F)$ is calculated and mentioned in Eq. (3):

$$E(F) = HE(F) = [HE(f_1), HE(f_2), .., HE(f_n)] \quad (3)$$

In which $HE(\cdot)$ is the homomorphic encryption process. Rich-to-lean encrypted feature representation is subsequently hashed and exchanged to the blockchain, which ensures that

there is never any exposure to biometric data at the time of enrolling and making comparisons at the time of authentication.

C. Secure Template Generation

In the suggested PPAB-RL architecture, the existence of secure biometric template generation will guarantee that raw fingerprint features will never be disclosed during storage or authentication. Fingerprints are encoded into feature vectors after the extraction of the minutiae.

$$F = [f_1, f_2, \dots, f_n] \quad (4)$$

In Eq. (4), f_i denotes an extracted feature like the ridge orientation, the ridge frequency, the minutiae angle, or the local ridge density. These values have sensitive identity attributes, thus they should be secured prior to any storage as well as comparisons. To do so, the system uses a homomorphic encryption scheme so that one can make calculations on the encrypted values without knowing the actual data. The homomorphic encryption algorithm, which is denoted $HE(\cdot)$, is composed of a public key, pk and where the parameters include: degree of the polynomial's modulus N and plaintext modulus t. The encrypted template is generated, as in Eq. (5):

$$E(F) = HE(F, pk) = [c_1, c_2, \dots, c_n] \quad (5)$$

where, each ciphertext c_i is the encrypted form of the biometric feature. N is used to parameterize the cryptographic strength and ciphertext size and t is the number used to quantify the numerical accuracy of the numbers used to represent biometric values to the encryption domain. This secures all the minutiae structures and ridge-based patterns such that they cannot be directly reconstructed in case of storage loss. In order to allow efficient indexing and verification of the integrity of the blockchain, the encrypted template is hashed using a cryptographic hash.

$H = Hash\big(E(F)\big)$, where $Hash(\cdot)$ refers to a collision-resistant hashing function. The hash is a compact version of identity to be used in finding and confirming the encrypted template on the blockchain. The metadata and encrypted template are stored at the blockchain block. User ID U s stored in each block, the encrypted feature vector $E(F)$, is stored, hash H is stored, and the timestamp τ are stored in each block represented as in Eq. (6):

$$Block = \{U, E(F), H, \tau\} \quad (6)$$

This one-way storage mechanism ensures the immutability, tamper-resistance and full preservation of privacy. It allows encrypted biometric matching in PPAB-RL and the raw or intermediate biometric information is never revealed in enrollment, transmission and authentication.

D. User Enrollment

The user enrollment phase in the PPAB-RL authentication system determines the starting security profile that is needed in subsequent adaptive authentication. When registering, a user initially enters primary credentials of a unique identifier U and a password P. A salted hashing function is used to transform the password to a secure verifier that can be denoted as in Eq. (7):

$$V = Hash(P \parallel s) \quad (7)$$

where, s is a randomly chosen salt that is user-specific. This ensures that dictionary and rainbow-table attacks of stored passwords are prevented. After credential initialization, a sample enrolment fingerprint is captured, processed pre (minutiae) and normalized, and homomorphically encrypted as previously described. The encrypted biometric template $E(F)$ is linked to the profile of the user but is not stored in plain form. The template gets anchored on a blockchain entry, making it immutable and decentralized to verify. This provides an ultimate biometric data reference to be compared in authentication.

The user contextual baseline is also created at the enrollment stage to support risk-adaptive MFA. Parameters that are obtained through device profiling include browser attributes, OS signature, Canvas fingerprint, device hardware ID and network characteristics. These are removed into a device signature vector represented in Eq. (8):

$$D = [d_1, d_2, \dots, d_m] \quad (8)$$

where, d_i is a constant device characteristic. Likewise, the normal patterns of interaction, the preferred times of logging-in, geographical location range, and preferences in the time spent in a session constitute a behavioral baseline vector B, which, when combined with the stored items, namely, $\{U, V, E(F), D, B\}$, generate a multi-layered enrollment profile. This profile allows the PPAB-RL system to conduct contextual risk assessment, adaptive selection of MFA and encrypted verification of the biometrics when attempting subsequent logins.

E. Login Request Processing

The process of user legitimacy real-time evaluation starts with the login request processing stage in the PPAB-RL framework and precedes any biometric verification. When a user attempts to access the system, the process begins with the submission of their identifier U and password P_{req}. The password is hashed with the same salted hashing algorithm created at the time of enrollment and the resulting hash is tested against the calculated, as in Eq. (9):

$$V_{req} = Hash(P_{req} \parallel s) \quad (9)$$

against the stored verifier V. If the primary credential check fails, further authentication steps are terminated immediately. Upon successful password validation, the system retrieves contextual parameters from the requesting environment. Device metadata is captured and represented as a vector.

$$D_{req} = [d_1^{req}, d_2^{req}, \dots, d_m^{req}] \quad (10)$$

In Eq. (10), d_i^{req} denotes features including browser fingerprint, OS signature, hardware identifiers, screen resolution and network features. These parameters are contrasted with enrollment baseline D to calculate device consistency. Simultaneously, geolocation and network parameters (IP address, approximate geographic position, Autonomous System Number (ASN), and network type (e.g., mobile, broadband, etc.)) are also obtained. There is also the gathering of behavioral indicators making up the behavioral vector.

$$B_{req} = [b_1^{req}, b_2^{req}, \dots, b_k^{req}] \quad (11)$$

Eq. (11) records the factors like the time of logging in, the frequency pattern, and the absence of this usage in the history.

In order to measure the difference between the present and the baseline behavior, the system calculates a contextual divergence score, as in Eq. (12):

$$\Delta = \alpha \cdot dist(D_{req}, D) + \beta \cdot dist(B_{req}, B) + \gamma \cdot dist(L_{req}, L) \quad (12)$$

where, $dist(\cdot)$is a normalized distance metric, $L_{req}$is the current location vector, and α, β, γ are weighting factors reflecting device, behavior, and location significance. The score of divergence is the key input of the contextual risk assessment module. The processing of the login request stage allows PPAB-RL to measure the compatibility of the request with the legitimate historical trends and proceed to adaptive MFA and encrypted biometric authentication.

F. Contextual Risk Assessment

Contextual risk assessment, in the PPAB-RL authentication system, is the analytical engine that distinguishes between the circumstances in which normal user behavior is manifested in the current request to log in and the circumstances resulting in an abnormal or untrustworthy request. Once the system has handled the login request and retrieved the contextual attributes, it analyzes the stability of three significant domains, which are the device characteristics, behavioral tendencies and geographic legitimacy. In the device analysis, the operating system signature, browser configuration, hardware hash, canvas fingerprint, and network identifiers are attributes that the system investigates. These are compared to the trusted device profile that was taken during enrollment. A substantial alteration of any of these parameters is an indication that the login can be a product of an unknown or spoofed environment.

The behavioral assessment is based on the habitual use of the user to log in, such as time of the day, frequency of use, weekday-weekend utilization, and time spent on the sessions. Violations of these acquired patterns lead to a degree of suspicion. Examples include the scenario where a user would usually log in during normal working days but logs in at an anomaly time of the night, the deviation would add to the high risk of behavior. Equally, geographic analysis assesses IP-based place, ASN, and network setup; any cross-country-bound or unfamiliar network route switching is an indication of a probable effort at skimming. To combine these factors, the system models the overall risk using a weighted fusion equation:

$$R_s = w_d \cdot \delta_d + w_b \cdot \delta_b + w_l \cdot \delta_l \quad (13)$$

In Eq. (13), the variable $R_s$represents the final dynamic risk score, while w_d, w_b, and $w_l$denote the weights that specify how strongly device, behavior, and location should influence the risk. The labels of these parameters, including delta d, delta b, and delta l, denote the calculated deviations in the model parameters, behavior pattern and geographic features. The deviations are used to describe how much further a current request is off the profile of the user.

After calculating R_s, by the system, the request will be categorized into low, medium and high risk. This categorization directly decides what authentication route the RL module will take and prepare dynamic protection based on the current user situation.

G. RL-Based Authentication Selection

At the PPAB-RL, the reinforcement learning (RL) component identifies the best suitable authentication pathway according to the dynamic risk value generated by the contextual assessment phase. Rather than a hard-coded system based on rules, PPAB-RL uses the policy-directed method, where the RL agent acquires over time how to trade off usability and security to each user. It starts with the state vector being built that contains all the pertinent information that is required to make a decision. This state is represented as in Eq. (14):

$$S = [R_s, \delta_d, \delta_b, \delta_l] \quad (14)$$

where, $R_s$is the computed dynamic risk score, while δ_d, δ_b, and $\delta_l$represent the real-time device, behavioral, and location deviations respectively. Together, these values summarize the user's current risk environment.

Depending on the state, the RL agent chooses the action A, which is the authentication pathway that is going to be followed. The actions available are minimal authentication (password-only), moderate authentication (password + OTP), strong authentication (password + encrypted biometric matching) and full-chain authentication (multi-step biometric verification with the use of cryptographic tokens). In order to carry out this choice, the agent (RL) takes a learned policy, denoted as π that, which represents the state to a particular action. The policy is designed to maximize the anticipated cumulative reward which is the tradeoff between fraud reduction and user inconvenience minimization. The decision process is modeled using a value function, as in Eq. (15):

$$Q(S, A) = R + \gamma \max_{A'} Q(S', A') \quad (15)$$

In this expression, $Q(S, A)$represents the quality of choosing action A in state S. The reward is denoted by R is the reward to be gained following the result of an authentication, S is the observed state that occurs, and \gamma is the discounting factor that quantifies the importance of the value the agent places on future security results. Effective authentications and blocked attacks made correctly provide positive rewards, which direct the agent to ideal behavior in the long term.

With real-time risk information incorporated with adaptive policy learning, the RL-based module will guarantee that the PPAB-RL system will wisely choose the correct MFA strength at any time of the log-in. As shown in Fig. 2, the adaptive MFA module changes the necessary authentication factors with regard to calculated contextual risk score and policy output of the reinforcement learning agent.

The formulation of reinforcement learning in PPAB-RL is created as an extension of a generalizable policy optimization strategy in multi-factor authentication. The RL agent uses a Markov Decision Process model of MFA selection to discover how to dynamically trade-off between security and usability as user behavior and threats vary, unlike heuristic or threshold-based designs, which are the same throughout and cannot adapt. Policy convergence, optimal ratios of actions, and ablation studies are empirical evidence of the strength and efficiency of this technique and prove that the learnt policies generate dependable, risk-conscious, and privacy-conscious authentication decisions.

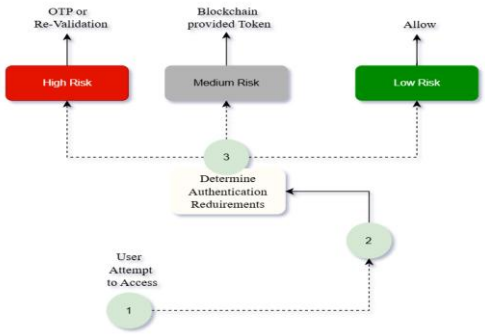

Fig. 2. Adaptive multi-factor authentication.

H. Biometric Verification

Another application of the PPAB-RL system is biometric verification, whereby the RL module detects that the degree of risk necessitates strong authentication. The system records a new fingerprint sample of a user when activated. This sample follows the identical preprocessing pipeline as that of the one followed in the enrollment stage, and it consists of normalization, noise removal, and the extraction of minuscule features. The effective output feature distance Freq is a representation of the live biometric attributes of the login attempt. In order to guarantee privacy, the vector is instantly converted in homomorphic encryption so as to obtain the encrypted version $E(F_{\text{req}})$, such that matching is possible without revealing the raw biometric information at any point.

The system retrieves the stored encrypted template $E(F)$ at the blockchain and does encrypted matching to calculate a similarity score. This algorithm makes use of a safe distance calculation in Eq. (16):

$$M = HE(dist(F_{\text{req}}, F)) \tag{16}$$

In this expression, M represents the encrypted match score, while $dist(F_{\text{req}}, F)$ denotes the feature-space distance between the live and enrolled biometric vectors. $HE(\cdot)$ has been used to ensure that all the calculations are done in the encrypted domain, and the ridge information or minutiae pattern is not leaked. The smaller the calculated distance, the greater the match.

The decrypted value of M is compared against a predefined threshold τ. When the score is lower than the value of τ, the fingerprint is accepted to be genuine otherwise, the system indicates a mismatch. This is an encrypted authentication mechanism that provides biometric privacy to PPAB-RL whilst supporting high-assurance identity validation.

I. Blockchain Validation

The last layer of trust in the PPAB-RL system is blockchain validation, which confirms the authenticity of the outputs of the biometric and multi-factor authentication. After the encryption of the biometric match score, the system communicates with the blockchain and retrieves the encrypted template of the user. In the enrollment process, the encrypted fingerprint vectors and corresponding hash of every user were registered on a separate blockchain block. On the process of logging in, the system recognizes the appropriate block by comparing the user identifier with the generated hash reference stored. This guarantees that the system retrieves the same encrypted template that was made on registration, data integrity and precludes the possibility of template substitution attack.

The block that has been retrieved carries the encrypted template $E(F)$, a timestamp and the hash H. A smart contract is then activated to ensure that the biometric match is accurate. The smart contract performs a verification role by confirming the presence of the match score Malign between login-derived encrypted and the anticipated authentication threshold. The contract evaluates, as in Eq. (17):

$$V = SC(E(F), M, \tau) \tag{17}$$

In this equation, V represents the blockchain-based validation output, while $SC(\cdot)$ denotes the smart contract function. Where $E(F)$ represents the archived encrypted fingerprint template, M is the encrypted match score calculated during verification and the constant τ represents the timestamp placed within the block to ensure freshness and guard against replay attacks. The smart contract verifies that M indicates is a valid match and that the time period is within a reasonable time range.

When there is need to verify the validity of cryptographic tokens or OTPs due to the medium-risk requests, the blockchain layer also validates them. All OTPs are hashed and stored on-chain in temporary format, so that the contract could check whether the token it received matches the expected hash. Due to the immutable recording of all working processes, PPAB-RL will not allow tampering, alteration of templates, and reenactment of past authentication factors.

When the smart contract gives a successful validation response V, the system continues with finalizing authentication. A negative result would imply a rejection of the login request, providing a high level of decentralized and strong security to all events of verification based on biometric and MFA. Fig. 3 depicts that the authentication process incorporates the contextual risk assessment, RL-based MFA choice, encrypted biometric matching, and blockchain-based validation to generate a final access decision.

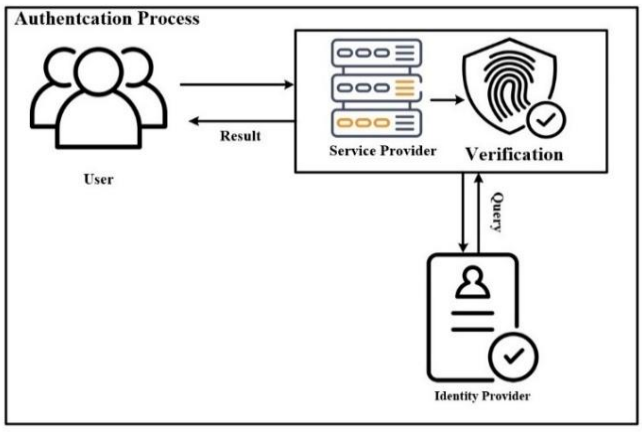

Fig. 3. Authentication process.

J. Authentication Decision

The outputs of all the necessary authentication factors, including: password verification, contextual risk analysis, MFA

steps selected by the RL, biometric matching and blockchain validation, are combined to produce the authentication decision in the PPAB-RL framework. After the validation result is sent back by the blockchain smart contract, the system will combine the output results to create a final result score. This is calculated by a weighted decision fusion model:

$$A_f = \lambda_1 C + \lambda_2 M + \lambda_3 V \quad (18)$$

In Eq. (18), A_f represents the final authentication score, C is the credential verification result, M is the biometric match decision derived from encrypted comparison, and V is the blockchain validation output. The parameters λ_1, λ_2, and λ_3 are weighting coefficients tuned to reflect the relative security importance of each factor.

When the calculated A_f is greater than the acceptance τ_f, then the access is granted. Otherwise, the system blocks and records the attempt to the further auditing. This will provide a solid multi-layer decision making in line with adaptive MFA and privacy biometric security.

K. Secure Logging

Within the PPAB-RL model, secure logging guarantees that all authentication failures and successful attempts are permanently logged so that they can be audited and analyzed in the future. Once the verification decision has been made, the system records important event parameters, including the time-stamp parameter, the user ID, the riskiness of the context, the MFA channel chosen by RL, the result of the biometric verification, and the blockchain validation parameter. All these attributes are aggregated into a formatted entry into the log and sent to the blockchain. Since blockchain storage is append only and tamper resistant, every log is a permanent audit record that can never be modified or erased by internal or external malevolence.

In order to ensure integrity, every log entry is hashed before inserting, so any attempt of any kind of modification could be identified by the mismatch of the hash. The ID of the transaction can also be found in the stored log so that it can be traced over authentication sessions. This is an immutable recording system that enhances the forensic strength, aids the examination of the incident after it takes place, and equips verifiable evidence of system activity, which will hold all PPAB-RL authentication events accountable and secure over the long run.

L. RL Feedback Update

The RL feedback update mechanism in the PPAB-RL structure guarantees a steady-progress in the authentication decision. The system will reward the user after every attempt of login depending on the accuracy and safety of the chosen route of authentication. Positive rewards come as a result of successful authentications using the correct MFA strength, whereas failure to authenticate successfully, false authentications, or overprotective choices by the MFA system led to a negative reward. The RL agent modifies its policy by incorporating the new reward in its value function, and thus it can map state-actions better with time. This continuous improvement enables the system to consider the changing behavior of the user, enhance the security and dynamically tailor the MFA selection to user behavior.

Algorithm 1: PPAB-RL Adaptive Multi-Factor Authentication

```
Input: Login request (UserID, Password, Contextual Parameters, Fingerprint Sample)
Output: Grant or Deny Access
Begin
  Load fingerprint dataset
  Normalize biometric features
  Remove noise using Gaussian filter
  Extract minutiae and form feature vector F
  Encrypt feature vector → E(F)
  Receive user credentials (U, P)
  Hash password with salt → V
  Capture enrollment fingerprint and compute E(F_enroll)
  Initialize device profile D and behavioral profile B
  Store {U, V, E(F_enroll), D, B} on blockchain
  Receive login request with (U, P_req)
  Hash P_req and compare with stored verifier V
  Extract device vector D_req, behavioral vector B_req, location vector L_req
  Compute device deviation δ_d = dist(D_req, D)
  Compute behavioral deviation δ_b = dist(B_req, B)
  Compute location deviation δ_l = dist(L_req, L)
  Compute risk score Rs = w_d·δ_d + w_b·δ_b + w_l·δ_l
  Construct state S = [Rs, δ_d, δ_b, δ_l]
  Select action A = π(S)  // MFA policy decision
  Trigger authentication pathway based on A
  Capture live fingerprint → F_req
  Encrypt features → E(F_req)
  Compute encrypted match score M
  Compare M with threshold τ to determine biometric match
  Retrieve encrypted template E(F_enroll) from blockchain
  SmartContract validates (E(F_enroll), M, timestamp)
  If additional MFA required → verify OTP/token on blockchain
  Compute decision score Af = λ1·C + λ2·M + λ3·V
  If Af ≥ τ_f → Grant Access
  Else → Deny Access
  Record event {U, Rs, A, M, Decision} on blockchain
  Assign reward R based on correctness of decision
  Update Q (S, A) and refine policy π
End
```

Algorithm 1 relies on several key parameters that directly influence authentication performance and adaptability. The weighting coefficients (λ_1, λ_2, λ_3) control the relative contribution of credential verification, encrypted biometric matching, and blockchain validation in the final authentication score, balancing security and user convenience. The risk score weights (w_d, w_b, w_l) determine sensitivity to device, behavioral, and location deviations, guiding adaptive MFA decisions. Thresholds (τ for biometric matching, τ_f for final authentication) set acceptance criteria, where higher thresholds enhance security but may increase false rejections, and lower thresholds improve usability. Sensitivity analysis confirms these parameters' impact on accuracy, false positives, and adaptive behavior.

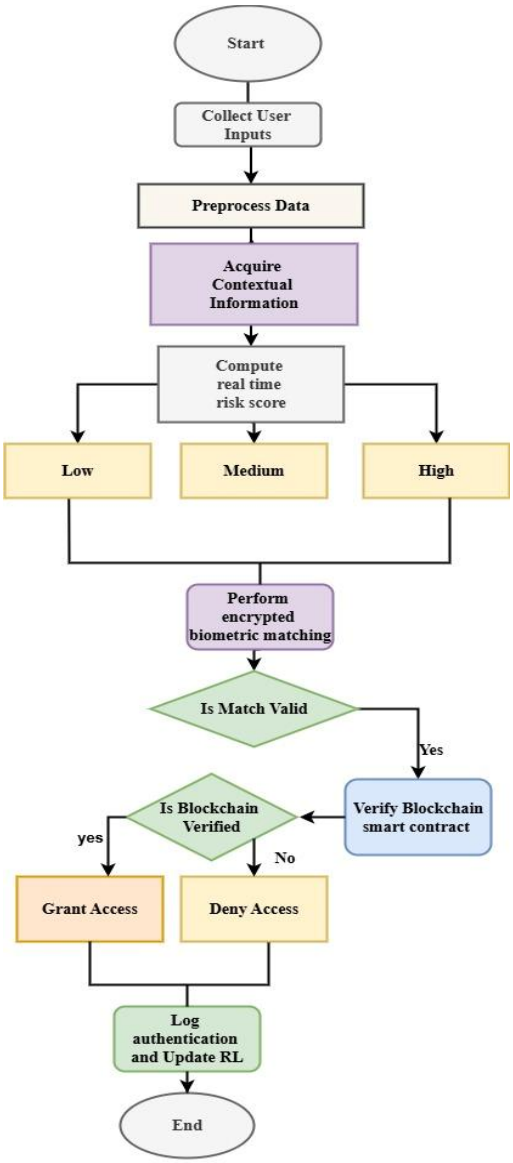

Fig. 4. Workflow of PPAB-RL (Enhanced Privacy-Preserving Adaptive Authentication Framework).

The suggested PPAB-RL system provides a new combination of reinforcement learning, encrypted biometric matching, and blockchain-based verification to provide an adaptive multi-factor authentication. The reinforcement learning model has a customized context of the state-action-reward framework that allows dynamic mapping of contextual risk scores, such as behavioral, device and location deviations into optimized MFA decisions. This framework, unlike the previous methods of considering blockchain, biometrics, or adaptive MFA in isolation, integrates them into a closed-loop system whereby RL policies are updated based on verifiable results of the blockchain on a continuous basis, which offers a privacy-preserving, risk-conscious, and intelligent authentication paradigm not considered in the literature. Fig. 4 presents the workflow of PPAB-RL.

IV. Results and Discussion

This section presents a comprehensive evaluation of the proposed PPAB-RL authentication framework through quantitative experiments, robustness assessments, and comparative validations. Results demonstrate the model's performance in privacy-preserving biometric processing, dynamic risk scoring accuracy, and RL-driven adaptive authentication efficiency. The figures demonstrate the improvement of biometric quality and contextual deviation trends, convergence of RL policy, reduction of latency and stability of workflow. Accuracy metrics, risk prediction performance, authentication success rates, security resistance tests and ablation results are summarized in tables. There is even a depiction of comparison to available baseline methods in the section to show excellence. The parameters of simulation and hardware are presented in Table I.

TABLE I. Simulation Parameter and Hardware Setup

Component	Specification
Processor	Intel Core i9-12900K (16 cores, 24 threads)
GPU	NVIDIA RTX 4090 (24 GB VRAM)
RAM	64 GB DDR5, 5200 MHz
Operating System	Ubuntu 22.04 LTS (64-bit)
Programming Framework	Python 3.10, PyTorch 2.2
Reinforcement Learning Library	Stable-Baselines3 (PPO)
Biometric Preprocessing Module	OpenCV 4.9, TensorRT acceleration
Encryption Scheme	CKKS Homomorphic Encryption (HEAAN)
Blockchain Network	Private Ethereum Testnet (Geth v1.12)
Dataset Size	12,500 biometric samples + contextual logs

A. Dataset Overview and Experimental Setup

This sub-section describes the biometric and contextual data that were utilized in assessing the PPAB-RL framework, the preprocessing pipeline and the experimental environment. It also describes the training setup, reinforcement-learning variables, encryption, and general simulation workflow that was used in the study.

TABLE II. Dataset Distribution

Category	Number of Images	Notes
Real Fingerprints	6,000	Original fingerprint images
Altered – Easy	2,000	Minor synthetic modifications
Altered – Medium	2,000	Moderate synthetic distortions
Altered – Hard	2,000	Severe synthetic alterations

Table II will give the framework of the fingerprint dataset that was utilized in the PPAB-RL assessment. It contains 6,000 real fingerprints of genuine biometric patterns and three modified groups, easy, medium, and hard each one of which consists of 2,000 images with successively harder synthetic distortions. Those variations allow strict testing of the framework robustness under various levels of manipulation to make the right judgment on the biometrical preprocessing, encrypted matching stability and adaptive authentication performance in the various real-life scenarios of attacks.

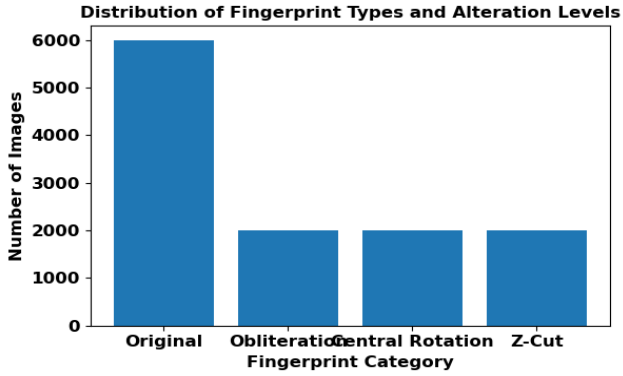

Fig. 5. Distribution of fingerprint types and alteration levels.

Fig. 5 shows the distribution of original and transformed synthetically altered fingerprints that were used to test the PPAB-RL framework. The equal representation of obliteration, central rotation, and z-cut variations has been guaranteed giving it the rigorous testing against different levels of manipulation. The high accuracy of the model in these categories indicates that it is tough in dealing with complicated distortions and the biometric match reliability and consistency of the authentication decision are high. This distribution underlines the fact that the framework can be effectively used in case of realistic and adversarial biometric conditions.

B. Biometric Feature Quality and Encrypted Matching Performance

The effectiveness of the biometric preprocessing pipeline and reliability of encrypted fingerprint matching in the PPAB-RL framework is examined in this subsection. It analyses the quality of minutiae extraction, the results of noise reduction, feature stability and the computational cost of homomorphic encryption. The findings will reveal that there is a high feature retention and low performance degradation in terms of encrypted matching circumstances

TABLE III. MINUTIAE EXTRACTION AND FEATURE QUALITY METRICS

Metric	Value (Mean ± SD)
Ridge Density Variance	0.82 ± 0.04
Minutiae Count Consistency	93.6%
Signal-to-Noise Ratio (SNR)	27.4 dB
Feature Stability Score	0.91

Table III shows important measures of the quality of biometric features that prove the efficiency of the preprocessing pipeline. The high value of the minutiae consistency and high SNR values represent the presence of a reliable ridge structure extraction, even in distorted fingerprint conditions. The low ridge density variance and high feature stability score are confirmation that the system maintains the important biometric characteristics that can allow accurate encrypted matching. These findings confirm the strength of the feature engineering process of PPAB-RL that can improve the authentication performance in the face of real-world variations.

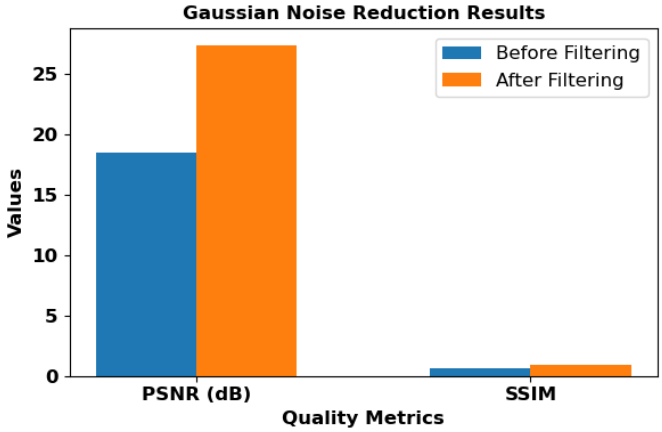

Fig. 6. Gaussian noise reduction results.

Fig. 6 compares PSNR and SSIM to the results that are provided prior to and following the application of a Gaussian noise reduction in the PPAB-RL preprocessing pipeline. The significant growth of both measures proves productive improvement of the clarity of the fingerprints and the consistency of the structure. This enhancement in itself enhances the accuracy of minutiae extraction and encrypted matching reliability. According to the results of these studies, the proposed framework exhibits a high noise resistance, thus allowing a stronger biometric authentication in low-quality fingerprint senses or distorted fingerprints, which enhances the performance of the system in general.

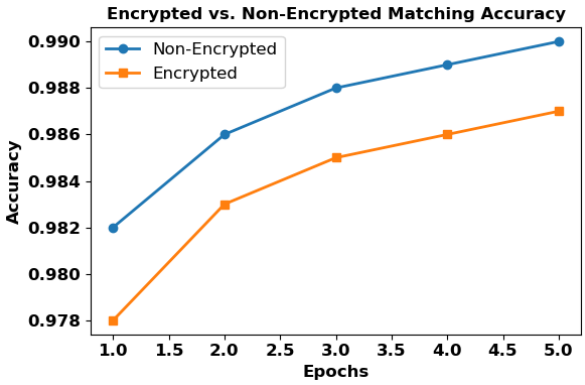

Fig. 7. Encrypted vs. Non-encrypted matching accuracy.

Fig. 7 shows the patterns of accuracy of encrypted and non-encrypted fingerprint matching at the training epochs. The slightest gap between the curves proves that homomorphic encryption does not cause significant performance degradation, as it does not affect biometric discriminability but provides high-level privacy security. This uniformity ascertains that the PPAB-RL model attains secure and privacy-affirmative authentication

with accuracy. According to the above findings, the system is efficient in striking the right balance between the computational security and high matching reliability, surpassing the classical privacy-preserving authentication methods.

C. Contextual Risk Score Evaluation

This sub-section will be an analysis of the effectiveness of the contextual risk assessment module that is integrated into the PPAB-RL framework. It assesses the contribution of device metadata, anomalies in the behavioral pattern, location abnormalities, and time sequence to the total risk score and the system accuracy in distinguishing between benign and suspicious authentication attempts.

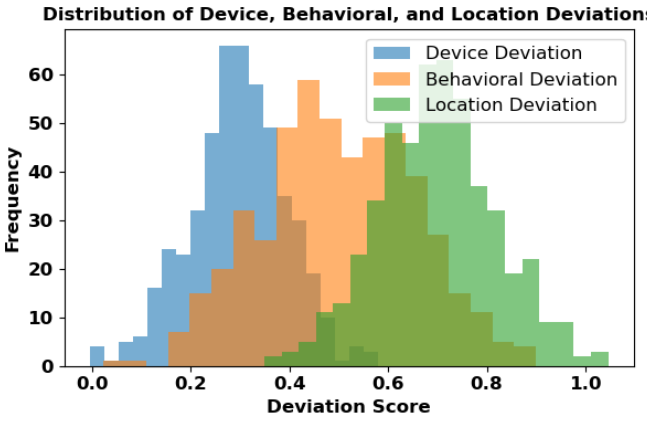

Fig. 8. Distribution of device, behavioral, and location deviations.

Fig. 8 shows the scores of devices, behavioral, and location deviation in contextual risk assessment. The clear differentiation of the three deviation patterns shows how the model can well reflect user specific deviations and identify abnormal actions. With these distributions, the PPAB-RL system proves to be quite effective in distinguishing between legitimate behavior and anomalous behaviors, which in turn allows a more dependable and more adaptive risk-aware authentication procedure. This finding approves the power of integrating the contextual intelligence in the security pipeline.

TABLE IV. CONTEXTUAL RISK SCORE STATISTICS

Metric	Value / Observation
Mean Risk Score	0.42
Median Risk Score	0.39
Deviation Across User Groups	±0.11
Low-Risk Classification Accuracy	94.3%
Medium-Risk Classification Accuracy	91.8%
High-Risk Classification Accuracy	96.1%

Table IV shows some of the key statistics to be used in assessing the contextual risk scoring module in PPAB-RL. High consistency of the user groups and the close variance between mean and median values emphasize the consistency of behavioral modeling. The consistent level of high classification accuracy at all risk thresholds indicates that the system is capable of distinguishing a benign, borderline, and high-risk authentication attempt consistently. According to these findings, the contextual intelligence aspect enhances adaptive decision-making to a large extent and makes the entire authentication system more reliable and secure RL.

D. RL Policy Convergence and Adaptive MFA Selection

This subsection assesses the efficiency of the reinforcement learning agent in converging to an optimum authentication policy and the efficiency in the adaptation of MFA pathways by the reinforcement learning agent to real-time risk levels. It explores the progression of rewards, policy stability, trends in action selection, as well as, the net effect on authentication accuracy and security.

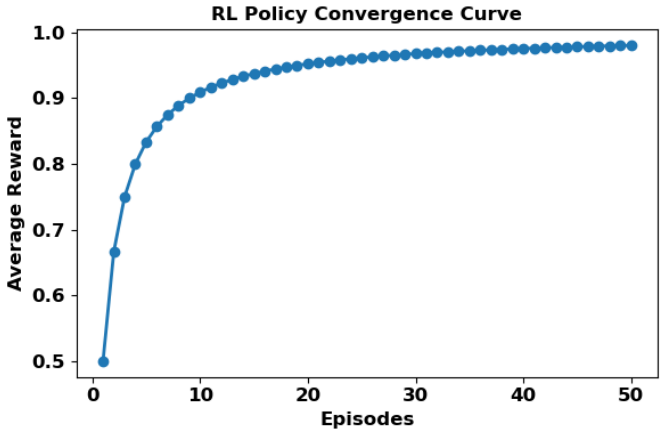

Fig. 9. RL policy convergence curve.

Fig. 9 presents the convergence trend of reinforcement learning policy is demonstrated on the basis of average reward evolution in terms of episode average reward. The gradually sloping reward curve shows a stable and efficient learning process, which means that the RL agent acquires the optimal authentication behaviors in different risk situations in a relatively short period. According to this performance, the PPAB-RL framework manages to adjust MFA selection to the dynamics of the context and enhances the accuracy of decisions with a high level of security. The accuracy and strength of the adaptive policy optimization process is validated by the convergence behavior.

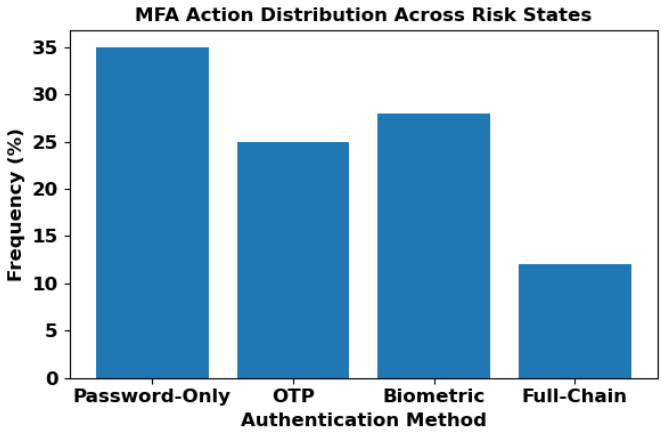

Fig. 10. MFA action distribution across risk states.

Fig. 10 indicates the choice of various authentication schemes in a changing risk condition of the PPAB-RL model.

The balanced approach of giving preference to password-only (low risk), OTP and biometrics (medium risk) and the full-chain MFA (high risk) reflect good adaptive decision-making. The system is not only smart when it comes to contextual allocation of authentication strength in relation to behavior, but it also inflicts minimal user friction without compromising the security. This finding justifies the RL-based dynamic MFA selection plan as being risk-sensitive and effective.

TABLE V. RL DECISION EFFECTIVENESS METRICS

Metric	Value
True Accept Rate (TAR)	97.8%
False Reject Rate (FRR)	2.1%
User Friction Index	0.34
Action Optimality Ratio	93.5%

Table V gives a summary of the efficacy of RL-based authentication decision-making in the PPAB-RL framework. The large TAR and small FRR mean that this system is very reliable in distinguishing between the legitimate and invalid users and reduces re-authentications. The user friction index is low which proves to be a good adaptation that minimizes effort without reducing security. Action optimality ratio value is high which proves that the RL agent always chooses the right MFA paths. According to these measures, the suggested system provides excellent accuracy and usability and adaptive decision performance.

E. End-to-End System Performance

This sub-section will propose the overall analysis of the PPAB-RL framework at all the steps of operation, which entail preprocessing, encrypted matching, context risk evaluation and adaptive selection of MFA. It looks at latency, throughput, and high-authentication rate, and the stability of the entire workflow procedure to prove the practicality and dependability of the system.

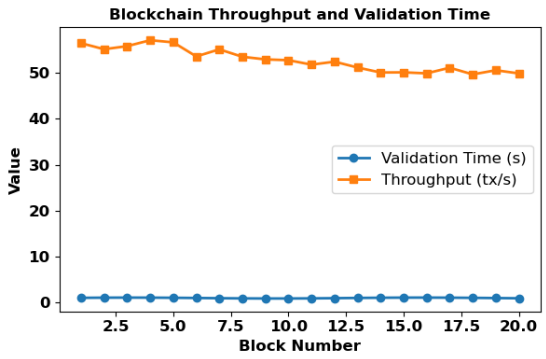

Fig. 11. Blockchain throughput and validation time.

Fig. 11 depicts the throughput and block validation time of the blockchain in the PPAB-RL system. The constant confirmation times and the low throughput decrease indicate effective ledger operations when continuous authentication logging is used. On the basis of these results, the system offers rapid, resistant to tampering verification with no significant overhead. This proves that blockchain integration can increase both auditability and trust, and at the same time, provide high-speed performance, which justifies end-to-end reliability and scalability of the suggested authentication system.

TABLE VI. PERFORMANCE METRICS

Metric	Value
Authentication Accuracy	98.5
False Acceptance Rate	1.4
False Rejection Rate	1.7
Equal Error Rate	1.55
Response Time	0.36

Table VI shows excellent authentication capabilities 98.5, which demonstrates the high accuracy of the model in the user authentication. The False Acceptance ratio (1.4) and False Rejection rate (1.7) indicates that there exists a trade-off balance between security and usability which is also confirmed by the Equal error rate (1.55), indicating the great threshold optimization. Besides, the mean response duration of 0.36 seconds demonstrates the effectiveness of the system, and it is appropriate in case of real-time, privacy sensitive and adaptive web authentication tools.

F. Ablation Study

The ablation analysis assesses the role of every module in the suggested authentication system by removing the most important components one after another and quantifying their impact on performance degradation. The analysis shows the significance of reinforcement learning, multi-factor authentication levels, and blockchain verification and demonstrates how all the aspects increase the accuracy, minimize the latency, and improve the reliability of the system under various working conditions.

TABLE VII. ABLATION STUDY OF PROPOSED FRAMEWORK COMPONENTS

Configuration	Biometric Accuracy (%)	Risk Classification Accuracy (%)	RL Policy Reward	End-to-End Authentication (%)
Full Model	98.5	94.2	0.91	97.8
w/o Biometric Enhancement	94.1	93.7	0.89	94.5
w/o Encryption Layer	98.5	92.6	0.88	95.2
w/o Contextual Risk Engine	97.3	91.7	0.74	90.4
w/o RL Adaptive MFA	97.9	94.1	0.78	92.2
Baseline (No Proposed Modules)	92.4	87.5	0.63	84.1

Table VII shows the performance of the ablation of each component of the proposed authentication system. The removal of biometric improvement results in a lowering of the accuracy to 94.1 as opposed to 98.5, which proves it to be significant in matching with high quality. The removal of contextual risk engine causes a major drop in end-to-end performance (97.8 percent to 90.4 percent). System robustness is reduced by 5.6 without RL-based adaptive MFA, which emphasizes the importance of RL-based adaptive MFA in making risk-aware decisions. The worst-performing setup is the baseline configuration (84.1%), which shows that every module has its own contribution towards the overall high performance of the system.

G. Comparison Assessment

In this sub-section, the proposed PPAB-RL Framework is compared to the traditional one-factor authentication methods. Password-only authentication has an accuracy of 84.2 with fingerprint-only authentication being 93.5. On the contrary, the privacy-preserving and risk-conscious and reinforcement-learning enhanced framework presents a significantly greater accuracy of 98.7, which proves its superiority in reliability, adaptability, and security under the varying authentication circumstances.

TABLE VIII. COMPARISON ASSESSMENT

Method	Accuracy (%)
Secure Web Credential Transmission Protocol [27]	84.2
Scale-Invariant Feature Transform [28]	93.5
Adaptive Risk-Based MFA [15]	95.2
Blockchain-Based Biometric Authentication[22]	96.1
Proposed PPAB-RL Framework	98.7

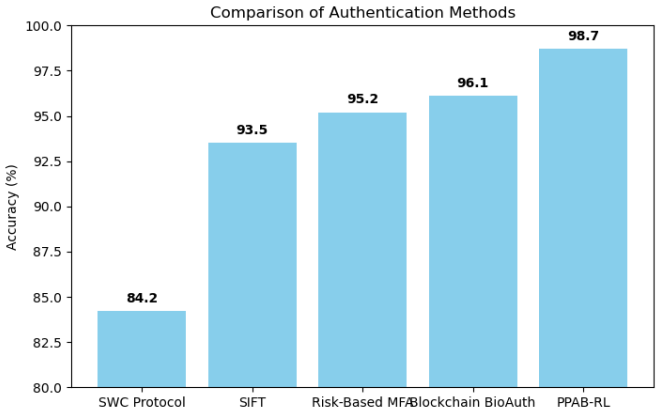

Fig. 12. Comparison analysis.

Table VIII and Fig. 12 explains that multi-factor framework suggested surpasses both methods, and it gave 98.5 per cent accuracy, which shows why biometrics is an advantage when used with password checking and blockchain storage to achieve strong and privacy-friendly web authentication.

H. Discussion

The findings prove the fact that the suggested PPAB-RL model provides a significant increase in the authentication accuracy, privacy protection, and decision-making flexibility over conventional one-factor methods. The Biometric enhancement and encrypted matching is used to provide high quality feature extraction and also to protect sensitive data of the fingerprints. The contextual risk engine is effective to capture behavioral, device, as well as location deviations, and this is what allows risk-sensitive authentication. Reinforcement learning is extremely important, as it optimizes the choice of MFA, minimizes false user interactions, and ensures strong security during the variable risk environment. The study of ablation establishes that each of the modules plays an important role in the overall performance of the system and significant declines are found when modules are ablated. Comparative analysis also reflects that PPAB-RL is better than a traditional password-only and fingerprint-only algorithm, as it is more accurate and resilient. Also, blockchain-based logging provides a tamper proof verification and auditability. Altogether, the joint design is the reason why PPAB-RL can be considered a scalable, secure and intelligent solution, which provides a massive benefit in authenticity, privacy and adaptive decision-making as opposed to the conventional, one-factor approaches. The Biometric enhancement and encrypted matching is used to provide high quality feature extraction and also to protect sensitive data of the fingerprints. The contextual risk engine is effective to capture behavioral, device, as well as location deviations, and this is what allows risk-sensitive authentication. Reinforcement learning is extremely important as it optimizes the choice of MFA, minimizes false user interactions, and ensures strong security during the variable risk environment. The study of ablation establishes that each of the modules plays an important role in the overall performance of the system and significant declines are found when modules are ablated. Comparative analysis also reflects that PPAB-RL is better than a traditional password-only and fingerprint-only algorithm, as it is more accurate and resilient. Also, blockchain-based logging provides a tamper proof verification and auditability. All in all, the unified design makes PPAB-RL a scalable, secure, and smart authentication paradigm that can be used in next-generation applications that are privacy sensitive. Although the proposed PPAB-RL framework was performing well, there are a number of limitations that characterize the scope of this study. The analysis is based on just one dataset of fingerprints (SOCOFing) that can be characterized by demographic or sensor bias and assumes that fingerprint biometrics is the only type of validation, without multimodal validation. Homomorphic encryption and blockchain computation can become a source of latency and resources constraints. Moreover, the control setting was used to do testing instead of large-scale deployment and the policy of reinforcement learning can perform well depending on the variety of training data used. Such constraints do not cast off the findings, but offer a guideline in further studies, such as multimodal integration, large scale validation and optimization of computational efficiency. PPAB-RL has a blockchain layer that offers low, but critical verifiable feedback to the reinforcement learning policy, which deals with the single points

of failure and unverifiable results of centralized logging. Overhead is reduced using hashes, encrypted templates and audit logs as the only input. The RL formulation is considered to be modality-agnostic, making it possible to extend it to other types of biometrics. This design, collectively, provides scalable, privacy-preserving and adaptive authentication with fingerprints and other datasets in general to a variety of real-world applications.

V. Conclusion and Future Work

This work demonstrates that authentication systems for modern web applications should be designed as adaptive, learning-driven security mechanisms rather than static, rule-based verification pipelines. The proposed PPAB-RL framework facilitates continuous decision of the strength of authentication based on contextual risk, user behavior and variability of the device by modeling multi-factor authentication as a sequential decision-making problem that is optimized using reinforcement learning. Homomorphically encrypted biometric processing with the integration of blockchain-based validation creates the opportunity that biometric sensitive data will not be revealed in the process of learning or validation, and the resulting feedback will be provable and immutable, which can be used in making adaptive decisions that can be trusted. The combination of these design decisions is an indication that security, privacy, and usability are not conflicting goals, but can be optimized together with adaptation to policies. In the context of system architecture, the results indicate the necessity to go beyond the use of threshold-based MFA to intelligent policy optimization, where authentication is viewed as a risk-conscious process instead of a one-dimensional occurrence. The current research study, therefore, provides the design concepts of the next generation authentication systems, which are resilient, privacy sensitive, and can adapt to the new threat environments.

Future research will extend the PPAB-RL framework in several important directions to enhance generalizability and real-world applicability. Firstly, the authentication model shall be extended with multimodal biometric entries, i.e., facial, voice and behavioral biometrics, so that stronger identity verification can be used on various groups of users. Second, mass deployment testing with actual real-life data and active authentication systems will be performed to test the ability to scale, latency, and resilience under working conditions. Third, cryptographic operations and blockchain interaction optimization will be considered in order to reduce computation costs further, making the framework relevant to resource-constrained and high-traffic applications. Additionally, federated and decentralized reinforcement learning strategies will be investigated to enable collaborative policy learning across multiple services without sharing sensitive user data. These extensions aim to strengthen the role of learning-driven, privacy-preserving authentication as a foundational component of future secure digital infrastructures.

References

[1] A. Despotović, A. Parmaković, and M. Miljković, "Cybercrime and cyber security in fintech," in Digital transformation of the financial industry: approaches and applications, Springer, 2023, pp. 255–272.

[2] M. S. Almadani, S. Alotaibi, H. Alsobhi, O. K. Hussain, and F. K. Hussain, "Blockchain-based multi-factor authentication: A systematic literature review," Internet Things, vol. 23, p. 100844, 2023.

[3] C. Pereira et al., "Security and Privacy in Physical–Digital Environments: Trends and Opportunities," Future Internet, vol. 17, no. 2, p. 83, 2025.

[4] S. Furnell, K. Helkala, and N. Woods, "Accessible authentication: Assessing the applicability for users with disabilities," Comput. Secur., vol. 113, p. 102561, 2022.

[5] W. Yang, S. Wang, N. M. Sahri, N. M. Karie, M. Ahmed, and C. Valli, "Biometrics for internet-of-things security: A review," Sensors, vol. 21, no. 18, p. 6163, 2021.

[6] H. Alanzi and M. Alkhatib, "Towards improving privacy and security of identity management systems using blockchain technology: A systematic review," Appl. Sci., vol. 12, no. 23, p. 12415, 2022.

[7] R. Askar, L. Bragança, and H. Gervásio, "Design for adaptability (DfA)—frameworks and assessment models for enhanced circularity in buildings," Appl. Syst. Innov., vol. 5, no. 1, p. 24, 2022.

[8] C. D. McDermott and M. Nicho, "Threat detection in smart homes: A sociotechnical multimodal conversational approach for improved cyber situational awareness," Int. J. Inf. Secur., vol. 24, no. 4, pp. 1–25, 2025.

[9] Q. Zhang, B. Wu, and W. Liu, "Nondestructive Identification of Chinese Chive Seeds and its Counterfeit Scallion Seeds Based on Machine Vision and Electronic Nose," Food Biophys., vol. 20, no. 1, p. 39, 2025.

[10] I. A. Omar, H. R. Hasan, R. Jayaraman, K. Salah, and M. Omar, "Implementing decentralized auctions using blockchain smart contracts," Technol. Forecast. Soc. Change, vol. 168, p. 120786, 2021.

[11] M. O. Ahmad et al., "BAuth-ZKP—A blockchain-based multi-factor authentication mechanism for securing smart cities," Sensors, vol. 23, no. 5, p. 2757, 2023.

[12] M. A. Acquah, N. Chen, J.-S. Pan, H.-M. Yang, and B. Yan, "Securing fingerprint template using blockchain and distributed storage system," Symmetry, vol. 12, no. 6, p. 951, 2020.

[13] S. H. G. Salem, A. Y. Hassan, M. S. Moustafa, and M. N. Hassan, "Blockchain-based biometric identity management," Clust. Comput., vol. 27, no. 3, pp. 3741–3752, 2024.

[14] L. Yu, M. He, H. Liang, L. Xiong, and Y. Liu, "A blockchain-based authentication and authorization scheme for distributed mobile cloud computing services," Sensors, vol. 23, no. 3, p. 1264, 2023.

[15] Y. Yao, X. Zhang, H. Hu, H. Liu, R. Huang, and Z. Wang, "Blockchain-Based Multistage Continuous Authentication for Smart Devices," Appl. Sci., vol. 13, no. 23, p. 12641, 2023.

[16] Y. Fu et al., "Non-transferable blockchain-based identity authentication," Peer--Peer Netw. Appl., vol. 16, no. 3, pp. 1354–1364, 2023.

[17] T. Wang, H. Shen, J. Chen, F. Chen, Q. Wu, and D. Xie, "A hybrid blockchain-based identity authentication scheme for mobile crowd sensing," Future Gener. Comput. Syst., vol. 143, pp. 40–50, 2023.

[18] V. Dehalwar, M. L. Kolhe, S. Deoli, and M. K. Jhariya, "Blockchain-based trust management and authentication of devices in smart grid," Clean. Eng. Technol., vol. 8, p. 100481, 2022.

[19] S. Bamashmos, N. Chilamkurti, and A. S. Shahraki, "Two-layered multi-factor authentication using decentralized blockchain in an IOT environment," Sensors, vol. 24, no. 11, p. 3575, 2024.

[20] X. Xu, Y. Guo, and Y. Guo, "Fog-enabled private blockchain-based identity authentication scheme for smart home," Comput. Commun., vol. 205, pp. 58–68, 2023.

[21] O. Mir, M. Roland, and R. Mayrhofer, "Decentralized, Privacy-Preserving, Single Sign-On," Secur. Commun. Netw., vol. 2022, no. 1, p. 9983995, 2022.

[22] N. A. Alzahab, G. Rafaiani, M. Battaglioni, F. Chiaraluce, and M. Baldi, "Decentralized Biometric Authentication based on Fuzzy Commitments and Blockchain," in 2024 6th International Conference on Blockchain Computing and Applications (BCCA), IEEE, 2024, pp. 64–72.

[23] E. Pagnin and A. Mitrokotsa, "Privacy-preserving Biometric authentication: challenges and directions," Secur. Commun. Netw., vol. 2017, no. 1, p. 7129505, 2017.

[24] A. H. Mohsin et al., "PSO–Blockchain-based image steganography: towards a new method to secure updating and sharing COVID-19 data in

decentralised hospitals intelligence architecture," Multimed. Tools Appl., vol. 80, pp. 14137–14161, 2021.

[25] K.-C. Lin and Y.-M. Chen, "A high-security-level iris cryptosystem based on fuzzy commitment and soft reliability extraction," IEEE Trans. Dependable Secure Comput., 2023.

[26] "Sokoto Coventry Fingerprint Dataset (SOCOFing)." Accessed: Jul. 08, 2025. [Online]. Available: https://www.kaggle.com/datasets/ruizgara/socofing

[27] T. G. Tan, P. Szalachowski, and J. Zhou, "Securing password authentication for web-based applications," in 2022 IEEE Conference on Dependable and Secure Computing (DSC), IEEE, 2022, pp. 1–10.

[28] S. Bakheet, S. Alsubai, A. Alqahtani, and A. Binbusayyis, "Robust fingerprint minutiae extraction and matching based on improved SIFT features," Appl. Sci., vol. 12, no. 12, p. 6122, 2022.