hbcLock: Encrypted RF Communication Utilizing Body-Coupled Keys for the Internet of Bodies

***Abstract*—Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.**

***Index Terms*—...**

I. Introduction

The Internet of Bodies (IoB) is an imminent extension of the vast Internet of Things (IoT) domain, in which smart devices like wearables, implants and embeds are interconnected forming their own personal network, while being placed in, on and around the body. The devices connected via IoB nodes constantly record body vital data from its surrounding and log it to a server remotely, where the data is analysed to procure meaningful information which is used by the user for healthcare purposes [1] .The concept of connecting various physical objects over a network where they can communicate with themselves came from the Internet of Things (IoT) domain, which motivated the researchers to extend it where it can be beneficial for the healthcare sector to diagnose body vitals continuously, which in turn helps in early detection of disease and increased chances of cure. The data acquisition performed by the IoB nodes is very important when it comes to designing personalised health care regimes for faster recovery and better results. With the recent technological advancements, IoB devices have become more secure, reliable and long-lasting, which helps patients for prolonged monitoring for extended periods of time [2]. IoB enabled wearables help continuously track an individual's body vitals, which in due time is used for early detection, diagnosis and treatment of various ailments and diseases.

Figure 1 (A) depicts a top-level view of an IoB enabled system for Cardiac Health Monitoring purposes(e,g, Electrocardiogram). The figure shows the on-body patch sensing the Electrocardiogram (ECG) and transmitting it uninterruptedly at real-time to a remote server for an individual via a smart-interface device. The knowledge attained from the data is used by the server to provide accurate status of an individual's heath.

People working in the field of IoB enabled wearables expect certain characteristics as in: Firstly, they should be capable of operating for extended periods of time, conceivably months or years.Secondly, IoB enabled wearables should not be bulky as then it can potentially cause discomfort to an individual and might adversely affect the body vital monitoring. Lastly, the IoB enabled wearables should have security as its highest priority when it comes to transmitting data, as data related to one's health is susceptible and should be averted from falling to unintended recipients [3]. However, wearables used in recent times preeminently use radiative wireless technologies namely Bluetooth or WiFi for communication purposes. These methods fall short when it comes to accomplishing above prerequisites for the reasons listed below:

Wearables with wireless radiative technology tends to be cumbersome due to their bulkier nature when it comes to prolong usage. Also, energy consumption is significant due to data transmission via air. Wearables using wireless radiative technologies have large range of connectivity, hence they are predisposed to eavesdropping. An unauthorized user can track the signal and possibly retrieve it, causing security breaches.

To overcome the above issues faced by researchers, some solutions proposed are Visible Light Communication (VLC) and Human Body Communication (HBC).Visible Light Communication (VLC) is a wireless technology that used the visible light spectrum to transmit data, offering advantages over existing radio frequency (RF) communication. It offers a vast, unsupervised spectrum, trivial interference and dual functionality. It is an optimistic solution for navigation done indoors, smart lighting and high-speed internet access [4] [3].On the other hand, Human Body Communication (HBC) is a technology that focuses data transmission using human body's conductive properties. It is a secure, low-power communication method ideal for wearables and personal area networks. The implementation of this technology enhances the efficiency and security of health monitoring and bio metric authentication systems [5] [6].

Although Visible Light Communications offers promising edge in data transmission over existing radiative technologies, the shortcomings which are to be addressed are limited coverage, including interference and major dependency on line-of sight. Adding to this, the high bandwidth of LED modulation and the need of standardisation gives rise to integration issues. [7] [8]. Human Body Communication (HBC) has its own shortcomings namely, name the propagation range of data, technical attributes related to tissues and body postures and thermal management. A significant amount of research is still

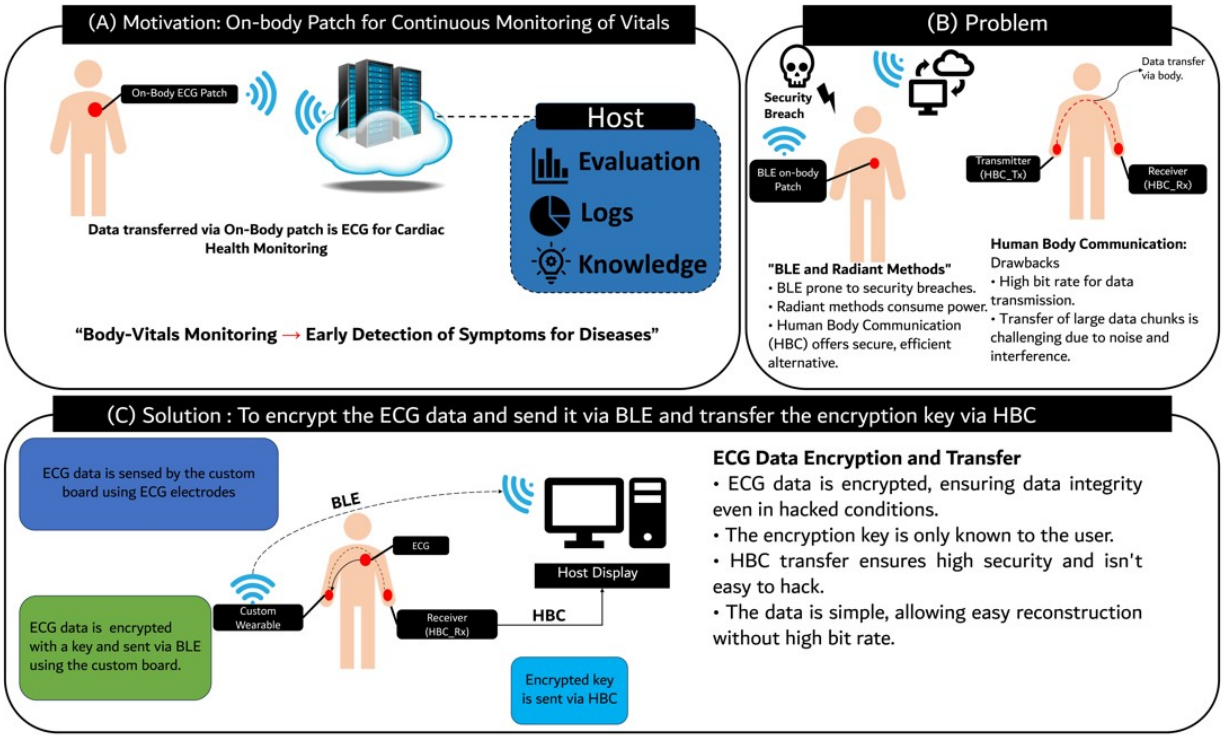

Fig. 1. Introduction

going on in the field of Human Body Communication. [9] [10]. Figure 1 (B) shows the shortcoming of the traditional radio frequency (RF) technologies and Human Body Communication (HBC).

For the first time, our work proposes Human Body Communication based key encryption for secured RF communications. HbcLock, as we name it and illustrated in Figure 1 (C), transmits encrypted ECG data via Bluetooth Low Energy (BLE) and the encryption key is transmitted via the body channel using Human Body Communication. At the receiving end, both the encrypted ECG data and encryption key is received and after performing decryption, the original ECG is plotted and processed for analysis of an individual's health status.

The rest of the paper is structured as follows, Section II is based on the reviews of the existing works in secured authentication of RF-based wearables, HBC systems and wearable security . In this section, we examine and differentiate existing works with our own. In Section III, we present the system design of hbcLock, addressing the hardware and software details of BLE transmitter and receiver and also HBC transmitter (HBC-Tx) and HBC Receiver (HBC-Rx). In Section IV we present the characterization results of HBC, including analysis of receiver performance and placements of transmitter electrodes. Lastly, we conclude the paper in Section V.

II. Related Work

We find several works on secure transmission of ECG data in literature. Most of the works focus on transmitting the data using RF technologies. In [11], the preservation of sensitive ECG data is being done by an authentication using manipulatable Haar transform (MHT), which is carried out by complex machine learning and deep learning based cryptography algorithms. A similar kind of work is done in [12], where improved Jules Sudan based cryptography algorithm is used to authentic the ECG data, with key agreement as message authentication. When coming to the security of Body Area Networks (BANs), work proposed by [13] uses media access control (MAC), which provides zero-administration security by automatic private key generation. Addressing to key generation and distribution, a two-tier authentication is proposed in [14] , where two sources randomness is utilized to perform simultaneous device authentication and key distribution through separate means. Two-factor authentication using mobile is being done in the work by [15] where Photoplethysmography (PPG) is leveraged to extract individual characteristics of the PPG signals . In the works [16], [17], [18], [19], [20] and [21], more emphasis has been put in to sensing the ECG data via on body wearables and transmitting it using different configurations of HBC transceivers with the help of different modulation techniques. Our work differs in a way that we use a simple encryption and decryption methodology and transmission of encrypted ECG is done via BLE and HBC is used to transmit encryption key.

We find very less work on our proposed HBC configuration, in which the ground electrode of the HBC transmitter (HBC-Tx) has a dielectric layer before it is placed on the body. Works in [22], [23], [24], [25], [26] and [27] discusses the different electrode placement of the TX signal and ground electrodes on body, with varying sizes of electrodes and also varying distance between the Tx signal and ground electrode. It has been seen that when the Tx ground is kept floating, there is a significant attenuation seen at the receiver end. The signal improves significantly when the when the ground electrode is placed directly on the body. Experiments conducted in the above mentioned works are done with regards to magnitude of electric field developed (dB/V) for different HBC-Tx ground placements, the most efficient transmitting path, different HBC-Tx and HBC-Rx configurations and different ground configurations of HBC-Rx.

On the major concerns of security in wearable communications, [28] proposed a passive Radio Frequency Identification (RFID) based a conductive thread knit fabric strain gauge assembly for wireless and smart-garment devices with continuous and secured biofeedback monitoring. In the work proposed by [29] , a secure RF based communication is implemented using VirtualWire protocol, complex computation techniques and hardware. Radio Frequency based fingerprinting for security of wearables has been proposed in [30]. In this work extraction of L-LTF signals from the WLAN physical layer production unit (PPDU) to obtain unique device fingerprints, followed by the use of convolutional neural network (CNN) with two convolutional layers and three fully connected layers to classify devices based on these fingerprints.

III. System Design

In this section, we describe the system design of the proposed hbcLock wearable. Figure 2 depicts the block level overview of hbcLock wearable. It used 1-Lead ECG electrodes to sense ECG data using AD8232. This data is fed into a 12-bit ADC for sampling, After the ECG data is sampled, it is encrypted using an encryption key. The encrypted ECG data is transmitted via Bluetooth Low Energy (BLE) 4.0. The PSoC 4 is also programmed to transmit the encrypted key via an assigned pin which is connected to the HBC transmitter, which is placed on the body to transmit the encrypted via HBC channel. The firmware flowchart in Figure 3, depicts the flow of instructions in the hbcLock band. The ADC and BLE is started in the beginning, after which the sensing of ECG data via the electrodes is done. Once the encrypted data is sensed, it is then sent for encryption and parallely the encryption key is generated via UART. Finally, the encrypted ECG data is sent via BLE and the encryption key is transmitted via HBC continuously.

A. 2-Lead ECG Acquisition Band

The hbcLock is incorporated with a 2-lead ECG Acquisition band, which uses two electrodes, namely Right Electrode(RA) and Left Electrode (LA) to sense the ECG and record it for further process. Here the Right Leg Drive is already grounded, which reduces the use of an extra electrode and hence device complexity and cost reduces. The ECG data sensed by the band is then fed into the ADC present in the microcontroller unit to sample the ECG signals and after encryption, sent via BLE.

B. BLE Transmitter and Receiver

The PSoC-4 MCU comes with an in built BLE provision (Bluetooth 4.0) . The on-chip BLE module acts as the transmitter which transmits the encrypted ECG data at a baud rate of 115200 bps. An external BLE module attached to the computer acts as a BLE receiver, which receives the data and the data is collected via the comport (COM) on the computer. From the comport, using python script the data is retrieved and saved. This data is further processed and analyzed for different conclusions. Figure 5 shows the BLE module which acts as the BLE receiver for the receiving of encrypted ECG data.

C. HBC Transmitter and Receiver

The HBC transmitter (HBC-Tx) configuration used in our hbcLock wearable consists of two electrodes: A signal electrode (SGN) and a ground electrode (GND). The dimensions of both the electrodes are 6cm x 3cm. The distance between the SGN electrode and GND electrode is kept at 3cm. The SGN electrode is placed directly on the body, whereas the GND electrode is kept floating by using insulation in between the plate and body. The HBC Receiver (HBC-Rx) is a copper electrode of dimension 12cm x 6cm. The received signal from the electrode is then fed to an RC high pass filter of cut-off frequency 15.923 kHz, which efficiently filters out the 50Hz noise. A PSoC-5 board is used to supply 4 V rail voltage so that the output of the RC high filter is clamped around 2.0 V range for improved demodulation. The signal from the RC high pass filter is then fed to a Picoscope. From the Picoscope, a csv file is generated which is fed to the system for demodulation and decoding of the encryption key. In the Figure 7, the whole HBC receiver system setup is depicted.

The proposed HBC model, as shown in the Figure for the hbcLock is focused mainly on transmission of the signal from the wrist, where the wearable is worn to the fingertip touching the ground. The operating frequencies are much higher in wavelength when compared to the human body, hence the transmission can be regarded as the quasi-static electric field. In our model, we have considered the arm and the torso as a non-ideal (lossy) conductor, hence modeled with the electrical parameters equal to that of the body muscle (relative permittivity ε_r = 81 and conductance σ = 0.62 S/m). The impedances inside the body are modeled as lumped RC circuits, with R and C parallel to each other, whereas the capacitive coupling through the air can be represented by a discrete capacitor. This way the whole transmission of signal via HBC can be expressed as an equivalent model [24], [23].

The equivalent circuit is composed of the following impedances:

- $C_{dielectric}$, which is the capacitance formed by the ground of the HBC-Tx and the surface of the arm, with a

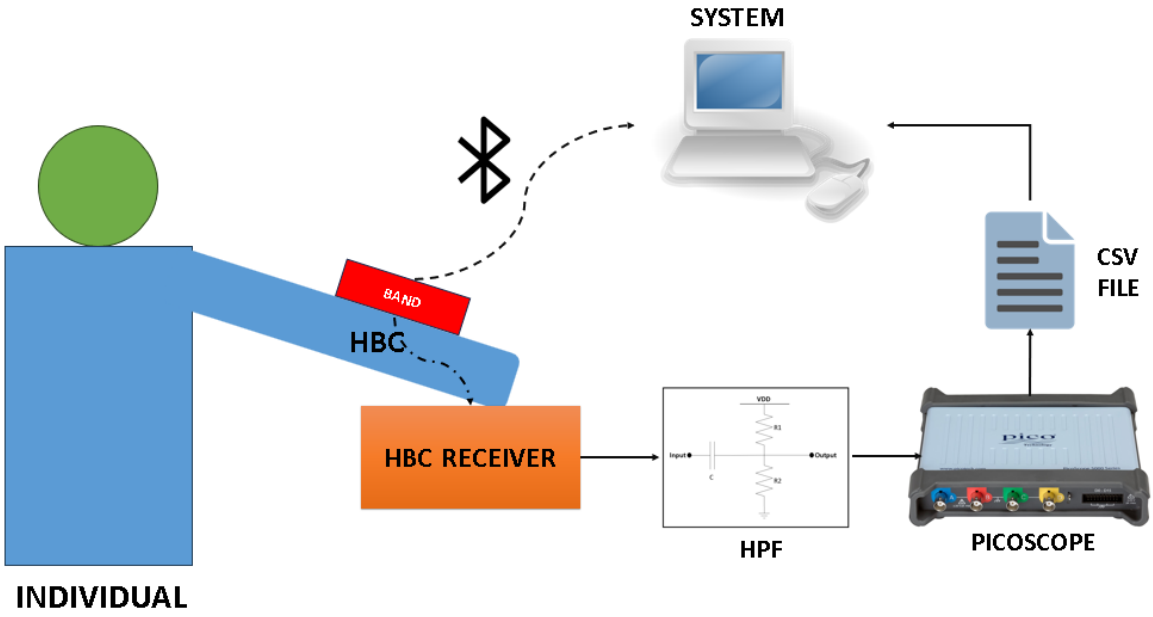

Fig. 2. Block-Level Overview

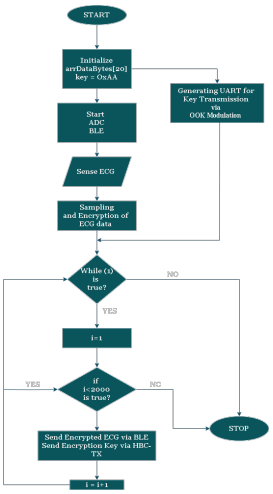

Fig. 3. Firmware Flowchart

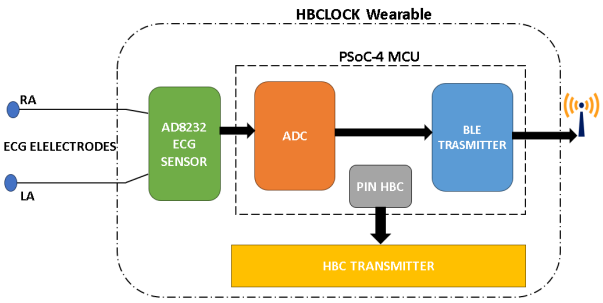

Fig. 4. Block level Overview of hbcLock band

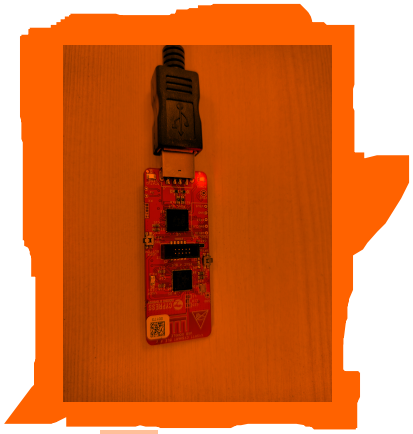

Fig. 5. BLE Receiver

dielectric of 1mm thickness in between which has relative permittivity ε_r = 4.0.

- $Z_{electrode}$, which is the impedance between the signal and the ground electrode of the HBC-Tx.
- Z_{arm}, which is the impedance between the signal electrode of the HBC-Tx and the HBC-Rx electrode.
- Z_{TX} , which is the impedance between the HBC-Tx wrist contact and HBC-Rx electrode
- Z_{arm_Body} , which is the capacitance formed by capacitive coupling of the arm and the body.
- Z_{Body} , which is the impedance offered by the body with respect to the HBC-Rx ground.
- Z_{RX_Body} , which is the capacitance formed by capacitive coupling of the body and the HBC -Rx ground.
- Z_{arm_RX} , which is the capacitance formed by capacitive

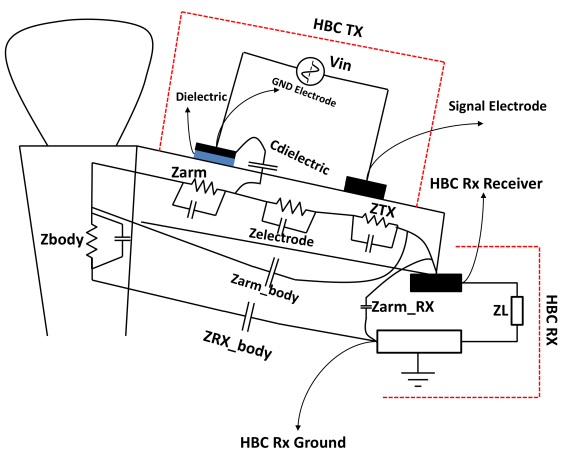

Fig. 6. Proposed HBC Model

coupling of the arm and the HBC -Rx ground.

- Z_L , which is the impedance of the whole HBC-Rx circuit.

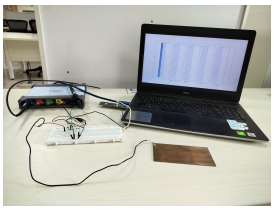

Fig. 7. HBC Receiver Setup

The capacitances are calculated by the formula : C = Aε_r ε_0 / d, Where

- A is the area of the capacitive plate.
- d is the distance between two capacitive plates.
- ε_0 is the absolute permittivity (8.854 x $10^{(}$ – 12) farads per meter (F/m).
- ε_r is the relative permittivity.

The impedances of the body are modeled as RC circuits, with resistance and capacitance set up in parallel. At frequencies of HBC transmission, the reactance provided by the capacitances of the get nullified and only the resistance acts. So the impedances are modeled as resistances when the body is considered as a non-ideal conductor.

The resistances are calculated by the formula : R = ρl / A, Where

- A is the area of the cross section of the modeled conductor.
- l is the length of the conductor.
- ρ is the resistivity of the material of the model.

The most important point to be kept in mind while evaluating HBC channel is the return path as the received signal strength depends on the return path. For our model, we have considered the return path as from the HBC-Tx Signal electrode, through the human arm and the fingertip, the HBC-Rx electrode, the whole HBC-Rx circuit, the capacitive coupling between receiver ground and the human body and finally return to the ground electrode of HBC-Tx via the human body. This is the best path for the transmitter signal to reach the receiver and return.Figure 8 shows the equivalent RC model of the proposed hbcLock. The input voltage is the 4 V supply from the PSoC-5 board and the output voltage signifies the receiver end obtained voltage, which is approximately the value we obtained during experiments.

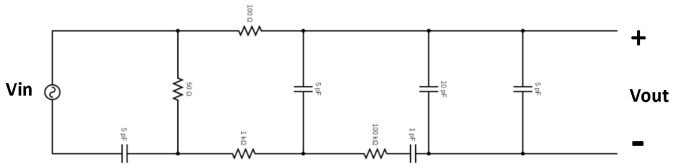

Fig. 8. Equivalent Circuit Model of the proposed HBC Model

IV. Results

For the evaluation of the hbcLock, we conduct several experiments . First, we demonstrate the fully functional hbcLock,from the encrypted ECG data transmission, the encryption key transmission, reconstructing the encryption key and finally decrypting and plotting the Original ECG. Second, we conduct experiments with different HBC-Tx electrode configurations to characterize the strength of received signal. Third, we conduct experiments with varying ground size of HBC-Tx electrode, keeping the size of the signal electrode of HBC-Tx constant to characterize the quality of the received signal. Fourth, we conduct the experiments with different thickness of dielectrics for the floating ground configuration of the HBC-Tx to characterize the attenuation. Lastly we conclude with conducting experiments with different HBC-Rx ground and observing the behaviour of the received signal.

A. Full demonstration of the hbcLock:

Towards demonstrating hbcLock, we use the setup described in Figure 2. The ECG is sensed using the ECG wet-electrodes and then it is sampled by the ADC. After the sampling the ECG data is encrypted using XOR encryption and transmitted via BLE. Simultaneously, the encrypted key is transmitted via HBC-Tx and received at the HBC-Rx side. The 1-byte encryption key is transmitted via HBC-TX using OOK modulation with carrier frequency of 500kHz and received by HBC-Rx circuit, which is directly fed to the Picoscope. The signal received by the Picoscope is displayed on the screen at the receiver's end, which has a sampling frequency set to 10MHz. Using the Picoscope software,a set of 64 waveform is collected and stored in csv file format. This set of 64 waveform is combined using a python script, keeping in mind the sample frequency(i.e., 10MHz). The script returns a combined csv of the whole data collected at the receiver's end with the help of Picoscope in a single csv file.

The combined csv is then given as input to OOK demodulation circuit in Simulink to obtain the demodulated data. The demodulation circuit consists of a Band-Pass filter, a non-linear squaring unit, a Low-pass filter, followed by a thresholding unit. Band Pass Filter is used to extract the data carried by the signal, from around the carrier frequency. In this process we get values on the negative axis as well due to carrier frequency being sinusoidal in nature. Figure 9 shows the output obtained after signal is passed through Band Pass Filter.

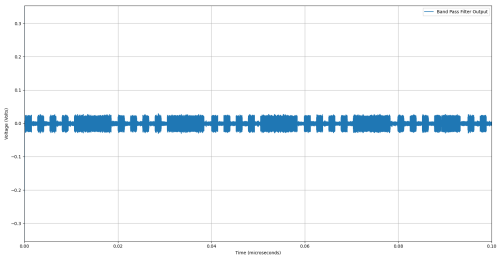

Fig. 9. Band Pass Output Waveform

After the signal is passed through the band pass filter, to recover the original nature of the signal as well as to have a component of data around the baud-rate frequency, non-linear squaring is done. Figure10 depicts the waveform obtained after non-linear squaring function. The Band-Pass filter removes low-frequency components, but when the band pass filtered signal undergoes non-linear operation like squaring, a low-frequency component emerges,which is then filtered using the Low-Pass filter. The Low-Pass filter is designed in such a way that it allows frequency in the range of the baud-rate of the UART signal, and passes all frequencies above that. So, we get the signal which has the data we need to recover. i.e., decode. Figure 11 describes the nature of the waveform after is passes through the Low Pass Filter.

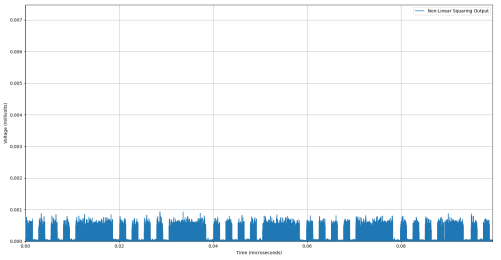

Fig. 10. Non-Linear Squaring Output Waveform

Thresholding is a crucial step in On-Off Keying (OOK) demodulation. After the signal is passed through a Low-Pass filter, it contains both the desired signal and some residual noise. The thresholding process helps to distinguish the signal from the noise. In OOK modulation, the presence of a signal represents a binary ‘1’, and its absence represents a binary ‘0’. However, due to noise and other factors, the received signal might not be a perfect representation of the transmitted signal. Therefore, a threshold is set to decide whether the received signal represents a ‘1’ or a ‘0’. The waveform observed at the output scope is the demodulated data which is then stored as a csv file using a MATLAB script. This demodulated data csv is put through the riply library present in python, which decodes the UART demodulated data and gives the reconstructed encrypted key which was initially transmitted via HBC. Figure 12 shows the waveform of the reconstructed 1-byte encryption key.

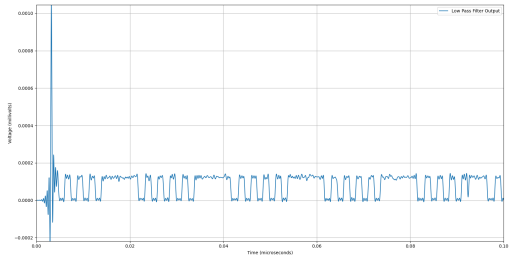

Fig. 11. Low Pass Filter Output Waveform

The reconstructed encrypted key is also stored in a csv file format. Here we are using XOR based encryption-decryption technique, wherein a dataset is XORed by a single key(encryption) and transmitted. The received dataset is then XORed again using the same key (decryption) and the dataset is transmitted securely. We received the encrypted ECG data via BLE, encrypted by 1 byte hexadecimal key and stored it in a csv. The reconstructed 1-byte hexadecimal encryption key transmitted via HBC is also saved in a csv.

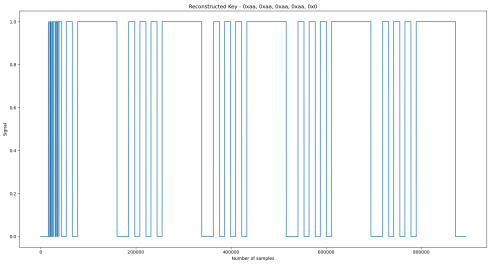

Fig. 12. Decoded Output Waveform

Both the encrypted ECG data csv and reconstructed encryption key csv is fed into a python script where all the samples of the encrypted ECG data is XORed with the reconstructed encryption key, stored in a new csv with all hexadecimal values converted into decimal and using the matplotlib library of python, Figure 13 shows the final output where the original ECG is obtained after decryption.

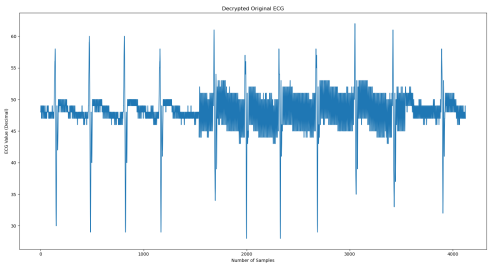

Fig. 13. Decrypted Original ECG Output

B. Influence of Varying the HBC Transmitter Dimensions:

Table 14 shows the experimental results of the relationship between the received signal side voltage to that of that of the varying HBC transmitter dimensions. The centric distance between the HBC signal electrode and the HBC ground electrode is kept constant, as well as the dielectric thickness between the HBC ground electrode and the skin. We have observed a significant decrease in the value of the received. Plot in the Figure 15 shows the variation of the received side

Tx-SGN size	Tx-GND size	TX Centric Distance	Dielectric Thickness	Received Signal	Attenuation (dB)
6cm x 3cm	6cm x 3cm	3 cm	1mm	0.60 V	-16.47
3cm x 3cm	3cm x 3cm	3cm	1mm	0.22 V	-27.13
2cm x 2cm	2cm x 2cm	3cm	1mm	0.17 V	-27.46
1cm x 1cm	1cm x 1cm	3cm	1mm	0.103 V	-31.78

Fig. 14. Table I Experimental Conditions

signal voltage with the decrease in the dimensions of the HBC-Tx. The received signal side voltage monotonically decreased from 0.6V to 0.103V, when the dimensions of the HBC-Tx was decreased from (6cm x 3cm) to (1cm x 1cm). The attenuation sees a decrease from -16.47 dB to -31.78 dB.

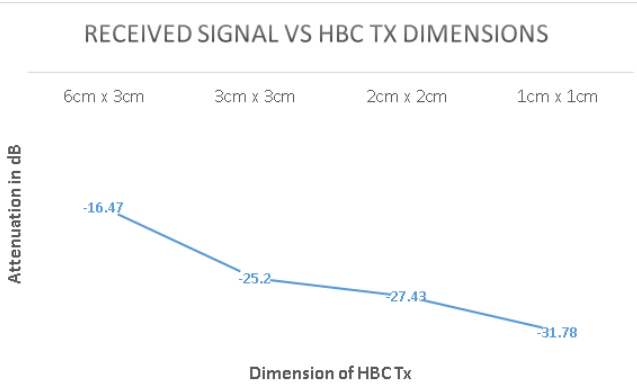

Fig. 15. Received Signal vs HBC-Tx Dimensions

C. Influence of Varying the HBC Transmitter Ground Dimensions:

Table 16 shows the experimental results of the relationship between the received signal side voltage to that of that of the varying HBC transmitter ground dimensions. The HBC-Tx signal electrode's dimension is kept constant, along with he centric distance between the HBC signal electrode and the HBC ground electrode is kept constant and the dielectric thickness between the HBC ground electrode and the skin. We have observed a significant decrease in the value of the received.

Tx-SGN size	Tx-GND size	TX Centric Distance	Dielectric Thickness	Received Signal	Attenuation (dB)
6cm x 3cm	6cm x 3cm	3 cm	1mm	0.60 V	-16.47
6cm x 3cm	3cm x 3cm	3cm	1mm	0.40 V	-20
6cm x 3cm	2cm x 2cm	3cm	1mm	0.33 V	-21.67
6cm x 3cm	1cm x 1cm	3cm	1mm	0.17 V	-27.43

Fig. 16. Table II : Experimental Setup

Plot in the Figure 17 shows the variation of the received side signal voltage with the decrease in the dimensions of the HBC-Tx ground electrode. The received signal side voltage monotonically decreased from 0.6V to 0.17V, when the dimensions of HBC-Tx ground electrodes were decreased from (6cm x 3cm) to (1cm x 1cm). The attenuation sees a decrease from -16.47 dB to -27.43 dB.

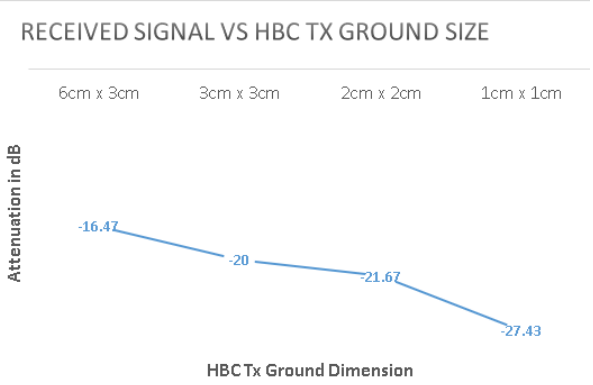

Fig. 17. Received Signal vs HBC-Tx Ground Dimensions

V. Conclusion

Our research successfully demonstrated the hbcLock, which encrypts the real time ECG data with the help of XOR encryption and transmits it real time via Bluetooth Low Energy (BLE) while simultaneously transmitting the 1-byte encryption key via Human Body Communication using UART protocol and OOK modulation. At the receiver's end, the 1-byte encryption key is reconstructed using demodulation circuit system in Simulink and decoded in Python script and XORed with the encrypted ECG data received to obtain the original ECG after decryption.

Our research demonstrates the performance of the hbcLock is sensitive to varying HBC transmitter electrodes dimensions and HBC transmitter ground electrode dimensions . The decrease in size of the HBC transmitter electrodes as well as HBC transmitter ground electrode saw a significant decrease in the receiver side signal, which was seen by the high attenuation

values in smaller dimensions of the HBC transmitter electrodes as well as HBC transmitter ground electrode.

There is enough future scope in this work in the areas of miniaturizing the HBC transmitter to obtain better attenuation; randomizing the generation of key which will enhance the security of the existing system multiple folds. At the receiver end, designing of HBC receiver is a imminent task that can gain provide significant noise-free for better demodulation such that low signals can be transmitted and reconstructed with greater ease. Deploying the hbcLock for other bio potential signal sensing is left for future research.

REFERENCES

[1] A. Celik, K. N. Salama, and A. M. Eltawil, "The internet of bodies: A systematic survey on propagation characterization and channel modeling," *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 321–345, 2021.

[2] A. Celik and A. M. Eltawil, "The internet of bodies: The human body as an efficient and secure wireless channel," *IEEE Internet of Things Magazine*, vol. 5, no. 3, pp. 114–120, 2022.

[3] K. Agarwal, R. Lalwani, U. Abeena, and K. Polachan, "Vlc-le: Energy-efficient and secure visible light communication for the internet of bodies," in *2024 International Conference on Smart Applications, Communications and Networking (SmartNets)*. IEEE, 2024, pp. 1–6.

[4] Z. N. Chaleshtori, S. Zvanovec, Z. Ghassemlooy, O. Haddad, and M.-A. Khalighi, "Impact of receiver orientation on oled-based visible-light d2d communications," in *2021 17th International Symposium on Wireless Communication Systems (ISWCS)*, 2021, pp. 1–6.

[5] A. AlAmoudi, A. Celik, and A. M. Eltawil, "Cooperative body channel communications for energy-efficient internet of bodies," *IEEE Internet of Things Journal*, vol. 10, no. 4, pp. 3468–3483, 2022.

[6] A. Vale-Cardoso, M. Moreira, K. K. Coelho, A. Vieira, A. Santos, M. Nogueira, and J. A. M. Nacif, "A low-cost electronic system for human-body communication," *Electronics*, vol. 9, no. 11, p. 1928, 2020.

[7] A. R. Ndjiongue, T. M. Ngatched, O. A. Dobre, and A. G. Armada, "Vlc-based networking: Feasibility and challenges," *IEEE Network*, vol. 34, no. 4, pp. 158–165, 2020.

[8] S. U. Rehman, S. Ullah, P. H. J. Chong, S. Yongchareon, and D. Komosny, "Visible light communication: A system perspective—overview and challenges," *Sensors*, vol. 19, no. 5, p. 1153, 2019.

[9] J. Petäjäjärvi, K. Mikhaylov, R. Vuohtoniemi, H. Karvonen, and J. Iinatti, "On the human body communications: wake-up receiver design and channel characterization," *EURASIP Journal on Wireless Communications and Networking*, vol. 2016, pp. 1–17, 2016.

[10] J. F. Zhao, X. M. Chen, B. D. Liang, and Q. X. Chen, "A review on human body communication: Signal propagation model, communication performance, and experimental issues," *Wireless Communications and Mobile Computing*, vol. 2017, no. 1, p. 5842310, 2017.

[11] W. Yang and S. Wang, "A privacy-preserving ecg-based authentication system for securing wireless body sensor networks," *IEEE Internet of Things Journal*, vol. 9, no. 8, pp. 6148–6158, 2021.

[12] Z. Zhang, H. Wang, A. V. Vasilakos, and H. Fang, "Ecg-cryptography and authentication in body area networks," *IEEE Transactions on Information Technology in Biomedicine*, vol. 16, no. 6, pp. 1070–1078, 2012.

[13] M. Kuroda, S. Qiu, and O. Tochikubo, "Low-power secure body area network for vital sensors toward ieee802. 15.6," in *2009 Annual International Conference of the IEEE Engineering in Medicine and Biology Society*. IEEE, 2009, pp. 2442–2445.

[14] S. Hylamia, W. Yan, C. Rohner, and T. Voigt, "Tiek: Two-tier authentication and key distribution for wearable devices," in *2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*. IEEE, 2019, pp. 1–6.

[15] Y. Cao, Q. Zhang, F. Li, S. Yang, and Y. Wang, "Ppgpass: Nonintrusive and secure mobile two-factor authentication via wearables," in *IEEE INFOCOM 2020-IEEE Conference on Computer Communications*. IEEE, 2020, pp. 1917–1926.

[16] D. Yang, S. Maity, and S. Sen, "Physically secure wearable–wearable through-body interhuman body communication," *Frontiers in Electronics*, vol. 2, p. 807051, 2022.

[17] J. Wang, T. Fujiwara, T. Kato, and D. Anzai, "Wearable ecg based on impulse-radio-type human body communication," *IEEE Transactions on Biomedical Engineering*, vol. 63, no. 9, pp. 1887–1894, 2015.

[18] S. Maity, D. Das, and S. Sen, "Wearable health monitoring using capacitive voltage-mode human body communication," in *2017 39th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*. IEEE, 2017, pp. 1–4.

[19] Q. Huang, W. Alkhayer, M. E. Fouda, A. Celik, and A. M. Eltawil, "Wearable vital signal monitoring prototype based on capacitive body channel communication," in *2022 IEEE-EMBS International Conference on Wearable and Implantable Body Sensor Networks (BSN)*. IEEE, 2022, pp. 1–5.

[20] J. Sakuma, D. Anzai, and J. Wang, "Performance of human body communication-based wearable ecg with capacitive coupling electrodes," *Healthcare technology letters*, vol. 3, no. 3, pp. 222–225, 2016.

[21] N. Fahier, C.-J. Yang, and W.-C. Fang, "Wearable cardiovascular monitoring system design using human body communication," in *2021 IEEE International Symposium on Circuits and Systems (ISCAS)*. IEEE, 2021, pp. 1–5.

[22] K. Fujii, K. Ito, and S. Tajima, "Signal propagation of wearable computer using human body as transmission channel," in *Proc. of ISAP i*, vol. 2, 2002, pp. 512–515.

[23] Y. Nishida, K. Sasaki, K. Yamamoto, D. Muramatsu, and F. Koshiji, "Equivalent circuit model viewed from receiver side in human body communication," *IEEE Transactions on Biomedical Circuits and Systems*, vol. 13, no. 4, pp. 746–755, 2019.

[24] T. N. Xuan, D. Muramatsu, and K. Sasaki, "Measurement of human body communication transmission characteristics at 20 mhz," in *2015 9th International Symposium on Medical Information and Communication Technology (ISMICT)*. IEEE, 2015, pp. 45–48.

[25] J. Mao, H. Yang, and B. Zhao, "An investigation on ground electrodes of capacitive coupling human body communication," *IEEE transactions on biomedical circuits and systems*, vol. 11, no. 4, pp. 910–919, 2017.

[26] N. Arai, D. Muramatsu, and K. Sasaki, "Transmission model of human body communication incorporating size and distance between the two electrodes of a transmitter," in *2016 International Conference on Electronics Packaging (ICEP)*. IEEE, 2016, pp. 461–464.

[27] J. Bae and H.-J. Yoo, "The effects of electrode configuration on body channel communication based on analysis of vertical and horizontal electric dipoles," *IEEE Transactions on Microwave Theory and Techniques*, vol. 63, no. 4, pp. 1409–1420, 2015.

[28] W. Mongan, E. Anday, G. Dion, A. Fontecchio, K. Joyce, T. Kurzweg, Y. Liu, O. Montgomery, I. Rasheed, C. Sahin *et al.*, "A multi-disciplinary framework for continuous biomedical monitoring using low-power passive rfid-based wireless wearable sensors," in *2016 IEEE International Conference on Smart Computing (SMARTCOMP)*. IEEE, 2016, pp. 1–6.

[29] J. Dudak, G. Gaspar, and P. Tanuska, "Implementation of secure communication via the rf module for data acquisition," *Journal of Sensors*, vol. 2019, no. 1, p. 7810709, 2019.

[30] N. S. Aminuddin, M. H. Habaebi, S. H. Yusoff, and M. R. Islam, "Securing wireless communication using rf fingerprinting," in *2021 8th International Conference on Computer and Communication Engineering (ICCCE)*. IEEE, 2021, pp. 63–67.