CardioTEXTIL: Wearable for Monitoring and End-to-End Secure Distribution of ECGs

Georg Bramm*, Matthias Hiller*, Christian Hofmann†, Stefan Hristozov*, Maximilian Oppelt†,
Norman Pfeiffer†, Martin Striegel*, Matthias Struck†, Dominik Weber†
*Fraunhofer Institute for Applied and Integrated Security AISEC, Garching near Munich, Germany
†Fraunhofer Institute for Integrated Circuits IIS, Erlangen, Germany
{forename.surname}@{aisec,iis}.fraunhofer.de

***Abstract*—In the wake of coronavirus disease 2019 (COVID-19), body sensor networks (BSNs) are a promising approach to provide mobile care and lower the burden on stationary health care providers. However, those BSNs collect health data which must be protected. In this paper, we introduce *CardioTEXTIL*, a three-channel electrocardiogram (ECG) system with dry polymer electrodes. It acquires ECG data and streams those over a gateway to a cloud application. Signal processing at the embedded device and machine learning (ML) algorithms in the cloud provide live diagnostics of cardiovascular events. Using Attribute-Based Encryption (ABE) gives the patient control over her data, permitting her to grant access to those data to selected parties, e.g., attending physicians. With this system, we demonstrate how to secure the complete data flow from data producer to consumer and stress that even during a pandemic, security must not be neglected to ensure the patient's security and privacy at all times.**

***Index Terms*—Body Sensor Network, Machine Learning, OSCORE, EDHOC, ABE**

I. Introduction

COVID-19 has pushed numerous healthcare systems around the world to their limits. Intensive care units were particularly overloaded at phases, which in several cases has led to a prioritization of medical assistance due to insufficient resources. Although patients with COVID-19 mainly manifest fever and respiratory symptoms, a number of cardiac complications and various electrocardiographic abnormalities may also occur [12]. Moreover, it has been observed that patients with cardiovascular risk factors and established cardiovascular disease (CVD) represent a vulnerable population when suffering from COVID-19 and therefore need constant condition monitoring [8]. This is particularly significant as CVD is the leading cause of disease burden worldwide. To cope with the pandemic situation and to ensure the continuity of medical care, wearable sensor technologies respectively BSNs are becoming increasingly important, as evidenced by the following potential applications [4]: (I) Monitoring of vulnerable populations, such as individuals with pre-existing conditions or medical personnel. (II) Monitoring of patients with relatively mild symptoms but whose clinical situation could suddenly worsen. (III) Telemedicine technologies for remote monitoring and diagnosis of COVID-19 and other diseases to decentralize patient care and thus prevent nosocomial infections in hospitals, especially infections caused by highly contagious pathogens such as severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2) or influenza viruses.

In order to provide a close-meshed monitoring but also to support the relocation of diagnostics and continuous monitoring to non-clinical settings, we present in this work a textile-integrated wearable system called *CardioTEXTIL*. The textile sensor system CardioTEXTIL collects a three-channel ECG and transmits acquired data to a cloud application. From there, the patient and selected physicians can access those data. As health data must be protected according to laws and regulations such as Medical Device Regulations (MDR) and General Data Protection Regulations (GDPR) in Europe and the Health Insurance Portability and Accountability Act (HIIPA) in the U.S., CardioTEXTIL ensures that those data are processed in a secure and privacy preserving way. To this, the security architecture of CardioTEXTIL utilizes ABE to give the patient control over their data. This permits them to grant fine-grained access to selected caregivers and protect the confidentiality and authenticity of the ECG data. Further, we propose a novel secure device provisioning method using the recently specified by IETF protocols Object Security for Contrained RESTful Environments (OSCORE) [16] and Ephemeral Diffie-Hellman Over COSE (EDHOC) [15]. We make the following contributions:

- We present CardioTEXTIL, a textile-integrated three-channel ECG with end-to-end secure architecture.
- We show how to employ signal processing and signal analysis in the cloud to detect cardiac events on the rhythm level such as abnormal T waves as well as rhythmical changes such as atrial fibrillation (Section III).
- We introduce a security architecture which provides secure device provisioning and end-to-end data security from data producer to data consumer utilizing ABE (Section IV).
- We show that this security architecture is applicable in practice and has low processing overhead (Section V).

II. State of the Art

A. Mobile ECGs

In medical application scenarios, mainly ECG monitors with adhesive silver/silver chloride (Ag/AgCl) electrodes are used to record cardiological signals. For these stationary scenarios, where patients are lying in a hospital bed or on a

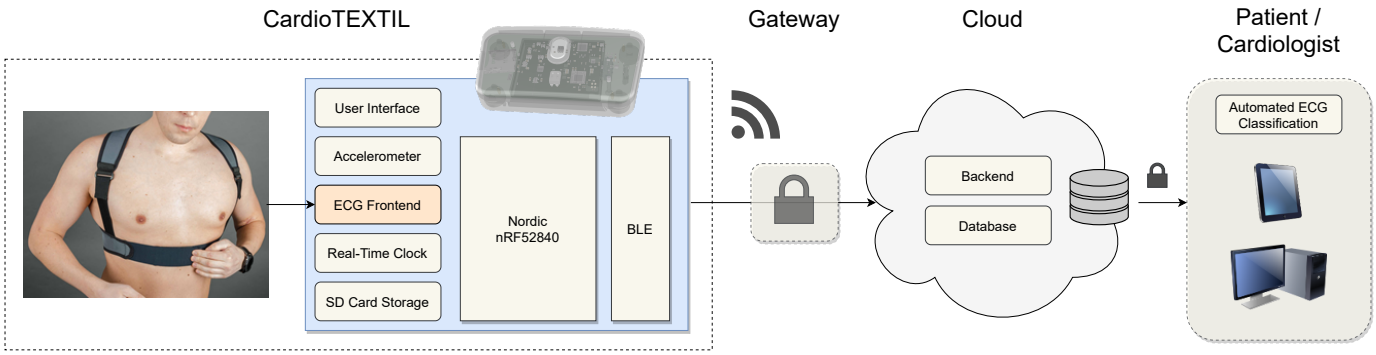

Figure 1. CardioTEXTIL system with transmission chain

treatment couch, the Ag/AgCl electrodes ensure low electrode-skin impedances and thus reliable signal recording. For mobile application scenarios, portable sensor units, so-called Holter ECGs, are used. The adhesive Ag/AgCl electrodes and cables used for this purpose can lead to severe restrictions in the patient's movement and to skin irritations. Smartwatches allow ECG signals to be recorded without adhesive electrodes, but require both hands for the measurement procedure which is often limited to a period of less than 1 minute. Textile-integrated electrodes are predestined to overcome these disadvantages, but suffer from other drawbacks such as high skin-electrode impedances or motion artifacts [3]. The latter can be reduced by a constant contact pressure and small relative movements of the electrodes to the skin. CardioTEXTIL represents a novel approach to adapting the electrode contact to the user's body position by means of an adjustable vest.

B. Secure Data Sharing in BSNs

Security requirements and practical issues for protected health information (PHI) and BSN have been stated in several works, e.g., [22], [1], [10]. Secure sharing of medical data in a cloud environment can be achieved with classical public key infrastructure [5], [7], or with novel functional encryption techniques [20], [9], [11], [10]. Our security architecture utilizes ABE, because it allows multiple recipients to access encrypted data using a fine grained access structure. Most recent approaches favour lightweight Identity based approaches, like [17], [18] with the disadvantage that only a single attribute may be used. Our ABEs approach allows a much more fine grained access decision by each patient compared to IBE. Other comparable approaches utilizing ABE to encrypt BSNs data are not end-to-end secure, as the ABE encryption process is carried out on an external device, in most cases a gateway or a mobile application, like in [19], [13]. In our approach, the ABE encryption process is carried out by the constrained BSNs itself.

III. Functional Architecture

The architecture of our system is shown in Figure 1. It comprises the CardioTEXTIL which records a three-channel ECG and transmits it to the Cloud via a Gateway. From there, the patient and parties selected by them can access the ECG records using their computers or mobile devices. Additionally, data are fed into ML algorithms for automated analysis. Our architecture secures data at rest and in motion from data generation at the CardioTEXTIL to the end-devices of the patient and parties authorized by them.

A. CardioTEXTIL and Data Acquisition

CardioTEXTIL is an adjustable vest with four dry electrodes and an attached sensor module with an ARM Cortex-M4 based nRF52840 Bluetooth Low Energy (BLE)-enabled microcontroller (MCU) by Nordic Semiconductor. CardioTEXTIL records Einthoven leads I-III at a sampling rate of 400 Hz with a spectral bandwith according to medical standards. Additionally, it captures accelerometer data as a reference for motion compensation. This, coupled with the tight fit provided by the adjustable vest permits more stable electrode contact and thus less susceptible signal acquisition. Utilizing a real-time clock, sensor data are labelled with timestamps. Labelled data are transmitted securely to the Gateway using the Constrained Application Protocol (CoAP) over BLE. Additionally, to preserve data in case of connectivity loss, data are stored on an encrypted onboard SD card. CardioTEXTIL is optimized for intuitive use. By pressing a single button on the sensor module and the Gateway, the user establishes connectivity to the Cloud. Despite using cryptography to secure data in motion, it has a battery life of up to 48 hours and thus is suitable for long-time ECG monitoring.

B. Gateway and Cloud

The gateway is a BLE capable device with Internet connectivity, e.g., a smart phone or tablet. It communicates with the CardioTEXTIL using CoAP over BLE and with the cloud application via CoAP over the mobile data connection. As CoAP is used as application layer protocol on both sides, the gateway is both simple and robust, contributing to the reliability of the system. The cloud application receives CoAP data over the Internet and stores the encrypted sensor readings in a database.

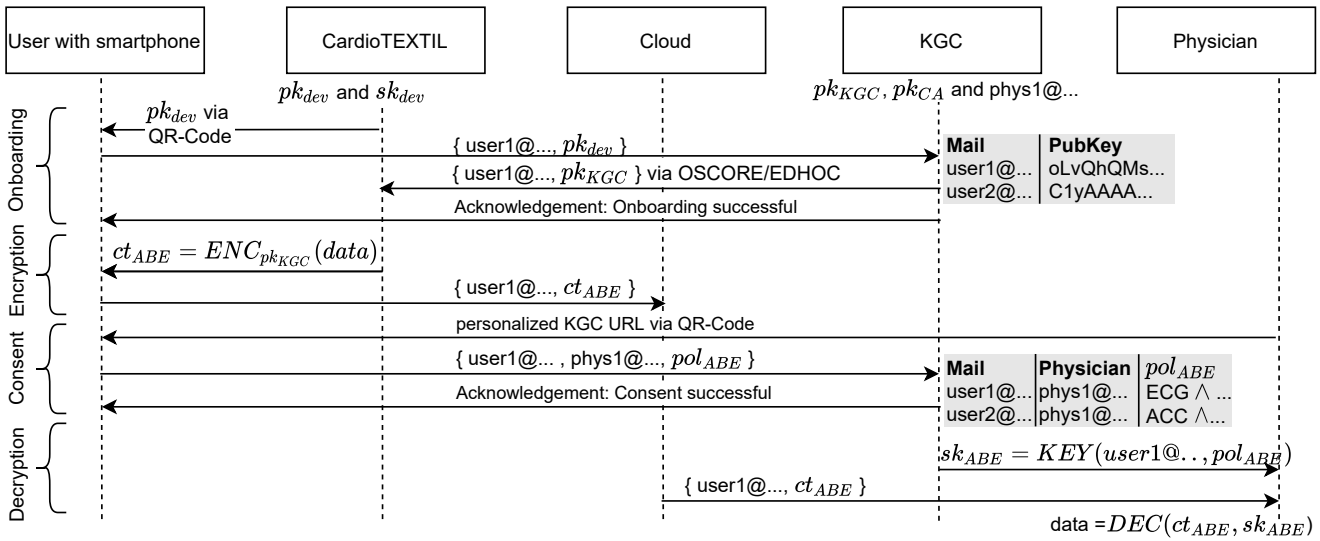

Figure 2. Security protocol of CardioTEXTIL

C. Automated ECG Classification

To detect cardiac abnormalities in ECG recordings, we employ a deep learning model based on a current state of the art architecture introduced in [14]. We modified the input dimension of our network to require only three Einthoven leads, provided by our signal acquisition front end CardioTEXTIL and selected this subset of leads from public 12 lead ECG databases that were used during PhysioNet/Computing in Cardiology Challenge 2020 [2]. Our classifier was trained to detect cardiac abnormalities that are relevant to the COVID-19 pandemic. These include morphological changes of the signal such as T wave abnormalities, as well as rhythmical changes such as bradycardia, tachycardia, atrial fibrillation and flutter. Our trained model is deployed on the cloud to enable automated classification and provide assistance for the medical professional.

IV. Security Architecture

Our security architecture aims at protecting PHI data exchanged over an untrusted network and stored on an untrusted cloud while permitting patients to share their health data with selected parties, e.g., physicians, in a user-friendly manner.

The security architecture is divided into two phases: *provisioning phase*, where credentials are exchanged between participants, and the *main operational phase*, where data is exchanged between CardioTEXTIL and legitimate users.

A. Threat Model

The attacker wants to learn or modify ECG data. Therefore, he is able to eavesdrop, manipulate and inject messages. Additionally, we assume that the attacker 1) can gain control over the Gateway, e.g., by installing malware on it and 2) has full access to the cloud data. The attacker is computationally bounded, hence he is not able to break state-of-the-art cryptographic algorithms. As one CardioTEXTIL is assigned to one user and worn at the body, we do not consider hardware attacks. We also assume that the attacker is not interested in preventing the access of users to the systems, e.g., by Denial of Service (DoS) and does not perform remote software-based attacks on the CardioTEXTIL device.

B. Provisioning Phase

In the top part of Figure 2 the protocol and the parties involved in the provisioning phase are shown. This phase begins during the manufacturing of CardioTEXTIL devices. Every device is supplied with a unique identifier, which allows the Key Generation Center (KGC) to establish a secure channel to the device. To register their CardioTEXTIL with the KGC, the user scans a quick response (QR)-code printed on the CardioTEXTIL with their smart phone. This QR code contains a hash of the identity and an activation token in form of a Uniform Resource Locator (URL). Next, the user enters their e-mail address into the smart phone. The e-mail address and the identity of the CardioTEXTIL are sent to the KGC, which uses the identity to establish a connection to the CardioTEXTIL. This established connection is end-to-end protected by EDHOC [15] and OSCORE [16] protocols. Once a secure channel is established, the KGC sends the e-mail of the user encrypted and authenticated by OSCORE. Finally, the KGC acknowledges the user about the successful completion of the provisioning phase.

C. Main Operational Phase

In the main operational phase, the CardioTEXTIL collects and caches sets of raw plaintext ECG and Accelerometer (ACC) data. This data set is encrypted and uploaded to the cloud periodically. The KGC allows the user to give consent to sharing their data with a physician. In turn, the KGC provides

a decryption key to the physician, who then can access the data. This allows the patient to share their data with multiple recipients without replication, while keeping it confidential against the gateway and the cloud.

1) Encryption: The collected data are encrypted ($ENC_{pk_{KGC}}$ in Figure 2) using a specific set of attributes in combination with the public key pk_{KGC}. The set of attributes is determined by the e-mail address of the user in combination with metadata of the specific data stream (i.e. "`user1@..,ECG`"). Yao's lightweight Key Policy Attribute Based Encryption (KP-ABE) scheme was specifically chosen in order to reduce the computational overhead on the CardioTEXTIL device as it is based on Elliptic Curve Cryptography (ECC) cryptography instead of traditional bilinear pairings. The ct_{ABE} is uploaded to and stored in the cloud database afterwards.

2) Consent: A registered physician hands out a personalized KGC URL, either in the form of a scannable QR code or as an URL. Once the patient authenticates himself as legitimate user via an Identity Provider, he is able to give the physician consent to decrypt the CardioTEXTIL data. This is done using a web form. The form data is converted into an ABE Policy (i.e. $pol_{ABE} =$ "`user1@..` $\wedge$ `ECG`") and stored on the KGC.

3) Decryption: A registered physician may authenticate himself at the KGC using an Identity Provider and fetch his ABE key, created using a policy given by the requested user. The key sk_{ABE} enables the decryption of the ct_{ABE} stored in the cloud, only if the attributes match the policy in sk_{ABE}.

V. Implementation and Evaluation

CardioTEXTIL consists of an ARM Cortex-M4 based nRF52840 BLE-enabled MCU running at 64 MHz, equipped with 1 MB flash and 256 KB RAM memory. For our experiments, we used a Raspberry Pi Model 3 as Gateway and user interface device. The KGC is implemented as cloud server. As a storage for encrypted medical data we use the AWS cloud. We used uoscore-uedhoc library as OSCORE and EDHOC implementation [6]. OSCORE uses the Advanced Encryption Standard (AES)-counter with cipher block chaining message authentication code (CCM) crypto suite. EDHOC uses ed25519 elliptic curve suite. We implemented the Yao ABE scheme [21] in Rust. Table I shows security related evolution results. In total, OSCORE/EDHOC and ABE require $\approx$112 KB of flash and peak stack usage of $\approx$ 24 KB. These are 10.72% and 9.20% of the available at nRF52840 flash and RAM respectively. OSCORE/EDHOC and ABE Init require in total 6.1 seconds, however those operations are executed only once at boot time. The OSCORE/EDHOC operations take significantly longer than ABE. This is due to the fact that EDHOC uses asymmetric certificates for authentication. Moreover, the asymmetric signing, verification and Diffie-Hellman operations performed by EDHOC are executed in software. The actual ABE encryption is performed once during the initialization process. The encryption of the packets is then performed using AES hardware accelerator.

Table I
Security evaluation–(a) memory requirements (in byte) and (b) computing time (in seconds)

(a)

	RAM	flash
OSCORE/EDHOC	4293	24193
ABE	24123	88290
flash total	—	112483

(b)

	Time
OSCORE/EDHOC	4.353
ABE Init	1.810
ABE Encrypt	0.128

VI. User experience

Data sharing by patients, or in other words the generation of an ABE policy, is carried out with the help of a web interface at the KGC. To make the user experience as easy as possible for patients, each participating physician can issue himself a personalised QR code, which automatically directs patients to the KGC and thus offers the possibility to release the recorded data with a simple one-click procedure to the corresponding physician. The generated policy is used to derive a secret key dynamically on demand by the pyhisician.

VII. Conclusion and Outlook

In this work, we have presented the CardioTEXTIL system for mobile and continuous acquisition and analysis of sensitive ECG data. In the pandemic context of COVID-19, it can monitor potentially at-risk populations or infected patients and be used for diagnosis. Thus, CardioTEXTIL aims to support a reduction in the burden on the healthcare system. We have shown, how to design and implement an architecture for securely gathering and distributing medical data at high data rates using OSCORE and ABE. This architecture puts the patient in charge of her data, which is only stored encrypted at the cloud. It allows her to fine-tune access to her data, while still making ML data analysis in the cloud possible. We implemented the complete system on off-the-shelf components and showed, that a high medical performance can be achieved despite security protocols being in place. The CardioTEXTIL has passed electromagnetic compatibility (EMC) and biocompatibility tests. We are preparing for a clinical evaluation.

References

[1] A. O. Akmandor and N. K. Jha, "Smart health care: An edge-side computing perspective," *IEEE Cons. El. Mag.*, vol. 7, no. 1, pp. 29–37, 2018.

[2] E. A. P. Alday, A. Gu, A. J. Shah, C. Robichaux, A.-K. I. Wong, C. Liu, F. Liu, A. B. Rad, A. Elola, S. Seyedi *et al.*, "Classification of 12-lead ecgs: the physionet/computing in cardiology challenge 2020," *Phys. meas.*, vol. 41, no. 12, 2020.

[3] A. Angelucci, M. Cavicchioli, I. A. Cintorrino, G. Lauricella, C. Rossi, S. Strati, and A. Aliverti, "Smart textiles and sensorized garments for physiological monitoring: A review of available solutions and techniques," *Sensors*, vol. 21, no. 3, p. 814, 2021.

[4] X. Ding, D. Clifton, N. Ji, N. H. Lovell, P. Bonato, W. Chen, X. Yu, Z. Xue, T. Xiang, X. Long, K. Xu, X. Jiang, Q. Wang, B. Yin, G. Feng, and Y. T. Zhang, "Wearable Sensing and Telehealth Technology with Potential Applications in the Coronavirus Pandemic," *IEEE Rev. in Biom. Eng.*, 2021.

[5] M. M. Haque, A.-S. K. Pathan, and C. S. Hong, "Securing U-Healthcare Sensor Networks using Public Key Based Scheme," in *ACT*, Feb. 2008, pp. 1108–1111.

[6] S. Hristozov, M. Huber, L. Xu, J. Fietz, M. Liess, and G. Sigl, *The Cost of OSCORE and EDHOC for Constrained Devices*, 2021, p. 245–250.

[7] Y. Huang, M. Hsieh, H. Chao, S. Hung, and J. Park, "Pervasive, secure access to a hierarchical sensor-based healthcare monitoring architecture in wireless heterogeneous networks," *IEEE J. SAC*, vol. 27, no. 4, pp. 400–411, May 2009.

[8] J.-S. Hulot, "Covid-19 in patients with cardiovascular diseases," *Archives of cardiovascular diseases*, vol. 113, no. 4, p. 225, 2020.

[9] N. T. Hung, D. H. Giang, N. W. Keong, and H. Zhu, "Cloud-enabled data sharing model," in *IEEE ISI*, 2012, pp. 1–6.

[10] M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," *IEEE Wirel. Com.*, p. 8, 2010.

[11] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption," *IEEE Trans. Parallel Distr. Sys.*, vol. 24, no. 1, pp. 131–143, 2013.

[12] B. Long, W. J. Brady, R. E. Bridwell, M. Ramzy, T. Montrief, M. Singh, and M. Gottlieb, "Electrocardiographic manifestations of COVID-19," *Am. J. of Emergency Med.*, 2021.

[13] B. P. No and J. Bersatu, "Design and implementation of key-policy attribute-based encryption in body sensor network," 2013.

[14] M. P. Oppelt, M. Riehl, F. P. Kemeth, and J. Steffan, "Combining scatter transform and deep neural networks for multilabel electrocardiogram signal classification," in *CinC*. IEEE, 2020, pp. 1–4.

[15] G. Selander, J. P. Mattsson, and F. Palombini, "Ephemeral Diffie-Hellman Over COSE (EDHOC)," Internet Engineering Task Force, Internet-Draft draft-ietf-lake-edhoc-06, Apr. 2021, work in Progress.

[16] G. Selander, J. P. Mattsson, F. Palombini, and L. Seitz, "Object Security for Constrained RESTful Environments (OSCORE)," RFC 8613, Jul. 2019. [Online]. Available: https://rfc-editor.org/rfc/rfc8613.txt

[17] C. C. Tan, H. Wang, S. Zhong, and Q. Li, "Body sensor network security: an identity-based cryptography approach," in *Proceedings of the first ACM conference on Wireless network security*, 2008, pp. 148–153.

[18] ——, "Ibe-lite: A lightweight identity-based cryptography for body sensor networks," *IEEE Transactions on Information Technology in Biomedicine*, vol. 13, no. 6, pp. 926–932, 2009.

[19] Y.-L. Tan, B.-M. Goi, R. Komiya, and S.-Y. Tan, "A study of attribute-based encryption for body sensor networks," in *International Conference on Informatics Engineering and Information Science*. Springer, 2011, pp. 238–247.

[20] D. H. Tran, Hai-Long Nguyen, Wei Zha, and Wee Keong Ng, "Towards security in sharing data on cloud-based social networks," in *ICSP*. IEEE, 2011, pp. 1–5.

[21] X. Yao, Z. Chen, and Y. Tian, "A lightweight attribute-based encryption scheme for the internet of things," *Fut. Gen. Comp. Sys.*, vol. 49, pp. 104–112, 2015.

[22] M. Zhang, A. Raghunathan, and N. K. Jha, "Trustworthiness of medical devices and body area networks," *Proc. IEEE*, vol. 102, no. 8, pp. 1174–1188, 2014.