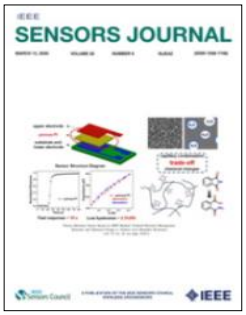
Journal Name: IEEE Sensors Journal **IF: 4.5**

Title: Advanced Heart Disease Detection: A Quantum Generative Attention Model for Sensing Networks

Author: Mythrayee D.; Vadde S.; Rajaropu N.; Anguraj D.K.; Guduri M.; Chakraborty C.

Details: Volume 26, Issue 7, February 2026

Abstract: The main challenge of predicting heart diseases accurately and securely on real-time data of wearable IoT-based monitoring systems has been a significant problem because of the high computational cost, low forecasting accuracy, and data security issues in the current systems. This paper outlines a robust, innovative system combining hybrid lightweight cryptography and attribute-based encryption to transmit authenticated, protected data. The wearable sensor data undergo secure encryption and transmission to the cloud, and are subsequently normalised using adjusted Min-Max with decimal scaling and statistical column normalisation. Feature learning is performed using a Prompt-Tuned Multi-Task Taxonomic Transformer, and classification is performed with the Efficient Hamiltonian Long-Range Quantum Generative Attention Network, which is optimized with the Elk Herd Optimizer. The Hungarian heart disease data show that experimental analysis achieves high prediction accuracy, greater security, and reduced computational cost, thereby enabling effective real-time healthcare monitoring.



URL: https://ieeexplore.ieee.org/document/11408129

SCHOLARLY PUBLICATIONS
Centres of Innovation and Research (COIR)
KIIT Deemed to be University

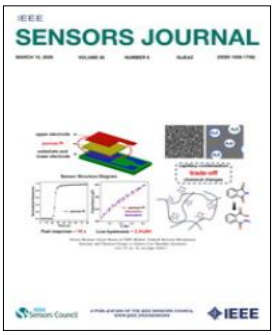
Journal Name: IEEE Sensors Journal **IF: 4.5**

Title: A Neuroentropy-Driven Nature-Inspired Framework for Adaptive Privacy and Lightweight Security in Sensor Devices

Author: Othman S.B.; Chakraborty C.; Singh S.; Frikha M.A.

Details: Volume 26, Issue 6, March 2026

Abstract: Sensor devices and Internet of Things (IoT) devices face a critical, fundamental challenge: deploying robust security while operating under severe constraints on energy, processing power, and memory. This article presents biologically inspired entropy security (BioEnS), a novel, closed-loop framework designed to overcome the inherent security–privacy–efficiency trilemma by achieving paretooptimal adaptive security. BioEnS models adaptive defense as a real-time, constrained multiobjective optimization problem, dynamically resolving the trade-off between security assurance (8) and resource consumption (9) based on current context. The framework core relies on a hardware root-of-trust entropy source (HRTES), which provides a quantifiable PUF-derived min-entropy rate (E_{rate}) for nondeterministic key derivation, feeding into an Adaptive Security Manager (ASM). This mechanism rigorously enforces context-dependent security requirements (8_{req}) through a dominant λ-penalty term, enabling ultralow latency policy decisions. Experimental validation on an ARM Cortex-M platform demonstrates exceptional performance: BioEnS maintains a near-zero security violation rate (SVR) (0.02%) while simultaneously yielding a superior lifetime extension ratio (LER) of 0.69× relative to the high-security baseline (HSB), confirming the validity of the guaranteed policy enforcement.



URL: https://ieeexplore.ieee.org/document/11370320