Encrypted Classification for Prevention of Adversarial Perturbation and Individual Identification in Health-Monitoring

Hiroaki Kawase[1,2], Waiman Meinhold[1], Clint Zeagler[3], Toni P Miles[4], and Jun Ueda[1]

Abstract— **Developments in sensing and analysis methods have significantly increased the scope of physiological monitoring for healthcare purposes. While the continuous monitoring of physiological measurements enables improved detection and management of many illnesses, accompanying cybersecurity concerns continue to evolve. The large amounts of individualized data necessary to enable learned models for analysis must be sufficiently protected. In addition, the analysis and classification methods themselves should not be vulnerable to attack. This work addresses adversarial individual identification with multiple forms of physiological data, as well as potential performance interruption attacks. The paper proposes a homomorphic encryption scheme to mitigate both of these threats.**

I. INTRODUCTION

Developments in digital health technologies will significantly increase the scope of telemedicine. Continuous monitoring of physiological data is increasingly common with modern advances in electronics for computing and sensing. Measurements are recorded in home as well as healthcare settings, and encompass a wide range of modalities, from temperature to Electroencephalography (EEG) [1]. This accumulation of health data provides numerous opportunities for augmented diagnosis and monitoring of both acute and chronic illness. However, these benefits can only be maximized through the storage and computationally intensive analysis of large amounts of individual specific physiological data. For instance, a large scale study on the detection of COVID-19 from temperature measurements utilized a 3-day recording window [2], containing significantly more information than a single measurement.

This work seeks to address the privacy and security concerns inherent to this type of storage and communication protocol. There are several different possible cyberattack scenarios. While continuous monitoring of physiological measurements enables improved detection and management of many illnesses, attendant cybersecurity and privacy concerns continue to evolve [3]. While data protection practices involving encryption of sensitive data exist, gaps in protection are still present [4]. These gaps are particularly common where data is assumed to be anonymous, where identifiers such as patient's names are not associated with the recorded measurements. Removing such metadata is often insufficient to preserve privacy for data-driven adversarial machine learning [5].

In particular, the analysis of this data has typically required plaintext, interpretable by humans. Although a single point in time measurement does not necessarily present a privacy concern, continuous monitoring does. As this and much prior work shows, identification of individuals from snippets of physiological data is feasible [6]. Another attack attempt may be against a classifier in the cloud such as a support vector machine (SVM) [7]. Within this particular attack attempt, there are two subcategories: one attack is to inject malicious training data to increase SVM test error, called *SVM poisoning* [7]. Another attempt is to directly falsify the classifier's parameters to slightly or significantly degrade the performance of classification. The latter attack can damage the operation of cloud-based diagnosis functions in the short or long term, as well as the service provider's reputation.

This paper proposes an encrypted classification technique to prevent adversarial perturbation to an illness detection system as illustrated in Fig. 1a. The paper will propose a protected classification technique called encrypted SVM with partially homomorphic encryption. The server that processes data to detect illness in a single person or group will receive only encrypted data that will never be decrypted during the processing. This procedure ensures data security. Detection will occur in the cloud via a machine-learning method such as an SVM. Physiological data serves as the feature data, with outputs of illness status and prediction. The SVM training approach will group patients into two classes based on their infection status, with the model trained to learn the grouping from physiological measurements. This work uses a linear SVM to show the effectiveness of the encryption approach on a demonstration model. This study makes the following contributions: it clarified that the encryption method was based on the Taylor expansion and numerically confirmed that the linearization error does not spoil the performance of the SVM classifier.

This paper also demonstrates possible attacks as illustrated in Fig. 1b: (a) adversarial subject identification from EEG and temperature recordings; (b) falsification of a classifier.

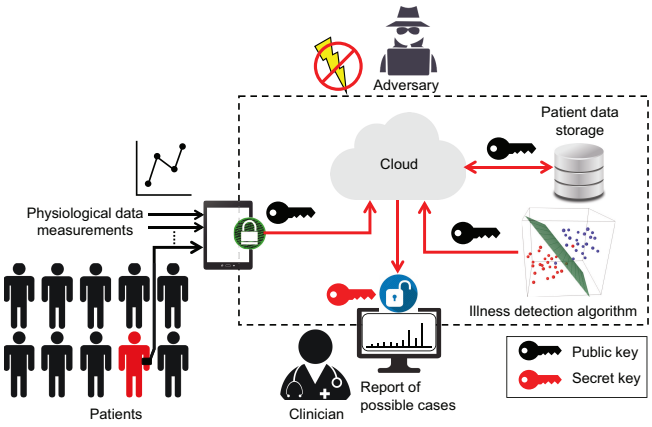
[1] Hiroaki Kawase, Waiman Meinhold, and Jun Ueda are with the Woodruff School of Mechanical Engineering, Georgia Institute of Technology, Atlanta, Georgia, USA. hiroaki.kawase@me.gatech.edu.

[2] Hiroaki Kawase is also with the Department of Mechanical and Intelligent Systems Engineering, The University of Electro-Communications, Tokyo, Japan.

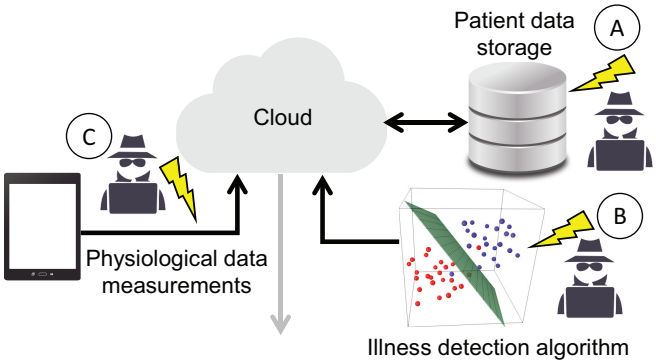
[3] Clint Zeagler is with the Institute for People and Technology, Georgia Institute of Technology, Atlanta, Georgia, USA.

[4] Toni Miles is with Department of Community Health and Preventive Medicine, Morehouse School of Medicine, Atlanta, Georgia, USA.

This study was supported in part by National Science Foundation Grant Nos. CMMI 2112793 and ERC 2124319. Hiroaki Kawase was also supported by JST SPRING, Grant Number JPMJSP2131.



(a) Proposed data and detection algorithm protection protocol



(b) Possible attack attempts. (A) adversarial individual identification due to patient data leak, (B) detection algorithm falsification, (C) malicious data injection (eavesdropping attack)

Fig. 1. The proposed data protection protocol and potential attack locations

II. Adversarial Individual Identification

A. Background

Electroencephalography is a common clinical tool for the diagnosis of both chronic and acute neurological disorders. In recent years, the use of EEG has expanded to applications such as a brain computer interface (BCI). EEG data, as a measurement of brain surface activity, enables the inference of many subject details, such as sleep stage [8], emotional state [9], as well as disease states in many neurological conditions such as Alzheimer's [10]. Two commonality among most EEG measurements is the long time frame and the high sample rate of data collection. Typical use involves band-pass filtering in an application specific window. With the high sample rate and long observation periods, a significant amount of data is collected, and the attendant privacy implications are the focus of this work.

Specifically, this paper investigates the feasibility of individual identification from arbitrary EEG snippets. Because of the varied conditions and stimuli associated with standard clinical practice for EEG, this work seeks to demonstrate the identification accuracy of randomly collected snippets over the course of other tasks. This mimics a situation in which a "bad actor" has gained access to the collected EEG data directly, but not a full study protocol.

Temperature recording is increasingly commonplace, particularly with the goal of detecting infection prior to the appearance of other symptoms. The proliferation of wearable devices and interest in analysis and detection methods have enabled large scale continuous temperature data collection from tens of thousands of participants outside of traditional healthcare settings [2]. While this large scale collection and storage of data enables effective algorithm development, privacy concerns exist. This work will show classification of individuals from continuously monitored temperature data.

More recently, glucose monitor data has been shown to readily identify individuals with standard application of a support vector machine (SVM) machine learning model [11]. While this work demonstrates and discusses the attendant privacy concerns, mitigation methods that are compatible with the needed analysis are not apparent. Particularly, the utility of an individualized reference point for glucose variability is negated if that reference point needs to be obfuscated for security, and that obfuscation prevents in-depth analysis or anomaly detection.

ECG measurement also has been shown to be individually identifiable via wavelet transform and a neural network based learned model [12]. EEG based detection of individuals has also been demonstrated on multiple channel recordings [13].

Privacy preservation is key to the future realization and deployment of physiological measurement monitoring systems. Methods such as clustering of data [14], have been shown to prevent identification of individuals from physiological data. However, a system for privacy and security analysis of individual sequence data is still lacking. This is the aim of the following work. EEG and temperature monitoring data were evaluated for their utility in adversarial individual identification via learned models. An encrypted SVM for privacy and performance protection is also proposed and evaluated.

B. Datasets

1) Electroencephalography Dataset: An open source dataset was utilized for the EEG portion of the study [15]. The study includes a range of BCI targeted tasks, with continuous EEG monitoring for each session. This work selected participants from the set who had at least 2 trials in the "standard" protocol condition: 5 of the 11 subjects met this threshold. Details of the experimental conditions can be found in the original work [15]. Of note, task labels beyond the session type were not considered in this work. This ensures that the selection of training and testing snippets is arbitrary, i.e., any classification accuracy is determined by individual differences across a range of mental states, rather than a reaction to a specific task. Task specific performance or activity has previously been used for individualization [6], but to the authors' knowledge, arbitrarily segmented activity has not. Recordings were made at 200Hz with multiple channels, however only a single channel was used for the purposes of this work. Data was segmented chronologically, at 2.5 second intervals for each of the sessions, with the last session completely held out for testing. A classification

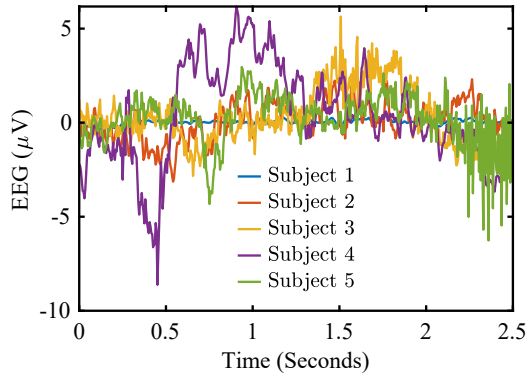


Fig. 2. Representative segments showing EEG recording snippets for each subject

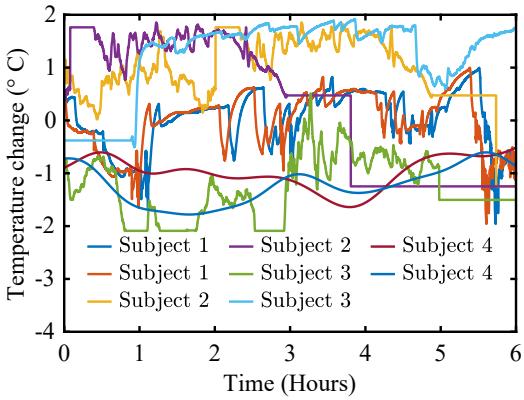


Fig. 3. Representative segments showing change in temperature from individual means

model was trained in MATLAB from the training segments in a randomized order, then tested on the test session segments.

2) EEG individual classification model: In order to predict the subject from EEG snippets, long short-term memory (LSTM) sequence-label networks were trained from the EEG dataset. LSTM networks were chosen due to the temporal nature of the data. Test and train data were taken from separate trials, with the last session for each subject used for testing. 1000 samples were used for each segment. Representative segments for each subject are shown in Figure 2. The LSTM network structure contained a bidirectional LSTM layer with 25 hidden units followed by a fully connected layer and softmax layer.

3) Temperature monitoring data: An open source temperature monitoring dataset was used to evaluate individual classification from temperature monitoring data [16]. The data consisted of combined (maximum) readings from three skin temperature sensors sampled at 0.25 Hz [16]. Data were available for 4 subjects, over a range of 3-5 days for each subject. Each individual subject's data was split into train and test pools, training data was taken from the first 48 hours, while the remaining data was held for testing. Training data was bootstrapped to 1000 sequences of six hours with random sampling. Test data was randomly divided into 200 segments of the same length for each subject. The mean temperature for each subject was subtracted to avoid biasing the results by individual baseline temperatures. An LSTM network was trained from the training data and four subject labels, which were then used to predict subject labels from the test data. The LSTM network structure contained a bidirectional LSTM layer with 100 hidden units followed by a fully connected layer and softmax layer. Representative segments for each subject are shown in Figure 3.

C. Adversarial individual identification results

1) EEG Results: The classification accuracy across all subjects was 70%. The classification rate from the validation set for each subject is shown in Table I. Four of the five subjects had classification rates above 66%, relatively high for single snippet classification from dissimilar recording sessions. Although the accuracy rate for individual subjects was as low as 43%, the mode for each of the subject test sets was correct. This means that individuals could be correctly identified 100% of the time if a full recording session was used for classification. This high individual classification rate demonstrates that identification may not require knowledge of EEG collection protocols or specific task windows.

TABLE I
EEG CLASSIFICATION ACCURACY BY SUBJECT

Subjects	1	2	3	4	5
Accuracy	99%	43%	70%	66%	72%

2) Temperature Results: The individual true positive classification rates are shown for each subject in Table II. Although classification rates ranged from 10% to 80%, the mode was correct for all but one of the subjects (75%).

These results demonstrate that temperature data can be used to identify individuals. Particularly with the increasing prevalence of temperature monitoring for infection prevention, solutions are needed to preserve privacy while maintaining the utility of common detection and analysis methods. The time window used for individual identification was much shorter than necessary for common applications, such as infection detection [2]. Without a method for encrypted classification, this application would then carry additional privacy and security risks.

III. ENCRYPTED SVM

A. Concept

The main concept presented in this paper is to enable computation of data-science classification algorithms in the cipher space by taking advantage of homomorphism. In contrast with the conventional approach of encrypting only signals on the communication line, the proposed approach is to encrypt both signals and data processing algorithms (an SVM model) by homomorphic encryption, as illustrated in Fig. 1a. One important feature of this architecture is that the secret key for decrypting signals does not need to be used in the cloud server, which is a frequent target of attack. Because the data and model are in ciphertext, this encryption

TABLE II

TEMPERATURE MONITORING CLASSIFICATION ACCURACY BY SUBJECT

Subjects	1	2	3	4
Accuracy	80%	10%	54%	56%

approach is suitable as a proactive measure to unauthorized login and falsification.

B. SVM classifier perturbations

Support vector machines for binary classification provide a linear discriminant model to classify inputs $x \in \mathbb{R}^n$ as follows:

$$f(x) = \beta x + b, \tag{1}$$

where $\beta \in \mathbb{R}^{1\times n}$ is a weight vector and $b \in \mathbb{R}$ is a bias parameter. This equation satisfies

$$\arg\min_{\beta,b} \left[\frac{1}{2}\|\beta\|^2 + \sum_i^N \xi_i\right],$$
$$\text{s.t. } t_i(\beta x_i + b) \geq 1 - \xi_i, \ {}^\forall i = 1, \cdots, N, \xi_i \geq 0,$$

where $t_i \in \{-1, 1\}$ is a data label, $x_i := [x_{i,1}, x_{i,2}, \cdots x_{i,N}]$ is a sample of the i-th training data, and $N \in Z$ is the length of a sample.

If the SVM model is implemented in plaintext, one likely scenario for a bad actor to perturb the classification performance without detection, would be to directly edit the parameters of a trained classifier. An illustrative example of this attack scenario with a 2-dimensional case with two classes is shown in Figure 4. The distribution that represents each class was assumed to be normal for simplicity. A line "original" between two distributions achieves classification with high accuracy. A modified line "attacked" with falsified β results in a classifier with no utility because the feature vectors will be mislabeled with a probability of 50% regardless of the correct labeling. In an n-dimensional model, a hyperplane would be modified by an equivalent attack.

The attack attempt, as demonstrated in Figure 4, intends to induce incorrect classifications between classes. To ensure the hyperplane passes though both distributions, the following problem is considered:

Problem 1. *Let* $\mu^+ := [\mu_1^+ \mu_2^+ \cdots \mu_N^+]^\top, \mu_i^+ := \frac{\sum_{\{j:t_j=1\}} x_{j,i}}{\#\{j:t_j=1\}}$ *and* $\mu^- := [\mu_1^- \mu_2^- \cdots \mu_N^-]^\top, \mu_i^+ := \frac{\sum_{\{j:t_j=-1\}} x_{j,i}}{\#\{j:t_j=-1\}}$ *be the average feature vectors of the original training data with labels. Find the weight* β *and the bias* b *that satisfy:*

$$\begin{bmatrix}\mu^{+\top} \\ \mu^{-\top}\end{bmatrix} \beta = \begin{bmatrix} b \\ b \end{bmatrix}. \tag{2}$$

To perform this attack, the adversary is required to know at least approximations of the mean values, μ^+ and μ^-, from eavesdropped signals and labels, if the original training data is protected and not accessible. Adversarial observation of the communication line for a relatively long period may enable this attack. This attack may also be applicable to compromise multi-class binary SVMs.

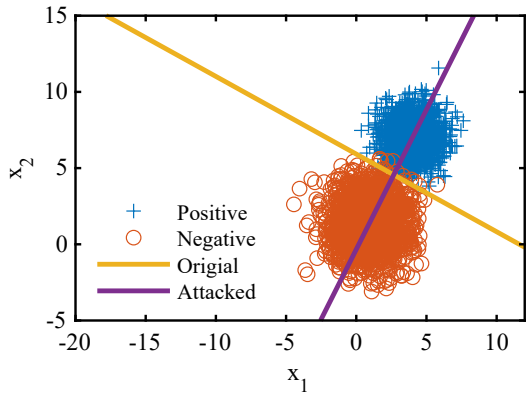


Fig. 4. Illustrative example of a modified two-class SVM by a falsification of β.

It is sufficient to change only β and keep b to arbitrarily modify the hyperplane.

Proposition 1. *For* $x \in \mathbb{R}^N$, $\beta \in \mathbb{R}^{1\times N}$, $b \in \mathbb{R}$, $c \in \mathbb{R}$: const., ${}^\exists\beta' \in \mathbb{R}^{1\times N}$ *exists that satsifies*

$$H := \{x : \beta x + b = 0\} = \{x : \beta' x + c = 0\} \tag{3}$$

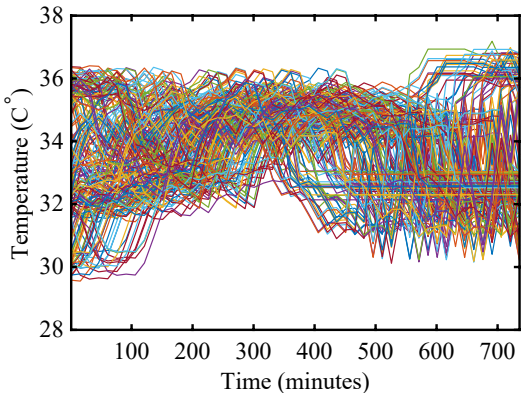
for any hyperplane H *but the plane passing through the origin.*

Proof: Multiplying the left-hand side expression by c/b yieds $\{x : \frac{c}{b}\beta x + c = 0\}$. $\beta' = \frac{c}{b}\beta$ exists since $b \neq 0$. □

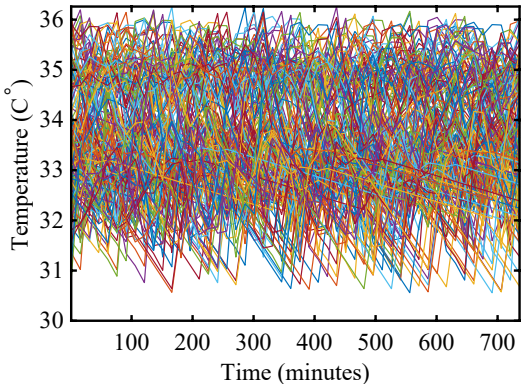
Classifiers were evaluated using the same temperature dataset used in Section II-B.3. The data was downsampled at 15-minute intervals and randomly selected 400 sample segments from raw data. Each feature vector consists of 50 values from the time-series data. The test data consists of two types: one is with a normal profile and the other is with a fevered profile as shown in Figure 5.

The data labeled as "normal" is the skin temperature data of one subject, which is measured as the baseline data in [16]. The data labeled "fevered" is the skin temperature data of two subjects who are applied a heating pad for three hours. The "fevered" feature vectors have at least 23 values in the heating period.

First, a linear discriminant model was trained using the generated training model via fitcsvm in MATLAB. The training data set has a total of 200 "normal" and "fever" labeled samples. Each sample has 200 elements. The collected data are classified into two classes; "Positive" and "Negative". Positive indicates that the classified data is supposed to have "fevered" features. Negative indicates that the data is supposed to be ordinary body temperature. Table III shows the performance of a baseline plaintext SVM. By solving for β based on (2), a falsified SVM was obtained whose performance is shown on the right of Table III. It should be noted that the modified classifier cannot classify the two classes sufficiently anymore, indicated by all of the performance metrics close to 50%.



(a) Time series data with subjects with fever (fever)



(b) Time series data with subjects without fever (normal)

Fig. 5. Temperature dataset for SVM training

TABLE III

CLASSIFICATION RESULT OF THE PLAINTEXT SVM BEFORE AND AFTER PARAMETER FALSIFICATION

	Before		After	
	Fever	Normal	Fever	Normal
Positive	76%	28.5%	40.5%	47.5%
Negative	24%	71.5%	59.5%	52.5%

C. Encryption of SVM

To conceal the parameters of the classifier model, a partially homomorphic encryption (PHE) scheme is applied [17]. Both the multiplication and addition in (1) may not be practically encrypted since fully homomorphic encryption (FHE) schemes are still highly computationally expensive. Recall *Proposition 1* that β can be a subject to attack. Therefore, a multiplicative PHE such as ElGamal, applied to βx in (1), is a reasonable choice.

The scheme ϵ has 3 functions as follows:

1) $\mathsf{Gen} : k \mapsto (\mathsf{pk}, \mathsf{sk})$, Generate a public key and a secret key with key length k
2) $\mathsf{Enc} : (\mathsf{pk}, m) \mapsto (c_1, c_2) \in \mathcal{C}$, Encrypt a message $m \in \mathcal{M}$. $\mathcal{M}$ is message space fixed by keys with a public key pk. $\mathcal{C}$ is ciphertext space
3) $\mathsf{Dec} : (\mathsf{sk}, (c_1, c_2) \in \mathcal{C}) \mapsto m$, Decrypt a ciphertext with a secret key sk.

The encryption enables to multiply messages using operation in ciphertext:

$$\mathsf{Enc}(\mathsf{pk}, m_1) \otimes \mathsf{Enc}(\mathsf{pk}, m_2) = \mathsf{Enc}(\mathsf{pk}, m_1 m_2)$$

Note that the scheme ϵ limits the number to be encrypted. We use the extended scheme ϵ^+ to operate multiplication of vectors in ciphertext. The extended scheme ϵ^+ use unequal quantizer to convert real number $\mathbb{R}$ to message space $\mathcal{M}$ and is defined to allow vector operation as follows:

2) $\mathsf{Enc} : (\mathsf{pk}, \Delta, m \in \mathbb{R}^{a\times b}) \mapsto c \in \mathcal{C}^n$, Encrypt quantized messages $m' \in \mathcal{M}^n$ from m with encoder as in the previous work [18].
3) $\mathsf{Dec}^+ : (\mathsf{sk}, \Delta, c \in \mathcal{C}^{a\times b}) \mapsto m \in \mathbb{R}^n$, Decrypt ciphertexts with a secret key sk, convert quantized messages into real number, and sum up in each row.

The element-wise product between vectors is defined as

$$\mathsf{Enc}(\mathsf{pk}, \gamma, x) \otimes \mathsf{Enc}(\mathsf{pk}, \gamma, y) := [c_i]$$
$$c_i = \mathsf{Enc}(\mathsf{pk}, \gamma, x_i) \otimes \mathsf{Enc}(\mathsf{pk}, \gamma, y_i),$$

where $x, y \in \mathbb{R}^n$.

Definition 1. *Encrypted SVM classifier is defined as follows:*

$$f_{\epsilon^+}(x) = \mathsf{Dec}^+(\mathsf{sk}, \gamma, \mathsf{Enc}(\mathsf{pk}, \gamma, \beta) \otimes \mathsf{Enc}(\mathsf{pk}, \gamma, x)) + b,$$

where $x \in \mathbb{R}^n$ is a sample, $\beta \in \mathbb{R}^{1\times n}, b \in \mathbb{R}$ are model parameters, and $\mathsf{pk}, \mathsf{sk}, \gamma \in \mathbb{R}$ are encryption parameters.

D. Encrypted SVM classification results

The choice of an appropriate key length is highly important in homomorphic encryption. Due to encryption, model parameters incur quantization errors. Some of the parameters with quantization errors are shown in Table IV. To evaluate how quantization errors impact the performance, two cases, with key lengths of 22 and 45 bits, were simulated and compared. The keys are shown in Tables V and VI. Scaling parameters were applied to input vectors x_i as follows: $\gamma = 100$ at 22 bit and $\gamma = 10^5$ at 45 bit. Scaling parameters were applied to weight vectors β as follows: $\gamma = 100$ at 22 bit and $\gamma = 10^6$ at 45 bit.

On the other hand, the increase of the key length results in a longer consumption time to compute the encrypted classifier f_{ϵ^+}. Computation time was measured using MATLAB Live Editor running on MacBook Pro 2017 (CPU: 2.8 GHz quad-core Intel Core i7). Table. VII show the average consumption time to classify one sample.

Tables VIII indicates the performance of the encrypted classifier with 22 and 45 bit keys, respectively. Comparing these results with that shown in Table III, a certain degree of performance degradation due to encryption was present with the 22-bit key. On the other hand, the performance of

TABLE IV

QUANTIZATION ERRORS IN CLASSIFIER PARAMETERS

Name	Value before Enc	Value after Enc
β_1	-0.340196	-0.340000
β_2	0.861865	0.855000
β_3	-0.319066	-0.325000

TABLE V

SECURITY PARAMETERS FOR 22 BIT KEY

Name	Value
p	0x70025F
q	0x38012F
g	2
h	0x60DD41
s	0x37617B

TABLE VI

SECURITY PARAMETERS FOR 45 BIT KEY

Name	Value
p	0x2867792A8A3B
q	0x1433BC95451D
g	3
h	0x1F43DC889DF9
s	0x12A3A19EB401

TABLE VII

AVERAGE EXECUTION TIME FOR ONE SAMPLE.

Task	Time @22 bit (sec.)	Time @45 bit (sec.)
Enc	1.24×10^{-2}	7.38×10^{-2}
Multiply	6.12×10^{-4}	8.80×10^{-4}
Dec^{+}	4.23×10^{-3}	1.80×10^{-2}
Total	1.73×10^{-2}	9.27×10^{-2}

the classifier with the 45-bit key was identical to that of the nominal plaintext classifier. This indicates that the secure encrypted SVM is achievable and capable of performing intended classification without ever needing to decrypt the model or data.

In terms of computation time, the encrypted classifier is expected to process approximately 480000 samples within each sampling window (for 750 minutes in this case) with a single consumer PC with a 45 bit key.

IV. CONCLUSIONS

This work presented initial results indicating the privacy concerns surrounding even anonymous EEG and temperature data collection and analysis. Subject identification was feasible with relatively small training data pools, necessitating better data protections. For a binary-class support vector machine to classify physiological measurements, falsification of parameters to degrade performance was demonstrated. Future works include expansion of the subject pool and applications. The encrypted illness detection methods will be integrated into a wearable patient monitoring system. Instead of partially homomorphic encryption, a somewhat homomorphic encryption scheme may be used to encrypt the entire classifier. Demonstration using a larger subject population in collaboration with a nursing home is currently planned for quantitative evaluation of the encrypted classifier.

REFERENCES

[1] A. Torku, A. P. Chan, E. H. Yung, J. Seo, and M. F. Antwi-Afari, "Wearable sensing and mining of the informativeness of older adults' physiological, behavioral, and cognitive responses to detect demanding environmental conditions," *Environment and Behavior*, vol. 54, no. 6, pp. 1005–1057, 2022.

TABLE VIII

CLASSIFICATION RESULT OF THE ENCRYPTED SVM

	22 bit		45 bit	
	Fever	Normal	Fever	Normal
Positive	66.5%	17.0%	76.0%	28.5%
Negative	33.5%	83.0%	24.0%	71.5%

[2] A. E. Mason, F. M. Hecht, S. K. Davis, J. L. Natale, W. Hartogensis, N. Damaso, K. T. Claypool, S. Dilchert, S. Dasgupta, S. Purawat *et al.*, "Detection of covid-19 using multimodal data from a wearable device: results from the first tempredict study," *Scientific reports*, vol. 12, no. 1, pp. 1–15, 2022.

[3] B. L. Filkins, J. Y. Kim, B. Roberts, W. Armstrong, M. A. Miller, M. L. Hultner, A. P. Castillo, J.-C. Ducom, E. J. Topol, and S. R. Steinhubl, "Privacy and security in the era of digital health: what should translational researchers know and do about it?" *American journal of translational research*, vol. 8, no. 3, pp. 1560–1580, 2016.

[4] K. Abouelmehdi, A. Beni-Hessane, and H. Khaloufi, "Big healthcare data: preserving security and privacy," *Journal of big data*, vol. 5, no. 1, pp. 1–18, 2018.

[5] N. Rieke, J. Hancox, W. Li, F. Milletari, H. R. Roth, S. Albarqouni, S. Bakas, M. N. Galtier, B. A. Landman, K. Maier-Hein *et al.*, "The future of digital health with federated learning," *NPJ digital medicine*, vol. 3, no. 1, pp. 1–7, 2020.

[6] A. J. Bidgoly, H. J. Bidgoly, and Z. Arezoumand, "A survey on methods and challenges in eeg based authentication," *Computers & Security*, vol. 93, no. 101788, pp. 1–16, 2020.

[7] B. Biggio, B. Nelson, and P. Laskov, "Poisoning attacks against support vector machines," in *29th International Conference on Machine Learning*. ArXiv e-prints, 2012, pp. 1807–1814.

[8] A. Supratak, H. Dong, C. Wu, and Y. Guo, "Deepsleepnet: A model for automatic sleep stage scoring based on raw single-channel eeg," *IEEE Transactions on Neural Systems and Rehabilitation Engineering*, vol. 25, no. 11, pp. 1998–2008, 2017.

[9] S. Valenzi, T. Islam, P. Jurica, and A. Cichocki, "Individual classification of emotions using eeg," *Journal of Biomedical Science and Engineering*, vol. 7, no. 8, pp. 604–620, 2014.

[10] C. Babiloni, A. I. Triggiani, R. Lizio, S. Cordone, G. Tattoli, V. Bevilacqua, A. Soricelli, R. Ferri, F. Nobili, L. Gesualdo *et al.*, "Classification of single normal and alzheimer's disease individuals from cortical sources of resting state eeg rhythms," *Frontiers in neuroscience*, vol. 10, no. 47, pp. 1–18, 2016.

[11] P. Herrero, M. Reddy, P. Georgiou, and N. S. Oliver, "Identifying continuous glucose monitoring data using machine learning," *Diabetes Technology & Therapeutics*, vol. 24, no. 6, pp. 403–408, 2022.

[12] N. Li, F. He, W. Ma, R. Wang, L. Jiang, and X. Zhang, "The identification of ecg signals using wavelet transform and woa-pnn," *Sensors*, vol. 22, no. 4343, pp. 1–15, 2022.

[13] G. Mohammadi, P. Shoushtari, B. Molaee Ardekani, and M. B. Shamsollahi, "Person identification by using ar model for eeg signals," in *Proceeding of World Academy of Science, Engineering and Technology*, vol. 11, 2006, pp. 281–285.

[14] P. Parameshwarappa, Z. Chen, and G. Koru, "An effective and computationally efficient approach for anonymizing large-scale physical activity data: Multi-level clustering-based anonymization," *International Journal of Information Security and Privacy*, vol. 14, no. 3, pp. 72–94, 2020.

[15] M. Kaya, M. K. Binli, E. Ozbay, H. Yanar, and Y. Mishchenko, "A large electroencephalographic motor imagery dataset for electroencephalographic brain computer interfaces," *Scientific data*, vol. 5, no. 1, pp. 1–16, 2018.

[16] J. Huan, J. S. Bernstein, P. Difuntorum, N. V. R. Masna, N. Gravenstein, S. Bhunia, and S. Mandal, "A wearable skin temperature monitoring system for early detection of infections," *IEEE Sensors Journal*, vol. 22, no. 2, pp. 1670–1679, 2022.

[17] T. El Gamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," in *Proceedings of CRYPTO 84 on Advances in Cryptology*. Berlin, Heidelberg: Springer-Verlag, 1985, pp. 10–18.

[18] K. Teranishi, N. Shimada, and K. Kogiso, "Stability analysis and dynamic quantizer for controller encryption," *IEEE Conference on Decision and Control*, pp. 7184–7189, 2019.