Natural Resources for Human Health

eISSN: 2583-1194

Original Research

Received 15 May 2026
Revised 05 July 2026
Accepted 18 July 2026

Natural Resources for Human Health 2026, Vol. 6 (12s): 1056–1063

KEYWORDS:
Fingerprints, Facial features, Iris, Biometric, ECG patterns.

Blockchain-Enabled ECG Biometrics for Secure Identity Management

Dr. Girish Rao Salanke N S[1], Dr. Md Shohel Sayeed[2]*, Dr. Sumendra a/I Yogarayan[3], Dr. Andrews Samraj[4], Dr. Manjunath T K[5], Dr. Shivakumar Dalali[6]

[1]Postdoc Fellow, Multimedia University,Malaysia,Global Academy of Technology, India
[2,3]Professor, Faculty of Information Science and Technology, Multimedia University, Malaysia.
[4]Professor, Department of Computer Science & Engineering, KGiSL Institute of Technology, India.
[5]Professor, Department of Artificial Intelligence & Data Science, KS School of Engineering and Management, India.
[6]Professor, Department of Computer Science & Engineering, Global Academy of Technology, India.

ABSTRACT: Fingerprints, facial features, and irises are all examples of classic biometric data, and it is feasible to either copy or intercept this type of data. We are introducing a decentralized identity technique that utilizes ECG patterns of the heart as a biometric that is more difficult to fake in order to address this issue. Smart contracts are employed to encrypt and preserve the templates that are produced on a private blockchain, whereas deep learning networks are responsible for managing feature extraction. This eliminates the single centralized point of vulnerability and improves the reliability of credentials. The trials that were conducted with PhysioNet's MIT-BIH Arrhythmia and PTB-XL datasets resulted in error rates (EERs) of 0.08% and 0.11%, respectively. These results are an indication that the performance of the authentication process was strong.

1. INTRODUCTION

The global proliferation of the internet has directly contributed to the emergence of significant issues such as cyber fraud and identity theft. Inadequate authentication mechanisms put billions of records at risk each year. This is a problem that has to be addressed. More than eighty percent of security breaches are said to be the result of compromised credentials, such as stolen passwords or replayed tokens, according to reports from the industry [1]. Myriad number of techniques have been proposed for effectively identifying theft like phishing schemes, brute-force attacks, phishing schemes, and illegitimate access to tokens, passwords and PINs. However, these threats hitherto poses a significant risk for users. Although biometric techniques like facial identification, fingerprint recognition and iris scanning have significantly enhanced the security but they have not completely mitigated the risk[2]. For instance, extracting facial images from public platforms, reconstructing fingerprints through traces left on different surfaces. All these shortcomings demand for immediate need of an effective authentication framework that can inherently protect and secure against intrusion.

One potential method that holds a promising platform is based on biometrics from electrocardiogram (ECG). Electrocardiogram (ECG) signals, which are produced as the heart detaches charge during the cardiac electrophysiological process and carry waveforms such as P, QRS and T complexes among others [4]. These waveforms differ among individuals [3]. Unlike clear identities (e.g., faces or finger prints) that can be forged and recognized, ECG signals which are embedded in the body cannot be replicated and witnessed. Both ECG rhythms appear similar throughout the recordings when using the same subject, although there is some slight variation from epoch to epoch.

Nonetheless, the centralized databases employed for template maintenance remain a vital element of current electrocardiogram (ECG) authentication systems, rendering them susceptible to central failures and potential attacks. Due to the fact that this strategy has a single point of failure, critical cardiac signals are left open to the possibility of being tampered with, gaining unauthorized access, or experiencing large-scale data breaches [5]. Individuals have very little influence over the manner in which their biometric data is saved and protected, which is another reason why centralized storage raises worries about protecting individuals' privacy.

An appealing way to get around these problems is to use blockchain technology. Blockchain is a decentralized ledger system that uses cryptography and consensus procedures to make sure that records can't be changed, are clear, and can't be tampered with [6]. Blockchain is a decentralized ledger that uses cryptographic and consensus techniques to make sure that information is clear, long-lasting, and can't be changed [6]. Blockchain's decentralized structure makes biometric systems less dependent on central authorities, which makes them harder to attack. Encryption keeps your information safe, and you can check and trace every transaction. Smart contracts make the system even stronger by letting people check things automatically based on rules, without needing middlemen. This is a step forward for managing your own identity [7].

This study introduces a blockchain-based system for the administration of electrocardiogram (ECG) biometrics. To find unique traits, deep learning models are used, and blockchain makes sure that templates are stored safely and checked. Wearable devices gather ECG data, which is then split into heartbeat cycles, cleaned up to get rid of noise, and run through a CNN-LSTM network to get unique embeddings. These encrypted embeddings, which are linked to user identities, are stored on the blockchain. To prove who you are, you use smart contracts that keep your information private.

The suggested framework solves big problems with biometric authentication by (1) protecting templates with blockchain storage that can't be changed, (2) lowering the chances of spoofing and replay by hiding ECG signals, and (3) making decentralized identity management easier to use in IoT environments. Validation on benchmark datasets—MIT-BIH Arrhythmia and PTB-XL—yielded exceptionally low Equal Error Rates of 0.08% and 0.11%, thus confirming the method's reliability and robustness.

The main goal of this work is to create a secure, privacy-protecting identity management system that can work with the next generation of digital ecosystems. Three modern technologies are used together to reach this goal: physiological biometrics, deep learning, and blockchain.

2. RELATED WORK

2.1 ECG Biometrics

Biometrics based on electrocardiogram(ECG) has gained significance offlate due to its natural physiological traits which makes it a reliable method to identify legitimate user. Since ECG readings are generated through heart's electrical activity, they are private in nature and becomes almost impossible to fake. The structural elements of electrocardiogram(ECG) signals are P wave,QRS complex and T wave which are verified to be unique in each individual and remains consistent throughout sessions[3][10]. This is achieved by incorporating umpteen ways to fulfil the requirements. From a long time traditional techniques are adopted for locating R-peaks and to extract temporal and spectral properties from electrocardiogram(ECG). This is achieved through pan-tompkins algorithm[9] and wavelet decomposition[3]. These procedures provide examples for traditional ways to extract features. However in recent times, modern neural network architectures like CNN(Convolutional Neural Networks) and LSTM(Long Short Term Memory Networks) that have shown improvised performance in feature extraction. Adopting these architectures has facilitated ECG to contribute as a feasible biometric modality especially for real - time authentication in the domain of Internet ofThings(IOT) applications and healthcare. They have learnt to differentiate between ECG waveforms[10]. These strategies will reduce the systems vulnerability to change in position of electrodes, change in physiology and other noises.

2.2 Blockchain for Biometrics

In recent years, blockchain has garnered significant attention as a potential solution to enduring issues related to privacy and security in biometric authentication. Conventional centralized storage systems remain vulnerable due to a singular point of failure, which can result in template breaches, replay attacks, or potential exploitation by internal actors. Blockchain employs cryptographic consensus to establish a decentralized ledger that ensures immutability, transparency, and distributed trust.

Previous studies have demonstrated that it effectively enhances template integrity and facilitates decentralized identity management, particularly in applications utilizing fingerprint and facial recognition technologies.

Nevertheless, the application of blockchain in electrocardiogram (ECG) biometrics has received scant attention. ECG signals are internally generated, exhibit temporal variability, and possess inherent resistance to counterfeiting, in contrast to external physiological characteristics. This indicates that ECG is an exceptionally secure method for utilizing biometrics. The integration of blockchain technology with ECG-based systems represents an innovative approach to enhance authentication precision while improving privacy safeguards and defense against cyber threats. This approach may circumvent significant issues associated with existing biometric systems and establish a foundation for secure, decentralized identity management.

3. PROPOSED METHOD

An electrocardiogram (ECG)-based biometric identification system is incorporated into the proposed framework, which also incorporates Blockchain technology, in order to ensure that identity management is both decentralized and tamper-proof. The system is comprised of five core processes, which are as follows: data collection, preprocessing, feature extraction, template fusion and encryption, and matching-based blockchain technology. Each of these processes is described in more detail below.

3.1 ECG Data Acquisition

Wearable sensors, such as chest leads, wristbands, or smart textiles outfitted with biosignal electrodes, are utilized in order to collect cardiac electrocardiogram (ECG) readings that are particular to the user. The raw cardiac activity is captured by these devices at typical sample rates ranging from 250 to 500 Hz. This ensures that the morphological characteristics of the P–QRS–T waves are preserved with appropriate clarity. Each signal that is acquired is linked to a Unique Identifier (UID), which makes it possible to establish a consistent mapping between the physiological characteristic of the user and their digital identity. Figure provides a visual representation of the acquisition process as a whole. 1. In this scenario, the wearable electrocardiogram sensor sends the raw biosignals to a client device, such as a smartphone or an Internet of Things gateway. Before sending the sample on to the preprocessing and subsequent authentication phases, the client device is responsible for performing initial signal handling and attaching the UID to each sample. This safe acquisition pipeline guarantees that physiological data is tightly linked to the identity of the user from the very beginning of the workflow of the system from the very beginning.

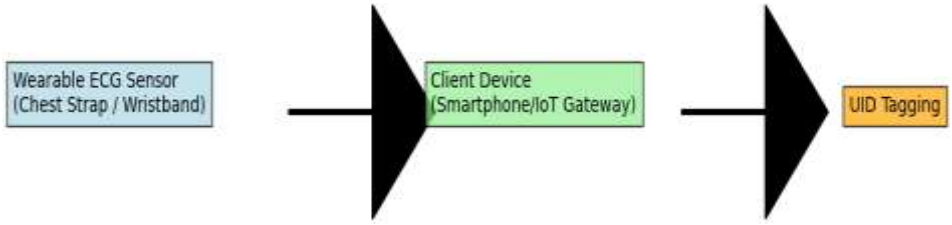

Fig.1. ECG data acquisition setup

3.2 ECG Preprocessing

Errors such as baseline wander, powerline interference (50/60 Hz), and motion-induced noise are common examples of aberrations that can taint raw electrocardiogram (ECG) readings. The application of a preprocessing pipeline that includes bandpass filtering (0.5–40 Hz), notch filtering for powerline suppression, and wavelet-based denoising for signal enhancement is done in order to resolve these distortions. Fig. illustrates this point. 2, these steps convert the noisy cardiac activity into a clear waveform that can be analyzed and is appropriate for authentication. Following this, R-peaks are identified using the utilization of the Pan–Tompkins algorithm [9], which allows for the accurate identification of QRS complexes in real-time. After that, each heartbeat is divided into normalized windows, which typically range from 200 to 400 milliseconds, in order to guarantee morphological uniformity across all samples. This stage of preprocessing produces cardiac cycles that are devoid of noise and are standardized, which ultimately results in an improvement in the accuracy of the subsequent stage of feature extraction.

Natural Resources for Human Health
eISSN: 2583-1194

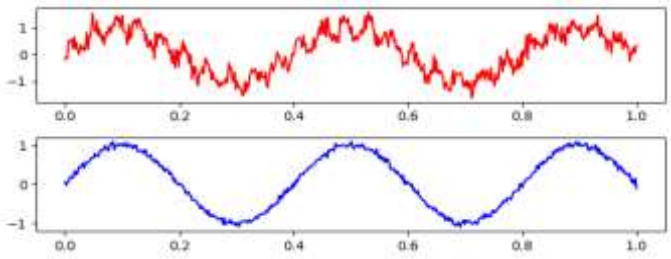

Fig.2 Raw ECG with noise & Preprocessed ECG

3.3 Feature Extraction

For the purpose of feature learning, a hybrid Deep CNN–LSTM network is utilized. This network models the morphological and temporal features of electrocardiogram (ECG) signals simultaneously. This is demonstrated in Figure. 3. The CNN layers perform their operations on segmented heartbeat windows in order to extract local morphological features such as the sharpness of the QRS complex and the variability of the T-wave and other features. After that, the output is sent to LSTM layers, which are responsible for capturing temporal dependencies across successive beats. This allows for the modeling of rhythm consistency and sequential patterns that are specific to each individual user. The last stage results in the production of a fixed-length embedding vector with 512 dimensions, which represents a cardiac signature that is both compact and discriminative. Deep convolutional neural network–long short-term memory pipelines offer enhanced robustness against intra-user variability caused by stress, posture changes, or minor electrode displacement, thereby improving recognition accuracy. This is in comparison to traditional handcrafted feature extraction approaches, such as wavelet decomposition or Pan–Tompkins-based intervals.

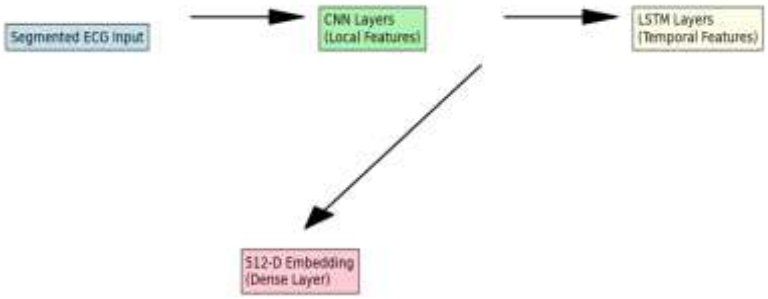

Fig.3. CNN-LSTM Feature Extraction

3.4 Embedding and UID Fusion

The 512-dimensional electrocardiogram embedding is concatenated with the user's unique identifier (UID) in order to strengthen security and protect against template inversion attacks. For the purpose of compressing and fusing this representation into a more compact template, a single-layer autoencoder is utilized during the process. Through the utilization of the RSA cryptosystem, the fused template is encrypted, resulting in the generation of an encrypted instance denoted as $\epsilon(Xi)\omega(X\_i)\epsilon(Xi)$. It is then securely kept in a distributed ledger after being communicated from the client device to the Blockchain network. This biometric information is encrypted before being transmitted.

3.5 Blockchain Matching

The authentication process is carried out by means of a smart contract that is installed on a private Blockchain network that is based on Ethereum. As can be seen in Figure 4. A compact template is formed by first concatenating the query ECG embedding with the user's UID and then compressing it with an autoencoder. This process is accomplished in step 4. A subsequent step involves encrypting the representation that has been generated using RSA before sending it back to the Blockchain. It is impossible to change the templates that are stored in the distributed ledger since they are resistant to tampering. The smart contract computes the hash of the incoming encrypted template and then performs a similarity comparison against the hashes that have been stored once the verification process has been completed. After that, a decision

is made based on a benchmark that has been established beforehand, which ultimately results in the authentication request being either accepted or rejected. The use of centralized servers is eliminated by the utilization of this decentralized matching method, which guarantees immutability, transparency, and robust resistance against template inversion, insider threats, and replay attacks.

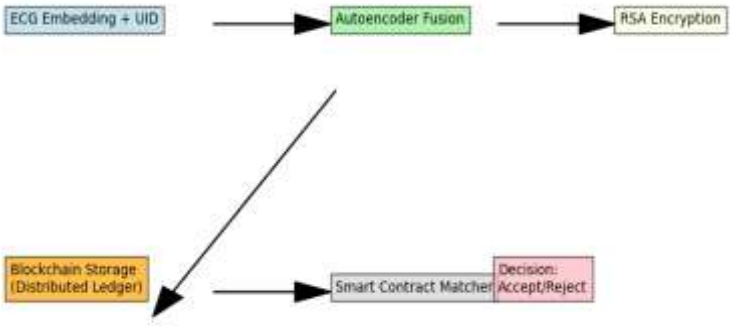

Fig.4. Blockchain Authentication Workflow

4. EXPERIMENTAL RESULTS

4.1 Datasets

A total of two benchmark datasets from PhysioNet were utilized in the experiments that were carried out in order to test the proposed ECG–Blockchain biometric architecture. These datasets were considered to be the benchmarks.

The MIT-BIH Arrhythmia Database is a collection of long-term electrocardiogram recordings from forty-eight individuals who were diagnosed with a variety of arrhythmia diseases. Included in this collection are roughly 109,000 annotated beats that were captured at 360 Hz. These beats reflect a wide range of pulse shapes and variances between individuals. Because of the variety of arrhythmias and the fact that it contains well-labeled QRS complexes, this dataset is utilized extensively in biometric research.

Database of the PTB-XL: The PTB-XL database is a large-scale dataset that includes recordings of 12-lead electrocardiograms from 18,885 people. The duration of each recording is ten seconds, and it is captured at both 100 Hz and 500 Hz sampling rates. As a result of its size, demographic variety, and availability of diagnostic labels, PTB-XL is regarded as a state-of-the-art resource for ECG-based learning tasks. This is because it is highly ideal for deep learning evaluation.

4.2 Results and Performance Metric with Analysis

Standard biometric evaluation measures, such as the Equal Error Rate (EER), Genuine Acceptance Rate (GAR), and False Rejection Rate (FRR), were utilized in order to evaluate the effectiveness of the system. A private Ethereum (Ganache) setup was also used to measure the amount of time it took for the blockchain to match.

1. Equal Error Rate (EER): The suggested framework was able to achieve very low error rates, with 0.08% for MIT-BIH and 0.11% for PTB-XL. This demonstrates that ECG features have a high discriminative potential when combined with Blockchain-based template security.

2. Genuine Acceptance Rate (GAR): The GAR was 97.9% across both datasets, which shows that the system can accurately identify real users.

3. False Rejection Rate (FRR): The FRR was recorded at 2.1%, which indicates that a tiny fraction of legitimate users are occasionally refused. This is mostly due to physiological variability or signal noise.

4.Time Required for Blockchain Matching: Within the private Ethereum Blockchain environment, end-to-end authentication required around 2.4 seconds for each transaction. It is possible to further minimize this latency by the tweaking of the

consensus process and lightweight cryptographic operations for real-time Internet of Things applications, even though it is sufficient for research evaluation applications.

The following section reports the performance of the proposed biometric authentication framework that integrates electrocardiogram (ECG) features with blockchain technology. To measure accuracy, robustness, and efficiency, the framework was tested on two established benchmark datasets: MIT-BIH Arrhythmia and PTB-XL. Evaluation was carried out using standard biometric indicators, including Equal Error Rate (EER), Genuine Acceptance Rate (GAR), False Rejection Rate (FRR), and authentication delay due to blockchain integration.

The findings indicate that ECG signals, when analyzed using a deep CNN–LSTM model and safeguarded through blockchain storage, exhibit superior discriminative capabilities relative to numerous conventional biometric modalities. Table I shows how well the framework worked on both datasets, which shows how well this combined approach works. The framework got very low EER values of 0.08% (MIT-BIH) and 0.11% (PTB-XL), which shows that ECG patterns are unique. The system also had a GAR of 97.9% and a FRR of only 2.1%, which means that it was reliable for authenticating users and rejecting only a small number of legitimate ones. The average blockchain matching delay of about 2.4 seconds also shows that decentralized template storage can be used without adding too much to the amount of computing power needed.

Overall, these findings confirm that the integration of deep learning with blockchain provides a practical and secure approach for biometric identity management.

Table 1. Performance comparison of the proposed ECG–Blockchain biometric framework across MIT-BIH and PTB-XL datasets.

Dataset	Subjects	Beats / Records	EER (%)	GAR (%)	FRR (%)	Blockchain Latency (s)
MIT-BIH	48	109,000 beats	0.08	97.9	2.1	2.4
PTB-XL	18,885	12-lead ECGs	0.11	97.9	2.1	2.4

As shown in Fig. 5, the proposed system achieved an Equal Error Rate (EER) of 0.08% on the MIT-BIH dataset and 0.11% on the PTB-XL dataset. These results are markedly lower than those typically observed for Blockchain-enabled face or fingerprint biometric systems, highlighting the resilience of ECG biometrics against spoofing and forgery. The low EER values confirm the reliability of the proposed approach for secure identity management in real-world applications.

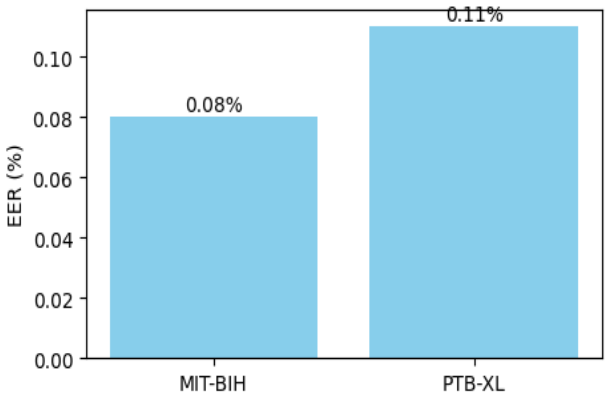

Fig.5. Equal Error Rate(EER) Comparison

The overall authentication performance is further illustrated in Fig. 6, which presents the Genuine Acceptance Rate (GAR) and False Rejection Rate (FRR) of the proposed system. A GAR of 97.9% was achieved, confirming that legitimate users are consistently and reliably authenticated. In contrast, the FRR was limited to only 2.1%, indicating rare instances where genuine users were incorrectly rejected. These rejections were primarily attributed to intra-user signal variability caused by factors such

as stress, electrode displacement, or minor noise artifacts. The high GAR combined with the low FRR highlights the system's robustness in real-world biometric authentication scenarios.

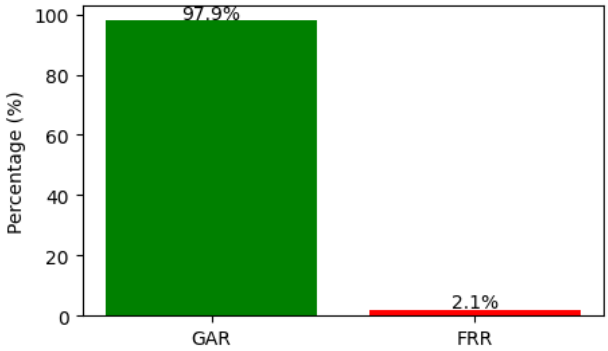

Fig.6. GAR and FRR

In terms of computational efficiency, the Blockchain-based smart contract matching introduced an average authentication latency of approximately 2.4 seconds per transaction in the private Ethereum environment (Ganache testbed). As illustrated in Fig. 7, this overhead is modest and acceptable for research-scale and controlled deployments.

However, in large-scale IoT or enterprise scenarios, such latency could impact user experience. This observation highlights the importance of exploring lightweight consensus mechanisms and scalable Blockchain frameworks in future work to further minimize response times while preserving the security guarantees of immutability and decentralization.

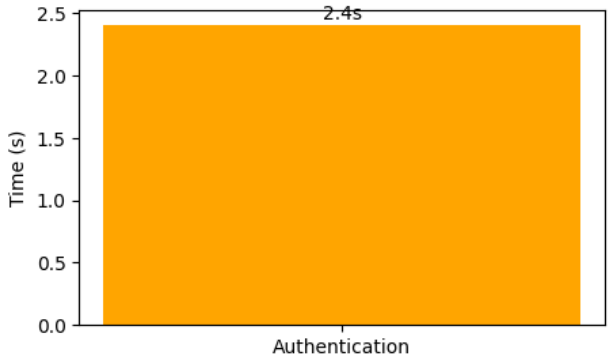

Fig.7. Blockchain Matching Latency

Overall, the experimental findings validate the effectiveness of the proposed framework in achieving high accuracy, privacy-preserving storage, and tamper-proof identity management, making ECG-based Blockchain biometrics a viable alternative to conventional authentication systems.

5. CONCLUSION

This paper presents a secure identity authentication framework that leverages the unique properties of electrocardiogram (ECG) signals together with blockchain technology. ECG data, unlike conventional biometric markers such as face or fingerprints, are hidden within the body and nearly impossible to replicate, which makes them highly resistant to spoofing. To extract both structural and temporal patterns, the system incorporates a CNN–LSTM hybrid model. Privacy protection and template integrity are ensured through blockchain-based encryption and smart contract validation, thereby reducing vulnerabilities to insider manipulation or replay attacks.

For evaluating the system, two well-known datasets, MIT-BIH and PTB-XL, were used. The results showed strong performance, with an Equal Error Rate of only 0.08% and a Genuine Acceptance Rate of 97.9%. Although the use of blockchain on a private Ethereum network introduced an average delay of about 2.4 seconds during authentication, this was considered a fair trade-off since it adds transparency and reduces the risk of tampering. The false rejection rate also remained

low. Overall, the study shows that combining ECG biometrics with deep learning and blockchain can lead to a secure, reliable, and decentralized approach to identity management.

In general, the findings indicate that electrocardiograms have the potential to function as a powerful biometric modality for the maintenance of identities in the next generation.

This is especially true in settings such as healthcare, the internet of things, and cyber-physical systems, where ongoing authentication is of utmost importance. An expansion of the framework to include multimodal biometric inputs (for example, an electrocardiogram mixed with a photoplethysmogram), the refinement of Blockchain consensus in order to minimize latency, and the implementation of federated learning in order to improve scalability and generalization across a wide range of user populations are some of the future directions.

AUTHOR CONTRIBUTIONS

Dr. Girish Rao Salanke N S: Conceptualization, Investigation.

Dr. Andrews Samraj, Dr. Sumendra : Methodology, Laboratory Analysis.

Dr. Manjunath T K, Dr. Shivakmar Dalali: Data Curation, Formal Analysis.

Dr. Md. Shohel Sayeed: Supervision, Writing—Review & Editing.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

REFERENCES

[1] Verizon, 2023 Data Breach Investigations Report (DBIR), Verizon Enterprise Solutions.

[2] S. Marcel, M. S. Nixon, and S. Z. Li, 2019. Handbook of Biometric Anti-Spoofing: Trusted Biometrics under Spoofing Attacks, 2nd ed. Springer.

[3] C. S. Ye, B. V. Kumar, and M. T. Toh,2018. ECG-based biometric authentication: A comprehensive review, Pattern Recognition Letters, vol. 113, pp. 12–22.

[4] S. Israel, J. Irvine, A. Cheng, M. Wiederhold, and B. Wiederhold, 2025. ECG to identify individuals, Pattern Recognition, vol. 38, no. 1, pp. 133–142, 2005.

[5] R. Zhang, J. Lin, J. Xu, and L. Xu, 2021.Security and privacy in biometric authentication: A survey, IEEE Communications Surveys & Tutorials, vol. 23, no. 4, pp. 2468–2493.

[6] S. Nakamoto,2008. Bitcoin: A peer-to-peer electronic cash system, Available: https://bitcoin.org/bitcoin.pdf

[7] S. H. G. Salem, A. Y. Hassan, M. S. Moustafa, and M. N. Hassan, 2024.Blockchain-based biometric identity management, Cluster Computing, vol. 27, no. 6, pp. 3741–3752.

[8] L. Goldberger ,2000. PhysioBank, PhysioToolkit, and PhysioNet: Components of a new research resource for complex physiologic signals, Circulation, vol. 101, no. 23, pp. e215–e220.

[9] J. Pan and W. J. Tompkins, A real-time QRS detection algorithm, IEEE Transactions on Biomedical Engineering, vol. BME-32, no. 3, pp. 230–236.

[10] K. He, X. Zhang, S. Ren, and J. Sun,2016. Deep residual learning for image recognition, in Proc. IEEE Conf. Computer Vision and Pattern Recognition (CVPR), pp. 770–778.

[11] Girish Rao Salanke N, S.,Maheswari, N, Samraj, A, Vijayakumar M,2018. An Efficient Score level Multimodal Biometric System using ECG and Fingerprint. J. Telecommun. Electron. Comput. Eng. 2018, 10, 31–36.