International Journal of Environmental and Ecology Research
www.environmentaljournal.in
Online ISSN: 2664-7117
Received: 21-01-2026, Accepted: 20-02-2026, Published: 07-03-2026
Volume 8, Issue 1, 2026, Page No. 45-50

A low power event driven VLSI architecture for autonomous environmental monitoring in remote riverine environments of Sri Lanka

Wasantha Samarathunga[1*], Risindu Ransen[2], Dr. Q. Li[3]
[1] Department of Electrical and Electronics Engineering, National Institute of Technology Kisarazu College, Chiba, Japan
[2] Thurstan College Colombo, Sri Lanka
[3] Electronics Consultant, Colombo, Sri Lanka
Corresponding Author: Wasantha Samarathunga

Abstract
Autonomous monitoring in remote riverine regions of Sri Lanka require systems that can operate for long periods without human presence or stable infrastructure. This research work presents a low power VLSI architecture designed for such conditions through a combination of multimodal sensing, event driven processing and hardware security. The front-end sensors capture vibration, acoustic, turbidity and passive infrared signatures that reveal different forms of environmental disturbance. These signals trigger an event driven processing core that performs threshold detection, lightweight feature extraction and simple on chip classification while keeping energy use to a minimum. Tamper resistance framework layer protects both the device and its data through enclosure penetration detection, intrusion sensing and secure boot. Solar based power management and multiple communication pathways support operation in locations where connectivity and maintenance access are limited. The architecture responds directly to the realities of difficult terrain, scarce manpower and the frequent destruction of deployed equipment. It provides a practical foundation for prototype development, laboratory evaluation and eventual field deployment in challenging riverine environments. This work represents the initial system-level phase of an ongoing research and development effort.

Keywords: Illegal sand mining in Sri Lanka, vlsi architecture, autonomous monitoring, multimodal sensing, tamper resistance, low power design

Introduction

Monitoring environmental disturbances in remote riverine environments of Sri Lanka often demands the use of monitoring technologies that can operate independently without the need for human intervention. Traditional methods of monitoring, such as the use of patrol teams, drones, and stationary CCTV cameras, have been found to be inadequate in such environments because they often require uninterrupted power supply, favorable weather conditions, and regular maintenance. Studies have shown that environmental disturbances, such as the carrying out of illegal extraction activities, often occur in environments where the deployment of manpower is not feasible and where equipment is often vandalized and removed [Perera, 2019; Fernando, 2020] [3, 11].

A hardware centered strategy offers a more dependable alternative. A VLSI based architecture provides predictable performance, low leakage operation and the ability to embed security mechanisms directly into the silicon. It also supports event driven behavior, allowing the system to remain dormant until meaningful activity is detected, which is essential for long term operation in power constrained environments [Ottoni *et al*. 2014; Rabaey *et al*. 2010] [19, 20]. By integrating sensing, computation and communication into a compact and energy efficient platform, architecture responds directly to the environmental and logistical constraints of long-term monitoring in remote riverbank environments.

A hardware centered strategy is taken here for a more dependable alternative. A VLSI based architecture provides predictable performance, low leakage operation and the ability to embed security mechanisms directly into the silicon. It also supports event driven behavior, allowing the system to remain dormant until meaningful activity is detected, which is essential for long term operation in power constrained environments [Ottoni *et al*. 2014; Rabaey *et al*. 2010] [19, 20]. By integrating sensing, computation and communication into a compact and energy efficient platform, architecture responds directly to the environmental and logistical constraints of long-term monitoring in remote riverbank environments of Sri Lanka.

This work presents a system-level VLSI architecture that is currently in the developmental phase. The focus is on design motivations, subsystem integration, and architectural feasibility. Detailed circuit-level implementation and silicon validation will follow in the next stage of development.

Background and Motivation

Remote riverine environments of Sri Lanka present a set of challenges that make continuous monitoring difficult to sustain. These areas known for lack of stable power sources, reliable communication coverage and safe access routes. High humidity, seasonal flooding and dense vegetation further complicate the use of conventional surveillance tools in the riverine areas. Studies on illegal resource extraction describe how many operations take place at night, in inaccessible terrain and in locations where equipment is frequently damaged or removed [Gunasekara 2018; Jayawardena 2020] [4, 6]. These conditions create a setting where human presence is limited and where deployed devices are exposed to both environmental stress and deliberate interference.

A monitoring system intended for such regions must therefore operate autonomously, tolerate harsh environmental conditions and protect its data even when physically compromised. A VLSI based solution aligns well with these requirements because it allows sensing, processing and security functions to be tightly integrated within a low power hardware platform. Event driven operation is preferring here due to reduces energy consumption by allowing the system to remain dormant until meaningful activity is detected.

This is a strategy that supports long term deployment in power constrained environments cited in [Rabaey *et al*. 2010 and Chen, Li *et al*. 2021] [1, 20]. These design motivations also reflect broader concerns about sustainable river management and the need for reliable monitoring tools in regions affected by illegal extraction and ecological degradation [UNEP 2020; Ministry of Environment 2022] [6, 9].

System Architecture

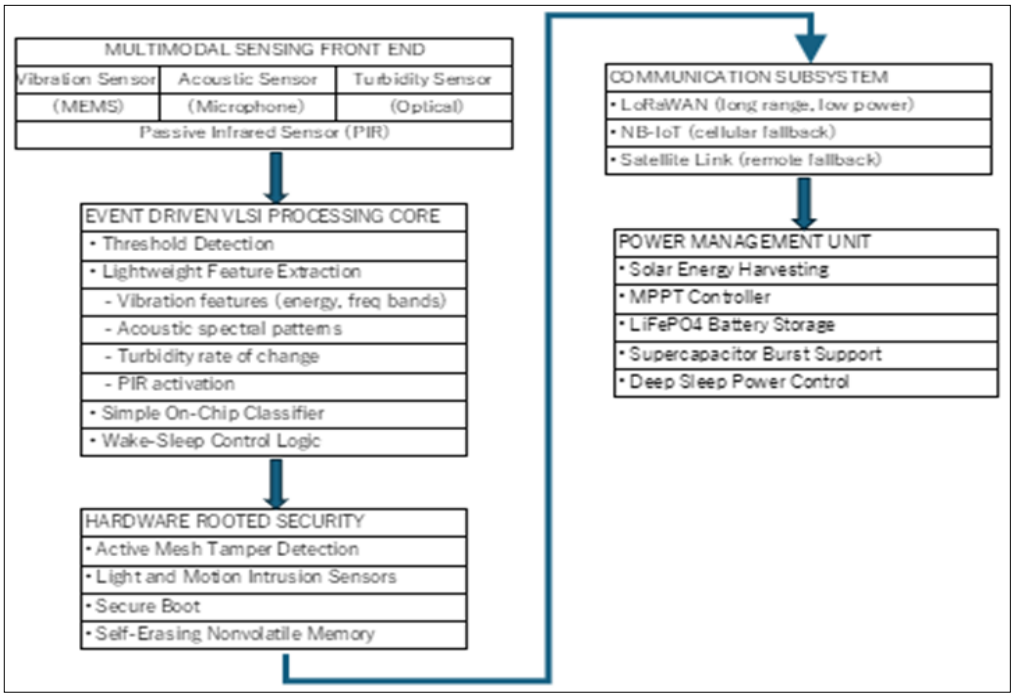

Fig 1: System-level architecture of the proposed monitoring platform

The figure1 outlines the flow from multimodal sensing to event driven processing, hardware rooted security, hybrid communication and power management, showing how the subsystems integrate into a unified low power design

Table 1: Subsystem roles and design constraints

Subsystem	Primary Role	Key Constraints Shaping the Design
Multimodal Sensing Front End	Captures vibration, acoustic, turbidity and PIR signatures that reflect different forms of environmental disturbance.	Signals are often weak, noisy or distorted by weather, terrain and human activity. Sensors must remain low power and reliable under humidity, flooding and vegetation cover.
Event Driven VLSI Processing Core	Performs threshold detection, lightweight feature extraction and simple on chip classification during short wake cycles.	Must remain dormant most of the time to conserve energy. Processing must be efficient enough to run within tight power budgets and short activation windows.
Hardware Rooted Security Layer	Protects the device and its data through tamper detection, intrusion sensing, secure boot and rapid data invalidation.	Devices may be discovered, handled or destroyed. Security must function even under physical access and must not rely on continuous connectivity or software level defenses.
Communication Subsystem	Transmits alerts through LoRaWAN, NB IoT or satellite links depending on availability.	Connectivity is inconsistent and infrastructure may be absent. Communication must be energy efficient and adaptable to changing signal conditions.
Power Management Unit	Harvests solar energy, manages storage and supports deep sleep operation for long term autonomy.	Sunlight is inconsistent and maintenance visits are rare. Power storage must be resilient, and energy use must remain tightly controlled.

Table1 summarizes the purpose of each subsystem and the environmental or operational constraints that shaped its design.

1. Multimodal Sensing Front End

The sensing subsystem brings together four complementary modalities that capture different physical signatures of activity along a riverbank. MEMS vibration sensors are used to detect ground movement produced by footsteps, vehicles or excavation machinery. Acoustic microphones are used here to capture the sound patterns associated with engines, metal tools and other mechanical disturbances. Turbidity sensors also needed to track on changes of clarity the water experiences when sediment is stirred up during an event of excavation. Passive infrared sensors can pick up the subtle shifts in human body heat that reveal when a person is

nearby. The proposed should only detects human patterns. PIR sensors known to react changes in infrared radiation. So, they cannot identify humans on their own. To keep the system focused on human activity, the PIR output is filtered using simple timing and amplitude checks together with vibration and acoustic cues. This combination reduces false triggers from animals and other warm objects.

Each modality brings a different point of view on the same event, which makes the reliability of the detection and the absence of false alarms more assured. This idea is in accordance with the well-known fact that the fusion of multiple senses is a more accurate way of detecting events in the environment by combining different data flows into a more coherent picture [Hall and Llinas 1997; Khaleghi *et al*. 2013] [25, 26]. In riverine environments where noise, weather and terrain can distort individual signals, a multimodal approach provides a more stable and trustworthy foundation for event detection.

2. Event Driven VLSI Processing Core

The core of the processing is centered around an event-driven philosophy that enables the system to conserve energy while still being sensitive to activity in its environment. By default, the architecture is designed to be in a low power sleep mode, drawing just enough current to monitor sensor thresholds. When any sensing modality detects activity that exceeds its predefined threshold, the VLSI core wakes and begins a short burst of computation. This behavior reflects long established principles in low power design, where dynamic activation and selective processing significantly extend operational lifetime in constrained environments [Benini and De Micheli 1998; Rabaey *et al*. 2010] [18, 20].

Once activated, the core performs lightweight feature extraction tailored to the characteristics of each sensor. Vibration signals are reduced to measures such as energy or dominant frequency bands. Acoustic inputs are processed into simple spectral patterns that distinguish machinery noise from background sound. Turbidity changes are summarized as rate of variation rather than continuous raw values. These compact features support local decision making without requiring complex algorithms or high computational load. The approach aligns with event driven architectures developed for sensor processing, where short, efficient computation cycles replace continuous sampling and analysis [Ottoni *et al*. 2014] [19].

The extracted features feed into a simple on chip classifier that determines whether the detected activity warrants communication or logging. By keeping classification local and lightweight, the system could avoid the need for data transmission, that feature is a deployment requirement on energy-intensive operation during working with remote data. It is this balance of responsiveness and restraint that allows architecture to operate for long periods of time in environments where power is scarce.

The classifier is implemented as a small rule-based model or a linear threshold unit. These models run with very little switching activity and do not need multipliers or large memory blocks. They are well suited for short wake periods and tight power budgets, and they can be replaced with a compact machine learning model in future revisions if energy margins allow it.

3. Hardware Rooted Security

Security in remote riverine environments of Sri Lanka must begin at the hardware level because devices placed in the field face both environmental stress and deliberate interference. The architecture therefore incorporates several layers of physical and logical protection that work together to safeguard the system even when an attacker has direct access to the device. Active mesh circuits detect enclosure penetration by monitoring disruptions in conductive patterns, a technique widely recognized in tamper resistant hardware design [Skorobogatov 2011] [21]. Light and motion sensors provide an additional layer of intrusion awareness by identifying unauthorized opening, displacement or exposure to unexpected illumination, which are common indicators of tampering attempts [Kuhn 2004] [22].

Secure boot should be used to ensures that only authorized firmware runs on the system. This prevents an adversary from replacing system firmware with unauthorized firmware. Secure boot ensures the integrity of the sensing and communication pipeline. Self erasing nonvolatile memory is used to store sensitive configuration data so that critical information is automatically cleared if tampering is detected. This approach aligns with broader strategies in tamper resistant system design, where rapid data invalidation is used to prevent extraction of keys or configuration parameters [Yuce *et al*. 2019] [24].

These mechanisms create a hardware rooted security framework that does not rely solely on software level defenses. In environments where devices may be discovered, handled or destroyed, this layered approach provides a practical and resilient foundation for protecting both the system and the data it collects.

4. Communication Architecture

Proposed communication subsystem is designed to operate reliably in Sri Lankan riverine regions. In these areas' connectivity is often known to be inconsistent and infrastructure are poor. To address this challenge, the architecture supports three complementary communication pathways. LoRaWAN provides long range, low power transmission that is well suited for rural and semi isolated environments. Its ability to cover large distances with minimal energy makes it a practical choice for riverbank deployments where gateways may be far apart [Centenaro *et al*. 2016] [28]. NB IoT has to be added as a second option when cellular coverage is available. It provides deeper penetration and connectivity through existing mobile networks, which may be advantageous especially when there is partial but not continuous coverage.

For the most remote sites, satellite communication serves as a fallback option. Although it consumes more energy than terrestrial links, it ensures that critical alerts can still be transmitted when no other network is reachable. This is because the use of multiple protocols will help in reducing the probability of communication failure by enabling the system to use the most reliable channel at any particular time. This is also in conformity with the general trend in the use of environmental IoT, where hybrid communication is used to ensure communication in diverse terrains, as discussed in [Al-Fuqaha *et al*. 2015] [29].

5. Power Management

The power subsystem is designed to support long term operation in environments where sunlight is inconsistent and maintenance visits are rare. Solar power is the main power candidate of proposed system while secondary source with less environmentally impact is preferred. The maximum power point tracking controller is also embedded to ensure

that the solar panel always operates at its best efficiency despite the changes in the amount of sunlight. MPPT unit uses a standard perturb and observe or incremental conductance method to adjust the operating point of the solar panel. These methods regulate the duty cycle of the DC to DC converter and do not require any mechanical tracking hardware. This approach is common in low power embedded systems because it is simple, stable and efficient. The energy collected from the solar panel should be stored in LiFePO4 batteries. These batteries guarantee a reliable performance and better safety compared to other types of batteries currently. But with option of replace-ability here. The supercapacitors play a crucial role in providing short bursts of current during wake-up and communication cycles without overloading the storage component.

Low power design principles guide the system's operation at every stage. The architecture relies on deep sleep states that draw only minimal current while maintaining threshold monitoring. Event driven activation ensures that the system becomes fully active only when meaningful activity is detected, which significantly reduces overall energy consumption [Rabaey *et al*. 2010] [20]. This is consistent with other strategies that are employed during long-term IoT deployments, where energy harvesting is considered crucial for devices that will be located in remote environments [Khan and Lee 2021] [8].

This is achieved through efficient harvesting, storage, and power usage, which enables the subsystem to function continuously in Sri Lanka's riverine environments where power availability cannot be guaranteed. This provides the basis for the continuous operation of the monitoring platform for long periods of time without the need for human intervention.

Environmental Deployment Considerations

The installation of monitoring systems within riverine regions demands that due consideration be given to physical and human factors that affect system performance. In riverine regions, high humidity and seasonal flooding are prevalent, and these factors can affect system performance. In one study on riverine regions used for extraction operations, it has been noted that environmental pressures continually damage or disable equipment that is not designed for such regions [Herath 2017; Ratnayake 2016] [5, 13].

Human activity adds Further layer of complexity. Devices that placed in visible or predictable locations may be discovered, tampered with or removed soon after installation. Prior studies indicate reports on illegal extraction note that equipment deployed for monitoring is often targeted or destroyed, especially when it interferes with ongoing operations [Gunasekara 2018; Karunaratne 2018] [4, 7]. Therefore, the system must balance concealment with effective sensing. Sensors must be positioned where they can capture meaningful signals without drawing attention and the device must be able to detect and respond to interference when it occurs.

Limited accessibility further shapes deployment decisions. Many deployment spots along the riverbank are tough to reach, particularly during rainy seasons or when the water runs high. This restricts opportunities for maintenance and makes long term autonomy essential. Power systems, communication pathways and security mechanisms expected to operate with reliably for long periods without intervention. These constraints reinforce the need for a robust, low power and tamper aware architecture that can withstand both environmental stress and deliberate disruption.

Design Insights

Several insights emerge from the system design process, each shaped by the environmental and operational realities of remote Sri Lanka riverine monitoring. First of that is the value of multimodal sensing. By combining vibration, acoustic, turbidity and passive infrared inputs, the system reduces false positives and builds a more reliable picture of activity along the riverbank. This principle is well supported in multisensor fusion research, which shows that independent data streams strengthen overall detection accuracy [Hall and Llinas 1997; Khaleghi *et al*. 2013] [25, 26].

A second insight is the importance of event driven processing. Continuous sampling drains energy quickly in remote deployments, but threshold-based activation allows the system to remain dormant until meaningful activity occurs. This approach aligns with long established low power design strategies that emphasize selective computation and dynamic power management [Benini and De Micheli 1998; Rabaey *et al*. 2010] [18, 20]. By limiting processing to short, purposeful bursts, the architecture extends operational lifetime and reduces the need for maintenance visits.

A third insight concerns tamper resistance. Field reports describe how monitoring equipment is often damaged, removed or deliberately interfered with in areas affected by illegal extraction [Gunasekara 2018; Karunaratne 2018] [4, 7]. This makes hardware rooted security essential rather than optional. Active mesh circuits, intrusion sensors and secure boot mechanisms create a layered defense that protects both the device and its data, reflecting best practices in tamper resistant hardware design [Skorobogatov 2011; Yuce *et al*. 2019] [21, 24].

A fourth insight relates to communication. No single communication pathway is reliable across all riverine environments. LoRaWAN, NB IoT and satellite links each offer strengths and limitations and a hybrid approach ensures that alerts can be transmitted even when infrastructure is inconsistent or partially unavailable as shown by [Centenaro *et al*. 2016; Al-Fuqaha *et al*. 2015] [28].

Finally, environmental constraints must be addressed from the earliest stages of design. High humidity, flooding, shifting terrain and human interference all influence enclosure design, sensor placement and power budgeting. These conditions reinforce the need for a system that is fault tolerant, energy efficient and capable of functioning autonomously for long periods [Herath 2017; Ratnayake 2016] [5, 13].

Expected Outcomes

The design phase produces several concrete outcomes that prepare the system for laboratory evaluation and actual field deployment. The first result is the creation of a unified system level blueprint that incorporates sensing, processing, communication, power and security into an architecture. This blueprint provides an understanding of how each of these systems will interact with the other systems, as well as ensuring that these systems are designed in an appropriate fashion for the remote Sri Lankan riverine environment.

A second outcome is a set of subsystem specifications that guide hardware selection. These specifications define sensing thresholds, feature extraction requirements, communication parameters and power budgets. They also outline the tamper resistance framework, which includes active mesh circuits, intrusion sensing and secure boot mechanisms informed by established practices in tamper resistant hardware design [Skorobogatov 2011; Yuce *et al*. 2019] [21, 24].

A third outcome is a set of assumptions for prototype validation. These assumptions identify the environmental conditions, activity patterns and power availability scenarios that the system must withstand. They also define the metrics that will be used to evaluate performance, such as wake up latency, feature extraction efficiency and the responsiveness of tamper detection circuitry. These metrics reflect priorities emphasized in low power and event driven architectures [Benini and De Micheli 1998; Rabaey *et al*. 2010] [18, 20].

Finally, the design phase produces a structured testing and deployment plan. This plan outlines laboratory tests, controlled field trials and long-term environmental assessments. It also considers the logistical challenges of deploying devices in areas affected by illegal extraction, where equipment may be targeted or destroyed cited in the studies of [Gunasekara 2018; Karunaratne 2018] [4, 7]. These outcomes create a clear pathway from conceptual design toward practical implementation.

Future Work

Future work focuses on transforming the system level design into a functioning prototype that can be evaluated under controlled and real-world conditions. The first stage involves hardware prototyping, where sensing modules, the event driven VLSI core, communication interfaces and tamper resistant features are integrated into a compact enclosure. This phase will verify whether the architectural assumptions made during design hold true when implemented in physical hardware. It will also allow early measurements of power consumption, wake up latency, feature extraction efficiency and the responsiveness of tamper detection circuitry, which are key indicators of long-term viability in low power deployments [Benini and De Micheli 1998; Rabaey *et al*. 2010] [18, 20].

Laboratory testing will follow, providing a controlled environment for evaluating subsystem performance. Vibration, acoustic, turbidity and PIR sensors will be tested against known stimuli to confirm that thresholds and feature extraction methods behave as expected. Communication pathways will be assessed under varying signal conditions to determine how reliably the system can transmit alerts through LoRaWAN, NB IoT and satellite links [Centenaro *et al*. 2016; Al-Fuqaha *et al*. 2015] [28]. Security features will also be validated through simulated tampering scenarios, including enclosure penetration, forced displacement and unauthorized exposure to light, reflecting common attack patterns documented in tamper resistance research [Skorobogatov 2011; Yuce *et al*. 2019] [21, 24].

Field surveys will identify suitable deployment sites along riverbanks, taking into account terrain, vegetation, accessibility and known patterns of illegal extraction. These field surveys futher help refine enclosure design, sensor placement strategies and concealment techniques on the proposed unit for Sri Lankan fields. Once prototyping is completed field tests will be conducted to measure how the system performs under real environmental conditions, including humidity, flooding, sediment movement and human interference. Prior studies highlight how equipment in these regions is often damaged or removed made a very valuable contribution in this case. This implies why rigorous field tests are necessary prior to deploy as in[Gunasekara 2018; Karunaratne 2018] [4, 7].

Environmental durability assessments will extend these trials over longer periods that covers seasonal monsoons to evaluate how the system withstands seasonal changes, shifting riverbanks and prolonged exposure to moisture and sediment. These assessments provide data for improvements to enclosure materials, sealing methods and mounting strategies. Such knowledge will inform improvements to the sensing, power, and resilience aspects.

The factors will result in an effective monitoring platform that will support the sustainable management of rivers [UNEP 2020; Ministry of Environment 2022] [6, 9].

Conclusion

The architecture presented in this paper demonstrates how a low power VLSI platform can support autonomous environmental monitoring in remote and tamper prone riverine settings. By integrating multimodal sensing, event driven processing, hardware rooted security and flexible communication pathways, the system is designed to remain operational in locations where power, connectivity and maintenance access are limited. These design choices respond directly to the environmental and logistical constraints described in studies of riverine extraction, which highlight difficult terrain, scarce manpower and the frequent destruction of deployed equipment [Gunasekara 2018; Karunaratne 2018] [4, 7].

The fusion of sensing modalities in vibration, acoustic, turbidity, and passive infrared sensing offers a more reliable means of detecting environmental disturbances in accordance with well-founded principles in multi-sensor fusion [Hall and Llinas 1997; Khaleghi *et al*. 2013] [25, 26]. The use of event-driven VLSI processing minimizes energy expenditure and facilitates deployment in environments with limited power supplies in accordance with well-founded principles in low-power design [Benini and De Micheli 1998; Rabaey *et al*. 2010] [18, 20]. The use of hardware-based security features minimizes the risk of malicious intervention in accordance with well-founded principles in physical security and secure hardware design [Skorobogatov 2011; Yuce *et al*. 2019] [21, 24]. The use of multi-protocol communication enables reliable transmission of alarms in environments characterized by inconsistent and partial infrastructures [Centenaro *et al*. 2016; Al-Fuqaha *et al*. 2015] [28, 29].

As the work progresses toward hardware implementation, prototype development and field validation will refine sensing performance, power efficiency and tamper resilience. Such refinements will also contribute to developing a strong monitoring system that will be instrumental in effective river management for sustainability, as well as addressing issues related to illegal extraction practices that affect the environment negatively [UNEP 2020; Ministry of Environment 2022] [9, 15]. The architecture therefore provides not only a technical foundation but also a practical pathway toward reliable, long term environmental monitoring in some of the most challenging real-world environments.

Although the architecture is designed for long term autonomous operation, several limitations remain. Classification complexity is constrained by the need to maintain low power operation, and solar harvesting may be affected by prolonged low light conditions. Extreme weather events may still distort sensor readings, and satellite communication introduces higher energy cost. These limitations will guide future refinements in hardware design and deployment strategy.

Acknowledgement

The authors thank Dr. Q. Li's funding agency for their support throughout this work. We also extend our appreciation to all field officers who assisted with access to remote riverine sites, and to all individuals and institutions whose guidance and cooperation contributed to this study.

References

1. Chen L, *et al*. Low Power Machine Learning Architectures for Edge Sensing. IEEE Transactions on Circuits and Systems,2021:67(4):12–20.
2. Dias N. Evaluating Drone Based Environmental Surveillance in Sri Lanka. Journal of Remote Sensing Studies,2019:8(2):60–70.
3. Fernando S. Challenges in Rural CCTV Deployment for Environmental Monitoring. Sri Lanka Journal of Engineering,2020:45(1):110–125.
4. Gunasekara D. Monitoring Illegal Resource Extraction in Sri Lanka. Environmental Policy Review,2018:12(3):70–90.
5. Herath H. Hydrological Impacts of River Sand Mining. Sri Lankan Journal of Hydrology,2017:5(1):80–95.
6. Jayawardena L. Environmental Consequences of Sand Extraction in Major Sri Lankan Rivers. Asian Water Research Review,2020:14(2):50–65.
7. Karunaratne M. Community Level Impacts of River Sand Mining. Journal of Environmental Sociology,2018:9(1):35–48.
8. Khan R, Lee J. Energy Harvesting Techniques for Long Term IoT Deployments. International Journal of Embedded Systems,2021:11(4):65–78.
9. Ministry of Environment Sri Lanka. National Policy on Sustainable River Management. Government of Sri Lanka, 2022.
10. NIST. Advanced Encryption Standard (AES) Specifications. National Institute of Standards and Technology, 2021.
11. Perera S. Limitations of Manual Environmental Patrols in Sri Lanka. Journal of Public Administration,2019:22(1):10–20.
12. Rahman A. Long Range IoT Communication Technologies for Remote Monitoring. International Journal of Wireless Systems,2020:7(3):30–40.
13. Ratnayake R. Geological Effects of Excessive Sand Mining. Earth Science Review of Sri Lanka,2016:6(2):110–125.
14. Silva P. Security Risks in Environmental Monitoring Equipment. Journal of Field Engineering,2021:19(4):200–210.
15. UNEP. Sand and Sustainability: Finding New Solutions for Environmental Governance. United Nations Environment Programme, 2020.
16. Wijesinghe T. Acoustic and Vibration Signatures of Illegal Sand Mining Machinery. Proceedings of the Sri Lanka Engineering Research Conference, 2019, 25–32.
17. Zhang W, Kumar A. Trends in Low Power Environmental IoT Systems. Sensors and Systems Review,2021:13(1):1–15.
18. Benini L, De Micheli G. Dynamic Power Management: Design Techniques and CAD Tools. Kluwer Academic Publishers, 1998.
19. Ottoni G, *et al*. Event-Driven Architectures for Low-Power Sensor Processing. IEEE Transactions on Very Large-Scale Integration (VLSI) Systems,2014:22(11):2340–2353.
20. Rabaey JM, *et al*. Ultra-Low-Power Design for Wireless Sensor Nodes. Proceedings of the IEEE,2010:98(2):205–223.
21. Skorobogatov S. Physical Attacks and Tamper Resistance. University of Cambridge Technical Report, 2011.
22. Kuhn MG. Optical and Power Analysis Attacks on Secure Hardware. IEEE Security & Privacy,2004:2(6):56–62.
23. Suh GE, Devadas S. Physical Unclonable Functions for Device Authentication and Secret Key Generation. Proceedings of the 44th Design Automation Conference, 2007, 9–14.
24. Yuce B, *et al*. Tamper-Resistant Hardware: A Survey. ACM Computing Surveys,2019:51(6):1–36.
25. Hall DL, Llinas J. An Introduction to Multisensor Data Fusion. Proceedings of the IEEE,1997:85(1):6–23.
26. Khaleghi B, *et al*. Multisensor Data Fusion: A Review of the State of the Art. Information Fusion,2013:14(1):28–44.
27. Ribeiro M, *et al*. Environmental Monitoring Using Acoustic and Vibration Sensors. Sensors,2020:20(12):1–18.
28. Centenaro M, *et al*. Long-Range Communications in Unlicensed Bands: The Rising Stars LoRaWAN and Sigfox. IEEE Wireless Communications,2016:23(5):60–67.
29. Al-Fuqaha A, *et al*. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Communications Surveys & Tutorials,2015:17(4):2347–2376.