1-1-2023

Never Lose Your ECG: A Novel Key Generation and Authentication Scheme for Implantable Medical Devices

Nima Karimian
San Jose State University

Gokay Saldamli
San Jose State University, gokay.saldamli@sjsu.edu

Younghee Park
San Jose State University, younghee.park@sjsu.edu

Victor Lui
USC Viterbi School of Engineering

Recommended Citation

Nima Karimian, Gokay Saldamli, Younghee Park, and Victor Lui. "Never Lose Your ECG: A Novel Key Generation and Authentication Scheme for Implantable Medical Devices" *IEEE Access* (2023): 81815-81827. https://doi.org/10.1109/ACCESS.2023.3302175

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 18 July 2023, accepted 1 August 2023, date of publication 4 August 2023, date of current version 9 August 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3302175

RESEARCH ARTICLE

Never Lose Your ECG: A Novel Key Generation and Authentication Scheme for Implantable Medical Devices

NIMA KARIMIAN[1], (Member, IEEE), GOKAY SALDAMLI[2], YOUNGHEE PARK[2], (Senior Member, IEEE), AND VICTOR LUI[3], (Member, IEEE)

[1]Lane Department of Computer Science and Electrical Engineering, West Virginia University (WVU), Morgantown, WV 26506, USA
[2]Department of Computer Engineering, San José State University, San Jose, CA 95192, USA
[3]Department of Electrical and Computer Engineering, University of Southern California, Los Angeles, CA 90007, USA

Corresponding author: Nima Karimian (nima.karimian@mail.wvu.edu)

This work was supported in part by the National Science Foundation (NSF) under Grant 2104520.

ABSTRACT Implantable medical devices, such as pacemakers, cardiac defibrillators, and insulin pumps, play a crucial role in monitoring patients' vital signs within healthcare systems. However, these networked devices are susceptible to external attacks and breaches of trust, hindering the potential innovation and social benefits of eHealth services. To address these concerns, we propose a novel ECG-based key generation scheme and blockchain-based authentication protocol to build a trustworthy healthcare service under any situation. The key will be extracted in a single heartbeat using fiducial features. Compared with the existing works, the proposed key generation achieves the most efficient and secure method by introducing newly designed techniques to identify the unique features based on the time differences within a small window of the ECG signals. In our key generation process, we utilized three distinct fiducial features: amplitude peak differences, time differences between peaks, and slope between each pair of peaks. After obtaining the distinct fiducial features, each set of features denoted as F undergoes an encoding process, resulting in 16-bit vectors. To ensure randomness, the most significant bits of the encoded vectors are discarded due to their low entropy and least significant bits, which offer a greater degree of variability has been used. To validate our key generation method, we conducted the NIST statistical suite test. Our key generation process successfully passed all the necessary criteria and requirements set by the NIST suite test for ensuring the security and reliability of cryptographic systems. The proposed authentication protocol for the interaction between a patient and a doctor consists of three parts, addressing different scenarios that may arise including a patient visits a new doctor and emergencies which may be necessary for emergency medical services (EMS) personnel to immediately access the IMD. Experimental results demonstrate the efficiency and effectiveness of our key generation, as it produces a key of the same length within a second while maintaining a high level of randomness. Furthermore, the communication overhead for providing authentication services on the Internet is minimal. To evaluate the vulnerability of an authentication protocol, we performed a thorough security analysis, with a specific focus on the adversary model within the IMD (Implantable Medical Device) and DP (Device Programmer) interaction. Additionally, we implemented the proposed methods on a hardware setup by considering several factors, including time, key bit size, and memory usage. Furthermore, the proposed biometric key generation is tested using the NIST standard suite, where it successfully satisfied all the major requirements.

INDEX TERMS Authentication, biometrics, biomedical, IMD security, ECG, blockchain.

The associate editor coordinating the review of this manuscript and approving it for publication was Zahid Akhtar.

I. INTRODUCTION

Implantable Medical Devices (IMDs) implanted in the patient's body have been the most promising and popular solution to remotely monitor patient's medical conditions such as cardiac arrhythmias, diabetes, and Parkinson's disease [12]. The IMDs are small electronic medical devices with communication capabilities and limited resources including small computing power, memory, storage, and battery. The health industry has developed different kinds of IMDs, such as implantable cardiac pacemakers, defibrillators, and glucose monitors. The top market research centers, TMR (Transparency Market Research) and *M&M* (Markets And Markets) have predicted that the size of the IMD industry will significantly grow to reach more than $20 billions by 2027 [22], [32].

However, the IMDs security issues have been open problems, putting patients directly at risk even though the research communities have been actively working on these problems for a decade. Many vulnerabilities and attacks under limited resources on IMDs still exist, such as device attacks, data leakage problems, and unauthorized access, as demonstrated in [8], [10], [11], and [13]. In other words, attackers can eavesdrop, hijack, or reprogram the IMDs without permission. Such passive and active attacks on the IMDs impact negative medical effects to the patients. Therefore, it is imperative to provide secure authorized access at all times only if the authorized users have sufficient privilege to order commands or requests. To achieve this security goal, many researchers have studied key generation methods to provide secure communication between authorized users and IMDs through mutual authentication. In particular, the ECG-based key generation solutions have gained a lot of interest in the uniqueness of bio-signals [3], [19], [29], [33], [42], [45]. Most of them utilized IPIs (Inter-pulse Intervals) to produce random bits for key generation, however, these methods impractically require more than ten seconds to measure ECG signals for the 128-bit key generation [1], [33], [42]. In addition, the previously proposed authentication protocols rely on physical contact or distance proximity approaches between users [20], [33], which is not ideal for remote health services. Therefore, we need a new efficient key generation and authentication method to improve the limitations of the current existing works.

This paper presents a novel key generation and authentication scheme to protect the patients from unauthorized access. First, we develop a new efficient and effective key generation method based on electrocardiogram (ECG) features, but we do not utilize the IPIs to significantly reduce the key generation time ($\approx$10 faster). In summary, proposed key generation scheme has six major steps: noise removal, R peak detection, extracting individual heartbeat, feature extraction, key generation, and bits concatenation. First, noise will be removed from the raw data to detect R peak using Pan-Tompkins [26] technique. Next it identifies individual heartbeat for each R peak and extracts a set of features (i.e., different fiducial points over time differences) per segment by sliding a window during measuring the ECG. Finally, it generates a unique random key based on our customized binarization and bit concatenation techniques, as described in Section IV. The final generated keys are used to encrypt secure data and to authenticate users because of uniqueness and randomness. For authentication, our scheme utilizes a decentralized immutable blockchain to store and update the historical secure data. Our authentication protocol can guarantee that only authorized users can communicate with the IMD under various situations including changing doctors and emergency, which requires surgery again in the existing schemes. Comparing to the existing schemes, our new approach significantly reduces the key generation time around one second while demonstrating a good randomness through various random tests. The proposed authentication is secure against attacks since the scheme never discloses any important key information and updates the key every time, as discussed in Section V. To the best of our knowledge, we propose the most efficient random key generation with the new designed techniques and utilize the blockchain to solve the security problems on the IMD-based applications. Our main contributions are described as follows:

- We have introduced novel methods for generating encryption keys using ECG signals, utilizing three distinct sets of fiducial features. These methods operate effectively with a small window size. Each feature set is encoded into 16-bit vectors, focusing on the least significant bits that demonstrate significant variability and high entropy. We consider the encoded vectors' most significant bits to have low entropy and discard them in the process.
- We propose new authentication protocol based on biometrics and block-chains. The authentication protocol for the interaction between a patient and a doctor comprises three parts, addressing different scenarios that may arise. The first case, where the patient's implanted medical device (IMD) device, IMD-*A*, interacts with a known Device Programmer *B*, DP-*B*, who can be associated with the most recent or implanting doctor. The second case considers a situation where the patient visits a new doctor, and the stored public key or shared key in the IMD memory cannot be used for authentication. To overcome this challenge, a private blockchain is employed as a solution, allowing for secure authentication even in the absence of previously established trust. In the third case, during emergencies, it may be necessary for emergency medical services (EMS) personnel to immediately access the IMD. To authenticate the EMS personnel, a Public Key Infrastructure (PKI) is proposed.
- In order to assess the vulnerability of an authentication protocol, we conducted a comprehensive security analysis. This analysis focused on evaluating the adversary model in the interaction between IMD (Implantable Medical Device) and DP (Device Programmer). We

considered three different scenarios and assumed that the adversary has complete access to the network.
- To assess the efficacy of our proposed approach, we have implemented it on a hardware setup. We conducted evaluations considering various factors such as time, key bit size, and memory usage. Moreover, the key generation has been tested under NIST standard suit test, where it successfully met all the major requirements.

The paper organizes as follows. Section II discusses the previous works and Section III discusses potential attacks while introducing our system environment. Section IV presents our new key generation scheme based on ECG with other techniques and shows the experimental results of the key generation. Section V and Section VI describe our new authentication protocol that covers various scenarios with the experiment results. Finally, we discuss our approach and conclude this paper in Section VII.

II. RELATED WORK

IMDs have been the most vulnerable device due to the constrained resources and the most attractive target for attackers to launch various passive and active attacks. Generating a secure key to protect the devices and to block unauthorized access is the most significant task for eHealth services. To achieve this goal, many electrocardiograms (ECGs)-based key generation methods have been proposed by using an entropy source for generating random binary sequences to generate a secure key while considering the limitations of the resource-constrained IMDs [3], [19], [29], [33], [42], [45]. Their methods utilize the inter-pulse intervals (IPIs) of the ECG, which is defined as the time interval between two successive R peaks, to generate biometric binary sequences. IPIs are a good source for a key generation due to its heart variable nature and ease of accessibility [1]. As proposed in [33] and [42], only the last four bits of the IPI are considered as random bits for key generation. Therefore, to generate a 128-bit random key, the method needs to process at least 32 IPIs. With a normal adult heart rate of 60-100 beats per minute, the key generation time would take approximately 30 seconds. It is not practical in real-time life-critical medical applications that require low latency [41]. Furthermore, the IPI values do not satisfy robustness and performance as an entropy source for key generation as discussed in [6]. Instead of using IPIs, the new approaches proposed to use multiple fiducial peaks of an ECG consisting of five distinct peaks (P, Q, R, S, T) to generate a random key [27], [39], [43]. Zheng et al. proposed a new method to extract at most 16 bits per heartbeat by extracting multiple time intervals from various fiducial peaks [43]. Their methods produced a significant improvement over the IPI based methods, resulting in a lower latency of approximately 6-10 seconds for a 128-bit random key. However, it still has a high latency and performance bottleneck if we consider remote communication between patients and doctors. Therefore, to improve the current key generation schemes with high randomness, we propose a new BioKey method that utilizes *multiple fiducial peak amplitude differences* as our features. The fiducial peak amplitude differences (FPAD) are heart variant, meaning they vary from person to person depending on their heart size and rate [1]. Islam [16] proposed three level of quantization to convert ECG features into binary string by incorporating re sampling under two public data-sets. The binary string then evaluated under permutation, chi-square, and restart tests. Their methods focused solely on key generation and did not include the authentication protocol or any security analysis in their scope. To the best of our knowledge, our scheme extracts eight features from each heartbeat, and it achieved the lowest latency in the current state of arts.

The suitability of using an electrocardiogram (ECG) signal for key generation depends on factors such as uniqueness, randomness, usability, and accessibility. ECG signals have been extensively studied for their individual uniqueness, as they exhibit variations in the electrical activity of the heart [15], [17], [18], [23]. This uniqueness makes ECG signals suitable for generating cryptographic keys that are specific to each individual. Moreover, the waveform patterns, rhythms, and non-stationary noise present in ECG signals can contribute to the generate random of high entropy key sequences, which is necessary for developing secure cryptographic keys. Acquisition and processing of high-quality ECG signals can be obtained using wearable devices such as the Apple Watch and Fitbit. These devices have advanced sensors and algorithms that ensure accurate measurement and reliable processing of ECG signals. These devices are user-friendly and accessible to individuals which makes them practicality for ECG-based key generation systems. With the generated security keys by using ECG, the most unsolvable problem is how to provide mutual authentication protocols for e-Health services on the Internet. The notion of using a patient's physiological signals as a method to secure inter-sensor communication was introduced in [5]. Since then, many researchers have adopted the use of physiological values in designing secure authentication protocols [3], [7], [33], [40], [42]. A common approach for securing authentication in ECG-based systems is to have two sensors synchronously measure the patient's ECG [21]. If the two measurements are similar within a calculated threshold, the authentication is successful [14], [39], [44]. In the case of IMDs, there are usually two known entities that record the ECG: the programmer and the IMD itself. In the H2H approach [33], the IMD and programmer must follow a touch to access policy, meaning the doctor and the patient need to be within physical contact of each other for authentication. However, Marin, Eduard et al. concluded that the physiological signal-based cryptographic protocols had security weakness; the state-of-art authentication protocol design was susceptible to reflection and man-in-the middle attacks [20]. Furthermore, the proposed protocol is not feasible as the patient needs to be in constant physical contact with the programmer for authentication. In other words, they assumed that the IMD would be in close proximity to

the programmer during every authentication phase, which is not practical for real practical scenarios. To provide an untouched secure mutual authentication protocol, this paper will propose a novel authentication protocol that utilizes the latest blockchain technology to secure remote authentication between the IMDs and the programmers or doctors, which can cover diverse medical situations including emergencies.

III. THREAT MODEL AND PROPOSED PROTOCOL

Designing a practical IMD system with precise security assurances to ensure patient safety, security, and privacy has effectively remained a major issue, one that raises several technical challenges. In this section, we discuss possible threat model scenarios for patients carrying IMDs, such as unauthorized access control and communications with IMD or Programmer. Adversarial models can be categorized into two main groups, including active and passive [4]. In the passive attack, transmitted ECG signal by the IMD system and by programmer communicating with the IMD can be eavesdropped using side-channel attack, Doppler [11]. In the active attack, we assumed that an adversary could initiate malicious communications with IMD by interfering legitimate communications during a Programmer-to-IMD authentication session [11]. The identity of a doctor and a patient must be confirmed before conducting any operation to implant any IMD into the patient's body. Within the domain of IMDs after the surgery, any device (IMDs, programmers or external devices) can be spoofed by attackers to impersonate legitimate entities. Moreover, the IMD should be resistant against denial-of-service (DoS), modify, replay, and forge messages [31], [33]. Moreover, targeted adversarial attacks on IMDs have been classified in [35]. Marin et al. [20] discovered the man-in-the-middle (MiMT) attack to capture the ECG signals during the communication between the IMD programmer and the patient to inject malicious messages. Due to the lack of authentication schemes in this domain, any spoofed attacks are able to capture any private data including device information, diagnosis, and therapy regimen. Moreover, data (i.e., ECG signals), a source of generating a secure key can be altered to break data integrity by injecting noises or by replacing the original data with attacker's data. For instance, the adversary can record and spoof the continuous ECG signal using Doppler [28]. Then, it can establish spoofed ECG signals to communicate with the programmer and doctor's office along to raise false alarms, and also modify the original ECG signals to fool the doctor into making wrong treatment decisions.

Fig. 1 shows an overview of secure IMD-based eHealth patients wearing implantable or externally mounted medical devices. The communication links between the patients and the doctors (or the programmers) on any communication links are vulnerable to passive and active attacks as we described. To protect the important communication lines among them, this paper proposes a new key generation and authentication method against the MiMT attacks and the spoofing attacks. The proposed scheme has three different layers in

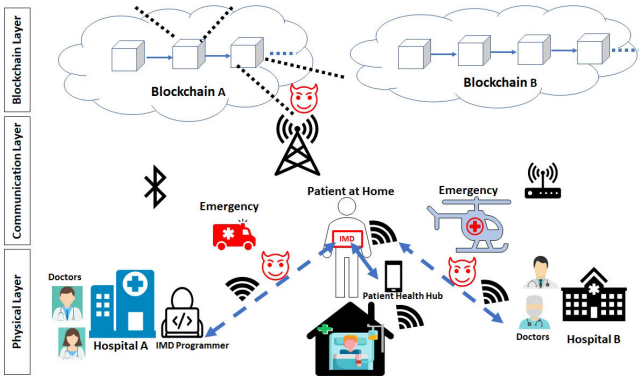

FIGURE 1. Overview of secure eHealth systems for patients with IMDs.

the environment settings: a physical layer, a communication layer, and a blockchain layer. In the physical layer, a doctor and an IMD programmer will first implant the medical device to a patient through surgery, and then they initially measure initial ECG signals to generate the first secure random key (i.e., a seed key) for further secure communications on the Internet. After the first setup, the patients will be remotely monitored by their doctor based on our proposed authentication method, and they can also securely change their primary doctor through the blockchain network without physical contact, surgery, or office visits. After the first setup through the operation, the doctor or the programmer can search and update their secure data (i.e., blocks) in the blockchain. The saved data in the blockchain can be used for authentication between a patient and a doctor (or a programmer). The IMDs do not require access the blockchain data since only the original IMD device can generate a correct key for secure communication and authentication at every single time. The physical attacks on the IMDs, such as breaking the medical devices and draining batteries, and the blockchain security problems are not within the scope of this paper.

IV. ECG-BASED BIOMETRIC KEY GENERATION

A. BACKGROUND ON ECG

ECG signals is measured by potential difference voltage between two electrodes attached to person's skin which are placed on the right arm, the left arm or chest. ECG signal comprises positive and negative waveform such as P, Q, R, S, and T waves that provide unique information about each individual [18].

In this study, we only need a single lead of ECG signal (Lead I) and would be sufficient to generate random binary sequences, continuously.

B. ECG KEY GENERATION

Fig. 2 illustrates a high-level overview and flow of our proposed ECG-based key generation process, which comprises of six major steps: *noise removal, R peak detection, extracting individual heartbeat, feature extraction, key generation* and *bits concatenation*. The IMD device collects the patient's

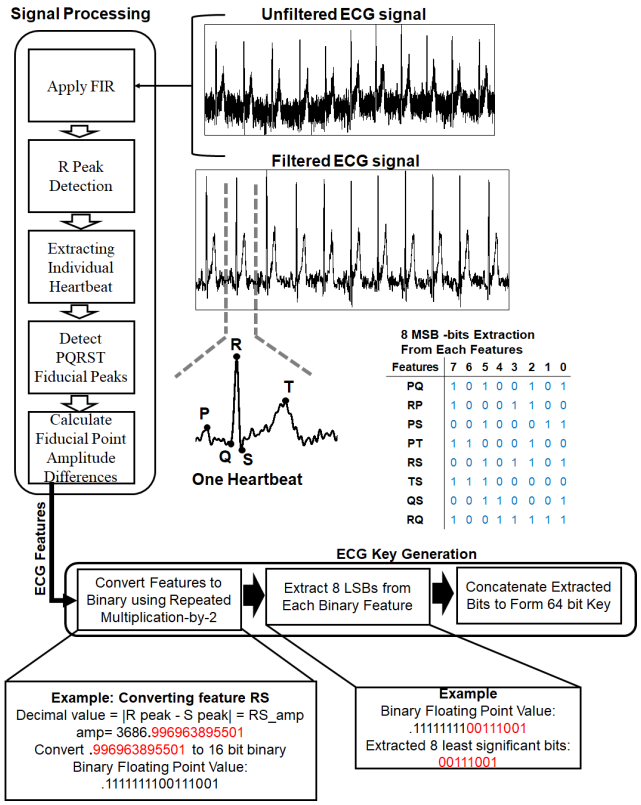

FIGURE 2. **Overview of our ECG key generation architecture based 128-bit random binary sequences.**

ECG signal. *Noise removal* processes the gathered ECG signal to remove various noise sources in order to enhance the quality of the pre-processing and key generation. *R peak detection* identity highest peak of ECG signal followed by *extracting individual heartbeat* splits the ECG signal into its different unique component waveforms in order to reduce the time for 128 key bits generation. *Feature extraction* extracts information that may enable the system to distinguish between different users and generate random sequence key bits. In what follows, we briefly describe the various steps of the ECG key generation algorithm and our approach for implementing the algorithm.

1) NOISE REMOVAL AND R PEAK IDENTIFIER

ECG signals are always combined with different noise sources such as baseline wander (BW), motion artifact (MA) and electrode movement (EM) [15]. Embedded noise in ECG signal (raw ECG) will make it difficult to detect the R peak in ECG signal which one of the requirements of the IPI technique or our scheme. To clean and smooth the ECG signal, we applied Savitzky-Golay [30] finite impulse response (FIR) smoothing filter with a polynomial order of 9. Savitzky-Golay can filter the ECG signal and make it smoother without destroying its original characteristics. This filtering technique provides better smoothing signal compared to one has been

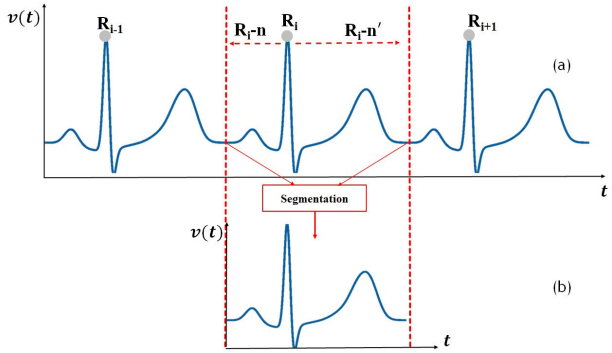

FIGURE 3. **Demonstrating example representing the Individual Heartbeat. (a) is the original ECG waveform, (b) depicts window based Individual Heartbeat extraction or segmentation. This method is repeated for each R peak and a heartbeat is extracted corresponding to each R peak. The optimal values of "*n*" and "*n′*" were calculated to be 0.2s and 0.4s.**

reported in [15]. To identify R in ECG signal, the Pan-Tompkins [26] technique is employed.

2) EXTRACTING INDIVIDUAL HEARTBEAT

The key factor for security of IMD is performance and speed. To best of our knowledge, ECG signal is nearly a periodic pattern contains P, QRS, and T waveform. Our proposed ECG-based key generation goal is to produce 128 key bits in a short time using ECG signal. In order to overcome the shortcomings of IPI for ECG key generation, our scheme segments ECG signals into individual heartbeats via R peak detection. Once R-peaks is identified, individual heartbeats were extracted using the "window" method [15]. The "window" algorithm slices a window beginning at "n" seconds before an R peak and ends at "n'" seconds after the R peak. This method is repeated for each R peak and an individual heartbeat is extracted corresponding to each R peak. The optimal values for "n" and "n'" were calculated to be 0.2 and 0.4 where each segment is composed of 300 sample points or equivalently about 0.6 seconds. Compared to the existing IPI scheme [1], [33], [42] which requires at least 10s of ECG signal to produce 128 key bits, our framework in the other hand needs two segment ECG which is equivalently 1.2s to achieve the same results. This scheme continuously generates ECG key bits from each individual which are unique and random. Fig. 3 illustrates our technique for segmenting ECG signals using sliding windows into different heartbeats.

3) FEATURE EXTRACTION

ECG is nearly a periodic signal with small variability over time in which cannot be substantially changed. However, heart rate variability (HRV) can change temporal fiducial features such as P, Q, R, S, and T waves; the effect of HRV on each temporal features varies [36]. Therefore, by measuring the difference between each temporal features, unique features will be obtained where the value for each cycle will not be similar. To ensure the randomness of biokey, temporal fiducial points cannot directly be used at the same time.

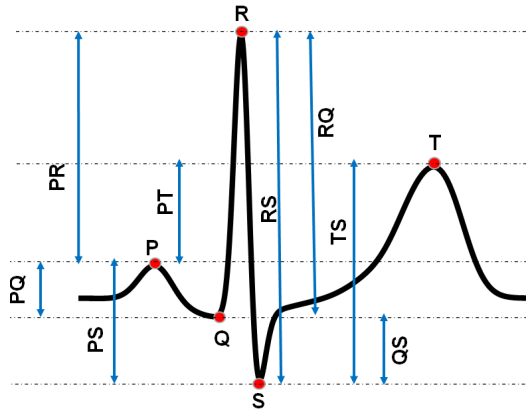

FIGURE 4. Extracted relevant features of ECG signal with single heartbeat which meet the requirement of randomness. Among all the candidates for feature extraction, only eight depicted features (*PQ, RP, PS, PT, RS, TS, QS,* and *RQ*) has been selected for the final stage to generate random binary sequences.

Once the ECG signal has been segmented into individual heartbeats, the next step is to extract random features F from fiducial points that will be used for bit extraction. In order to explore the optimal features from a single ECG, we examine multiple experimental from our feature extraction design. *Note that optimal features are those that can pass the NIST test*. To that end, several experiments were performed by testing a variety of fiducial-based features ranging from simple and direct measurements based on fiducial points to more complex ones that are based on the slopes and angular such lines between two peaks. As can be seen in Fig 4, fiducial points of the ECG signal mainly denoted as five fiducial points P, Q, R, S, T as essential features where other features depend on detecting five fiducial features [9]. From fiducial points, time-related features which represent the intervals from each peak to other peaks including PQ_{int}, PR_{int}, PS_{int}, PT_{int}, QR_{int}, QS_{int}, QT_{int}, RT_{int}, RS_{int}, and ST_{int} can be calculated (*int* represents interval). Moreover, amplitude-based features which represent fiducial peak amplitude differences including $PQ_{amp}, PR_{amp}, PS_{amp}, PT_{amp}, QR_{amp}, QS_{amp}$, QT_{amp}, RT_{amp}, RS_{amp}, ST_{amp} (*amp* represents amplitude). In addition, we have design slope-based features which are defined by calculating:

$$\text{slope} = \frac{y_2 - y_1}{x_2 - x_1} \tag{1}$$

where the y_1 and y_2 represent amplitude of each fiducial points; x_1, and x_2 are denoted by location time of each fiducial points. For better understanding, we defined PR slope calculation using Eq. 2:

$$slope(PR) = \frac{PRy}{PRx} = \frac{Ry - Py}{Rx - Px} \tag{2}$$

Similar to amplitude-based features and time-related features, 10 slope based features has been calculated. The slope feature sets are PQ_s, PR_s, PS_s, PT_s, QR_s, QS_s, QT_s, RT_s, RS_s, ST_s (s represents slope). As per the testing of entropy values through NIST, fiducial peak amplitude differences yielded the best results compared to other features (e.g., slopes, time differences, and distances between peaks). The feature set F includes the fiducial peak amplitude differences for PQ, RP, PS, PT, RS, TS, QS, and RQ.

4) KEY GENERATION

Key generation involves utilizing the extracted features F to generate a unique random key K for data encryption between the patient and their healthcare provider. In order to extract a number of bits from each feature, the features F need to be encoded to binary values through binarization. Binarization is the process of transforming data into vectors of binary numbers. In this study, the feature set F is converted to unique binary using the repeated multiplication-by-2 technique. The method is outlined as followed (example of each step are demonstrated in Fig 2):

1) Take the fractional component of each feature.
2) Multiply the fraction by 2.
3) Append the whole number component of the result to a binary vector (whole number can only be 0 or 1).
4) Repeat the steps above until binary vector is 16 bits long.

This binary vector will be unique to each feature as the entropy of the bits are attributed by the varying nature of an ECG cycle. Once each feature has been binarized, a number of bits can be extracted from them. The extracted bits are an essential element in generating the random binary key. Each feature in F is encoded into a unique 16-bit vector. The extracted bits need to be random in order for them to be utilized in a cryptographic setting. Therefore, the most significant bits are discarded due to their inherent low entropy. This leaves the least significant bits, which have high variability. Due to this variability, these bits will be difficult for adversaries to predict, making them suitable for key generation. With this distinction, the optimal number of bits to be extracted from each feature needed to be determined. If the number of extracted bits exceeds the amount of sufficiently entropic bits that the binary feature could provide, there would be a loss of entropy in generating the key. However, if the number of extracted bits is less, then the binary feature is not being maximized to its full key generating potential. With this constraint, the maximum number of bits that could be extracted from each feature, while retaining high entropy, was calculated to be 8. This means that the 8 least significant bits are extracted from each feature to construct unique binary features. Note that since our focus is not on the integer value of fiducial features, the conversion of QR_{amp}, which is supposed to be the sum of PQ_{amp} and PR_{amp}, becomes independent of generating the same binary string. This is because only the fraction of QR_{amp} is taken into account in the process. For example, assuming PQ_{amp} is 2.876 and PR_{amp} is 4.235, QR_{amp} would be 7.201. Consequently, the fraction of QR_{amp} is 201, while the fractions of PQ_{amp} and PR_{amp} are

TABLE 1. Summary of the PTB-XL dataset in terms of diagnostic.

# Records	Superclass	Description
9528	NORM	Normal ECG
5486	MI	Myocardial Infarction
5250	STTC	ST/T Change
4907	CD	Conduction Disturbance
2655	HYP	Hypertrophy

876 and 235, respectively. This difference in fractional values leads to distinct binary strings.

5) BITS CONCATENATION

After all the bits have been extracted from the feature set, we are left with a binary feature set BF that is unique to each heartbeat, such that $BF = \{BPQ, BRP, BPS, BPT, BRS, BTS, BQS, BRQ\}$. With each 8-bit binary feature, it needs to be concatenated together using concatenation to form the random binary key. Concatenation is the process of appending an element with another to form a singular output. The binary features are concatenated as followed:

$$K_j = BPQ_j \parallel BRP_j \parallel BPS_j \parallel BPT_j \parallel BRS_j \parallel BTS_j \parallel BQS_j \parallel BRQ_j \quad (3)$$

where K_j is a random binary sequence from the jth heartbeat and $\parallel$ represents the concatenation operation. With each binary feature set BF having a total of 8 binary features, this means that the maximum key length that can be generated from an individual heartbeat is 64 bits. However, this can be increased by concatenating multiple Ks to form a key of desired different lengths. This concatenation of Ks is as followed:

$$K_x = K_1 \parallel K_2 \parallel K_3 \parallel \ldots\ldots K_n \quad (4)$$

where x is the desired key length and n is the total number of Ks to be concatenated.

Once all the binary features have been concatenated, the result will be a random binary key that is based on an individual's biometrics. The key's randomness is guaranteed as it is attributed by the real-time evaluation of a patient's ECG signals, making it difficult for adversaries to replicate the patient's key without having access to the necessary ECG signals.

C. HARDWARE SETUP

For a fair comparison, we set-up hardware to calculate memory usages, timing requirements, and several keys that can be generated at a fixed range of time. To do that, we incorporated an AD8232 single lead sensor that acts as an op-amp to help collect a clear ECG signal from the heart. Moreover, we used the Arduino UNO R3 development board to conduct key generation using ECG source. Fig. 5 is illustrated hardware setup for ECG key generation. This paper performed various experiments and compared our new ECG key-based generation in Section IV with Inter-pulse intervals (IPIs) from Heart-to-heart (H2H) [33]. As can be seen in Table 2, the

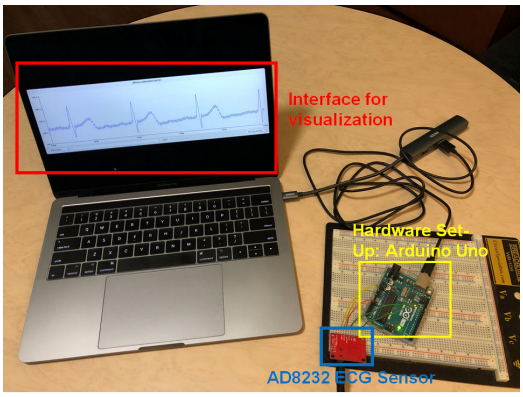

FIGURE 5. Hardware setup and the approach used to record the ECG and generate random keys.

TABLE 2. NIST results of amplitude difference features.

	Memory usage	# Key bits	Average time
Our method	0.1357	1024	1.2328s
IPI technique	0.1356s	64	10.0311s

memory usage based on two techniques is similar. However, the number of key bits that can be generated from 10s of ECG signal is 8×128 for our approach and 64 for H2H [33], respectively. Moreover, the average time to generate 128 key bits is 1.2328s for our approach and 10.0311s for the H2H approach, respectively. Our new ECG based key generation scheme is much faster ($\approx$10) than the H2H approach, and our method is more feasible and practical in real-world applications. In order to ensure randomness, as demonstrated in Section VI-A, the proposed technique can produce random and robust keys at every single time against the MiMT and spoof attacks.

V. REMOTE AUTHENTICATION THROUGH BLOCKCHAIN

Blockchain is a technology that enables to store and verify transactions securely on an open, immutable, and decentralized database system [38]. The early success of Bitcoin [24] as a digital currency made the bitcoin's ingenious solution to the trust problem in open networks quite popular. When this is followed by the recent technological advances in distributed and decentralized networking, we discover a new set of applications that is beneficial in virtually every aspect of the digital world including finance, healthcare, education, and a variety of other fields. Some of these fields are welcoming this new technology as a new layer that could impact and change the information retrieval that is based on the transactions. Other use cases include reducing fraud or counterfeiting as every transaction is recorded and distributed on a public platform.

In this study, we propose to use a private blockchain of doctors or Device Programmers (DP) called *DP blockchain* to manage the keys to access the IMD devices by storing the sensitive information in a tamper-resistant and distributed database system. A private blockchain (or a permissioned blockchain) is a network where accessing the network is restricted. Unlike in an open blockchain, admission and

membership policies build the trust between the members of a private blockchain. Participating in a private blockchain may include rules that the network requires. Admissions might include invitations or strict processes similar to opening a bank account. Thus, we assume that DPs has to provide the necessary documentation to be admitted to the DP blockchain. The network has the power not to admit or revoke an existing member. Note that any malpractice or wrongdoing should be punished severely to keep the trust in the network.

The DP blockchain with the doctors being the blockchain nodes creates a verifiable and timestamped access to the patients' IMDs. Such an access management system enjoys all the benefits of a decentralized networks. The system operates in a peer-to-peer fashion and the data is stored across the network, hence the DP blockchain eliminates the risks associated to centralized architectures and their single point of failure weakness; it provides a guarantee of being safe and resistant to the most damaging denial of service attacks.

A. THE PROTOCOL

The authentication protocol consists of three parts covering cases that may occur in the interaction between a patient and a doctor. We assume that provisioning takes places during an IMD implantation where the DP and IMD device create and store the initial secret key k_0. Although we do not require a public key infrastructure (PKI) for device programmers, we assume they are utilized with some public/private key pairs that are managed by a private blockchain. During the provisioning, we assume DP's public key is stored in the IMD device in secure memory. IMD devices may update DP public keys if they interact with other DPs. However, this needs to be done via Case #2 as follows. The simplest secure communication is the case where the patients want to interact with the last communicated DP. This may be generalized to have a whitelist of known DPs, but we reserve this scenario for future research.

Case #1: The simplest case is the one where the IMD device A, IMD-A interact with a known Device Programmer B, DP-B. DP-B can be associated with the lastly visited doctor including the one who implanted the IMD. Hence, we assume that the IMD device and the doctor have some shared secret k_0 generated from the ECG signal from an earlier visit or the initial implantation. Moreover, the IMD also holds pub_B, Device Programmer B's public key as seen in Fig. 6.

When DP-B sends the initial "hello" message IMD-A creates a new ECG key k_1 but does not use it immediately. Instead IMD-A uses the last shared secret used (i.e. k_0) to authenticate DP-B, hence replies back with ID of A, stored public key pub_B of the lately visited DP and encrypted "$ID_A||pub_B||n_1||ECG_1$" value using k_0.

Since IMD-A and DP-B share k_0, DP-B can easily get the values ID_A, pub_B, n_1 and ECG_1 where "$ID_A||pub_B$" needs match the clear-text, n_1 is a nonce for validating the freshness of the message and ECG_1 is the current ECG signal. DP-B also creates the new ECG key k_1 from ECG_1. DP-B encrypts and sends n_1-1 using a symmetric key algorithm with key k_1.

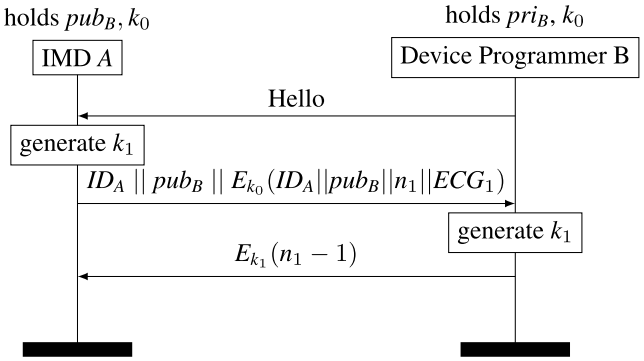

FIGURE 6. Authentication for interacting with the same DP.

IMD-A decrypts the message with k_1 and verifies the nonce. Both parties update the lastly shared key with k_1. DP-B writes the IMD-A interaction record to the DP blockchain as a transaction with the lastly used shared key k_1.

$$ID_A \,||\, pub_B \,||\, E_{k_1}(ID_A||pub_B||n_1) \tag{5}$$

Note that this simple interaction only uses symmetric key encryption. Although the message includes the public key information, it is never used in encryption. The intent is to broadcast the lastly paired DP's public key so that a new DP can reach and request a referral as described next.

Case #2: If the patient visits a new doctor, the stored public key or shared key in IMD memory could not be used for authentication. However, a private blockchain can be used to solve this problem.

Similar to Case #1, IMD-A creates a new ECG key k_2 after getting the "hello" message but does not use it immediately. Instead, IMD-A replies back the same message to DP-C as in Case #1. Note that DP-C cannot read the IMD-A's message. However, DP-C may query the DP blockchain for IMD-A's records and find Transaction (10) showing the last DP that had interaction with IMD-A. DP-C signs and posts IMD-A's message to the DP blockchain to request a referral (see Fig. 7).

Referral request is a transaction that is written to DP blockchain and DP-B has to take an action. Since DP blockchain is private, DP-B trusts DP-C. After decrypting the request message, DP-B captures the values ID_A, pub_B, n_2, and ECG_2. DP-B checks the nonce for freshness. If ID_A, pub_B matches with the clear text, DP-B writes a referral transaction including the following information to the DP blockchain.

$$ID_A \,||\, pub_C \,||\, E_{pub_C}(ID_A||pub_C||n_2||ECG_2)$$

DP-C reads the referral from the DP blockchain and using the private key, $priv_C$, DP-C decrypts the values ID_A, pub_C, n_2 and ECG_2. In particular, n_2 and ECG_2 now can be used for setting up an authenticated channel with IMD-A. DP-C generates the new ECG key k_2 from ECG_2, which makes k_2 a ECG shared key between IMD-A and DP-C.

DP-B simply encrypts and sends "$n_2 - 1||pub_C$" using a symmetric key algorithm with the shared ECG key k_2.

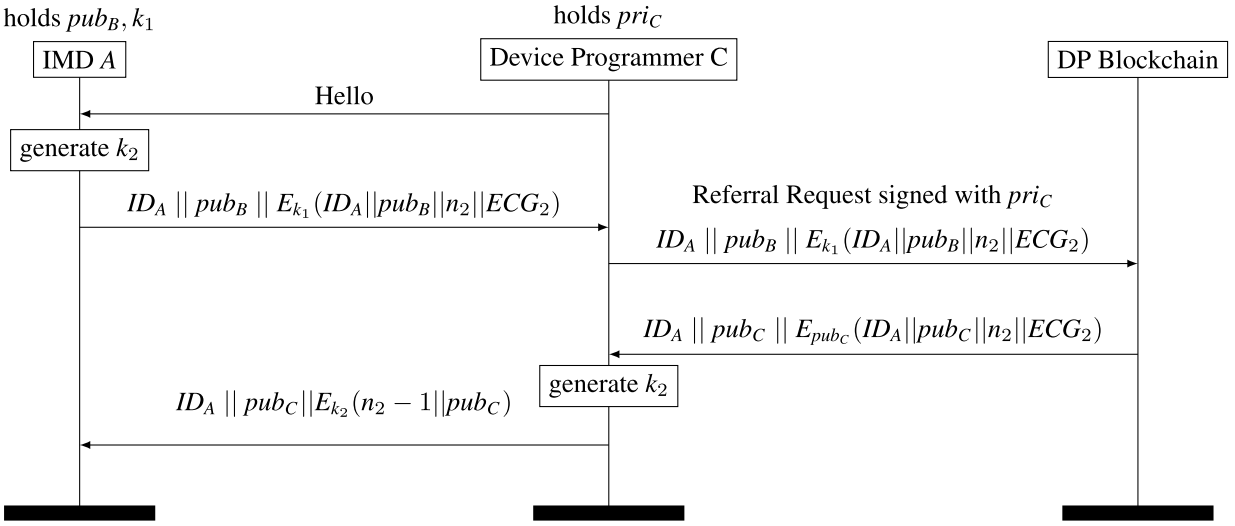

FIGURE 7. Authentication for a different DP interaction.

IMD-A decrypts the message with k_2 and verifies the nonce. Both parties update the lastly shared key with k_2.

IMD-A updates the latest DP by adding pub_C to its secure storage. DP-C writes the IMD-A interaction record to the DP blockchain as a transaction with the lastly used shared key k_2.

$$ID_A \,||\, pub_C \,||\, E_{k_2}(ID_A||pub_C||n_2)$$

Case #3: In case of an emergency, the emergency personal could need to access the IMD immediately. Referral requests might take some time due to DP responses and this might cause fatalities. To authenticate the emergency medical services (EMS), we propose to use a PKI. The number of emergency technicians (EMT) in the US is comparably small (about 200K [25]) and since EMS organizations are strictly regulated and mostly hierarchically structured, it is easy to manage a PKI in these organizations. A single root CA would suffice to manage the whole emergency organization. Daily or some short-term certificates would solve the revocations.

We assume that root EMS CA ($EMS - CA$) certificates are embedded in all the IMD devices during provisioning. We also let the EMT certificates are signed by the root CA. Even managing a daily certificate should not be a problem considering the total number of EMTs in duty. Whenever an EMT (e.g., EMT_X) needs to access an IMD device, EMT_X sends a "Hello Emergency" message. IMD-A generates a new ECG key k_3 but does not use it immediately. Instead sends

$$ID_A \,||\, n_0 \,||\, pub_B \,||\, E_{k_0}(ID_A||pub_B||n_1)$$

to authenticate EMT_X where n_0 is a nonce in addition to the information shares in previous cases. From these EMT_X might check the DP blockchain for patient's or DP's records (if EMTs have access to the DP blockchain).

We assume EMT_X has physical access to the patient and can generate the ECG key k_3 from synchronized ECG readings. EMT_X sends EMT certificate signed by the $EMS - CA$ as seen in Fig. 8. Knowing the $EMS - CA$'s public key IMD-A simply validates pub_X by verifying the $EMS - CA$'s signature. Moreover, IMD-A may also authenticate EMT_X by verifying the EMT_X's signature on the nonce n_3. After these verifications, IMD-A encrypts and sends $n_X - 1$ using a symmetric key algorithm with key k_3.

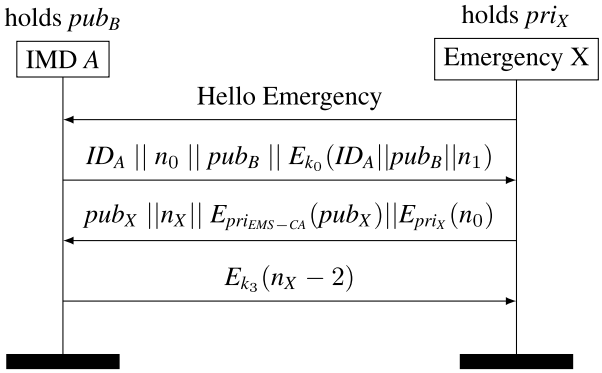

FIGURE 8. Authentication in case of an emergency.

Notice that Case #3 requires public key encryption capacity on the IMD device where more common cases #1 and #2 only need symmetric key algorithms. Since the total number of IMD devices and EMTs are fairly small, some group key scheme with blockchain-based symmetric key management can possibly be deployed to have a symmetric key only solution to cover the emergency use case. We reserve such an approach for future research.

B. SECURITY ANALYSIS

We simply adopt the adversary model in the literature for IMD and DP interactions [31], [33]. The adversary is assumed to be active and has full access to the network. It cannot compromise the Programmer or IMD but may modify, replay,

drop and forge messages in the network. We address weaknesses found in recent protocols including reflection and man-in-the-middle (MITM) attacks presented in [20].

We analyze the security protocol case-by-case:

Case #1: is a standard shared key scheme where IMD and DP have a shared secret k_0. The DP who has the key may decrypt and access n_1. The message authentication is provided by adding the clear-text values ID_A and pub_A to the plaintext. Therefore, IMD would only start to use the newly generated ECG key k_1 once the nonce is validated.

Case #2: is the solution where the patient interacts with a new doctor. Since there are no pre-shared keys, IMD would want to authenticate the new DP, $DP - C$. Therefore, we naturally want a token from the last DP that had interacted with the IMD device. For this, a trust relationship between all DPs is necessary and a private blockchain may provide such trust relations.

We assume that a private DP blockchain with a strict membership process builds the trust between all the DPs that are in the network. All the IMD interaction records can be stored in the DP blockchain. By assigning different IDs in every visit may even anonymize the patients' doctor's visit if needed but this is not in our scope at this study.

We follow the protocol; whenever DP-C gets the "hello" response, DP-C learns that IMD-A is a new patient. DP-C now needs to get the referral token n_2 from the DP-B holding the pri_B. In fact, this is not much different from Case #1, it is still a standard shared key scheme but DP-C needs to find the DP in the blockchain that holds the key k_1. DP-C requests a referral to the DP blockchain by signing the message coming from the IMD-A.

Note that if an adversary becomes a DP fraudulently (e.g. DP-E), the adversary DP-E may sign and send the referral request (5) to DP-A via blockchain. However, this would be easily detectable by DP-C while waiting for a token but seeing DP-E is getting it. DP-C may report the incident and the private network may take the necessary actions including DP-E revocation and transaction callback.

Another scenario could be that DP-E sneakily wants to get a referral and access to a patient's IMD at some other time. Since every interaction is recorded in the DP blockchain, these activities could also be revealed by the patient once querying the DP blockchain. There could be a decentralized application (called dAPP in the blockchain) that can notify patients once their IMD device is referred. Therefore, an attack of this type is unlikely to happen in a referral requesting.

The referral is written to the blockchain, and the information needed by the new DP is provided by public-key encryption. The new DP simply decrypts and gets these values where the ECG key k_2 can be generated. These operations and symmetric key operation encrypting $(n_2 - 1||pub_C)$" are standard. Once IMD-A verifies n_2, authentic communication becomes possible.

Case #3: to analyze the emergency case is easy as there is a PKI in place. Since IMD devices include $EMS - CA$, the certification of EMT_X is verifiable. Moreover, the signature on n_0 verifies that the message really sends by EMT_X. After these verifications, a symmetric key algorithm with ECG generates key k_3.

VI. EXPERIMENTAL SETUP AND RESULTS

A. BENCHMARK

To evaluate our ECG key generation, we utilize the largest ECG benchmark called PTB-XL dataset. The PTB-XL contains 21837 users collected from a 12-lead ECG sensor (I, II, III, AVL, AVR, AVF, V1, …, V6) with 10 seconds length from 18885 patients. Schiller AG devices have been employed to measure the PTB-XL ECG dataset over nearly seven years between October 1989 and June 1996. The PTB-XL database contains diverse demographic information such as gender, age, healthy, unhealthy, where 52% of the records are male and 48% of the records are female with ages covering the whole range from 0 to 95 years. In addition, the PTB-XL are collected with 16-bit precision at a resolution and a sampling frequency of 500Hz. *Note that sum of statements exceeds the number of records because of potentially multiple labels per record*. Table 1 is a summary of the PTB-XL database in terms of normal status. Here, healthy ECG records are set with NORM as the only diagnostic label and non-healthy as its complement. *Note that while the different health conditions have no tangible impact on our ECG key generation, we have included them to illustrate the robustness of our scheme to different kinds of input signals.*

B. TESTING PROCEDURE FOR RANDOMNESS

In order to evaluate and analyze randomness of generated keys from ECG signal, min-entropy and several statistical NIST tests has been performed [34], [37]. **Entropy Analysis:** Min-entropy is used as the conservative measure of the strength of the key and should be large enough to resist against attacks. In this paper, we calculate the min-entropy of a feature k as follows

$$H_\infty(k) = -\xi \log_2 (\max \{P_i(k)\}) \tag{6}$$

where $P_i(k) = \Pr(X = i)$ for the k^{th} key bits. ξ is a normalizing parameter set equal to $\frac{1}{8}$ for 8-bits binary of each feature. Note that the maximum min-entropy (1) occurs when $P_i = \frac{1}{2^n} \forall i$, where the n indicates 8-bits quantization per feature sets. If the min-entropy is close to 1, this means that the adversary has the smallest chance of guessing the correct key in the first try. We have tested more than 21,000 user ECG keys to evaluate the min-entropy from all possible key generation. Fig 9, illustrate the average min-entropy results for all the user. As can be seen in Fig 9, the min-entropy value is larger than 0.9 which is statistically close to uniform [2].

We also computed the average hamming distance (HD) fraction among all pairs of ECG key bits that were extracted from the different users and segments based on our ECG key based generation scheme. Fig. 10 shows the distribution of HD fraction (percentage of zeros and ones in a sequence of key bits) from the 21837 users along with 10 segments

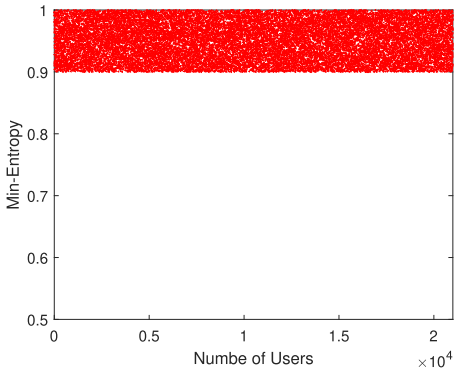

FIGURE 9. Min-entropy value for every 128 key bits from all individuals.

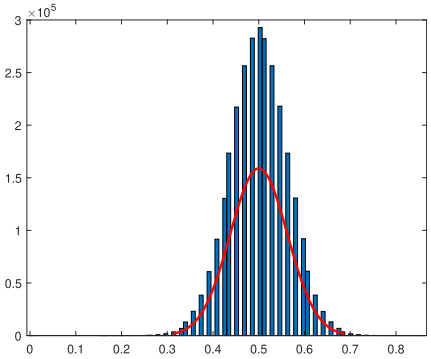

FIGURE 10. Distribution of Hamming wight of 21837 user's ECG among the different extracted keys.

per users. The average HD is 0.50 and it is the ideal 0.5. Hence, the proposed ECG key can provide unique identifiers. As shown in Fig. 10, the HD points tend to be very close to the mean of the set, as can be seen by the very small standard deviation of 0.0325. *Note that if the HD uniqueness measure discussed above is 50%, it does not grantee that data are necessarily random. To evaluate the randomness of a biokey, statistical tests such as the NIST test [34]*

C. NIST STATISTICAL TESTS SUITE

NIST suite is useful platform to check in deviations of a binary sequence from randomness in different applications. A statistical test is formulated to test a specific **null hypothesis** (the randomness hypothesis). NIST suite test consisting of fifteen different tests that were developed to test the randomness of, and for each applied test, a decision or conclusion from randomness statistic is used to determine the acceptance or rejection of the null hypothesis. If the randomness assumption is true for data, it outcomes in P values that shows the given sequences based on that test is random (if values larger than 0.01) else not. In other word, A p-value≥0.01 (normally 1%) that means the key bits will be considered to be random with a confidence of 99% [34]. Following are 15 statistical tests of NIST which are carried out on generated ECG key bits in this study.

TABLE 3. NIST results of amplitude difference features.

Test Name	P-Value	Result
Frequency Test	0.1078	Random
Frequency Test Within a Block	0.6912	Random
Run Test	0.3531	Random
Longest Run of Ones in Block	0.83	Random
Binary Matrix Rank Test	0.38	Random
Discrete Fourier Transform (Spectral) Test	0.5088	Random
Non-Overlapping Template Matching Test	0.5328	Random
Overlapping Template Matching Test	0.136	Random
Maurer's Universal Statistical Test	0.638	Random
Linear Complexity Test	0.9804	Random
Serial Test	0.0675	Random
Approximate Entropy Test	0.4541	Random
Cumulative Sums (Forward) Test	0.2087	Random
Cumulative Sums (Reverse) Test	0.1805	Random
Random Excursion Test	0.666	Random
Random Excursion Variant Test	0.7414	Random

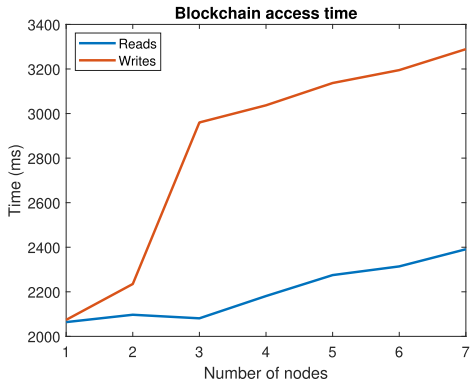

FIGURE 11. IMD write timings & read timings from to blockchain (ms) & blockchain (ms).

If the computed P-value is <0.01, then conclude that the sequence is non-random. Otherwise, conclude that the sequence is random. As can be seen in Table 3, several analysis has been conducted in NIST 800-22 statistical test suite that can determine whether ECG keys has a recognizable pattern. In other word, the ECG key based generated from our scheme is significantly random. Table 3 shows that all the NIST tests p-value are greater than 0.01, this indicates that the measurements pass the requirements for randomness.

D. EXPERIMENTS FOR THE BLOCKCHAIN-BASED AUTHENTICATION PROTOCOL

We evaluated the proposed authentication protocol on Ethereum where we setup our personal Blockchain network. We used OpenSSL version 2.8.3 to generate public/private key pairs; crypto.js version 4.0.0 for encryption and decryption; Go-Ethereum version v1.9.25 to execute commands and run tests; Solidity version 0.4.17 for smart contracts.

We run the above software stack on Ubuntu 16.04.1 LTS (64-bit) CPU Intel(R) Xeon(R) CPU E5-4620 0 @ 2.20GHz VM Machine having 4 cores and 16 GB memory. Fig. 11 shows a communication overhead for a small private Ethereum network having several nodes running the protocol.

The communication cost can be considered between a doctor (or a programmer) and the private blockchain network. As demonstrated in Fig. 11, the overhead of the writing time is greater than the reading time as the number of nodes increases. The overhead cost will vary depending on the communication environment.

VII. CONCLUSION

This paper proposes a new key generation scheme for Implantable Medical Devices (IMD) and a new authentication protocol for the IMD applications. Previous research has shown that ECG can be taken as a basis for key generation using IPI techniques. However, these approaches do not consider fiducial features and generally require approximately 30 seconds to generate a 128-bit random key. To address these drawbacks, we proposed a novel key generation mechanism by focusing on a single ECG heartbeat to generate a 128-bit random key using amplitude differences from fiducial features. To evaluate and analyze the randomness of generated keys, several statistical NIST tests have been performed. Moreover, to address the weaknesses of active attacks on authentication protocols, such as man-in-the-middle (MITM) attacks and replay attacks, novel authentication using blockchain technology has been proposed with three different important scenarios. With the security analysis, the three cases have been studied as follows; (i) where the IMD device A, IMD-A interacts with a known Device Programmer B, DP-B;(ii) where the patient visits a new doctor and the stored public key or shared key in the IMD memory could not be used for authentication, a private blockchain can be used to solve this problem; (ii) where the emergency personal need to access the IMD immediately. As a result, we achieved the most efficient and secure key generation and authentication method with high speed and randomness to prevent network-based attacks.

REFERENCES

[1] D. K. Altop, A. Levi, and V. Tuzcu, "Towards using physiological signals as cryptographic keys in body area networks," in *Proc. 9th Int. Conf. Pervasive Comput. Technol. Healthcare (PervasiveHealth)*, May 2015, pp. 92–99.

[2] L. Ballard, S. Kamara, and M. K. Reiter, "The practical subtleties of biometric key generation," in *Proc. USENIX Secur. Symp.*, 2008, pp. 61–74.

[3] S.-D. Bao, C. C. Y. Poon, Y.-T. Zhang, and L.-F. Shen, "Using the timing information of heartbeats as an entity identifier to secure body sensor network," *IEEE Trans. Inf. Technol. Biomed.*, vol. 12, no. 6, pp. 772–779, Nov. 2008.

[4] C. Camara, P. Peris-Lopez, and J. E. Tapiador, "Security and privacy issues in implantable medical devices: A comprehensive survey," *J. Biomed. Informat.*, vol. 55, pp. 272–289, Jun. 2015.

[5] S. Cherukuri, K. K. Venkatasubramanian, and S. K. S. Gupta, "BioSec: A biometric based approach for securing communication in wireless networks of biosensors implanted in the human body," in *Proc. Int. Conf. Parallel Process. Workshops*, Oct. 2003, pp. 432–439.

[6] H. Chizari and E. Lupu, "Extracting randomness from the trend of IPI for cryptographic operations in implantable medical devices," *IEEE Trans. Dependable Secure Comput.*, vol. 18, no. 2, pp. 875–888, Mar. 2021.

[7] K. Cho and D. H. Lee, "Biometric based secure communications without pre-deployed key for biosensor implanted in body sensor networks," in *Proc. Int. Workshop Inf. Secur. Appl.* Cham, Switzerland: Springer, 2011, pp. 203–218.

[8] C. Li, A. Raghunathan, and N. K. Jha, "Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system," in *Proc. IEEE 13th Int. Conf. E-Health Netw., Appl. Services*, Jun. 2011, pp. 150–156.

[9] S. Eberz, N. Paoletti, M. Roeschlin, M. Kwiatkowska, I. Martinovic, and A. Patané, "Broken hearted: How to attack ECG biometrics," in *Proc. Network Distrib. Syst. Secur. Symp.*, 2017, pp. 1–15.

[10] K. Fu, "Inside risksReducing risks of implantable medical devices," *Commun. ACM*, vol. 52, no. 6, pp. 25–27, Jun. 2009.

[11] D. Halperin, T. S. Heydt-Benjamin, K. Fu, T. Kohno, and W. H. Maisel, "Security and privacy for implantable medical devices," *IEEE Pervasive Comput.*, vol. 7, no. 1, pp. 30–39, Jan. 2008.

[12] J. A. Hansen and N. M. Hansen, "A taxonomy of vulnerabilities in implantable medical devices," in *Proc. 2nd Annu. Workshop Secur. Privacy Med. Home-Care Syst.*, Oct. 2010, pp. 13–20.

[13] X. Hei, X. Du, J. Wu, and F. Hu, "Defending resource depletion attacks on implantable medical devices," in *Proc. IEEE Global Telecommun. Conf. GLOBECOM*, Dec. 2010, pp. 1–5.

[14] C. Hu, X. Cheng, F. Zhang, D. Wu, X. Liao, and D. Chen, "OPFKA: Secure and efficient ordered-physiological-feature-based key agreement for wireless body area networks," in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 2274–2282.

[15] M. Ingale, R. Cordeiro, S. Thentu, Y. Park, and N. Karimian, "ECG biometric authentication: A comparative analysis," *IEEE Access*, vol. 8, pp. 117853–117866, 2020.

[16] M. S. Islam, "Using ECG signal as an entropy source for efficient generation of long random bit sequences," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 34, no. 8, pp. 5144–5155, Sep. 2022.

[17] M. S. Islam, N. Alajlan, Y. Bazi, and H. S. Hichri, "HBS: A novel biometric feature based on heartbeat morphology," *IEEE Trans. Inf. Technol. Biomed.*, vol. 16, no. 3, pp. 445–453, May 2012.

[18] N. Karimian, Z. Guo, M. Tehranipoor, and D. Forte, "Highly reliable key generation from electrocardiogram (ECG)," *IEEE Trans. Biomed. Eng.*, vol. 64, no. 6, pp. 1400–1411, Jun. 2017.

[19] Q. Lin, W. Xu, J. Liu, A. Khamis, W. Hu, M. Hassan, and A. Seneviratne, "H2B: Heartbeat-based secret key generation using piezo vibration sensors," in *Proc. 18th ACM/IEEE Int. Conf. Inf. Process. Sensor Netw. (IPSN)*, Apr. 2019, pp. 265–276.

[20] E. Marin, E. Argones Rua, D. Singelée, and B. Preneel, "On the difficulty of using patient's physiological signals in cryptographic protocols," in *Proc. 24th ACM Symp. Access Control Models Technol.*, May 2019, pp. 113–122.

[21] E. Marin, M. A. Mustafa, D. Singelee, and B. Preneel, "A privacy-preserving remote healthcare system offering end-to-end security," in *Proc. Int. Conf. Ad-Hoc Netw. Wireless*. Cham, Switzerland: Springer, 2016, pp. 237–250.

[22] MarketsAndMarkets. (Jun. 12, 2005). *Active Implantable Medical Devices Market*. [Online]. Available: https://www.marketsandmarkets.com/

[23] P. Melzi, R. Tolosana, and R. Vera-Rodriguez, "ECG biometric recognition: Review, system proposal, and benchmark evaluation," *IEEE Access*, vol. 11, pp. 15555–15566, 2023.

[24] S. Nakamoto. (2009). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: http://www.bitcoin.org/bitcoin.pdf

[25] *Data USA: Emergency Medical Technicians Paramedics*. [Online]. Available: https://datausa.io/profile/soc/emergency-medical-technicians-paramedics

[26] J. Pan and W. J. Tompkins, "A real-time QRS detection algorithm," *IEEE Trans. Biomed. Eng.*, vol. BME-32, no. 3, pp. 230–236, Mar. 1985.

[27] S. Peter, B. Pratap Reddy, F. Momtaz, and T. Givargis, "Design of secure ECG-based biometric authentication in body area sensor networks," *Sensors*, vol. 16, no. 4, p. 570, Apr. 2016.

[28] V. L. Petrovic, M. M. Jankovic, A. V. Lupsic, V. R. Mihajlovic, and J. S. Popovic-Božovic, "High-accuracy real-time monitoring of heart rate variability using 24 GHz continuous-wave Doppler radar," *IEEE Access*, vol. 7, pp. 74721–74733, 2019.

[29] C. C. Y. Poon, Y.-T. Zhang, and S.-D. Bao, "A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health," *IEEE Commun. Mag.*, vol. 44, no. 4, pp. 73–81, Apr. 2006.

[30] W. H. Press and S. A. Teukolsky, "Savitzky-Golay smoothing filters," *Comput. Phys.*, vol. 4, no. 6, pp. 669–672, Nov. 1990.

[31] K. B. Rasmussen, C. Castelluccia, T. S. Heydt-Benjamin, and S. Capkun, "Proximity-based access control for implantable medical devices," in *Proc. 16th ACM Conf. Comput. Commun. Secur.*, Nov. 2009, pp. 410–419, doi: 10.1145/1653662.1653712.

[32] T. M. Research, "Implantable medical devices market—Global industry analysis, size, share, growth, trends, and forecast, 2019–2027," Tech. Rep., 2020.
[33] M. Rostami, A. Juels, and F. Koushanfar, "Heart-to-heart (H2H): Authentication for implanted medical devices," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2013, pp. 1099–1112.
[34] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Booz-Allen and Hamilton, Mclean, VA, USA, Tech. Rep., 2001.
[35] M. Rushanan, A. D. Rubin, D. F. Kune, and C. M. Swanson, "SoK: Security and privacy in implantable medical devices and body area networks," in *Proc. IEEE Symp. Secur. Privacy*, May 2014, pp. 524–539.
[36] F. Shaffer and J. P. Ginsberg, "An overview of heart rate variability metrics and norms," *Frontiers Public Health*, vol. 5, p. 258, Sep. 2017.
[37] E. Simion, "The relevance of statistical tests in cryptography," *IEEE Secur. Privacy*, vol. 13, no. 1, pp. 66–70, Jan. 2015.
[38] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: A state of the art survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 858–880, 1st Quart., 2019.
[39] K. K. Venkatasubramanian, A. Banerjee, and S. Kumar S. Gupta, "PSKA: Usable and secure key agreement scheme for body area networks," *IEEE Trans. Inf. Technol. Biomed.*, vol. 14, no. 1, pp. 60–68, Jan. 2010.
[40] K. K. Venkatasubramanian and S. K. S. Gupta, "Physiological value-based efficient usable security solutions for body sensor networks," *ACM Trans. Sensor Netw.*, vol. 6, no. 4, pp. 1–36, Jul. 2010.
[41] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, "EKG-based key agreement in body sensor networks," in *Proc. IEEE INFOCOM Workshops*, Apr. 2008, pp. 1–6.
[42] F. Xu, Z. Qin, C. C. Tan, B. Wang, and Q. Li, "IMDGuard: Securing implantable medical devices with the external wearable guardian," in *Proc. IEEE INFOCOM*, Apr. 2011, pp. 1862–1870.
[43] G.-H. Zhang, C. C. Y. Poon, and Y.-T. Zhang, "Analysis of using interpulse intervals to generate 128-bit biometric random binary sequences for securing wireless body sensor networks," *IEEE Trans. Inf. Technol. Biomed.*, vol. 16, no. 1, pp. 176–182, Jan. 2012.
[44] Z. Zhang, H. Wang, A. V. Vasilakos, and H. Fang, "ECG-cryptography and authentication in body area networks," *IEEE Trans. Inf. Technol. Biomed.*, vol. 16, no. 6, pp. 1070–1078, Nov. 2012.
[45] G. Zheng, G. Fang, R. Shankaran, and M. A. Orgun, "Encryption for implantable medical devices using modified one-time pads," *IEEE Access*, vol. 3, pp. 825–836, 2015.

NIMA KARIMIAN (Member, IEEE) is currently an Assistant Professor with the Lane Department of Computer Science and Electrical Engineering (LCSEE), West Virginia University. His research interests include biometric security and the application of machine learning in the field of cybersecurity. He has made significant contributions to these areas and has been recognized with several notable awards. He has been an active member of several technical program committees, including HOST and ISQED. He received the IAPR TC4 Best Student Paper Award from the International Joint Conference on Biometrics (IJCB), the Best Technical Paper Award from the 30th International Conference on VLSI Design (VLSID), and the Best Poster Award from the FICS Research Conference on Cybersecurity. In 2021, he was honored with the Faculty Excellence in Scholarship Award from San José State University (SJSU). He served on the organizing committees of various conferences, such as ISQED and SVCC. He is serving as an Associate Editor for the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—I: REGULAR PAPERS, and the *Discover Internet of Things* (DIoT) journal and *SN Computer Science* journal (Springer).

GOKAY SALDAMLI received the Ph.D. degree in electrical and computer engineering from Oregon State University, in June 2005. He was with the Samsung Smartcard Division, Glaneyre Technologies, Hewlett-Packard Enterprise, Samsung Research America, and security-related startups. He has been an Assistant Professor of computer engineering with San José State University, San Jose, CA, USA, since 2016. He has been working in the areas of computer and network security, privacy, applied cryptography, computer arithmetic, and embedded computing more than 15 years. He is currently with the Computer Engineering Department, San José State University. His research interests include applied cryptography, blockchains, secure cloud computing, private big data analytics, and security of mobile systems and applications.

YOUNGHEE PARK (Senior Member, IEEE) received the Ph.D. degree in computer science from North Carolina State University, in 2010. She is currently an Associate Professor of computer engineering with San José State University (SJSU) and a Visiting Professor with IBM Almaden Research. She is a coordinator for the cybersecurity certificates program with SJSU, supported by the National Information Assurance Education and Training Program (NIETP). Her research interests include network and system security with an emphasis on malware detection, insider attacks, botnets, SDN/NFV security, and the IoT security. She served as the Kordestani Endowed Chair for the College of Engineering, SJSU, in 2016 and 2017, and as a Distinguished Research Professor. She received the Best Paper Award-Honorable Mention Award from the 21st ACM SACMAT, in 2016, and the Best Paper Award from ACM SIGCSE, in 2018. She received the Faculty Excellence Award in scholarship from the College of Engineering, SJSU, in May 2018.

VICTOR LUI (Member, IEEE) received the bachelor's degree from San José State University, in 2021. He is currently pursuing the degree in electrical and computer engineering with the University of Southern California, Los Angeles, CA, USA. His research interests include machine learning (ML), blockchain, and security and privacy of implantable medical device.