2023 IEEE 66th International Midwest Symposium on Circuits and Systems (MWSCAS)
Phoenix, Arizona, USA, August 6-9, 2023

Invited: IoB: The Vision of the Internet of Bodies

Arunashish Datta, *Student Member, IEEE* and Shreyas Sen, *Senior Member, IEEE*
Elmore Family School of Electrical and Computer Engineering, Purdue University, West Lafayette, USA
E-mail: datta30@purdue.edu, shreyas@purdue.edu

2023 IEEE 66th International Midwest Symposium on Circuits and Systems (MWSCAS) | 979-8-3503-0210-3/23/$31.00 ©2023 IEEE | DOI: 10.1109/MWSCAS57524.2023.10405903

***Abstract*—Over six decades of semiconductor technology scaling (Moore's Law) and subsequently system size scaling (Bell's Law) has reduced the size of unit computing to virtually zero. This has led to computing becoming ubiquitous in everything around us, making everyday things smart. Similarly, tremendous progress in communication capacity (Shannon's theorem) has made these smart things connected to the internet and forming the Internet of Things (IoT). Many of these smart, connected devices are present in, on, or around the human body. This subset of IoT around the human body has a distinguishing feature, that it has a common medium, i.e. the body itself. This subset is increasingly becoming popular as the Internet of Bodies (IoB). In this paper, we look into the need and growth of IoB devices, including the technological landscape, current challenges and the future that IoB will enable for empowering humans.**

***Index Terms*—Internet of Bodies (IoB), Body Area Network (BAN), Ubiquitous Computing, Internet of Things (IoT)**

I. Introduction

Decades of scaling semiconductor technology [1], [2] has ushered in the age of ubiquitous computing (Fig. 1). Numerous day-to-day activities have been simplified, which have made humans dependent on such devices. These benefits have kept pushing the boundaries of what is possible using semiconductor technology. It is now possible to imagine a future where we no longer co-exist with these electronics and rather co-operate with electronic devices. This close collaboration between electronics and humans is the essence of Internet of Bodies or "IoB", as described in the IEEE Spectrum feature paper [3] on secure body networks and TEDx talk [4].

Internet of Bodies [4]–[11] is the confluence of miniaturized electronic devices in and around the human body communicating and sharing information between themselves to improve their performance. The recent boom in wearable and implantable devices around the body has created a network of devices which is commonly termed as Body Area Network (BAN). These BAN devices consist of various wearable devices that are nowadays commonplace like smartphones, smartwatches and smart glasses as well as implantable devices that are becoming more and more common like pacemakers and insulin pumps. Some of the devices carry multiple sensors which collect data from in and around the body, which can be further analyzed either locally or using a hub to connect to the internet to provide detailed results which can impact the day-to-day life of a person. Thus, this subset of Internet of Things consisting of devices which share a common medium which is the human body forms the Internet of Bodies. In summary,

This work was supported by the National Science Foundation Career Award under Grant CCSS 1944602

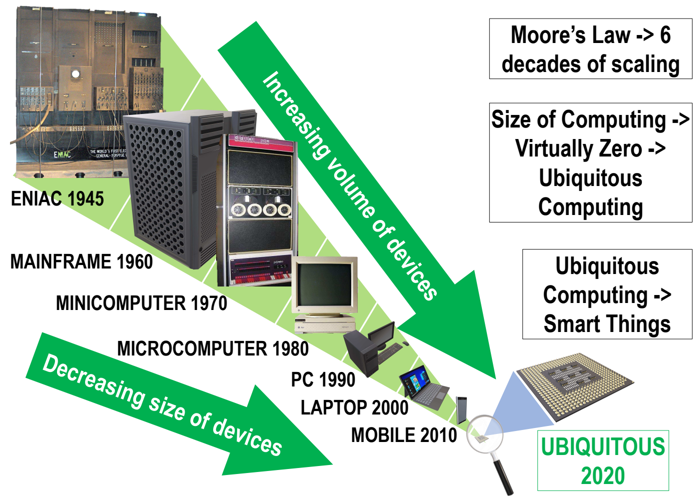

Fig. 1. Semiconductor technology scaling and subsequent miniaturization of devices leading to ubiquitous computing.

IoB is the confluence of *co-operating smart connected* electronics around humans to empower humans.

Internet of Bodies is changing our way of life with increased amount of information available to people assisting their daily activities. In terms of healthcare, it has ushered in the age of remote health monitoring, where critical data from the patient can now be analyzed by the doctors without the patient having to regularly visit the hospital. Wearable and implantable sensors has the potential to improve quality of life by ensuring that any anomalies in vital signals of the body are detected at the earliest and met with the appropriate response. In this study, we explore the future of IoB, focussing on the technological landscape that it promises in terms of computation and communication as well as the work to be done in this space to enhance its impact and enable the adoption of IoB at a large scale.

II. Internet of Bodies: What brought it upon us

A. IoB is not just BAN

Body Area Networks (BAN) as a concept has existed for over a decade which was derived from the existing Personal Area Network. Body Area Network is formed by the interconnected network of devices around the human body. IoB is an emerging concept which has been gaining popularity over the past five years primarily due to the shrinking size of computing thus making computing localized within a large set of wearable and implantable devices. This has resulted in the formation of a subset of Internet of Things where the devices

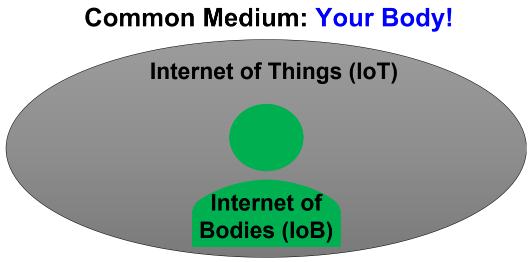

Fig. 2. Internet of Bodies (IoB) is a subset of IoT where devices share a common medium - the human body.

share a common medium, which is the human body (Fig. 2). IoB opens up a whole new world of possibilities where miniaturized devices around the body collaborate and assist in improving quality of life. *Is Wireless Local Area Network (WLAN) the same as IoT?* The answer is WLAN enabled IoT, but the impact of IoT is much bigger than WLAN, as it includes the 'things', the connectivity and data the flows through the connectivity to the algorithms and intelligence that is enabled on the collective data back to either real-time or non-real-time meaningful feedback and actuation, creating value that was not possible before. BAN enables IoB in the same way WLAN enabled IoT. However, IoB is much bigger than just BAN, as it spans from devices to algorithms, creating tangible value for empowering humans.

B. Growth of IoB Devices

We look at common consumer and healthcare devices (illustrated in Fig. 3) that are a vital part of IoB and their future directions in brief, with a focus on progressive miniaturization of devices while packing an increasing amount of functionality in these tiny nodes.

1) Consumer Electronics:

- **Large Form Factor:** These devices are either large wearables or portable devices. Because of their size, they can perform a huge number of applications and can be used as hubs to collect data from other wearables and then communicate to off body nodes. Devices like **smartphones** and **headphones** have already penetrated the market successfully and their applications keep increasing with time as more wearable devices come up working in symbiosis with the larger wearables.
  The introduction of **Augmented** and **Virtual Reality** can change the landscape of wearable hubs drastically over the next decade. **AR smart glasses** have the ability to change the way we interact with electronics by bringing the virtual world to the real world. Similarly, **VR headset** has changed gaming industry by bringing us physically to the virtual world. Further applications of AR and VR will drive the next generation of IoB devices.
- **Medium Form Factor:** These are more general purpose than the small form factor devices, while not being very bulky wearable devices. **Fitness trackers** and **smartwatches** have become mainstays in the IoB ecosystem. More than 200 million people have smartwatches currently. The popularity of smartwatches can be attributed

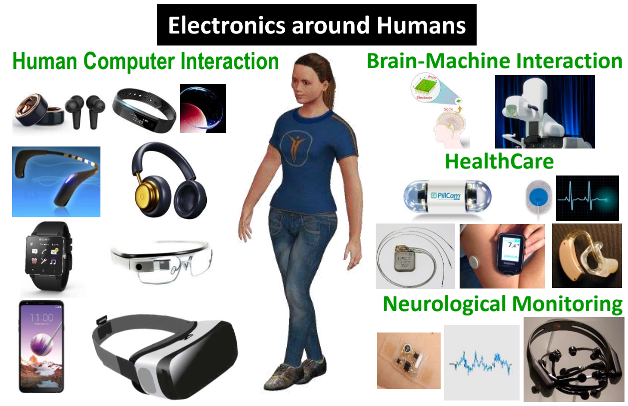

Fig. 3. Popular wearable devices in the commercial and healthcare space are illustrated.

to the multitude of tasks it can perform, the scale of which was previously only associated with smartphones. **Smart headband** has come up in the commercial space, but is still in its nascent stages in terms of its usage. It has potential applications in biopotential signal monitoring and fitness tracking.
- **Small Form Factor:** These devices are lightweight and typically have specialized functions. **Smart Rings** for fitness tracking, payment, and general applications like controlling music are becoming increasingly popular. **Earbuds** have exploded into the wearable market over the last decade due to their portability over traditional wireless headphones. AR based **Smart Contact Lenses** are being developed to revolutionize the way people connect with technology.

2) Medical Electronics for Healthcare:

- **Physiological Sensors:** Physiological sensors embedded in smartwatches, smart rings, and other smart devices have become commonplace. More and more sensors are being embedded in these devices with increasing accuracy. Sensors measuring ECG, EMG, EEG, Heart Rate, Glucose etc. are being embedded into wearable smart devices to continuously monitor fitness levels.
- **Implantable Medical Devices:** Pacemakers, ICD, insulin pumps, spinal cord stimulators, and vagus nerve stimulators are commonly used implantable devices that have

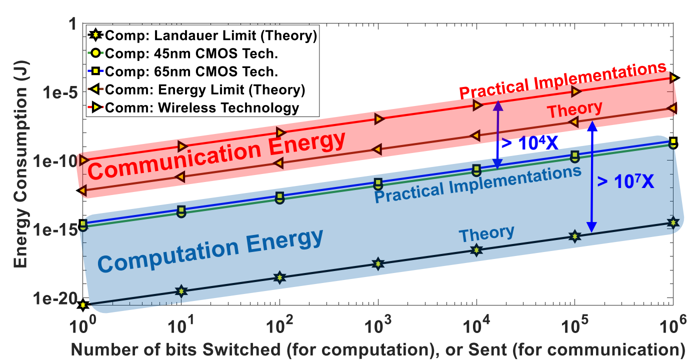

Fig. 4. High communication energy compared to computation is a major bottleneck in widespread adoption of IoB [11], [12].

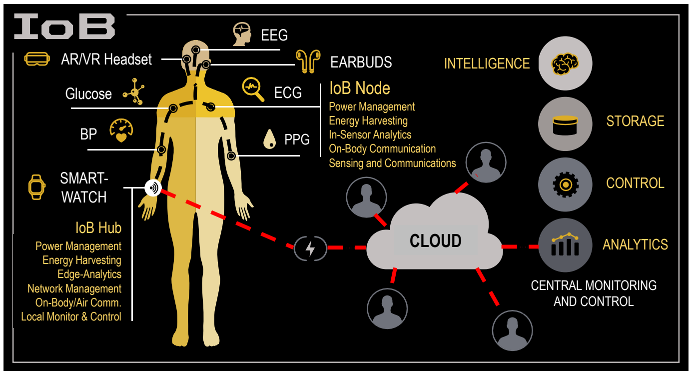

Fig. 5. Connected smart devices around body forming IoB [5].

been incorporated into IoB to employ connected healthcare. This has further enabled Remote Patient Monitoring, which is a boon for patients for whom traveling to and from a hospital is not always feasible.

- **Ingestible Device:** Ingestible medical devices is a technique which is being explored in research community due to the miniaturization of sensing equipment and cameras. Using ingestible sensors and systems has the potential to replace a lot of invasive procedures, making them more comfortable for the patient.

C. IoB Connectivity and Networks

The wearable nodes connected in, on and around the body are resource constrained. The resources on the edge nodes can be enough for in-sensor analytics, low power computation and communication of data around the body. However, as illustrated by Fig. 4, communication power is typically $3-4$ orders of magnitude higher power than computation [11], [12]. Off-body communication and extensive computation being high power consumption tasks are performed at the IoB Hub. The IoB hub can be devices with higher power consumption like smartphones or smartwatches, which enables edge-analytics and off-body communication for further analysis on the cloud. The complete IoB architecture is shown by Fig. 5.

III. Bottlenecks to Widespread Adoption

Internet of Bodies as a concept has not been around for a long time but has created a buzz in the landscape of development of next generation of miniaturized devices employing ubiquitous computing. However, there are various challenges facing its wide scale adoption and acceptance by the masses.

A critical issue for most miniaturized devices and any such upcoming device is to increase device operating life and ideally make it perpetually operable. However, these devices being size constrained, have a small battery and therefore require frequent charging. This is a major hindrance as using multiple devices around the body that need to be connected to a wall unit to charge frequently is a major distraction and very difficult to keep track of. A critical reason for this is that batteries haven't scaled as fast as semiconductor technology has managed to and thus energy storage is still playing catch up with the miniaturization of devices.

Another major problem facing IoB is data privacy. Data security has been a topic of extensive research for most technological innovations over the last decades. However, it is specially critical in case of the IoB ecosystem. This is because a large part of the data that is being stored, communicated and computed upon is extremely personal. Healthcare and neurological signal monitoring devices deal with information which can potentially lead to fatal consequences when in the wrong hands. Connected healthcare devices, despite the extremely private nature of data they store, analyze and communicate, have been shown to be specially lacking in terms of security. It was demonstrated in a series of conferences in $2011-2012$ by Barnaby Jack that connected medical devices could be hacked remotely with fatal consequences [3]. Even almost a decade after these demonstrations, United States Department of Homeland Security recalled models of connected implantable devices which had severe security risks while some of the devices were transmitting data without any encryption too [13]. Further, recorded speech and voice data as well as other biometrics stored also require a secure and trustworthy system for communication and storage.

IV. Technological Growth Accelerating IoB

Wearable devices have increased exponentially over the last decade (Fig. 6), which has prompted further research to solve the problems discussed in the last section to bridge the gap between the reality and the potential of IoB. Promising techniques that have been developed to mitigate the hindrances preventing widespread deployment of IoB are investigated.

A. Energy-Efficiency towards Perpetual Operation

1) Reduce Computation Power: The first method of reducing power consumption is to remove computation from size and resource constrained edge nodes. This will enable the devices to sense data and communicate to the hub for communication. However, this strategy further depends on a low-power communication methodology.

2) In-Sensor Computing: As shown by Fig. 4, communication power has been a major bottleneck in reducing power consumption of devices. Computation power is typically $3-4$ orders of magnitude less than communication power [11], [12]. More computation to communicate lesser data has been one of the strategies to lower overall power consumption of devices. Intelligent sensing can be performed to remove redundant data that need not be communicated. Further, in-sensor analytics can be performed at the edge nodes to reduce the data to be communicated to the hub for further processing. Lightweight analysis using TinyML [14] has been used to bring data analysis to microcontrollers at the edge nodes.

3) Reduce Communication Power: Reduction of communication power in an attempt to reduce overall power consumption of a device is of paramount importance. Methodologies efficient for communication in BAN devices have been investigated, and the attempt is to increase energy efficiency of communication to perform $\leq 1pJ/bit$ communication to bridge the communication-computation energy gap.

Human Body Communication (HBC) [15]–[19] an exciting alternative to traditional RF based communication protocols, which uses the conductive properties of the tissues to transmit data through the body to a wearable/implantable device, has been demonstrated for energy efficiencies of less than $10pJ/bit$ [20]–[25]. Traditional RF based protocols have high energy efficiency ($> 1nJ/bit$) due to the electromagnetic radiation around the room. HBC for BAN devices, in conjunction with RF protocols like Bluetooth, LoRa and ZigBee for long range communication, has the potential to extend device lifetimes by orders of magnitude over the current state-of-the-art communication methodologies for BAN devices [26]–[28].

4) Wireless Powering: Another thrust towards perpetual operation of IoB devices is the research in wireless powering methodologies. Promising technologies include RF based long range powering, where a power transmitter uses phased array antennas to locate and deliver power to wearable devices. Human Body Powering has been proposed where power is transferred through the body to a miniaturized IoB device. However, current wireless powering methodologies can reliably transfer $100s$ of μW in indoor environments, powering some low-power sensors. This is mainly because of high loss from shadowing due to the body, as well as obstacles in the surroundings impeding power delivery. Safe power delivery has also been a challenge, with RF beams potentially crossing the safety limits for power density around the body setup by the Federal Communications Commissions (FCC). However, with more innovative methods to deliver power wirelessly and reducing power consumption of IoB nodes, the prospect of perpetually operating IoB devices all around us may happen in the near future.

B. Security, Safety and Trust

Data collected by IoB devices is more personal than ever as physiological sensors, fitness trackers and implantable medical devices are increasing in popularity. The security of data in IoB devices is being studied extensively to mitigate potential threats in these resource constrained nodes.

1) Security Research for Resource Constrained Nodes: Considerable enhancements in security standards and encryption have been developed for low power devices over the last few decades. Lightweight ciphers (e.g. SIMON, PRESENT) working with Wireless BAN devices have been investigated. Recent research on low power countermeasures [29], [30] have increased resilience against physical attacks against encryption. Hardware security primitives, and hardware as a root of trust such as Physically Unclonable Functions (PUF), True Random Number Generators (TRNG) and secure enclave, are becoming popular. Finally, privacy preserving encryption (e.g. homomorphic encryption) is heavily being looked into.

2) Physical Layer Security: Physically securing data prevents data from landing into wrong hands. Human Body Communication has been shown to be much more secure than its RF counterparts [31]–[35]. RF-PUF (Physically Unclonable Function) [36] has been proposed, which is artificial intelligence based technique for real-time authentication of wireless nodes using their inherent process specific properties. RF based authentication has also been used in RF-PSF (Process Specific Functions) [37] to exploit process-specific inherent properties to differentiate process technologies.

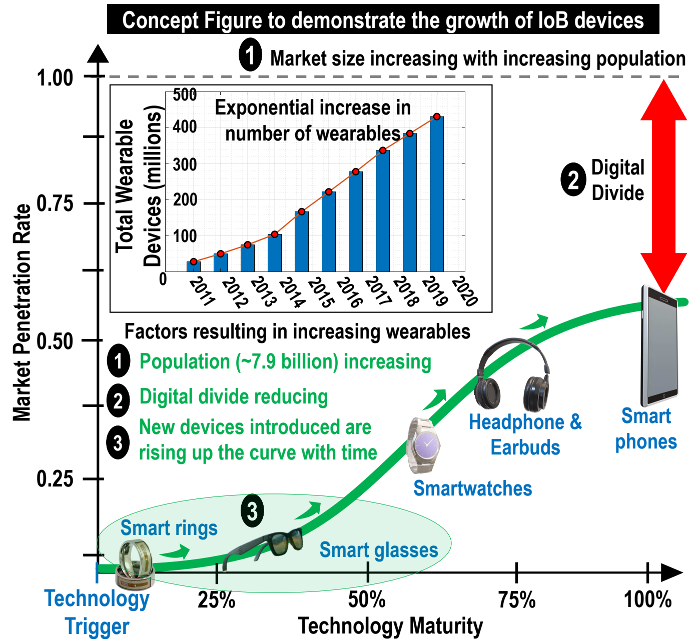

Fig. 6. Growth of wearable devices fueling the rise of IoB.

V. The Vision of IoB

IoB in its current form comprises primarily of a few self-contained power hungry devices (smartphones, smartwatches, biosensors), each with its own CPU, connected using energy inefficient wireless communication. However, in the foreseeable future, a combination of miniaturization, increase in compute efficiency in the nodes, ultra-low power body communication forming distributed on-body networks, distribution and aggregation of computation on the hub promises the design of multi-node distributed networks enabling a variety of electronics closely cooperating with humans, leading to the development of newer forms of Human-Computer Interaction (HCI) which will help the interaction with IoB devices. The vision for Internet of Bodies is to take us from the current form of Human-Electronics co-existence to Human-Electronics co-operation and further lead to Human-Electronics and Human-AI symbiosis in a paradigm where the body and surrounding electronics assist each other in achieving their goals.

VI. Conclusion

We study the changing technological landscape due to the advent of Internet of Bodies (IoB). The potential of IoB is discussed and the research being done for wide scale adoption of IoB is investigated.

Acknowledgment

The authors would like to acknowledge the support of Center of Internet of Bodies (C-IoB) and thank Professor Baibhab Chatterjee, Department of ECE at University of Florida, members of Sparclab, and collaborators from C-IoB at Purdue University for their immense cooperation and support.

REFERENCES

[1] G. E. Moore, "Cramming more components onto integrated circuits, reprinted from electronics, volume 38, number 8, april 19, 1965, pp. 114 ff." *IEEE Solid-State Circuits Society Newsletter*, vol. 11, no. 3, pp. 33–35, 2006.

[2] R. Dennard, F. Gaensslen, H.-N. Yu, V. Rideout, E. Bassous, and A. LeBlanc, "Design of ion-implanted mosfet's with very small physical dimensions," *IEEE Journal of Solid-State Circuits*, vol. 9, no. 5, pp. 256–268, 1974.

[3] S. Sen, S. Maity, and D. Das, "The body is the network: To safeguard sensitive data, turn flesh and tissue into a secure wireless channel," *IEEE Spectrum*, vol. 57, no. 12, pp. 44–49, 2020.

[4] Shreyas Sen. (2019) How your body will play an integral role in the future of wearable security. [Online]. Available: https://www.ted.com/talks/shreyas_sen_how_your_body_will_play_an _integral_role_in_the_future_of_wearable_security

[5] Purdue University. (2019) Center for Internet of Bodies. [Online]. Available: https://engineering.purdue.edu/C-IoB

[6] S. Maity, D. Das, X. Jiang, and S. Sen, "Secure human-internet using dynamic human body communication," in *2017 IEEE/ACM International Symposium on Low Power Electronics and Design (ISLPED)*. IEEE, 2017, pp. 1–6.

[7] Rand Corporation. (2022) Internet of Bodies: Our Connected Future. [Online]. Available: https://www.rand.org/about/nextgen/art-plus-data/giorgia-lupi/internet-of-bodies-our-connected-future.html

[8] M. Lee, B. Boudreaux, R. Chaturvedi, S. Romanosky, and B. Downing, *The internet of bodies: Opportunities, risks, and governance*. Rand Corporation, 2020.

[9] Rand Corporation. (2020) Internet of Bodies: Our Connected Future. [Online]. Available: https://www.rand.org/about/nextgen/art-plus-data/giorgia-lupi/internet-of-bodies-our-connected-future.html

[10] Forbes. (2019) What Is The Internet Of Bodies? And How Is It Changing Our World? [Online]. Available: https://www.forbes.com/sites/bernardmarr/2019/12/06/what-is-the-internet-of-bodies-and-how-is-it-changing-our-world/?sh=269b998968b7

[11] B. Chatterjee, P. Mohseni, and S. Sen, "Bioelectronic sensor nodes for the internet of bodies," *Annual Review of Biomedical Engineering*, vol. 25, no. 1, p. null, 2023, pMID: 36913705. [Online]. Available: https://doi.org/10.1146/annurev-bioeng-110220-112448

[12] S. Sen, "Context-aware energy-efficient communication for iot sensor nodes," in *Proceedings of the 53rd Annual Design Automation Conference*, 2016, pp. 1–6.

[13] US FDA. (2019) Certain Medtronic MiniMed Insulin Pumps Have Potential Cybersecurity Risks: FDA Safety Communication. [Online]. Available: https://www.fda.gov/medical-devices/safety-communications/ certain-medtronic-minimed-insulin-pumps-have-potential-cybersecurity -risks-fda-safety-communication

[14] tinyML Foundation. (2023) Community for ultra-low power machine learning at the edge. [Online]. Available: https://www.tinyml.org/

[15] S. Maity, M. He, M. Nath, D. Das, B. Chatterjee, and S. Sen, "Bio-physical modeling, characterization, and optimization of electro-quasistatic human body communication," *IEEE Transactions on Biomedical Engineering*, vol. 66, no. 6, pp. 1791–1802, 2018.

[16] A. Datta, M. Nath, D. Yang, and S. Sen, "Advanced biophysical model to capture channel variability for EQS capacitive HBC," *IEEE Transactions on Biomedical Engineering*, 2021.

[17] N. Modak, M. Nath, B. Chatterjee, S. Maity, and S. Sen, "Bio-physical modeling of galvanic human body communication in electro-quasistatic regime," *bioRxiv*, 2020.

[18] S. Maity et al., "On the safety of human body communication," *IEEE Transactions on Biomedical Engineering*, pp. 1–1, 2020.

[19] A. Datta, M. Nath, B. Chatterjee, N. Modak, and S. Sen, "Channel modeling for physically secure electro-quasistatic in-body to out-of-body communication with galvanic tx and multimodal rx," in *2021 IEEE MTT-S International Microwave Symposium (IMS)*. IEEE, 2021, pp. 116–119.

[20] S. Maity *et al.*, "Bodywire: A 6.3-pj/b 30-mb/s -30-db SIR-tolerant broadband interference-robust human body communication transceiver using time domain interference rejection," *IEEE Journal of Solid-State Circuits*, vol. 54, no. 10, pp. 2892–2906, Oct 2019.

[21] S. Maity, N. Modak, D. Yang, S. Avlani, M. Nath, J. Danial, D. Das, P. Mehrotra, and S. Sen, "A 415 nw physically and mathematically secure electro-quasistatic hbc node in 65nm cmos for authentication and medical applications," in *2020 IEEE Custom Integrated Circuits Conference (CICC)*. IEEE, 2020, pp. 1–4.

[22] S. Maity, N. Modak, D. Yang, M. Nath, S. Avlani, D. Das, J. Danial, P. Mehrotra, and S. Sen, "Sub-μwrcomm: 415-nw 1-10-kb/s physically and mathematically secure electro-quasi-static hbc node for authentication and medical applications," *IEEE Journal of Solid-State Circuits*, 2021.

[23] N. Modak, D. Das, M. Nath, B. Chatterjee, G. K. K, S. Maity, and S. Sen, "Eqs res-hbc: A 65-nm electro-quasistatic resonant 5–240 w human whole-body powering and 2.19 w communication soc with automatic maximum resonant power tracking," *IEEE Journal of Solid-State Circuits*, vol. 57, no. 3, pp. 831–844, 2022.

[24] B. Chatterjee, G. K. K, M. Nath, S. Xiao, N. Modak, D. Das, J. Krishna, and S. Sen, "A 1.15w 5.54mm3 implant with a bidirectional neural sensor and stimulator soc utilizing bi-phasic quasi-static brain communication achieving 6kbps-10mbps uplink with compressive sensing and ro-puf based collision avoidance," in *2021 Symposium on VLSI Circuits*, 2021, pp. 1–2.

[25] B. Chatterjee, A. Datta, M. Nath, G. K. K, N. Modak, and S. Sen, "A 65nm 63.3µw 15mbps transceiver with switched-capacitor adiabatic signaling and combinatorial-pulse-position modulation for body-worn video-sensing ar nodes," in *2022 IEEE International Solid- State Circuits Conference (ISSCC)*, vol. 65, 2022, pp. 276–278.

[26] B. Chatterjee, N. Cao, A. Raychowdhury, and S. Sen, "Context-aware intelligence in resource-constrained iot nodes: Opportunities and challenges," *IEEE Design & Test*, vol. 36, no. 2, pp. 7–40, 2019.

[27] B. Chatterjee, D.-H. Seo, S. Chakraborty, S. Avlani, X. Jiang, H. Zhang, M. Abdallah, N. Raghunathan, C. Mousoulis, A. Shakouri *et al.*, "Context-aware collaborative intelligence with spatio-temporal in-sensor-analytics for efficient communication in a large-area iot testbed," *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6800–6814, 2020.

[28] N. Cao, B. Chatterjee, M. Gong, M. Chang, S. Sen, and A. Raychowdhury, "A 65nm image processing soc supporting multiple dnn models and real-time computation-communication trade-off via actor-critical neuro-controller," in *2020 IEEE Symposium on VLSI Circuits*, 2020, pp. 1–2.

[29] D. Das, M. Nath, B. Chatterjee, S. Ghosh, and S. Sen, "Stellar: A generic em side-channel attack protection through ground-up root-cause analysis," in *2019 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. IEEE, 2019, pp. 11–20.

[30] A. Ghosh, D. Das, J. Danial, V. De, S. Ghosh, and S. Sen, "Syn-stellar: An em/power sca-resilient aes-256 with synthesis-friendly signature attenuation," *IEEE Journal of Solid-State Circuits*, vol. 57, no. 1, pp. 167–181, 2021.

[31] D. Yang, S. Maity, and S. Sen, "Physically secure wearable–wearable through-body interhuman body communication," *Frontiers in Electronics*, vol. 2, p. 29, 2022.

[32] S. Maity, D. Yang, S. S. Redford, D. Das, B. Chatterjee, and S. Sen, "Bodywire-hci: Enabling new interaction modalities by communicating strictly during touch using electro-quasistatic human body communication," *ACM Trans. Comput.-Hum. Interact.*, vol. 27, no. 6, nov 2020. [Online]. Available: https://doi.org/10.1145/3406238

[33] D. Das et al., "Enabling covert body area network using electro-quasistatic human body communication," *Scientific Reports*, vol. 9, no. 1, Mar 2019. [Online]. Available: http://par.nsf.gov/biblio/10153369

[34] M. Nath, S. Maity, S. Avlani, S. Weigand, and S. Sen, "Inter-body coupling in electro-quasistatic human body communication: Theory and analysis of security and interference properties," *Scientific Reports*, vol. 11, no. 1, pp. 1–15, 2021.

[35] A. Datta and S. Sen, "Physically-secure low-power human state measurement using eqs-hbc and edge-analytics : Invited paper," in *2021 IEEE Research and Applications of Photonics in Defense Conference (RAPID)*, 2021, pp. 1–2.

[36] B. Chatterjee, D. Das, S. Maity, and S. Sen, "Rf-puf: Enhancing iot security through authentication of wireless nodes using in-situ machine learning," *IEEE internet of things journal*, vol. 6, no. 1, pp. 388–398, 2018.

[37] M. F. Bari, B. Chatterjee, L. Duncan, and S. Sen, "RF-PSF: Zero-Trust Radio Frequency Process Specific Functions as Process Distinction Method," in *2022 IEEE/MTT-S International Microwave Symposium-IMS 2022*. IEEE, 2022, pp. 599–602.