Privacy Assured Recovery of Compressively Sensed ECG Signals

Hadi Zanddizari, Sreeraman Rajan, Houman Zarrabi, Hassan Rabah

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received January 27, 2022, accepted February 2, 2022, date of publication February 7, 2022, date of current version February 16, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3149890

Privacy Assured Recovery of Compressively Sensed ECG Signals

HADI ZANDDIZARI[1], (Student Member, IEEE), SREERAMAN RAJAN[2], (Senior Member, IEEE), HOUMAN ZARRABI[3], (Senior Member, IEEE), AND HASSAN RABAH[4], (Senior Member, IEEE)

[1]Department of Electrical Engineering, University of South Florida, Tampa, FL 33620, USA
[2]Department of Systems and Computer Engineering, Carleton University, Ottawa, ON K1S 5B6, Canada
[3]Department of Communications Technology, ITRC, Tehran 1439955471, Iran
[4]Institut Jean Lamour (IJL), Université de Lorraine, UMR 7198, 54000 Nancy, France

Corresponding author: Hadi Zanddizari (hadiz@usf.edu)

This work was supported by the Natural Science and Engineering Research Council of Canada (NSERC).

ABSTRACT In the areas of communications engineering and biomedical engineering, cloud computing for storing data and running complex algorithms have been steadily increasing due to the increase in internet of things and connected health. As connected IoT devices such as wearable ECG recorders generally have less storage and computational capacity, acquired signals get sent to a remote center for storage and possible analysis on demand. Recently, compressive sensing has been used as a secure, energy-efficient and fast method of signal sampling in such recorders. In this paper, we propose a secure procedure to shift away the total recovery of compressively sensed measurement to cloud and introduce a privacy-assured signal recovery technique in the cloud. We present a fast, and lightweight encryption for secure CS recovery outsourcing that can be used in wearable devices, such as ECG Holter monitors. In the proposed technique, instead of full recovery of CS-compressed ECG signal in the cloud, to preserve privacy, an encrypted version of ECG signal is recovered by using a randomly bipolar permuted measurement matrix. The user with a key, decrypts the encrypted ECG from the cloud to obtain the original ECG signal at their end. We demonstrate our proposed method using the ECG signals available in the MIT-BIH Arrhythmia Database. We also demonstrate the strength of the proposed method against partial exposure of the key. Experimental results on client and cloud sides show our proposed method has lower complexity and consuming time compared to the recent related works, while maintaining the quality of outsourcing task in cloud.

INDEX TERMS Compressive sensing, ECG signal, privacy-preserving outsourcing, IoT, connected health.

I. INTRODUCTION

In biomedical area, there are equipment and devices that produce huge amount of data. As an example, Holter monitor, a wearable device, is used for continuous monitoring of the electrical activity of the heart, namely electrocardiogram (ECG). Holter monitor is used by cardiac patients for several days to capture events such as cardiac arrhythmia. Even in cases where physiological signals are recorded only intermittently, say by devices such as Empatica watch that have limited on the device storage memory, the amount of data produced is large that an external storage solution is in order. The ECG data produced by devices such as a Holter monitor is large and therefore, need to be stored for analysis and tracking improvements in the physiology for medical interventions to be undertaken. Under such circumstances, compression can be used for efficient use of communication channel bandwidth and storage in such devices.

Recently, compressive sensing (CS) has emerged as a fast and energy-efficient algorithm for simultaneous sampling and compressing of potentially sparse signals [1], [2]. CS has a wide variety of applications in signal processing such as biomedical signal compression, enhancement, and recovery [3]. The applications of CS has also been extended to ECG signal under the assumption that ECG signals are compressible signal [4]–[11]. In [4], CS-based compression was shown to present the best overall energy efficiency due to its lower complexity and also reduced CPU execution time. Since compression phase in CS is simple, fast, and energy efficient, CS has been chosen for compression in many sensing applications. However, recovery phase which is non-linear and complex in terms of computations demands the use

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

of processors that have speed, large on-board memory and computational capability. Currently, wearable devices do not have such capabilities and storage; therefore, recovery need to be outsourced. In addition, clinics and hospitals, usually generate enormous amount of data, thereby requiring a place to store the data. Cloud environments generally provide ''unlimited'' resources and facilities. Hence, cloud can be used for storing CS-based compressed ECG signal, and based on user request, ECG signal can be recovered. However, the cloud as a third party between the real user (patient) and the clinic should not be permitted to have access to the recovered ECG signal which will be referred to as the plaintext in this paper. In this case we should consider using edge computing for recovery.

There are numerous works that have proposed different procedures for secure CS recovery outsourcing [12]–[14]. There are some research papers that specifically focus on methods for assuring the secrecy of ECG data in communication [15]–[17]. Recently, T.Y. Liu et al proposed a new encryption-then-compression (ETC) method for the ECG signal [15]. In this work, authors encrypt ECG signal with a common key. Their proposed key is a square orthogonal random matrix that changes after sending every encrypted ECG signal (ciphertext). Hence, their method can be classified as a one-time-pad cryptosystem. For compression, they apply a transformation based algorithm in which singular value decomposition (SVD) technique is used [18]. However, the cryptosystem just focuses on compression and does not consider the security of the data. In [15], a modification has been made on SVD technique to provide secrecy as well. SVD-based methods bring higher compression ratio (CR). They are computationally intensive and may introduce delay in the system. In contrast, at the expense of having a lower CR, CS-based methods are linear, faster, and energy efficient [19].

Compression may be used for efficient storage of recorded ECG signals in ECG recorders. CS can also be used on edge devices as it requires less computational resources to acquire and store signals. Recovery of compressed signals need a lot of computational resources and therefore need to be outsourced to a cloud. Compression will also help in the efficient use of communication channel bandwidth between the edge device (or an ECG recorder) and the cloud. Compressive sensing is advantageous for IoT devices because these devices have limited storage and computational facilities when compared to a remote computing centers or cloud. However, recovering an ECG signal on the cloud may compromise the privacy of data. Therefore, this paper proposes a light-weight privacy-preserving CS recovery service on cloud environment. The proposed method not only preserves the privacy, but it also maintains the quality of recovery.

The paper is arranged in the following manner. In next section, CS is introduced and presented as a cryptosystem, and followed by the background research in secure CS recovery outsourcing. Section III contains the proposed method followed by security analysis and experimental results to verify the secrecy of the method in section IV. Finally Section V concludes the paper.

II. BACKGROUND

A. COMPRESSIVE SENSING

Compressive sensing (CS) is a sampling technique for efficiently sampling a signal by solving under-determined linear systems [1], [2]. It takes advantage of the signal's sparsity, and the signal can be effectively represented by fewer number of measurements than the Nyquist rate. For instance, given an ECG signal $\mathbf{x} \in \mathbb{R}^N$ and an orthogonal basis $\mathbf{\Psi} \in \mathbb{R}^{N\times N}$, then one can map the ECG signal to sparse domain via, $\mathbf{x} = \mathbf{\Psi} s$, where $\mathbf{s} \in \mathbb{R}^N$ is sparse vector with k ($k \ll N$) nonzero entries. In other words, $\mathbf{s}$ is a sparse representation of $\mathbf{x}$ under the chosen predefined dictionary. Compression phase in CS provides the measurement vector through a linear operation as given below:

$$\mathbf{y} = \mathbf{\Phi x} = \mathbf{\Phi \Psi s} \tag{1}$$

where, $\mathbf{y} \in \mathbb{R}^M$ is the measurement vector and $\mathbf{\Phi} \in \mathbb{R}^{M\times N}$ is the measurement matrix. For simplicity, let $\mathbf{A} = \mathbf{\Phi \Psi}$. $\mathbf{A} \in \mathbb{R}^{M\times N}$ is a rectangular matrix, sometimes referred to as ''total'' dictionary in the CS literature. For exact and stable recovery of sparse signal, *restricted isometry property* (RIP) is a sufficient condition [20]. RIP is satisfied if there exists a restricted isometry constant (RIC) δ_K, $0 < \delta_K < 1$ such that

$$(1 - \delta_K)\|\mathbf{s}\|_2^2 \leq \|\mathbf{As}\|_2^2 \leq (1 + \delta_K)\|\mathbf{s}\|_2^2 \tag{2}$$

where δ_K denotes isometry constant of a matrix $\mathbf{A}$, and its value belongs to a set of real numbers between zero and one. But, checking the RIP condition of a matrix or calculating the value of its isometry constant is difficult to verify. Hence, conditions that lead to RIP were proposed [21], [22]. Another condition, which is easier to verify in practice, is the requirement that measurement matrix $\mathbf{\Phi}$ must be incoherent with the sparsity basis $\mathbf{\Psi}$. Mutual coherence μ between $\mathbf{\Phi}$ and $\mathbf{\Psi}$ is defined as follow:

$$\mu(\mathbf{\Phi}, \mathbf{\Psi}) = \sqrt{N} \max_{i,j} \frac{|\langle \boldsymbol{\phi}_i, \boldsymbol{\psi}_j \rangle|}{\|\boldsymbol{\phi}_i\|_2 \|\boldsymbol{\psi}_j\|_2} \tag{3}$$

where $\boldsymbol{\phi}_{i\in\{1,\ldots,M\}}$ and $\boldsymbol{\psi}_{j\in\{1,\ldots,N\}}$ respectively represent the row vectors of $\mathbf{\Phi}$ and the column vectors of $\mathbf{\Psi}$. The coherence measures the maximum correlation between the two matrices. Smaller coherence can lead to better signal reconstruction performance [23]. Since $\mu \in [1, \sqrt{N}]$, the matrices $\mathbf{\Phi}$ and $\mathbf{\Psi}$ are incoherent if $\mu(\mathbf{\Phi}, \mathbf{\Psi})$ is closer to one, which corresponds to the lower bound of μ.

A step called the *recovery process* reconstructs the input signal $\mathbf{x}$ from the measurement vector $\mathbf{y}$ by solving the equation (1). Since $\boldsymbol{A}$ is a rectangular matrix ($M < N$), the problem formulated in equation (1) is ill-posed and has infinite solutions. However, based on the knowledge that $\mathbf{x}$ has a sparse representation with respect to a basis $\mathbf{\Psi}$, the recovery process can be performed in two steps [20]. The

first step finds the sparse vector $\tilde{\mathbf{s}}$ by solving the following equation:

$$\min_{\tilde{\mathbf{s}}} \|\tilde{\mathbf{s}}\|_0 \text{ such that } \boldsymbol{A}\tilde{\mathbf{s}} = \mathbf{y}. \tag{4}$$

Once the vector $\tilde{\mathbf{s}}$ has been obtained, the second step reconstructs the original signal as follows:

$$\tilde{\mathbf{x}} = \boldsymbol{\Psi}\tilde{\mathbf{s}}. \tag{5}$$

Various methods have been proposed to find an appropriate solution to equation (4) leading to numerous recovery algorithms such as Basic Pursuit [24], [25], StOMP [26], OMP [27], CoSAMP [21], Belief Propagation [28] and SL0 [29].

B. CS AS A CRYPTOSYSTEM

From a different viewpoint, CS can be assumed as a cryptosystem [30]. Since CS can map every sparse signal from N dimensional space to M dimensional space, where $M \ll N$, numerous researchers have considered CS as a strong cryptosystem [30]–[41]. In [41], it was proved that under certain conditions, CS can even meet the perfect secrecy as defined by Shannon. In [42], [43], linear feedback shift registers have been used to generate CS measurement matrix as a key. In [44], a low-complexity approach for privacy-preserving compressive analysis based on subspace-based representation has been proposed to preserve privacy from an information theoretic perspective.

After encrypting the signals using any of the techniques in the previous paragraph, CS-recovery is assumed to be done by the real user. However, in many contexts, devices at the user end may not have enough computational resources to implement the CS recovery. A third party like cloud can be used for doing the recovery process. When privacy needs to be preserved during the recovery process, the key should not be shared with the cloud; therefore the cloud should conduct the CS recovery on encrypted data. After recovery, the data is still encrypted.

Privacy-preserving outsourcing techniques can be used to overcome these concerns when the recovered signal contains private information of an individual. For example, ECG signal contains information that enable unique identification of an individual. Recently, there have been increased interest on ECG for biometric recognition [45]. Temporal features, amplitude features and morphological features of an ECG signal have been used for ECG-based biometric. As ECG signal contains biometrics of the person, privacy is exposed when ECG signals are recovered in the cloud. Hence, a solution that avoids complete recovery to preserve privacy is in order. Cloud environments can be a good option to store the compressed data. But on-demand through CS-recovery, the plaintext should not be exposed in the cloud. This paper provides a privacy assured CS outsourced recovery. Researchers have proposed different methods to shift away the recovery phase of CS in a secure manner [12]–[14]. In this paper, a fast and lightweight privacy-preserving CS recovery approach for ECG signal is proposed.

C. PRIVACY-PRESERVING CS-RECOVERY OUTSOURCING

In privacy-preserving CS-recovery outsourcing, there are three levels of data namely the ciphertext, the intermediate ciphertext, and the plaintext to be considered. The ciphertext is the measurement vector which is compressed or encrypted. Since cloud should not obtain the plaintext, recovery in the cloud yields an encrypted signal. This encrypted signal is called intermediate ciphertext. Intermediate ciphertext is sent to the real user, and real user (let us say Alice) with a private key can decrypt this intermediate ciphertext to obtain the plaintext. Plaintext is the original raw signal that got compressed initially.

Recently, "*Outsourced Image Recovery Service (OIRS)*" was proposed by Cong Wen et al [12] where a technique to securely shift away the recovery of CS in cloud environment was presented. However, the proposed method in [12] required the cloud to solve linear programing (LP) problem to reconstruct the CS-encrypted image (the ciphertext). In other words, OIRS required the cloud to use LP method to convert ciphertext to an intermediate ciphertext. But, LP is only one of the CS recovery methods and its order of complexity is $\mathcal{O}(N^3)$. There are other efficient and faster algorithms from the family of greedy algorithms such as OMP with the order of complexity $\mathcal{O}(kMN)$, or SL0 with the order of complexity $\mathcal{O}(MN)$ that can be used instead of LP method. In addition, OIRS uses multiple keys for assuring privacy. This leads to heavy computation and consumes large time for processing. Such algorithms may not be appropriate for simultaneous encryption and compression of wearable ECG recorders where we have limited power and computational capability. "*Kryptein*" is another CS-based encryption scheme for the internet of things (IoT) that has been proposed by Xue et al [13]. In this work, CS has been used as compression and encryption algorithm. The secrecy of proposed cryptosystem mainly revolves around the sparsifying dictionary. However, it limits CS by choosing the adaptive sparsifying dictionaries. In other words, it uses an adaptive dictionary learning to generate sparsifying dictionary. Then singular value decomposition of the learnt dictionary is used to generate the measurement matrix. This measurement matrix along with a perturbation matrix are used for designing their secret key. Basically dictionary learning and singular value decomposition are two computationally complex and time consuming tasks which may not be implementable on resource constraint edge-devices. In [14], a secure reconstruction of image from CS in cloud was introduced. It assumed CS as a compression algorithm, and not as a sampling method. The pre-processing used in this work led to delays in generating compressed and encrypted signal. This method mapped the initial signal to a sparse domain and then used a threshold to force negligible coefficients to be zero. This method, thus, required all the components of sparse vector to be checked for zeroing, which may not be an efficient way of utilizing the limited computational capability and power of the weak devices such as ECG wearable recorders.

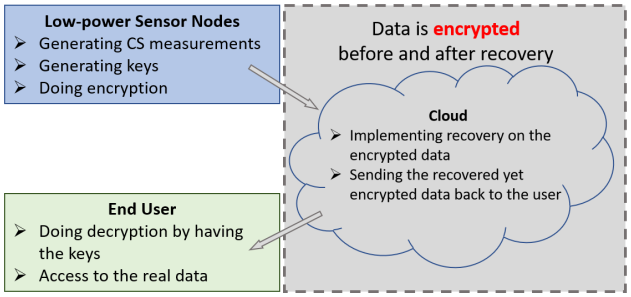

FIGURE 1. Proposed privacy-preserving outsourcing.

In [46], a lightweight privacy-preserving system has been introduced. However, to assure privacy, the sensors after each acquisition will need to send the sensing matrix along with the measurement vector (compressed) to the cloud. This method although may bring high security, it requires very high communication bandwidth as one needs to send the sensing matrix in each acquisition. The gain achieved using CS (that is reduction of the communication costs) is lost in this case and in general, is not an efficient approach when it comes to implementation. In [47], a secure CS recovery service in the cloud that is verifiable and confidential was proposed. The sensing matrix was considered as a public key while a secret orthogonal sparsifying basis was used as a private key. The proposed cryptosystem in [47] cannot maintain the perfect CS recovery quality. Although the approach is applicable for secured image recovery where some degradation in quality can be tolerated, for several compressible biomedical signals such as ECG, quality degradation will lead to possible misdiagnosis. Also, the privacy preserving CS recovery for image signal introduced in [48] suffers from degradation in quality of recovered signal when the signal is encrypted. High quality recovered signal is needed in several areas such as medical diagnosis to make meaningful decisions and take actions based on those decisions. This is a further motivation for our proposed method.

Fig. 1 provides an overall generalized summary of the proposed privacy-preserving outsourcing. Resource-constraint, low power CS sensor(s) (denoted as low-power sensor nodes in the Fig. 1) generates CS measurements from the sparse signal and encrypts the data. The encrypted data is then transferred to the cloud. Then on demand, the cloud implements the CS recovery on encrypted data. After recovery, the recovered data which is still encrypted is sent to the end user. Then, the end user with the keys decrypt the encrypted recovered data.

In this paper a light-weight encryption is applied to map the initial sparse signal to another sparse signal. Considering the fact that sparsity is a required condition for CS, we are limited in options as we cannot violate this condition. In order to maintain sparsity and still achieve light weight encryption, two keys are used: a random square matrix and a random bipolar permutation matrix. The former encrypts the measurement matrix uniquely for each wearable recorder, and the latter encrypts signal after reconstruction in the cloud for secure transmission back to the user.

The contributions of this paper are summarized below:

- A fast and light-weight encryption method that can be implemented on resource constraint edge devices is proposed. Our proposed encryption enables any cloud to do the recovery with the encrypted measurement data. After recovery, the recovered sparse signal is still encrypted. Experimental results on client-side show that our proposed method has lower complexity and execution time when compared to the related works in the recent literature.
- In the proposed approach, the cloud can choose any CS recovery algorithm, and by choosing a fast recovery algorithm, the complexity and the execution time may be reduced.
- It is theoretically shown that the proposed cryptosystem does not affect the quality of recovery. Quality of recovery using the proposed system and the performance of the proposed system is verified through experimentation using MIT physiological signal database.
- The strength of the proposed method against partial exposure of the key is also demonstrated.
- The proposed method can be used for privacy assured recovery of any compressible (or sparse) signal.

III. PROPOSED METHOD

Consider a common scenario where an ECG sensor sends $\mathbf{y} = \mathbf{\Phi x} = \mathbf{\Phi\Psi s}$ to cloud environment for storage. For simplicity, let us suppose $\mathbf{A} = \mathbf{\Phi\Psi}$. On demand for recovery, the cloud (or the remote server) can reconstruct the sparse signal $\mathbf{s}$ if it is supplied with both $\mathbf{y}$ and $\mathbf{A}$. Cloud can choose any CS recovery algorithm to solve the following ℓ_1 *minimization* problem:

$$\min_{\mathbf{s}} \|\mathbf{s}\|_1 \text{ s. t. } \mathbf{As} = \mathbf{y}. \tag{6}$$

Once $\mathbf{s}$ is obtained, the initial ECG signal can be generated using $\mathbf{\Psi}$, i.e; $\mathbf{x} = \mathbf{\Psi s}$. In order to securely shift away the full CS-recovery task, the use of two keys is proposed. The first key is used to encrypt $\mathbf{\Phi}$. Because, measurement matrix is a specific information of every CS-based sensing device, it should not be shared with the third party. In addition, besides the random class of measurement matrices that preserve RIP condition, there are also deterministic approaches to generate a measurement matrix [49]–[51]. Since such deterministic matrices have defined structures, if we encode these structures, then we may increase the secrecy of cryptosystem. To do so, we use a random measurement matrix $\mathbf{Q}_{M\times M}$ to encrypt initial measurement matrix. Then, instead of sending $\mathbf{A}$ to the cloud, $\hat{\mathbf{A}} = \mathbf{Q}(\mathbf{\Phi\Psi}) = \mathbf{QA}$ will be sent. If we multiply $\mathbf{Q}$, the recovery relation is changed as follows:

$$\min_{\mathbf{s}} \|\mathbf{s}\|_1 \quad \text{s. t. } \hat{\mathbf{A}}\mathbf{s} = \mathbf{Qy} = \hat{\mathbf{y}}. \tag{7}$$

When $\hat{\mathbf{A}}$ and $\hat{\mathbf{y}}$ are provided to the cloud, the cloud can reconstruct the sparse vector $\mathbf{s}$. This level of encryption

just hides the measurement matrix but the secrecy of reconstructed signal is still not preserved. To further maintain secrecy, a second key is used in the following manner. We multiply the encrypted measurement matrix with a random bipolar permutation matrix $\mathbf{P}$, an invertible matrix that contains either "$\boldsymbol{\alpha}$ or $-\boldsymbol{\alpha}$" in each row and column at random positions, where $\boldsymbol{\alpha}$ is a random scalar number. For example, a 5×5 $\mathbf{P}$ may be as follows

$$\mathbf{P}_{5\times5} = \begin{bmatrix} 0 & -\boldsymbol{\alpha} & 0 & 0 & 0 \\ +\boldsymbol{\alpha} & 0 & 0 & 0 & 0 \\ 0 & 0 & +\boldsymbol{\alpha} & 0 & 0 \\ 0 & 0 & 0 & 0 & -\boldsymbol{\alpha} \\ 0 & 0 & 0 & +\boldsymbol{\alpha} & 0 \end{bmatrix}. \tag{8}$$

By multiplying $\hat{\mathbf{A}}$ with $\mathbf{P}$, a resultant new matrix $\mathbf{A}^* = \hat{\mathbf{A}}\mathbf{P}$ results. The effect of $\mathbf{P}$ is to map the reconstructed sparse signal into a random permuted sparse signal and to randomly change the sign of the sparse components. After this multiplication, the recovery in cloud becomes:

$$\min_{\mathbf{P}^{-1}\mathbf{s}} \|\mathbf{P}^{-1}\mathbf{s}\|_1 \text{ s. t. } (\hat{\mathbf{A}}\boldsymbol{P})(\mathbf{P}^{-1}\mathbf{s}) = \mathbf{A}^*(\mathbf{P}^{-1}\mathbf{s}) = \hat{\mathbf{y}}. \tag{9}$$

By sending $\mathbf{A}^*$ and $\hat{\mathbf{y}}$ to the cloud, the cloud would be able to recover the intermediate ciphertext, $\mathbf{P}^{-1}\mathbf{s}$. Since the inverse of a permutation matrix is also a permutation matrix, the recovered signal from cloud is still sparse. Note that $\mathbf{P}$ has the following two effects on $\mathbf{s}$. It randomly permutes the components and it randomly multiplies components with $\pm\boldsymbol{\alpha}$. These two operations do not affect the order of sparsity of any k-sparse vector. Therefore, we can guarantee that the sparsity of signal is preserved. Note that sparsity is a required condition for CS recovery, and without it, recovery cannot be done accurately. In words, in our proposed method, the original sparse vector is now mapped into another sparse vector; this mapping is done in the sparse domain and not in the domain in which signal is acquired. In the proposed privacy-assured recovery, the cloud after recovery yields $\mathbf{P}^{-1}\mathbf{s}$, which is a mapped sparse vector or encrypted sparse vector. Cloud may then send the encrypted sparse vector, $\mathbf{P}^{-1}\mathbf{s}$, to the real user, and the user would be able to reconstruct initial signal by using corresponding key, $\mathbf{P}$ as follows:

$$\mathbf{P} * \mathbf{P}^{-1}\mathbf{s} = \mathbf{s}; \quad \boldsymbol{\Psi}\mathbf{s} = \mathbf{x} \tag{10}$$

Note that $\mathbf{P} = \boldsymbol{\alpha}\mathbf{P}'$ where $\mathbf{P}'$ is an orthonormal matrix. Multiplication of an orthonormal matrix with a measurement matrix does not affect the RIP condition. Multiplying $\hat{\mathbf{A}}$ by $\mathbf{P}$ would still preserve the RIP inequality:

$$(1-\delta_K)\|\mathbf{P}\mathbf{s}\|_2^2 \leq \|\hat{\mathbf{A}}\mathbf{P}\mathbf{s}\|_2^2 \leq (1+\delta_K)\|\mathbf{P}\mathbf{s}\|_2^2. \tag{11}$$

As $\mathbf{P} = \boldsymbol{\alpha}\mathbf{P}'$, the above equation can be rewritten as follows:

$$(1-\delta_K)\|\mathbf{P}'\mathbf{s}\|_2^2 \leq \|\hat{\mathbf{A}}\mathbf{P}'\mathbf{s}\|_2^2 \leq (1+\delta_K)\|\mathbf{P}'\mathbf{s}\|_2^2 \tag{12}$$

Note that $\|\mathbf{s}\|_2^2 = \|\mathbf{P}'\mathbf{s}\|_2^2$, that is, $\mathbf{P}'$ does not change the norm of a sparse vector. In this case, left and right sides of inequality shown in equation 12 would be same as without encryption mode which means, $\mathbf{P}$ does not affect the RIP condition.

TABLE 1. Assessment of quality of reconstruction [52].

PRD	SNR	Quality
$0 < PRD < 2\%$	$SNR > 33\ dB$	"Very Good"
$2\% < PRD < 9\%$	$20\ dB < SNR < 33\ dB$	"Good"
$PRD \geq 9\%$	$SNR \leq 20\ dB$	"Undetermined"

IV. RESULTS

In order to assess the quality of reconstruction, appropriate metrics need to be considered. There are a few metrics proposed in the literature to measure the quality of reconstructed signal. Three such metrics that are commonly used for assessing the quality of recovered ECG signals are *percentage root-mean-square difference* (PRD), the normalized version of PRD namely PRDN, and signal to noise ratio (SNR),

$$PRD[\%] = 100\sqrt{\frac{\sum_{n=0}^{N-1}(x(n)-\tilde{x}(n))^2}{\sum_{n=0}^{N-1}x^2(n)}}, \tag{13}$$

$$PRDN[\%] = 100\sqrt{\frac{\sum_{n=0}^{N-1}(x(n)-\tilde{x}(n))^2}{\sum_{n=0}^{N-1}(x(n)-\bar{x}(n))^2}}, \tag{14}$$

$$SNR[\text{dB} = -20\log_{10}\left(\frac{PRD}{100}\right), \tag{15}$$

where $x(n)$ is the original signal, $\tilde{x}(n)$ is the recovered signal, $\bar{x}(n)$ is the mean of original ECG signal (uncompressed), and N denotes the length of ECG signal. In [52], Zigel *et al.* established a link between the PRD and the diagnostic distortion. In [52], different values of PRD for the reconstructed ECG signals were considered and a qualitative assessment as perceived by the specialist was given. Table 1 shows the classified quality and corresponding PRD and SNR.

A. ANALYSIS OF ATTACKS ON INTERMEDIATE CIPHERTEXT

Cloud should have a pair of $(\boldsymbol{A}^*, \hat{\mathbf{y}})$ to conduct the recovery process. Two scenarios, one obtaining $\boldsymbol{P}$ based on $\boldsymbol{A}^*$ and the other obtaining $\boldsymbol{P}$ based on the recovered signal or intermediate ciphertext are considered. In the first scenario, it is statistically impossible to separate $\boldsymbol{P}$ from $\boldsymbol{A}^*$. To prove this, we consider a simpler condition where there is no first key. The measurement matrix is assumed to be an i.i.d. Gaussian matrix with $\mu_{ij} = 0$ and $\sigma_{ij} = 1/M$, where μ_{ij} and σ_{ij} are the mean and standard deviation of the i.i.d. Gaussian matrix entries, respectively. As the distribution of the linear combination of multiple independent random variables having a normal distribution is also a normal distribution, $\boldsymbol{A}^* = \boldsymbol{\Phi\Psi P}$ is also a Gaussian matrix. The entries of $\boldsymbol{A}^*$ and the mean and variance of its entries are obtained as follows:

$$\mathbf{A}^*_{ij} = (\boldsymbol{\Phi\Psi P})_{ij} = \sum_{k=1}^{N} \boldsymbol{\Phi}_{ik}(\boldsymbol{\Psi P})_{kj}, \tag{16}$$

$$\mathbb{E}(\mathbf{A}^*_{ij}) = \sum_{k=1}^{N} \mu_{ij}(\mathbf{\Psi P})_{kj} = 0. \tag{17}$$

$$\begin{aligned} Var(\mathbf{A}^*_{ij}) &= \sum_{k=1}^{N} \sigma^2_{ij}(\mathbf{\Psi P})^2_{kj}, \\ &= (\boldsymbol{\alpha}/M)^2 \sum_{k=1}^{N} (\mathbf{\Psi P})^2_{kj}, \\ &= (\boldsymbol{\alpha}/M)^2 \sum_{k=1}^{N} (\mathbf{\Psi})^2_{kj}, \\ &= \frac{\boldsymbol{\alpha}^2 \boldsymbol{\beta}}{M^2}, \end{aligned} \tag{18}$$

where subscript ij refers to the element of ith row and jth column of the matrix. $\boldsymbol{\beta}$ is the Euclidean norm of the rows of sparsifying dictionary, and $\mathbb{E}(.)$ and $Var(.)$ are the mean and variance of random variable. Almost all sparsifying dictionaries are orthonormal, which makes $\boldsymbol{\beta} = 1$; therefore, the resultant matrix in the cloud-side is a Gaussian matrix with zero mean and variance $\boldsymbol{\alpha}^2/M^2$. Also, the covariance of $\mathbf{A}^*$ can be calculated as follows:

$$\begin{aligned} Cov(\mathbf{A}^*) &= \mathbb{E}((\mathbf{\Phi\Psi P})(\mathbf{\Phi\Psi P})^T) \\ &= \mathbb{E}(\mathbf{\Phi\Psi P P}^T \mathbf{\Psi}^T \mathbf{\Phi}^T) \\ &= \mathbb{E}(\mathbf{\Phi}(\boldsymbol{\alpha}^2\mathbf{I})\mathbf{\Phi}^T) \\ &= \boldsymbol{\alpha}^2\, \mathbb{E}(\mathbf{\Phi\Phi}^T) = \boldsymbol{\alpha}^2 Cov(\mathbf{\Phi}) \\ &= \frac{\boldsymbol{\alpha}^2}{M^2}\mathbf{I} \end{aligned} \tag{19}$$

where superscript T denotes the matrix transpose, and $\mathbf{I}$ is the identity matrix. Since the entries of $\mathbf{\Phi}$ were chosen from an i.i.d Gaussian distribution, the covariance matrix of $\mathbf{A}^*$ is a diagonal matrix which shows its entries are i.i.d as well. Therefore, the statistical distance of $\mathbf{A}^*$ in cloud and any Gaussian matrix $\mathcal{N}(0, \boldsymbol{\alpha}/M)$ is zero. In other words, given $\mathbf{A}^* = \mathbf{\Phi\Psi P}$, cloud cannot reveal any information about $\mathbf{P}$, and there is no statistical difference between $\mathbf{\Phi\Psi P}$ and any random Gaussian matrix $\mathcal{N}(0, \boldsymbol{\alpha}/M)$.

In the second scenario, a ''curious'' cloud or an attacker tries to discover $\mathbf{P}$ based on intermediate ciphertext. Given the intermediate ciphertext, $\mathbf{P}^{-1}\mathbf{s}$, the initial ECG signal cannot be obtained by $\mathbf{\Psi}$, because $\mathbf{x} = \mathbf{\Psi s}$ and not $\mathbf{\Psi P}^{-1}\mathbf{s}$. Meanwhile, an attacker or curious cloud may try to find the bipolar matrix and reconstruct the plaintext or initial uncompressed ECG signal. To do this, attacker should exactly detect the bipolar permutation key. Any change in original key will be completely propagated into the actual time domain values of the signal and corrupt the signal. In other words, as bipolar permutation matrix is applied in sparse domain, the position and sign of elements of sparse vector are changed arbitrarily. After transforming back into the time domain, the recovered signal will be totally different from the original signal. Hence, a small change in permutation matrix can lead to a small change in sparse domain, but a major change in the domain in which signal acquired (generally time domain). To demonstrate the role of bipolar permutation matrix in maintaining the secrecy, recovery was tested with a number of estimated bipolar permutation matrices with different levels of similarity with the original key. Let the estimated bipolar permutation matrix be $\mathbf{E}^r$ which $\mathbf{E}^r$ contains exactly $r\%$ of the columns of the $\mathbf{P}$ and only $(100 - r)\%$ of its columns is unclear or unknown for the attacker. Intermediate ciphertext with different estimated permutation matrices (estimated key) were decrypted and the similarity of the estimated key with the actual key, were measured using Frobenius norm. Given a $M \times N$ matrix $\mathbf{A}$, its Frobenius norm is defined as the square root of the sum of the absolute squares of its elements and is given below.

$$\|\mathbf{A}\|_F = \sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N} |\mathbf{A}_{ij}|^2} \tag{20}$$

where the $\mathbf{A}_{ij}$ is the element of ith row and jth column of $\mathbf{A}$. Accordingly, the Frobenius norm of the difference between the true key and the estimated key can be obtained as follows,

$$\|\mathbf{P} - \mathbf{E}^r\|_F = \sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N} |\mathbf{P}_{ij} - \mathbf{E}^r_{ij}|^2} \tag{21}$$

where the $\mathbf{P}_{ij}$ and $\mathbf{E}^r_{ij}$ are the elements of ith row and jth column of $\mathbf{P}$ and $\mathbf{E}^r$, respectively. Equation 21 was considered as a metric to show the similarity of the estimated key to the actual key. Three estimated matrices were generated by copying 99%, 98% and 97% of the columns of the $\mathbf{P}$ into 3 estimated matrices $\mathbf{E}^{99}$, $\mathbf{E}^{98}$, and $\mathbf{E}^{97}$, respectively. Then, the elements of rest of 1%, 2%, and 3% columns of these estimated matrices were randomly generated. One ECG signal, record number 101 was selected from the MIT Arrhythmia database [53]. First 1000 samples of this ECG signal was selected as plaintext, $\mathbf{x}$, and the orthogonal Daubechies wavelets (db 10) was considered as sparsifying dictionary. Daubechies wavelet (db 10) is the most popular wavelet basis used in ECG transform-based compression techniques [54]. A random bipolar permutation matrix of size $\mathbf{P}_{1000\times1000}$ was chosen, and the estimated keys were generated accordingly. The simulation results are available in Table 2 and it shows that a small difference in permutation matrix (or a small dissimilarity) leads to a major difference in decrypted ECG signal. For instance, the $\mathbf{E}^{99}$ contained 99% of the columns of actual key, and just 1% of its columns were chosen randomly. In other words, 990 columns were the exact replica of the main key, and just 10 columns were randomly estimated. The simulation results show that these 10 columns contributed to a totally different decrypted signal from the originally considered plain text ECG signal.

Table 2 shows that the permutation key is very sensitive and a small change in its elements can fail to provide exact decryption. Also, consider the scenario that, for instance $\mathbf{E}^{99}$, 99% of its columns are truly estimated. However, in practice such estimation demands heavy computational resources

TABLE 2. The strength of bipolar permutation key.

Key	$\|\mathbf{P}-\mathbf{E}\|_F$	PDRN(%)
$\mathbf{P}$	0	30
$\mathbf{E}^{99}$	4.47	249
$\mathbf{E}^{98}$	6.32	370
$\mathbf{E}^{97}$	7.73	450

and time. Because, there are $2^N \times N!$ bipolar permutation matrices of size N, where ! represents the factorial operation, need to be tried. For the case of $N = 1000, 512, 256,$ or 128, the number of permutation matrices is a very huge number,[1] and the probability of estimating actual key is negligible. However, while considering a systematic attack scenario, an unfaithful cloud or eavesdropper may try to employ the order of sparsity (k) as a side information and then attempt to estimate the initial sparse vector. Also, if the cloud uses a greedy recovery algorithm such as OMP, it would require the knowledge of the order of sparsity. Although employing the order of sparsity might decrease the search space for an attacker, but the attacker still face the issue of searching for a solution. This search for a solution is infeasible as for a large N and for a certain given k, the search requires non-polynomial (NP) time to solve. To estimate the initial sparse vector, an attacker will have to perform $2^k\binom{N}{k}$ exhaustive searches. To clarify the complexity of breaking the ciphertext, if the recovered sparse signal has 1024 components, and if the sparse vector has at least 64 nonzero elements (our experiments show more than 64) then $2^{64}\binom{1024}{64} \cong 4.8 \times 10^{102}$ trials are required for the attacker to guess the plaintext. Moreover, the diagnostic information of an ECG signal is very sensitive, and a small change in recovered signal can disturb the real information within the signal. The ultimate goal of the proposed method was to provide a simple and secure outsourcing method that is robust to the aforementioned issues. In comparison to one of the strongest outsourced CS-recovery service proposed in [12], this method of encryption demands less computational resources. In [12], cloud had to do CS-recovery based on LP method, however, in the proposed method cloud is free to choose any CS-recovery algorithm. For instance, through faster and simpler algorithms such as SL0, cloud can recover intermediate ciphertext three times faster than LP method [29]. Also, in [12], five keys were used which led to a further computational burden in ECG recorders. In comparison with the very recent work, "*Kryptein*", in which adaptive dictionary learning was used for generating sparsifying dictionary, in the current proposed work, any dictionary either fixed or adaptive dictionaries can be used. By selecting fixed dictionaries, such as wavelet transform family or discrete cosine transform (DCT), the heavy task of training dictionary can be removed [13].

[1] $1000! \cong 4 \times 10^{2567}$, $128! \cong 3.8 \times 10^{215}$

B. EXPERIMENTAL RESULTS

ECG signals from MIT-BIH Arrhythmia Database [53] were used. This is a two-channel database of 47 ECG signals obtained from 22 women and 25 men, representing different age groups. All recordings have been digitized at 360 samples per second per channel with 11-bit resolution over a 10 mV range. As ECG signal is used for diagnosis, the morphology and relative time positions of the various morphological features are important. We considered the diagnostic needs and proposed our method of encryption. Figure 2 shows the initial ECG signal (record number 105), recovered in cloud and then decrypted with and without the actual key. In this simulation, 2000 samples of data record 105 were chosen. Also, the deterministic binary block diagonal (DBBD) sensing matrix of size $\mathbf{A}_{128\times512}$ as suggested in [49] was used. DCT was used as sparsifying basis, and the first key $\mathbf{Q}$ was randomly chosen from a normal distribution $\mathcal{N}(0, 1/128)$ to encrypt the measurement matrix. The second key $\mathbf{P}$ was randomly selected as a bipolar permutation key. According to the size of measurement matrix, the CR is $M/N = 1/4$. The important portion of diagnostic information of an ECG signal lies between its two consecutive QRS complexes, Fig. 2 shows that bipolar permutation conceals the diagnostic information, and without having the actual key, the decrypted signal is totally wrong.

To evaluate the effectiveness of this approach from the attacks perspective, the process of estimating the bipolar permutation key was simulated. Four keys were chosen: one of them was the actual key and the others were 90%, 80%, and 70% replica of actual key, i.e. $\mathbf{P}$, $\mathbf{E}^{90}$, $\mathbf{E}^{80}$ and $\mathbf{E}^{70}$. For instance, for the case of 90%, 90% of the actual key's components were copied into another matrix as estimated key and the remaining 10% columns were randomly guessed. The simulation results verify that the bipolar permutation is strong enough for assuring privacy in the recovery of compressed ECG signals. The proposed approach was tested with DCT and orthogonal Daubechies wavelets ($db10$) dictionaries as these two are the fixed sparsifying dictionaries commonly used in the CS studies using ECG signals. In this simulation, 1024 ECG samples of five different signals and $CR = M/N = 1/8$ were chosen. The results are shown in Table 3.

In the aforementioned simulations, the fixed sparsifying dictionary was assumed to be available on the cloud-side. On the other hand, if we employ adaptive dictionary learning, beside bipolar permutation matrix, sparsifying dictionary will also be unknown for the "curious" cloud or attacker. Hence, if adaptive dictionary learning were used, the secrecy of the system can be increased. Adaptive dictionaries usually yield higher quality in reconstruction at the expense of computational burden to the system. Since, the learning process needs to be executed only once for a subject, this complexity may be conveniently ignored. There are numerous adaptive dictionary learning methods such as method of optimal direction MOD [55], and K-singular value decomposition (K-SVD) [56]. In order to demonstrate

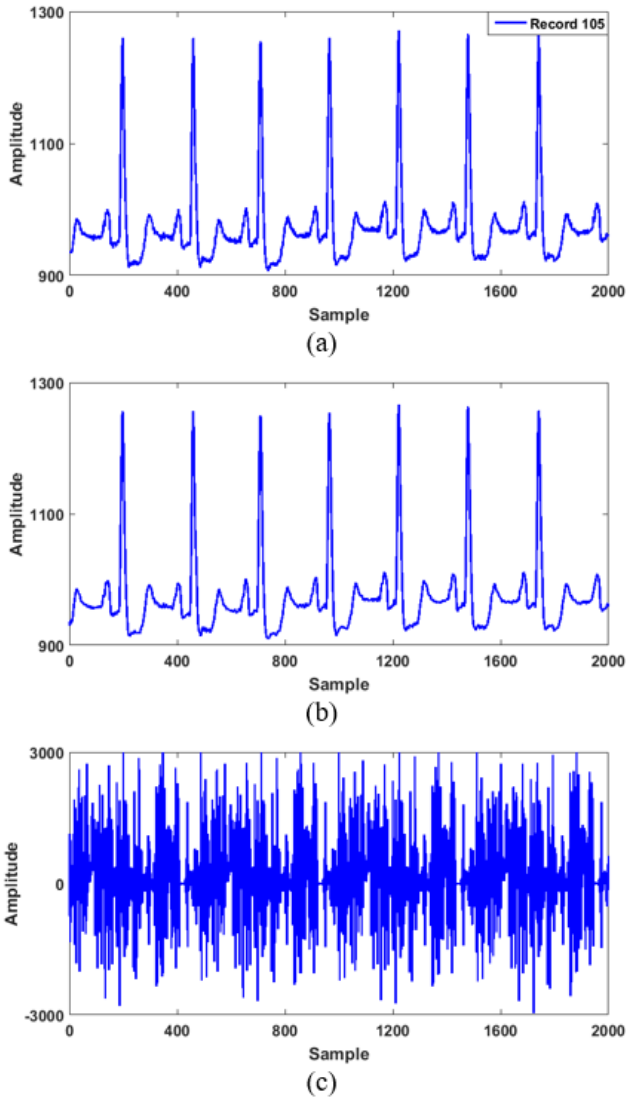

FIGURE 2. Recovery of ECG signal via DCT dictionary with and without actual key. (a) Initial ECG signal (plaintext).(b) Recovery of ECG Signal on client-side with the actual key ($PRD = 0.29\%$, $SNR = 50.6dB$). (c) Recovery of the ECG signal in cloud-side with the wrong key ($PRD = 10^6\%$, $SNR = -30.22dB$).

the proposed method with the adaptive dictionary learning, MOD, which is one of the fastest method to learn sparsifying dictionary, was chosen. Figure 3 shows the result obtained using the adaptive sparsifying dictionary while using the ECG signal (record number 101) from the MIT-BIH Arrhythmia database. It is evident that recovery without key, or recovery of encrypted signal leads to totally wrong recovery. The recovered signal has no features of the original ECG signal.

Proposed method does not affect the quality of the reconstruction. In Section III it was shown that after recovery in cloud, an end user should be able to exactly recover the initial signal at their end. This aspect of the proposed method was also tested for a number of ECG signals from the database, (records no. $100-109$). Table 4 shows that there is no difference in the quality of the reconstructed signal with and without the proposed encryption system.

TABLE 3. Recovery by different keys and sparsifying basis (PRD%).

Records	DCT				Wavelet			
	$\mathbf{P}$	$\mathbf{E}^{90}$	$\mathbf{E}^{80}$	$\mathbf{E}^{70}$	$\mathbf{P}$	$\mathbf{E}^{90}$	$\mathbf{E}^{80}$	$\mathbf{E}^{70}$
100	1.8	30.3	54.2	97.2	1.6	54.8	77.1	89.9
101	1.4	30.2	68.0	105	1.3	54.0	76.3	93.6
102	1.2	2.1	16.8	36.6	1.2	51.7	73.6	90.4
103	2.3	7.5	41.6	61.0	2.3	52.7	76.3	90.2
104	1.3	16.8	58.7	68.7	1.3	56.7	76.6	93.2
105	0.6	7.2	54.9	84.0	0.6	55.3	75.8	91.6
106	2.6	1.7	41.1	64.9	1.8	49.4	72.2	88.0
107	1.5	21.2	55.8	95.3	2.2	53.3	71.8	87.6
108	0.4	15.4	59.3	63.7	0.4	55.0	73.6	88.8
109	0.6	17.6	42.0	84.5	0.8	52.1	71.9	86.0

TABLE 4. Impact of proposed security approach on the quality of reconstruction. The quality of recovery with and without proposed security approach are exactly the same.

Records	SNR(dB)					
	CR=1/2		CR=1/4		CR=1/8	
	Ordinary	Secure	Ordinary	Secure	Ordinary	Secure
100	57.02	57.02	45.56	45.56	35.28	35.28
101	58.35	58.35	47.14	47.14	35.81	35.81
102	56.21	56.21	44.16	44.16	38.24	38.24
103	60.08	60.08	49.44	49.44	33.23	33.23
104	52.15	52.15	42.44	42.44	37.31	37.31
105	60.30	60.30	52.13	52.13	45.48	45.48
106	52.95	52.95	43.02	43.02	33.14	33.14
107	45.09	45.09	39.98	39.98	34.23	34.23
108	59.02	59.02	50.40	50.40	46.81	46.81
109	54.05	54.05	48.02	48.02	42.62	42.62

Also, any change in mutual coherence can be reflected to the quality of reconstruction [10], [23], [49]. With this regard, we checked the effect of proposed method on the mutual coherence. Figure 4 shows this effect for random and deterministic measurement matrices as a function of number of measurements. For the class of random measurement matrices, we generated by a zero-mean and variance $1/M$ i.i.d. Gaussian process, denoted by $\mathbf{\Phi}_{Gaussian}$. For the class of deterministic measurement matrices, DBBD matrix $\mathbf{\Phi}_{DBBD}$ was used. DCT matrix $\mathbf{\Psi}_{DCT}$ and encrypted DCT matrix $\mathbf{\Psi}_{DCT} \times \mathbf{P}$ were used as sparsifying and encrypted sparsifying dictionary, respectively. In this simulation, $N = 500$ and the number of measurements was changed to check the effect of mutual coherence on different sizes of matrices. The results show the bipolar permutation matrix does not affect the mutual coherence.

To the best of knowledge of the authors, there has been no specific work on secure CS recovery outsourcing for the ECG signal. However, there are two methods in the literature, namely OIRS and Kryptein, that are related to the

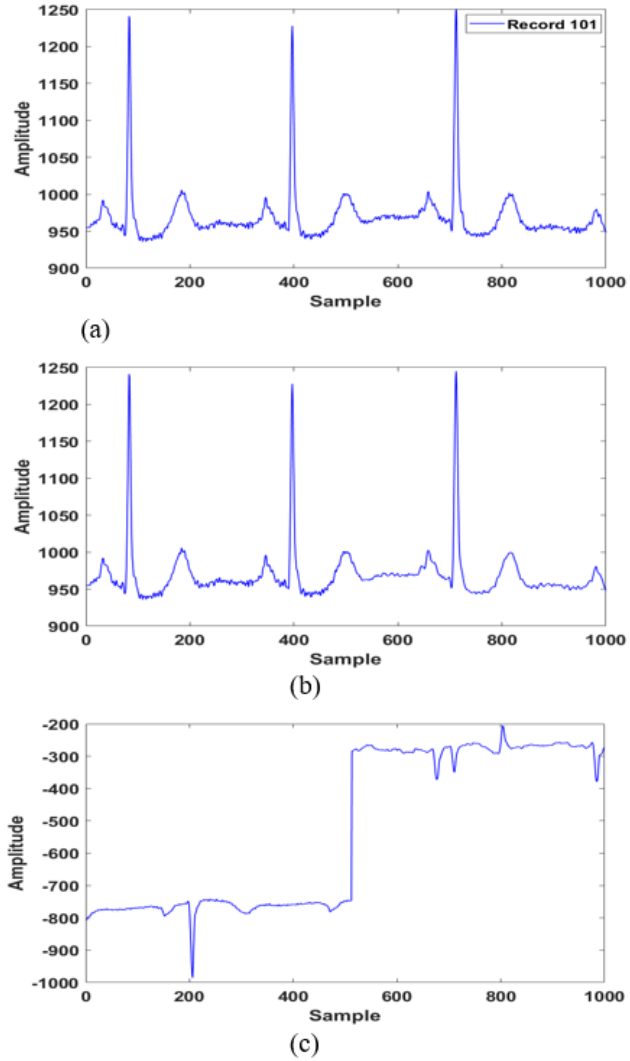

FIGURE 3. Recovery via adaptive dictionary learning (MOD) with and without actual key. (a) Initial ECG signal (plaintext). (b) Recovery of ECG Signal on user-side with the true key $PRD = 0.09\%$, $SNR = 60.4dB$. (c) Recovery of the ECG signal in cloud-side with the wrong key $PRD = 150\%$, $SNR = -3dB$.

proposed method for secure CS recovery outsourcing. The proposed work was compared with these related methods under the following considerations: recovery algorithms, sparsifying bases and computational complexity. Table 5 shows comparison of the proposed method with the ORIS and Kryptein. The proposed method can be applied for any CS recovery algorithm and has low overload both on the user-side and the cloud.

A comprehensive experiment to evaluate the time required to perform encryption and recovery on the client and cloud, respectively was performed. 10 ECG records (#100, #101 #102, #103, #104, #105, #106, #107, #108, #109) were considered, and 5120 samples were selected from each of these signals to conduct the experiment. The length of the window to set to 1024 and $CR = 256/1024 = 1/4$, i.e., every 1024 samples was compressed to 256 measurements. The experiments were repeated 10 times and the average

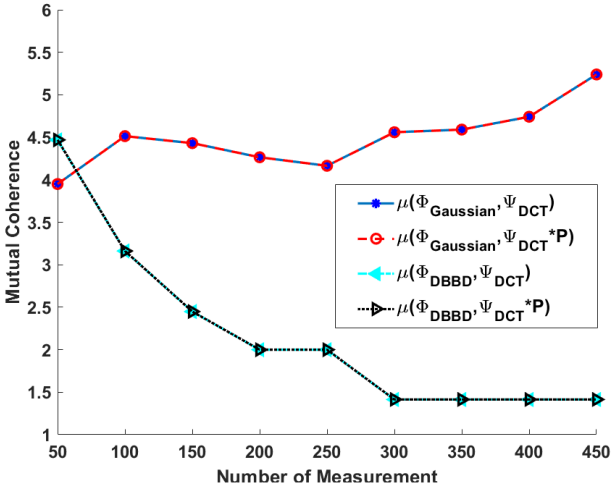

FIGURE 4. Impact of proposed encryption on mutual coherence.

TABLE 5. Comparison of functionality.

Functionality	OIRS [12]	Kryptein [13]	Proposed
Recovery based on LP methods	Yes	Yes	Yes
Recovery based on Matching pursuit, Belief Propagation, and SL0	No	Yes	Yes
Using DCT/Wavelet sparsifying dictionaries	Yes	No	Yes
Using adaptive sparsifying dictionary	Yes	Yes	Yes
Complexity in User end (multiplication operation)	$4N^2$	N^2	N^2

of the elapsed times was calculated. Our experiment on the client-side was run on MATLAB environment, with *Intel(R) Core(TM) i7-8550U CPU @ 1.80GHz* processor with 16G RAM. Experiment on the cloud-side was implemented on MATLAB environment provided in the MathWorks Cloud. The required time to encrypt the data on the client-side was compared with two other techniques proposed in the literature. As shown in Table. 6, the proposed method requires lower time to encrypt the data. Kryptein takes much longer time since it implements two tasks on client-side: dictionary learning and singular value decomposition. Also, since the OIRS uses five keys to encrypt the data, it takes longer time than our proposed method. Furthermore, the time taken for recovery of ECG on the cloud was also compared. The proposed and Kryptein methods can choose any CS recovery algorithm. For example, SL0 which is one of the fastest and most accurate recovery algorithms can be considered. In contrast, the OIRS cryptosystem requires running a linear programming (LP) algorithm which takes longer time than the SL0. To run the LP problem, the $\ell 1$-magic algorithm that is based on the standard interior-point method [57] was used. As shown in Table. 1, the proposed method and Kryptein needed the same recovery time for recovery, however, while OIRS needed longer time to recover.

TABLE 6. Comparison of the execution time (milliseconds).

	Client-Side (Encryption)										
	#100	**#101**	**#102**	**#103**	**#104**	**#105**	**#106**	**#107**	**#108**	**#109**	Avg
Kryptein [13]	1786	1766	1794	1807	1845	1753	1838	1839	1870	1815	1811
OIRS [12]	319	320	330	319	341	317	325	341	345	341	329
Proposed	16	17	16	18	16	17	17	16	21	17	17
	Cloud-Side (Recovery)										
	#100	**#101**	**#102**	**#103**	**#104**	**#105**	**#106**	**#107**	**#108**	**#109**	Avg
Kryptein [13]	86	75	73	71	72	71	75	82	79	80	76
OIRS [12]	457	437	453	449	447	467	458	480	466	466	458
Proposed	86	75	73	71	72	71	75	82	79	80	76

C. COMPLEXITY OF THE PROPOSED METHOD

The proposed method can be categorized as a fast and energy efficient method of encryption. Proposed method requires two keys; a random square matrix as the first key and a bipolar permutation matrix as the second key. The first key is used to encrypt the measurement matrix. As sensors might use deterministic or structured measurement matrices in certain applications, attacker may use the structure in measurement matrix and consequently detect the bipolar permutation matrix. When using deterministic measurement matrices for the recovery service, cloud has $\mathbf{A}^*$, where $\mathbf{A}^* = \hat{\mathbf{A}}\mathbf{P} = \mathbf{QAP} = \mathbf{Q\Phi\Psi P}$. For the case where $\mathbf{\Phi}$ is deterministic, without the first key, an attacker can separate $\mathbf{\Psi}\boldsymbol{P}$ from $\mathbf{\Phi\Psi}\boldsymbol{P}$. Since $\mathbf{\Psi}$ are known, say a DCT or wavelet dictionary, then the permutation matrix may be revealed. But, if the first key is applied in addition, this attack can be avoided. Let the first key be chosen from Gaussian distribution as it has maximum entropy that causes maximum diffusion. The overload of the first key is just $M \times M$ multiplications and $M \times (M-1)$ addition operations for sending each measurement vector. The measurement matrix that is shared with the cloud would be $\mathbf{Q\Phi\Psi P}$ instead of $\mathbf{Q\Phi\Psi}$. This leads to N random shift in the columns of $\mathbf{Q\Phi\Psi}$ and its components are randomly multiplied by $-\boldsymbol{\alpha}$ or $+\boldsymbol{\alpha}$. The matrix $\mathbf{Q\Phi\Psi P}$ must be available in cloud to do the recovery process. To further enhance privacy, every individual user would have a unique key. Also, after certain number of queries, to prevent potential known plaintext attack (KPA), the key can be updated.

V. CONCLUSION

For doing CS-recovery service in cloud environment, the secrecy of information should be preserved. When ECG measurements are transmitted to the cloud, the cloud with its strong resources can do the CS recovery for the client.

A fast and light-weight encryption method that can be implemented on resource constraint edge devices was proposed in this paper. The experimental results on client-side and cloud-side showed that this method has lower complexity and execution time compared to the related works. Through the proposed method, not only does the cloud conduct the CS-recovery, but after recovery it also delivers an encrypted version of signal, thereby preserving the privacy of client information during the entire process. The proposed encryption is carried out in the sparse domain. Through a bipolar permutation matrix, the initial sparse vector (plaintext) is mapped into to another sparse vector (ciphertext). The cloud after recovery presents a permuted sparse vector to the user and without knowing the key, it would be very difficult to guess the original signal as the degree of freedom for this guess is small. In other words, with respect to the ECG signal where small changes might distort the signal, it is practically very hard to guess the information contained in the signal for ''curious'' cloud or semi-trusted cloud or an eavesdropper. The role of the sparsifying basis in improving the secrecy of information is also demonstrated in this study. Appropriate choice of adaptive sparsifying basis can also provide additional secrecy. In this paper, ECG signals were considered. However, CS has been applied for other biomedical signals like the electro-encephelogram (EEG) signals and heart rate signals that are compressible in some domain as well. The proposed method can be used with such biomedical signals. Further, this research is not restricted to biomedical signals. For instance, one may apply the proposed method to sparse signals such as seismic signals or images. Thus this proposed method opens avenue for investigating the privacy-preserving recovery of sparse and compressible signals while maintaining the quality of recovery.

REFERENCES

[1] R. G. Baraniuk, ''Compressive sensing [lecture notes],'' *IEEE Signal Process. Mag.*, vol. 24, no. 4, pp. 118–121, Jul. 2007.

[2] D. L. Donoho, ''Compressed Sensing,'' *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1289–1306, Jan. 2006.

[3] S. A. Khoshnevis and S. Ghorshi, ''Enhancement of the tomo-SAR images based on compressive sensing method,'' in *Proc. 6th Int. Conf. Space Sci. Commun. (IconSpace)*, Jul. 2019, pp. 41–46.

[4] H. Mamaghanian, N. Khaled, D. Atienza, and P. Vandergheynst, ''Compressed sensing for real-time energy-efficient ECG compression on wireless body sensor nodes,'' *IEEE Trans. Biomed. Eng.*, vol. 58, no. 9, pp. 2456–2466, Sep. 2011.

[5] J. K. Pant and S. Krishnan, ''Compressive sensing of electrocardiogram signals by promoting sparsity on the second-order difference and by using dictionary learning,'' *IEEE Trans. Biomed. Circuits Syst.*, vol. 8, no. 2, pp. 293–302, Apr. 2014.

[6] L. F. Polanía, R. E. Carrillo, M. Blanco-Velasco, and K. E. Barner, ''Exploiting prior knowledge in compressed sensing wireless ECG systems,'' *IEEE J. Biomed. Health Inform.*, vol. 19, no. 2, pp. 508–519, Mar. 2015.

[7] M. M. Abo-Zahhad, A. I. Hussein, and A. M. Mohamed, ''Compression of ECG signal based on compressive sensing and the extraction of significant features,'' *Int. J. Commun., Netw. Syst. Sci.*, vol. 8, no. 5, pp. 97–117, 2015.

[8] A. M. R. Dixon, E. G. Allstot, D. Gangopadhyay, and D. J. Allstot, ''Compressed sensing system considerations for ECG and EMG wireless biosensors,'' *IEEE Trans. Biomed. Circuits Syst.*, vol. 6, no. 2, pp. 156–166, Apr. 2012.

[9] A. Mishra, F. Thakkar, C. Modi, and R. Kher, "Comparative analysis of wavelet basis functions for ECG signal compression through compressive sensing," *Int. J. Comput. Sci. Telecommun.*, vol. 3, no. 5, pp. 23–31, May 2012.
[10] H. Zanddizari, S. Rajan, and H. Zarrabi, "Increasing the quality of reconstructed signal in compressive sensing utilizing Kronecker technique," *Biomed. Eng. Lett.*, vol. 8, no. 2, pp. 239–247, May 2018.
[11] L. F. Polania, R. E. Carrillo, M. Blanco-Velasco, and K. E. Barner, "Compressed sensing based method for ECG compression," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, May 2011, pp. 761–764.
[12] C. Wang, B. Zhang, K. Ren, and J. M. Roveda, "Privacy-assured outsourcing of image reconstruction service in cloud," *IEEE Trans. Emerg. Topics Comput.*, vol. 1, no. 1, pp. 166–177, Jun. 2013.
[13] W. Xue, C. Luo, G. Lan, R. Rana, W. Hu, and A. Seneviratne, "Kryptein: A compressive-sensing-based encryption scheme for the Internet of Things," in *Proc. 16th ACM/IEEE Int. Conf. Inf. Process. Sensor Netw.*, Apr. 2017, pp. 169–180.
[14] H. Zanddizari, A. Falahati, and H. S. Shahhoseini, "Secure reconstruction of image from compressive sensing in cloud," in *Proc. 2nd Annu. Conf. Comput. IT Tehran Univ.*, 2015, pp. 1–8.
[15] T. Y. Liu, K. J. Lin, and H. C. Wu, "ECG data encryption then compression using singular value decomposition," *IEEE J. Biomed. Health Inform.*, vol. 22, no. 3, pp. 707–713, May 2018.
[16] M. Fira, "Applications of compressed sensing: Compression and encryption," in *Proc. E-Health Bioengineering Conf. (EHB)*, Nov. 2015, pp. 1–4.
[17] F. Sufi and I. Khalil, "Enforcing secured ECG transmission for realtime telemonitoring: A joint encoding, compression, encryption mechanism," *Secur. Commun. Netw.*, vol. 1, no. 5, pp. 389–405, Sep. 2008.
[18] J.-J. Wei, C.-J. Chang, N.-K. Chou, and G.-J. Jan, "ECG data compression using truncated singular value decomposition," *IEEE Trans. Inf. Technol. Biomed.*, vol. 5, no. 4, pp. 290–299, Dec. 2001.
[19] C. Karakus, A. C. Gurbuz, and B. Tavli, "Analysis of energy efficiency of compressive sensing in wireless sensor networks," *IEEE Sensors J.*, vol. 13, no. 5, pp. 1999–2008, May 2013.
[20] E. J. Candès, "The restricted isometry property and its implications for compressed sensing," *Comp. Rendus Math.*, vol. 346, nos. 9–10, pp. 589–592, May 2008.
[21] D. Needell and R. Vershynin, "Uniform uncertainty principle and signal recovery via regularized orthogonal matching pursuit," *Found. Comput. Math.*, vol. 9, no. 3, pp. 317–334, Jun. 2008.
[22] J. A. Tropp and A. C. Gilbert, "Signal recovery from random measurements via orthogonal matching pursuit," *IEEE Trans. Inf. Theory*, vol. 53, no. 12, pp. 4655–4666, Dec. 2007.
[23] W. Yan, Q. Wang, and Y. Shen, "Shrinkage-based alternating projection algorithm for efficient measurement matrix construction in compressive sensing," *IEEE Trans. Instrum. Meas.*, vol. 63, no. 5, pp. 1073–1084, May 2014.
[24] S. S. Chen, D. L. Donoho, and M. A. Saunders, "Atomic decomposition by basis pursuit," *SIAM Rev.*, vol. 43, no. 1, pp. 129–159, Jan. 2001.
[25] W. Dai and O. Milenkovic, "Subspace pursuit for compressive sensing signal reconstruction," *IEEE Trans. Inf. Theory*, vol. 55, no. 5, pp. 2230–2249, May 2009.
[26] D. L. Donoho, Y. Tsaig, I. Drori, and J.-L. Starck, "Sparse solution of underdetermined systems of linear equations by stagewise orthogonal matching pursuit," *IEEE Trans. Inf. Theory*, vol. 58, no. 2, pp. 1094–1121, Feb. 2012.
[27] Y. Pati, R. Rezaiifar, and P. Krishnaprasad, "Orthogonal matching pursuit: Recursive function approximation with applications to wavelet decomposition," in *Proc. 27th Asilomar Conf. Signals, Syst. Comput.*, vol. 1, 1993, pp. 40–44.
[28] S. Sarvotham, D. Baron, and R. G. Baraniuk, "Bayesian compressive sensing via belief propagation," *IEEE Trans. Signal Process.*, vol. 58, no. 1, pp. 269–280, Jan. 2010.
[29] H. Mohimani, M. Babaie-Zadeh, and C. Jutten, "A fast approach for overcomplete sparse decomposition based on smoothed ℓ^0 norm," *IEEE Trans. Signal Process.*, vol. 57, no. 1, pp. 289–301, Jan. 2009.
[30] T. Bianchi, V. Bioglio, and E. Magli, "Analysis of one-time random projections for privacy preserving compressed sensing," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 2, pp. 313–327, Feb. 2016.
[31] Y. Zhang, Y. Xiang, L. Y. Zhang, Y. Rong, and S. Guo, "Secure wireless communications based on compressive sensing: A survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1093–1111, 2nd Quart., 2019.
[32] S.-H. Hsieh, T.-H. Hung, C.-S. Lu, Y.-C. Chen, and S.-C. Pei, "A secure compressive sensing-based data gathering system via cloud assistance," *IEEE Access*, vol. 6, pp. 31840–31853, 2018.
[33] V. Cambareri, M. Mangia, F. Pareschi, R. Rovatti, and G. Setti, "On known-plaintext attacks to a compressed sensing-based encryption: A quantitative analysis," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 10, pp. 2182–2195, Oct. 2015.
[34] X. Yuan, X. Wang, C. Wang, J. Weng, and K. Ren, "Enabling secure and fast indexing for privacy-assured healthcare monitoring via compressive sensing," *IEEE Trans. Multimedia*, vol. 18, no. 10, pp. 2002–2014, Oct. 2016.
[35] Z. Yang, W. Yan, and Y. Xiang, "On the security of compressed sensing-based signal cryptosystem," *IEEE Trans. Emerg. Topics Comput.*, vol. 3, no. 3, pp. 363–371, Sep. 2015.
[36] M. Mangia, F. Pareschi, R. Rovatti, and G. Setti, "Low-cost security of IoT sensor nodes with rakeness-based compressed sensing: Statistical and known-plaintext attacks," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 2, pp. 327–340, Feb. 2018.
[37] J. Barceló-Lladó, A. Morell, and G. Seco-Granados, "Amplify-and-forward compressed sensing as a PHY-layer secrecy solution in wireless sensor networks," in *Proc. IEEE 7th Sensor Array Multichannel Signal Process. Workshop (SAM)*, Jun. 2012, pp. 113–116.
[38] X. Chu, M. C. Stamm, and K. J. R. Liu, "Compressive sensing forensics," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 7, pp. 1416–1431, Jul. 2015.
[39] X. Zhang, Z. Qian, Y. Ren, and G. Feng, "Watermarking with flexible self-recovery quality based on compressive sensing and compositive reconstruction," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 4, pp. 1223–1232, Dec. 2011.
[40] P. Lu, Z. Xu, X. Lu, and X. Liu, "Digital image information encryption based on compressive sensing and double random-phase encoding technique," *Optik*, vol. 124, no. 16, pp. 2514–2518, Aug. 2013.
[41] M. R. Mayiami, B. Seyfe, and H. G. Bafghi, "Perfect secrecy via compressed sensing," in *Proc. Iran Workshop Commun. Inf. Theory*, May 2013, pp. 1–5.
[42] R. Dautov and G. R. Tsouri, "Securing while sampling in wireless body area networks with application to electrocardiography," *IEEE J. Biomed. Health Inform.*, vol. 20, no. 1, pp. 135–142, Jan. 2016.
[43] T. P. Jose and D. P. P, "Secure sensor node design for ECG in body area network," in *Proc. IEEE Region 10 Conf. (TENCON)*, Nov. 2016, pp. 2957–2961.
[44] C.-Y. Chou, E.-J. Chang, H.-T. Li, and A.-Y. Wu, "Low-complexity privacy-preserving compressive analysis using subspace-based dictionary for ECG telemonitoring system," *IEEE Trans. Biomed. Circuits Syst.*, vol. 12, no. 4, pp. 801–811, Aug. 2018.
[45] A. Fratini, M. Sansone, P. Bifulco, and M. Cesarelli, "Individual identification via electrocardiogram analysis," *Biomed. Eng. OnLine*, vol. 14, no. 1, pp. 1–23, Aug. 2015.
[46] T.-H. Hung, S.-H. Hsieh, and C.-S. Lu, "Privacy-preserving data collection and recovery of compressive sensing," in *Proc. IEEE China Summit Int. Conf. Signal Inf. Process. (ChinaSIP)*, Jul. 2015, pp. 473–477.
[47] Y. Zhang, Y. Xiang, L. Y. Zhang, L.-X. Yang, and J. Zhou, "Efficiently and securely outsourcing compressed sensing reconstruction to a cloud," *Inf. Sci.*, vol. 496, pp. 150–160, Sep. 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0020025519304293
[48] P. Wang, "Privacy-assured outsourcing of compressed sensing reconstruction service in cloud," 2021, *arXiv:2103.15164*.
[49] A. Ravelomanantsoa, H. Rabah, and A. Rouane, "Compressed sensing: A simple deterministic measurement matrix and a fast recovery algorithm," *IEEE Trans. Instrum. Meas.*, vol. 64, no. 12, pp. 3405–3413, Dec. 2015.
[50] L. Applebaum, S. D. Howard, S. Searle, and R. Calderbank, "Chirp sensing codes: Deterministic compressed sensing measurements for fast recovery," *Appl. Comput. Harmon. Anal.*, vol. 26, no. 2, pp. 283–290, Mar. 2009.
[51] R. Calderbank, S. Howard, and S. Jafarpour, "Construction of a large class of deterministic sensing matrices that satisfy a statistical isometry property," *IEEE J. Sel. Topics Signal Process.*, vol. 4, no. 2, pp. 358–374, Apr. 2010.
[52] Y. Zigel, A. Cohen, and A. Katz, "The weighted diagnostic distortion (WDD) measure for ECG signal compression," *IEEE Trans. Biomed. Eng.*, vol. 47, no. 11, pp. 1422–1430, Nov. 2000.
[53] A. L. Goldberger, L. A. N. Amaral, L. Glass, J. M. Hausdorff, P. C. Ivanov, R. G. Mark, J. E. Mietus, G. B. Moody, C.-K. Peng, and H. E. Stanley, "PhysioBank, PhysioToolkit, and PhysioNet: Components of a new research resource for complex physiologic signals," *Circulation*, vol. 101, no. 23, Jun. 2000.

[54] P. S. Addison, "Wavelet transforms and the ECG: A review," *Physiol. Meas.*, vol. 26, no. 5, pp. R155–R199, Aug. 2005.
[55] K. Engan, S. O. Aase, and J. Husøy, "Multi-frame compression: Theory and design," *Signal Process.*, vol. 80, no. 10, pp. 2121–2140, Oct. 2000.
[56] M. Aharon, M. Elad, and A. Bruckstein, "K-SVD: An algorithm for designing overcomplete dictionaries for sparse representation," *IEEE Trans. Signal Process.*, vol. 54, no. 11, pp. 4311–4322, Nov. 2006.
[57] E. J. Candés and J. Romberg. (2005). *ℓ_1-Magic: Recovery of Sparse Signals Via Convex Programming*. [Online]. Available: https://statweb.stanford.edu/ candes/software/l1magic/

HADI ZANDDIZARI (Student Member, IEEE) received the master's degree in electrical engineering from the University of Science and Technology, Iran, in 2015. He is currently pursuing the Ph.D. degree with the University of South Florida. From 2015 to 2017, he worked at Pardis Technology Park as a Researcher and a Programmer. His research interests include sparsity, compressive sensing, cybersecurity, machine learning, and robustness of machine learning algorithms.

SREERAMAN RAJAN (Senior Member, IEEE) is currently the Canada Research Chair of Advanced Sensor Systems and Signal Processing and a Professor with the Department of Systems and Computer Engineering, Carleton University, Ottawa, Canada. He is also the Director of the Ottawa-Carleton Institute for Biomedical Engineering. Before joining Carleton University, he was with Defence Research and Development Canada (DRDC), Ottawa, as a Senior Defence Scientist. His industrial experiences include areas of nuclear science and engineering, control, electronic warfare, communications and biomedical engineering in addition to research experience in areas of sensor signal/image processing, and pattern recognition and machine learning. He is currently the Chair of the IEEE Ottawa Engineering in Medicine and Biology (EMB) Society and Aerospace and Electronic Systems Society (AESS) Chapters, the North America Region Director, and IEEE Consumer Technology Society (CTSoc). He is an appointed member of Board of Governors and IEEE CTSoc. He has been represents CTSoc in IEEE Biometric Council, since 2021. He has served IEEE Canada as its board member (October 2010–October 2018) and the IEEE MGA in its Admissions and Advancement Committee, Strategic and Environment Assessment Committee. He was awarded the IEEE MGA Achievement Award, in 2012, and recognized for his IEEE contributions with Queen Elizabeth II Diamond Jubilee Medal, in 2012. IEEE Canada recognized his outstanding service through 2016 W.S. Read Outstanding Service Award. IEEE Ottawa Section recognized him as an Outstanding Volunteer, in 2012, an Outstanding Engineer, in 2018, and an Outstanding Engineering Educator, in 2019. He has been involved in organizing several successful IEEE conferences and has been a reviewer for several IEEE journals and conferences. He is the holder of two patents and two disclosures of invention. He has authored more than 200 journal articles and conference papers. He is a member of IEEE Instrumentation and Measurement, Engineering in Medicine and Biology, Signal Processing, Consumer Technology and Aerospace and Electronic Systems Societies.

HOUMAN ZARRABI (Senior Member, IEEE) received the Ph.D. degree in engineering from Concordia University, Montreal, Canada, in 2011. Since then, he has been involved in various industrial and research projects. His research interests include the IoT, M2M, big data, embedded systems, and VLSI. He is currently the National IoT Program Director and a Faculty Member of ITRC.

HASSAN RABAH (Senior Member, IEEE) received the M.S. degree in electronics and control engineering and the Ph.D. degree in electronics from Henri Poincaré University, Nancy, France, in 1987 and 1993, respectively. He became an Associate Professor in electronics microelectronics and reconfigurable computing with the University of Lorraine, Nancy, in 1993, and a Full Professor, in 2011. In 1997, he joined the Architecture Group of LIEN, where he supervised research on very large-scale integration implementation of parallel architecture for image and video processing. He also supervised research on the field-programmable gate array (FPGA) implementation of adaptive architectures for smart sensors in collaboration with industrial partners. He participated in several national projects for quality of service measurement and video transcoding techniques. He joined the Institut Jean Lamour, University of Lorraine, where he held the position of the head of the Measurement and Electronics Architectures Group, from 2013 to 2021. His current research interests include design, implementation of FPGA-based embedded systems with an emphasis on power optimization, video compression decompression and transcoding, compressive sensing, sensor networks, and machine learning. He has been a Program Committee Member, and has organized special sessions for a number of conferences. He is currently the Vice-Chair of IEEE Instrumentation and Measurement France Chapter.