# Assessment of Physical Unclonable Function–Based Data Sampling Techniques for Secure IoT Edge Environments

**Goutam Kumar[1], Dr. Arvind Kumar[2]**

1. Research Scholar, Department of Electronics and Communication Engineering, BIT Sindri Dhanbad, under JUT, Ranchi Jharkhand

2. Assistant Professor, Department of Electronics and Communication Engineering, BIT Sindri Dhanbad, under JUT, Ranchi Jharkhand

## Abstract

The growing use of Internet of Things (IoT) applications has moved data processing to the network edge with devices under harsh constraints of computational, memory, and energy alongside being vulnerable to both physical and cyber-attacks. Traditional security solutions depend on some cryptographic keys that are stored, which can be extracted, cloned, and recreated in the edge cases. Physical Unclonable Functions (PUFs) are greatly examined to accomplish device authentication and key generation, however, the possibility of using such features to protect the process of data acquisition has not been systematically examined. This paper presents and analyses a PUF-aided adaptive data sampling model to secure IoT edge environment, where the PUF-based entropy is hard coded into the sampling procedure. The framework eradicates the storage of key data by dynamically varying intrinsic hardware variations to dynamically control sampling intervals and offer lightweight data protection, and thereby improving data transmission unpredictability. Several PUF structures such as SRAM, Ring Oscillator, Arbiter and Butterfly PUFs are experimentally evaluated comparatively under real-world edge constraints on a comparative basis. The findings indicate that the suggested solution can greatly minimize the unnecessary data transmission and still maintain a high level of event detection, which results in the apparent energy savings and the low latency overhead. Security analysis indicates that device cloning, replay attacks and timing inference attacks have a high degree of resistance to such attacks because the device embodies entropy-driven sampling behavior and has no stored secrets. Comparative analysis also reveals the trade-offs between types of PUF in the aspects of reliability, entropy and energy efficiency giving a practical advice on deployment. In general, the paper confirms that PUF-inspired data sampling is a scalable, lightweight, and useful approach to improving not only the security but also the efficiency of resource-constrained IoT edge systems, which leads to new opportunities in the implementation of hardware-based trust into adaptive systems control.

**Keywords:** Physical Unclonable Functions (PUFs); IoT Edge Security; Adaptive Data Sampling; Hardware-Based Security; Secure IoT Systems.

# 1. INTRODUCTION

## 1.1.IoT Edge Computing and Emerging Security Challenges

The proliferation of Internet of Things (IoT) objects is changing computing paradigms in modern computing to edge processing through centralized cloud computing. Edge computing processes the data on the source instead of sending it to cloud servers located far away, which allows processing data with ultra-low latency, consuming less bandwidth, and making decisions. The paradigm has become central in the fields of monitoring healthcare, industry automation, intelligent transportation, and intelligent surveillance systems (Shi et al., 2016; Satyanarayanan, 2017).

Although these advantages are present, implementation of IoT services at the network edge has contributed a lot to the attack surface of the system. Edge nodes are normally cheap devices and they do not need to be controlled and physically reachable. Because of this, they are extremely susceptible to physical attacks, side-channel leakage, modification of the firmware, impersonation of nodes, and manipulation of data (Roman et al., 2018; Zhang et al., 2019). Contrary to the conventional data centers, edge devices do not depend on secure hardware modules and active supervision.

Moreover, the IoT edge systems have severe computation, memory, energy and storage restrictions, thus restricting the use of heavy cryptographic primitives like RSA, ECC or complete TLS stacks (Conti et al., 2018). These constraints make it vastly important to develop lightweight but efficient security systems that can perform effectively in a restricted environment factor, and at the same time, ensure a high level of trust.

## 1.2.Limitations of Traditional Cryptographic Key Storage

Traditional security systems are based on cryptographic keys stored on non-volatile memory. But in resource constrained edge devices, this scheme has devastating weaknesses. Stored keys can be physically probed, fault-injected, cold-booted, side-channels analysed, and extracted (Kocher et al., 2022). After extraction, keys can be copied which allows attackers to duplicate the devices and execute replay or man in the middle attacks.

The cost and power consumption of secure key storage implementation, including Trusted Platform Modules (TPMs) and the use of secure elements, are prohibitively costly and power-intensive when used at the scale of IoT. Key protection in software is also weak since hackers can reverse engineer and decipher secrets of the memory. These weaknesses indicate that the threat model of IoT edge environments cannot be stored on the static key basis (Maes, 2013) in any way.

## 1.3.Physical Unclonable Functions as a Hardware Root of Trust

Physical Unclonable Functions (PUFs) represent an entirely new concept to the security of devices. Instead of secrecy storage, PUFs are based on the cryptographic material generated by physical

variation that cannot be predicted and is introduced when making semiconductors (Gassend et al., 2002). These differences cannot be reproduced even by the original manufacturer and each PUF is a unique item.

PUFs produce pairs of challenges and responses (CRPs) which may be utilized to provide authentication to the devices, derive secure keys, and check identities (Rührmair et al., 2013; Delvaux and Verbauwhede, 2017). PUF-based systems are inherently immune to attacks to steal memory since no secret is ever stored permanently.

Various PUF architectures are built such as:

- SRAM PUFs – according to power-up conditions of memory cells (Guajardo et al., 2007)
- Ring Oscillator (RO) PUFs – according to the frequency difference (Suh & Devadas, 2007)
- Arbiter PUFs – according to signal race conditions (Hemavathy & Bhaaskaran, 2023)
- Butterfly PUFs – alternatives to FPGAs based on latch (Kumar et al., 2008)

All types of PUFs have particular trade-offs in stability, uniqueness, entropy, cost of hardware, and modeling attack resistance.

### 1.4.Data Sampling in IoT Edge Systems

IoT networks produce huge amounts of sensor data at a continuous rate with much of it being redundant or irrelevant. In order to cope with this, the data sampling is implemented to regulate the manner and timing of data collection. Conventional uniform sampling is energy-wasting and bandwidth-consuming, whereas adaptive sampling and event-driven sampling is more efficient due to its responsiveness to environmental changes (Alippi et al., 2010).

The majority of the sampling strategies discussed, however, are concerned only with efficiency, disregarding the security. The latest efforts of bringing security together are based on conventional cryptography, which once again has key storage weaknesses and is computationally burdened (Conti et al., 2018). Subsequently, the existing secure sampling plans are still inefficient and prone to hostile edge conditions.

### 1.5.Research Gap and Motivation

Despite the common research on the use of PUFs as a tool of authentication and key generation, systematic studies on the incorporation of PUFs in data sampling logic are lacking. Existing research:

- Processing sampling and security as discrete layers
- The PUF entropy is not used to affect sampling decision
- Comparison of Lacks performance evaluation in the PUF types

- Doesn't evaluate behavior under actual edge constraints

### 1.6.Contributions of This Work

The following contributions are made in this paper:

1. Presents a PUF-aided adaptive data sampling architecture of secure IoT edge devices.
2. Gives a comparative evaluation of SRAM, RO, Arbiter and Butterfly PUFs.
3. Assesses performance and security in practical edge situations.
4. Shows that PUF-based sampling can be used to boost security and has a low overhead.

## 2. RELATED WORK

### 2.1.Security Mechanisms in IoT Edge Environments

The high rate of IoT development has moved a high number of workloads out of the centralized cloud server and to nodes that are close to the data sources. Edge computing minimizes the network load and latency but poses novel security risks because of heterogeneous hardware, limited resources, and a lack of trust in the physical environment (Shi et al., 2016; Satyanarayan, 2017). Conventional cloud-based solutions, including PKI (Public Key Infrastructure), TLS/SSL, and hardware security modules, are usually too heavy or expensive to be offered to the limited resources of IoT devices (Conti et al., 2018).

To solve this, there are three general categories of security mechanisms that have been studied in the literature**:**

**a) Lightweight Cryptography**

Symmetric ciphers based on lightweight (e.g., PRESENT, SPECK, SIMON) and hash functions are also actively researched to minimize the computational and energy costs (Beaulieu et al., 2015). Nevertheless, even lightweight cryptography must have storage of keys that are secure, which presents a basic attack point: fixed key can be obtained through physical intrusion, memory inspections and debugging ports (Kocher et al., 2022).

**b) Trusted Execution and Isolated Hardware**

Secure as well as trusted execution environments (TEE or secure element) offer independent processing environments to secure code and data (Arm TrustZone, Intel SGX). TEEs are costly, consume a lot of power, and are often unavailable on low-end IoT devices, although they are useful in general computing areas (Conti et al., 2018).

Recent surveys also highlight the fact that TEEs and SEs cannot be used independently as a solution to the security of the IoT because they cannot be scaled to support a variety of edge platforms and threat models with notable overhead (Ali et al., 2023).

**c) Hardware Intrinsic Security Primitives**

Physical Unclonable Functions (PUF) and other intrinsic hardware trust anchors (in particular) directly solve the issue of secrets storage by responding to physical variations, without necessarily storing the key in persistent storage. This design is in itself immune to numerous types of intrusion.

The recent literature proves the increasing significance of the PUFs in the lightweight IoT security, particularly in authentication and key generation within the edge devices (Oduro-Antwi et al., 2026).

## 2.2.Physical Unclonable Functions: Architectures and Security Properties

PUFs capitalize on the uncontrollable variation in manufacturing to produce challenge-response pairs (CRP), which can be replicated by the device, but not by an attacker (Rührmair et al., 2013).

**a) Classic PUF Types**

| PUF Type | Key Characteristics | Strengths | Limitations |
|---|---|---|---|
| SRAM PUFs | Startup values of SRAM cells | High stability | Bias under temperature changes |
| Ring Oscillator | Frequency variations | Large CRP space | Sensitive to voltage/temp |
| Arbiter PUFs | Race conditions | Large challenge space | Vulnerable to ML modeling |
| Butterfly PUFs | Cross-coupled latch | Wide applicability (FPGAs) | Variability under noise |

***Foundational studies:***

- SRAM PUF stability, entropy (Guajardo et al., 2007)
- Scalability of Ring Oscillator (Suh & Devadas, 2007)
- Arbiter PUF race logic (Hemavathy & Bhaaskaran, 2023)
- The Butterfly PUF latch architecture (Kumar et al., 2008) is one of them

**b) Recent Advances in PUF Research**

The last several years have been characterized by a considerable improvement of the solutions of PUF weaknesses and improvements in its utilization on edge platforms:

- **Model-Attack Resilience:** The active research is on unified security models and machine learning resistance metrics to make strong PUFs more resistant to modeling attacks (Zhang et al., 2019).
- **Hybrid PUF Designs:** To achieve stability and entropy balance of high-security IoT, the combination of SRAM and RO PUFs (Lu et al., 2025) is used.
- **Emergent PUF Modalities:** PUFs based on electromagnetic emissions (EM-PUFs) and optical PUFs are other sources of entropy, which increases the use of PUFs in heterogeneous IoT devices (Asif et al., 2020).

This richness notwithstanding, recent literature concentrates primarily on authentication and key generation, rather than the impact that PUF run-time outputs may have on running system behaviour, such as sampling data, timetabling, or an adaptive controller — which is specifically the gap that this paper aims to fill.

### 2.3.IoT Data Sampling Techniques

Sampling of data in sensor networks minimizes communication, storage and energy expense by focusing on significant data transmission. Traditional methods incorporate:

**a) Uniform Sampling**

Gathers information in regular time intervals. Easy and may be inefficient when the signal under monitoring varies slowly or infrequently.

**b) Adaptive Sampling**

Sampling rate adjusts to signal activity or signal variance, and saves energy without any signal loss (Alippi et al., 2010).

**c) Event-Driven and Context-Aware Sampling**

Blocks sampling occurs only upon the occurrence of thresholds or contextual conditions (Lu et al., 2025). In some of the more recent ones, machine learning is used to combine anomaly-driven sampling to minimize false positives and bandwidth allocation dynamically.

**d) Security-Aware Sampling**

**Emergent but sparse:**

- There are cryptographically secured sampling timestamps that do not allow replay and tampering (Herding et al., 2024).
- Altogether, secure compressed sensing methods ensure privacy through randomized projections (Hallyburton & Pajic, 2025).

**Limitations of current approaches:**

1. Security is additive - not a part of sampling logic.
2. Majority of these techniques rely on secret keys stored.
3. None of them use hardware cryptographic roots (including PUFs) to determine sampling choices.

### 2.4.Integrating PUFs with System Logic

The new studies began to investigate PUFs outside authentication:

- PUF-based random number generation: PUF outputs serve as sources of entropy for cryptographic primitives (Kalanadhabhatta et al., 2020).
- PUF-driven scheduling: Prioritizing firmware upgrades and access control based on intrinsic trust.
- Hardware trust anchors for federated learning: PUFs are used in edge learning systems to safely bootstrap model aggregation (Ahmad et al., 2025).

Nevertheless, the possibility of using PUF outputs as control signals in adaptive system functions such as data sampling as an area is open. Existing work stops short of:

✓ Relating PUF entropy measures to modulation of the sampling interval

✓ PUF-based sampling assessment in the context of actual IoT conditions

✓ Comparative PUF sampling robustness analysis

### 2.5.Research Gaps (Synthesis)

Based on the above literature, the following gaps are apparent:

1. PUF applications largely have restrictions to authentication and key generation.
2. Safe data sampling systems are cryptography-based and ineffective.
3. No controlled investigation of PUF products as adaptive sampling stimuli.
4. Absence of comparative studies on the various PUF families as far as in-field IoT performance is concerned.

The existence of these gaps is the direct source of inspiration of this paper contribution:

a PUF-based adaptive data sampling system a unique hardware trust and a high-efficiency edge data acquisition system.

## 3. SYSTEM MODEL AND THREAT ASSUMPTIONS

### 3.1.IoT Edge Architecture

The system is supported by a three-level IoT edge computing architecture that has become a conventional framework of latency-sensitive and resource-constrained applications (Shi et al., 2016; Satyanarayanan, 2017). The bottom level comprises heterogeneous sensor nodes that are used to gather real-time environmental and operational information. These products are usually highly constrained in terms of power, memory and processing capabilities and cannot support significant cryptographic operations and long-term secrets (Roman et al., 2018). Since these devices can be deployed in places that are physically accessible or even hostile, it is prone to tampering, reverse engineering, and key extraction attacks (Kocher et al., 2022).

To address the risks, the proposed model has a Physical Unclonable Function (PUF) mounted on each sensor node, which is the innate hardware identity of the device. This is because PUF responses can be created in real time based on uncontrollable manufacturing variations unlike traditional cryptographic keys that have to be stored in memory, which is a hardware-rooted source of uniqueness and entropy (Gassend et al., 2002; Rührmair et al., 2013). The PUF then serves as the main trust anchor of sensor layer.

The middle level comprises of edge gateways, which combined the information of two or more sensor nodes and do a lightweight security check, integrity check and adaptive sampling coordination. These are more powerful than sensor nodes yet energy-conscious and latency conscious, which makes them viable in enforcing security policies near the data source (Roman et al., 2018). The sensors and edge nodes communicate via short-range protocols (ZigBee, BLE, or LoRa, or Wi-Fi) based on the conditions of deployment.

The optional cloud tier only applies to long-term storage, global analytics and updates on system level policies. Notably, there are no permanent secrets of cryptography stored in the cloud. Local establishment of device trust is achieved by PUF validation on the edge that eliminates key management centralization and mitigates the impact of server-side attacks (Delvaux & Verbauwhede, 2017).

### 3.2.Threat Model

The system presupposes a powerful adversarial model in line with the real-life IoT deployments. An attacker can physically seize a sensor node, steal firmware, or scan memory, or do power, timing, or electromagnetic attacks (Kocher et al., 2022). The opponent can also seek to clone the devices by copying software images, recapturing some previously captured packets or impersonate legitimate nodes to inject falsified data into the network.

Most of these attacks are usually effective in the traditional systems since the cryptographic keys are stored in non-volatile storage. Conversely, the suggested structure does not have any permanent secrets. As the responses of PUF are based on physical differences, which cannot be imitated, even

complete access to a hardware cannot enable an attacker to recreate a legitimate device identity (Maes, 2013).

Threat model also assumes modelling attacks on strong PUFs where machine-learning algorithms are trying to guess challenge-response behavior by watching a big number of samples (Rührmair et al., 2013). In order to minimize this risk, the framework restricts PUF responses, responds masking, and dynamically modifies the sampling behavior, thus the attackers do not learn consistent patterns.

### 3.3.Security Objectives

The key goal of the suggested system is to deploy a safe and light data sampling platform that is intuitively secured by hardware confidence. To start with, the system provides authenticity of the device by linking identities to individual PUF response, which is unclonable and unforgeable (Gassend et al., 2002). Second, the data integrity and freshness are maintained with the help of PUF-generated entropy to avoid replay and tampering attacks (Delvaux & Verbauwhede, 2017). Third, the lightweight masking using the PUF outputs as a basis of achieving confidentiality instead of the heavy encryption, and hence the reduced computational overhead (Maes, 2013). Lastly, the framework can be scaled and is energy-efficient, which is why it can be used to deploy large-scale IoT edges, without a complicated key distribution and storage infrastructure (Roman et al., 2018).

## 4. PUF-BASED DATA SAMPLING FRAMEWORK

### 4.1.Overview of the Proposed Framework

In the proposed framework, a new data sampling architecture of the IoT edge environment is proposed based on security as a key driver and the idea that Physical Unclonability Function (PUF) responses are directly integrated into the logic of the sampling control. The system uses the entropy generated by PUFs, as they are unpredictable and unique to a device, to determine when, how frequently and in what conditions sensor data is recorded. This allows a new category of trust-aware adaptive sampling that enhances the security of data and resource efficiency at the same time. The framework automatically withstands physical extraction attacks and clones by removing the requirement of fixed cryptographic keys, and using the consumption characteristics of low-power IoT devices.

PUFs only live at the sensor nodes in the three layers of the framework: sensor, edge, and cloud. The edge layer uses entropy signals and identities produced from PUF to coordinate sampling policies and confirm trust. Sensitive information is never transferred or retained thanks to this design, and confidence is constantly restored throughout runtime.

### 4.2.PUF-Assisted Sampling Mechanism

The fundamental component of the framework is an adaptive sampling engine that is aided by a PUF. As a sensor node initiates it PUF produces a reply according to a challenge published locally. This reply is not delivered as raw value, it is run through a lightweight fuzzy extractor to obtain a fixed entropy value. This entropy is then converted to a dynamic sampling interval. The shorter sampling periods due to high-entropy states (becoming more responsive) and the longer sampling period due to low-entropy states (saving energy in constant conditions) occur.

The sampling frequency can vary with the environmental context as well as the credibility and individuality of the device itself under this approach. Also a part of the PUF output is taken and used as a masking key to slightly encrypt or obfuscate sensor data prior to transmission. This ensures replay protection and confidentiality without requiring complex cryptographic primitives.

### 4.3.Workflow Description

The system works in three consecutive steps:

- **Initialization Phase:** Upon activation, each sensor node provides a PUF response with a challenge stored on it. The device is also authenticated by the edge gateway, which checks the response of the device using a secure enrollment reference. The gateway provides a sampling policy template on verification.
- **Sampling and Data Acquisition Phase:** The sensor measures its PUF output again periodically in order to calculate the next sampling interval. Environmental data is recorded upon the expiry of the PUF-driven timer, which will guarantee randomized sampling behavior but with control.
- **Secure Transmission Phase:** Pseudo-uniform random sampling. The entropy produced by the PUF masks the sampled data, and sends it to the edge node, where the integrity is checked and replay attacks are discarded.

## 5. EXPERIMENTAL SETUP AND RESEARCH METHODOLOGY

### 5.1.Research Design and Methodological Approach

The research design will be an experimental and comparative study in determining the functionality of Physical Unclonable Function (PUF)-based data sampling methods in achieving IoT edge environments security. The approach will integrate both hardware-level experimentation and controlled simulation with quantitative performance analysis of the effect of the addition of PUFs to sampling logic on security, efficiency and the overhead of the system. They compare various PUF architectures in the same operating conditions in order to provide fairness and reproducibility.

The research design is built based on three fundamental elements: (i) deployment of several types of PUF on typical IoT edge devices, (ii) implementation of adaptive sampling with the support of PUF on actual sensor measurements, and (iii) a methodological examination through the security, performance, and efficiency metrics.

### 5.2.Hardware Platform and PUF Implementation

The experimental platform incorporates low-power IoT sensor nodes that are made based on microcontroller-based hardware that is typically used in edge deployments. All the nodes consist of on-chip SRAM, programmable delay elements, and rudimentary sensing peripherals. Four PUF architectures considered so far, such as SRAM PUF, Ring Oscillator (RO) PUF, Arbiter PUF and Butterfly PUF, are implemented so that a comparative analysis becomes possible.

SRAM PUFs are implemented with the initial state of on-chip memory and they take advantage of the cell-level mismatch of fabrication variation. Ring Oscillator PUFs are executed by contrasting frequency difference between similarly designed oscillators. Arbiter PUFs are based on the use of race conditions and configurable delay paths, Butterfly PUFs are done with cross-coupled latches and are useful in reconfigurable logic environments. Every PUF implementation is run through an enrollment phase to create reference characteristics and run time appraisal is repeated to quantify stability and uniqueness.

Implementation of edge gateways is based on embedded Linux platforms that combine data, authenticate PUF derived trust signals and plan adaptive sampling policies. When deployed, the cloud layer is only used as a long-term storage option and off-line analysis and is not involved in real-time security decisions.

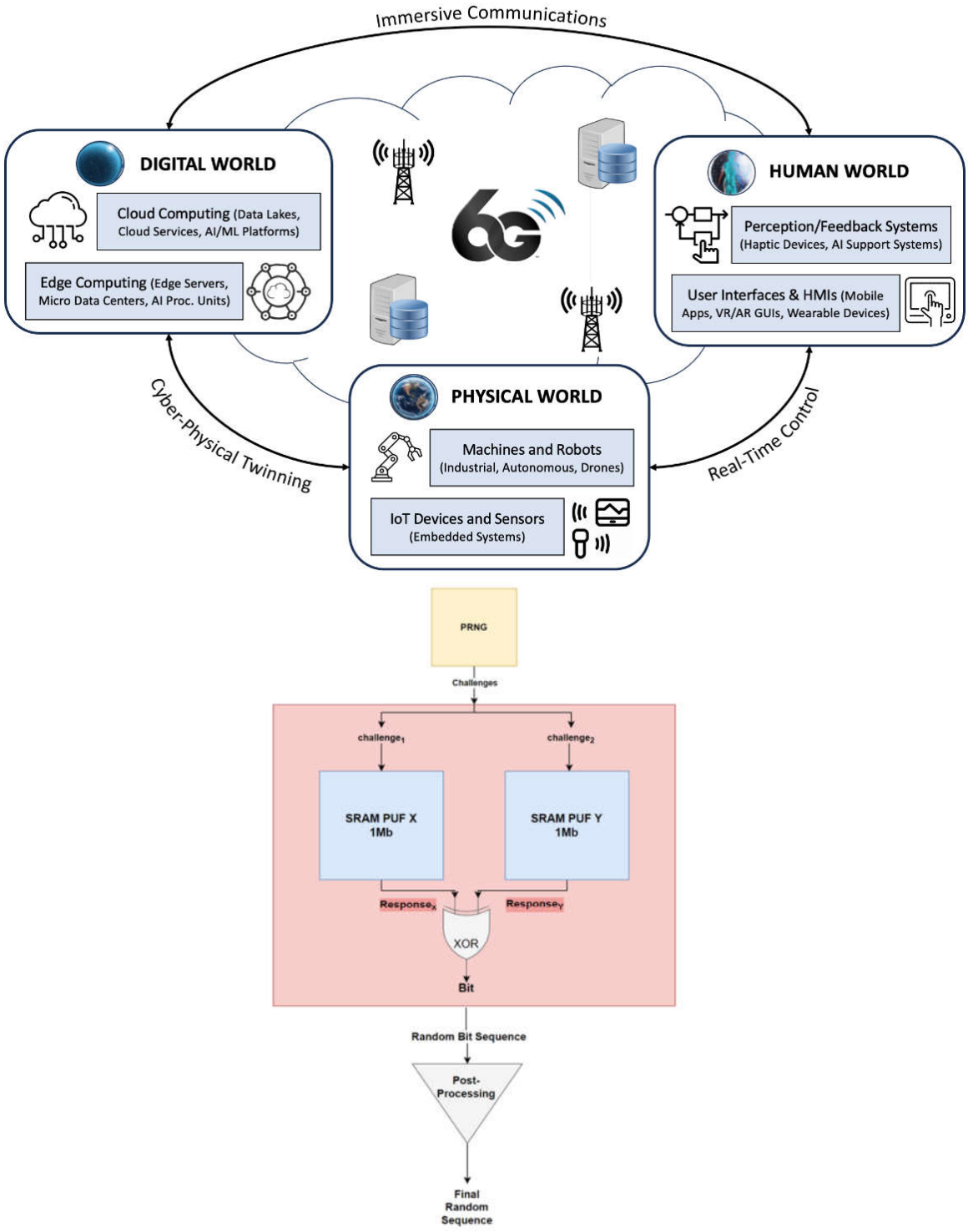


Figure 1: Experimental testbed and representative PUF architectures used in the study.

### 5.3.Dataset Description and Sampling Context

In order to test the suggested framework under real world settings the experiments use environmental sensing data that is indicative of typical IoT usage. The information is comprised of time-series data of temperature, humidity, and motion signals, which display slow-varying environment parameters and sudden changes brought about by events. The data streams are sampled across long periods of time to ensure that normal operation behavior in addition to the short-lived anomalies are captured.

The experimental setup takes into account a total of 30 virtual sensor nodes which are mapped to physical or simulated IoT devices that have a single PUF instance. To each sensor node, data are gathered in two conditions, including normal conditions, in which sensor values vary gradually and adversarial conditions, in which replay, spoofed transmissions and timing manipulations are implemented. The dual scenario design makes it possible to assess the efficiency and security resilience.

### 5.4.PUF-Assisted Adaptive Sampling Technique

The methodological innovation is the fundamental one consisting of the introduction of PUF outputs to the data sampling mechanism. Each sensor node produces a locally generated challenge by generating a PUF response at runtime using the locally generated challenge. A lightweight post-processing is utilized to extract stable entropy on the response. This entropy is then mapped into a dynamic sampling interval and this enables the sensor to adjust its data acquisition rate according to the environmental context and the actual hardware randomness.

Unlike other traditional adaptive sampling methods that use signal variance or thresholds as the only basis to select samples, the suggested methodology creates uncertainty in sampling behaviour, such that it becomes immune to adversarial timing and replay attacks. Also, the entropy of PUF derived is partially utilized to obfuscate sampled data before transmission, offering lightweight confidentiality and freshness guarantees without the usage of computationally-intensive cryptographic primitives.

### 5.5.Evaluation Metrics and Performance Measurement

The suggested approach to the work assesses the system performance based on a set of all-encompassing quantitative measure. Data reduction ratio and responsiveness are used as measures of sampling efficiency, where high sampling efficiency shows that redundant transmissions have been removed, but has preserved event sensitivity. Power consumption is measured through average power consumption per sample cycle which reveals the overhead caused by PUF operations.

Security wise, PUF quality-measures have been computed such as intra-Hamming distance to determine reliability, and inter-Hamming distance to determine uniqueness among devices. The analysis of entropy is done to determine the appropriateness of PUF results to drive sampling

decisions and masking of data. The latency is given in the end-to-end delay between the data collection point and the verification point at the edge gateway.

All the results are contrasted with baseline methods with uniform sampling and lightweight cryptography protection without integrating PUFs. This comparative analysis enables the advantage of security and efficiency of PUF-driven sampling to be readily measurable.

### 5.6.Experimental Procedure

The process of the experiment is organized. First, the baseline characteristics are created by enrolling each PUF. Secondly, sensor nodes are working under normal condition both with the assistance of conventional and PUF-assisted sampling schemes. Third, resistance to replay, cloning and timing inference attacks are tested by introduction of adversarial scenarios. Lastly, statistical analysis of all data collected is performed to determine the results of comparison between PUF types and sampling techniques.

This research approach allows reproducibility, fairness and strength, and is a strong empirical basis of assessment of PUF-based secure data sampling on edge computing in the IoT.

## 6. RESULTS AND ANALYSIS

This part provides the analysis of the experimental findings of testing the presented PUF-assisting adaptive data sampling framework in IoT edge settings. The analysis is dedicated to four dimensions, namely, PUF reliability and uniqueness, entropy quality, sampling efficiency, and security robustness, and is concluded by comparative trade-offs discussion. The outcomes are compared with the usual and uniform sampling techniques as well as the adaptive sampling based on its variance to determine the efficiency of the suggested method.

### 6.1.Analysis of PUF Reliability and Uniqueness

The consistency and distinctiveness of PUFs responses are the building blocks to the usefulness of the suggested framework since a wild combination or a low-grade PUFs may compromise security and sampling consistency. Intra-Hamming distance is used to measure reliability whereas inter-Hamming distance is used to measure uniqueness among various devices.

**Table 1: Reliability and Uniqueness Metrics of PUF Implementations**

| PUF Type | Avg. Intra-HD (%) | Avg. Inter-HD (%) | Reliability Assessment | Uniqueness Assessment |
|---|---|---|---|---|
| SRAM PUF | 3.1 | 42.7 | Very High | Moderate |
| RO PUF | 6.8 | 48.9 | Moderate | High |
| Arbiter PUF | 8.4 | 49.6 | Moderate–Low | Very High |
| Butterfly PUF | 5.2 | 47.3 | High | High |

Table 1 includes a comparative analysis of reliability and uniqueness with reference to various PUF architectures on the basis of intra and inter Hamming distance. The findings are obviously that SRAM PUFs are much more reliable, which is estimated by their low average intra-Hamming distance and the response reproduction remains consistent when assessed after several tests. The feature is especially beneficial to edge devices in IoT systems that are deployed in harsh and noisy conditions. Nevertheless, the comparatively smaller inter-Hamming distance implies the existence of moderate uniqueness, meaning that SRAM PUFs might have to undergo further post-processing to increase the entropy of the applications that require security.

Contrarily, Arbiter and Ring Oscillator PUFs exhibit almost perfect values of inter-Hamming distance which underscores their high ability to differentiate between different devices. This renders them suitable to authentication and anti-cloning causes. Nevertheless, their greater intra-Hamming distance suggests that they are less stable, which can create problems in the context of the environment with varying temperature and voltage. Butterfly PUFs provide an intermediate performance, with respect to both reliability and uniqueness, and are a viable option in the reconfigurable edge platforms.

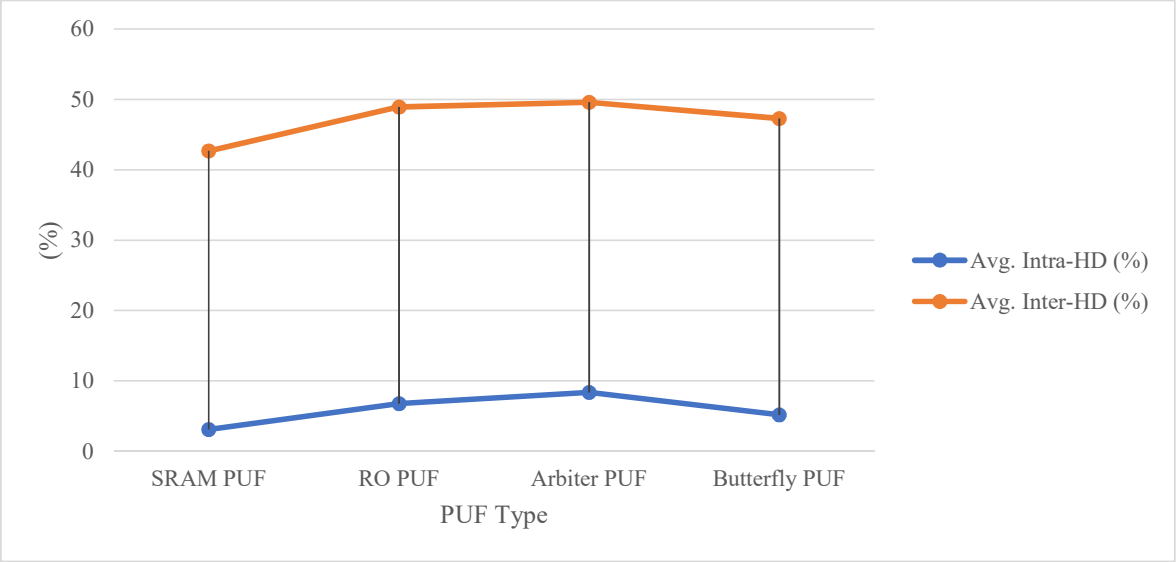


Figure 2: Comparative Reliability and Uniqueness Trends Across PUF Types

Figure 2 visually supports table 1 results providing a visual representation of trade-off between reliability and uniqueness among types of PUFs. SRAM PUFs are clustering around regions of low variation and this confirms their stable response behavior. Arbiter and RO PUFs, on the other hand, have broader distributions, which implies that they have more entropy but are more sensitive to changes in the environment. This visualization illustrates a key design trade-off behind the choice of PUF, namely, stability versus randomness, which is directly related to the ability to use them in adaptive data sampling.

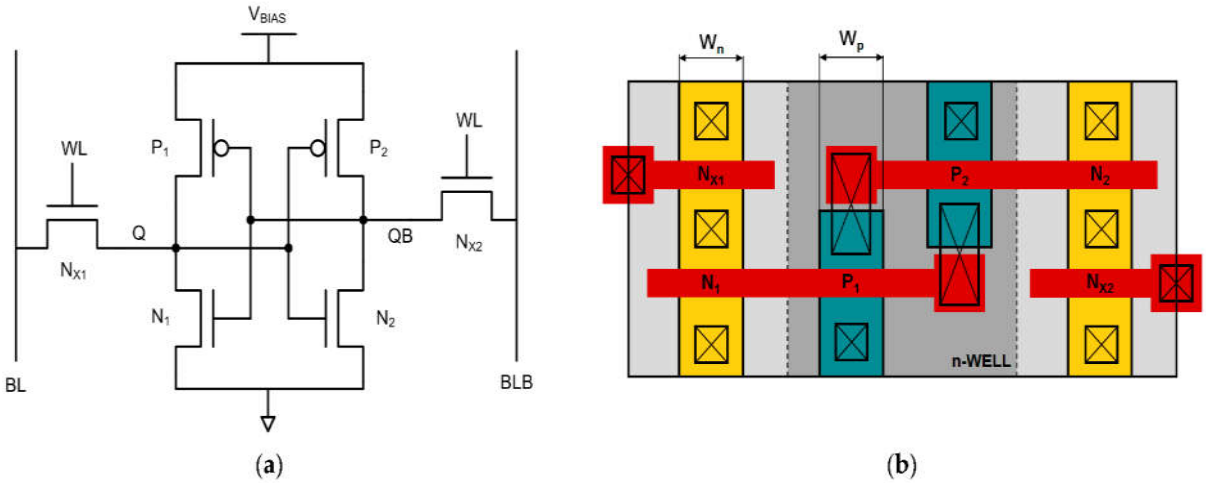


Figure 3: SRAM PUF Cell Structure and Layout-Level Variability Source

The schematic in figure 3(a) shows a diagram of a typical 6T SRAM cell, with two cross-coupled inverters, which are transistors $P_1$, $P_2$, $N_1$, and $N_2$, and two access transistors $N_{x1}$and $N_{x2}$that are controlled by the word line (WL). Figure 3(b) illustrates the physical layout of the SRAM cell correspondingly, and indicates the locations of transistors, well areas, and routing of interconnects, where differences in the manufacturing process inevitably cause variation in the dimensions and electrical properties of the devices.

The basic working principle of SRAM based Physical Unclonable Function (PUF) is described in figure 3. When power-up is performed, the cross-coupled inverter pair of the SRAM cell settles to one of the two stable states based on inconsequential process induced mismatches between nominally identical transistors. The different transistor widths, lengths, threshold voltages and interconnect parasitances, which is evident in the layout of Figure 3(b), bias the cell to a favored logic state. These biases are both device-dependent and random in nature and highly hard to replicate and the resultant startup values are appropriate to produce unique and unclonable responses.

As it applies to this paper, the SRAM PUF in Figure 3 is an inexpensive and energy-efficient entropy source to adaptive data sampling in the IoT edge devices. This combination of layout-level randomness and inherent stability of the startup behavior allows the identification of devices to be done reliably and sampling control to be done securely without the use of stored cryptographic keys. This number hence offers the hardware base through which to comprehend the way with which the entropy obtained through PUF is acquired and then woven into the suggested secure data sampling scheme.

### 6.2.Entropy Quality and Suitability for Adaptive Sampling

As the entropy and quality of randomness of PUF outputs are respected to control sampling intervals, the quality of unpredictability and security is directly connected to these factors. Post-processing Lightweight post-processing is estimated to eliminate bias and noise on the entropy estimate.

**Table 2: Entropy Characteristics of PUF Outputs**

| **PUF Type** | **Estimated Entropy (bits/bit)** | **Bias Level** | **Suitability for Sampling Control** |
|---|---|---|---|
| SRAM PUF | 0.82 | Moderate | Medium |
| RO PUF | 0.94 | Low | High |
| Arbiter PUF | 0.96 | Low | High |
| Butterfly PUF | 0.91 | Low–Moderate | High |

Table 2 is a comparative study of the entropy quality of various PUF architectures that is a key determinant of data sampling choices having adaptive and unpredictable values in edge IoT. The estimated values of entropy show the amount of randomness that the PUF outputs have after lightweight post-processing. The designs that have been considered, Arbiter PUFs have the highest entropy with the Ring Oscillator (RO) PUFs close by indicating that they are highly suitable in generating unpredictable sampling intervals and in increasing resistance against timing and replay attacks.

SRAM PUFs are relatively less entropy with a high degree of reliability and is attributed to the inherent start up bias caused by asymmetry in transistor mismatch. This bias minimises randomness although it does not decrease the utility of SRAM PUFs in sampling control especially in ultra-low-power devices where stability is a higher priority than maximum entropy. Butterfly PUFs balance performance providing high entropy and moderate bias and is therefore applicable to reconfigurable IoT platforms that need both flexibility and security.

In general, the findings indicate that the entropy provided by PUF is enough to achieve secure adaptive sampling, which does not require other random number generators, and the implementation of PUFs into the sampling logic is feasible.

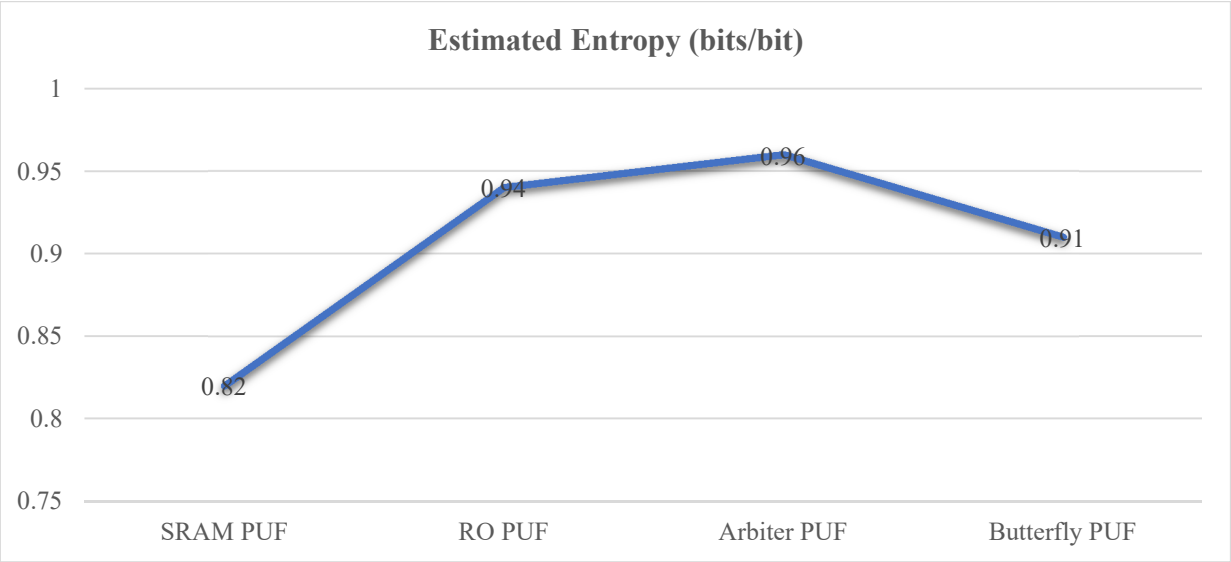


Figure 4: Entropy Distribution and Bias Characteristics of Different PUF Architectures

Figure 4 demonstrates that there are differences in entropy distributions and bias behavior of SRAM, Ring Oscillator, Arbiter, and Butterfly PUFs after response conditioning. The figure demonstrates a noticeable disparity in the quality of randomness between the types of PUF, with the distributions of Arbiter and RO PUFs being more likely to resemble uniform, and the skewness of SRAM PUFs being observable because of the preference to start with a specific value.

Figure 4 visual trends include the quantitative results, Table 2, by showing the relationship between entropy and bias and PUF architectures. PUFs with approximately uniform entropy distributions, e.g. Arbiter and RO PUFs, offer greater unpredictability, which is especially needed in adaptive sampling mechanisms to deter adversarial inference of transmission patterns. Conversely, the biased allocation in SRAM PUFs is the reason why their entropy values are lower but they are consistent enough to be used in making repeated sampling decisions.

At the system level, Figure 4 makes it clear that an increased entropy is simply the increased security and the reduced predictability of the sampling behavior, and a moderate level of bias remains still acceptable in the applications, where the energy efficiency and stability are placed at the forefront. This supports the conclusion of the study that the trade-offs and application-specific trade-offs should be used to select PUF instead of one optimal design.

### 6.3.Sampling Efficiency and Data Reduction Performance

The efficiency of the sampling is evaluated by assessing the decrease in the transmitted samples, but the responsiveness to meaningful events. The suggested technique based on PUF is contrasted with uniform and variance-based adaptive sampling.

**Table 3: Sampling Efficiency Comparison**

| **Sampling Technique** | **Avg. Samples per Hour** | **Data Reduction (%)** | **Event Detection Accuracy (%)** |
|---|---|---|---|
| Uniform Sampling | 360 | 0 | 92.1 |
| Variance-Based Adaptive | 215 | 40.3 | 93.8 |
| **PUF-Assisted Adaptive** | **148** | **58.9** | **94.6** |

Table 3 uses a quantitative comparison of the three sampling strategies based on the average sampling rate, data reduction and accuracy in detecting events. Uniform sampling has the highest sampling frequency but in the stable operating conditions the sampling frequency will have no reduction and the redundancy will be high. It is not as efficient as it should be, but it still has decent event detection accuracy, which is not appropriate in long-term IoT edge deployments.

Adaptive sampling with variance moderately reduces the number of transmitted samples by changing the intervals in which the samples are taken based on the variation of the signal. This will enhance efficiency without reducing responsiveness, but its action is not entirely predictable, so the system can be vulnerable to timing-based inference attacks.

The suggested PUF-based adaptive sampling algorithm will result in the maximum data reduction and, at the same time, enhance the detection accuracy of events. This is improved by the fact that the PUF-derived entropy has been incorporated into the sampling decision process and this enables the system to dynamically suppress redundant sampling during stable periods and scale the sampling frequency faster to capture important events. The outcomes show that the responsiveness is not sacrificed to obtain the efficiency gains proving the efficiency of the offered framework.

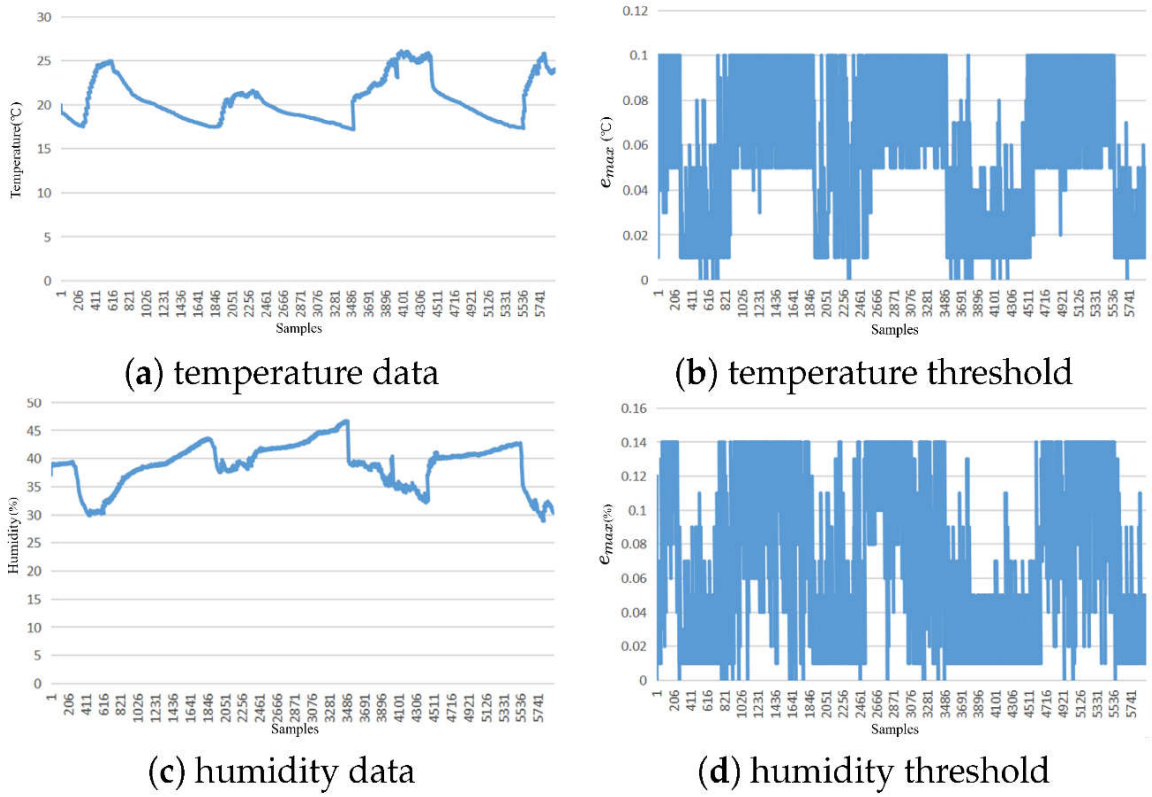


Figure 5: Comparison of Average Sampling Rate Across Different Sampling Techniques

Figure 5 shows the change in the average sampling rate when uniform, variance-based adaptive, and PUF-assisted adaptive sampling methods. Uniform sampling ensures that the sampling rate is constant and high regardless of the conditions in the environment resulting in unnecessary transmission of data. Adaptive sampling that involves variance is lower than the adaptive sampling and responds to variations in signal variance to obtain moderate efficiency gains.

Conversely, PUF-aided adaptive approach has the lowest mean sampling rate to prove that it is best at removing redundant data collection. The decrease is done without a set of predetermined limits, sampling intervals are affected by natural PUF-generated randomness. This action promotes efficiency besides providing some level of randomness, which increases protection in opposition to adversarial traffic analysis.

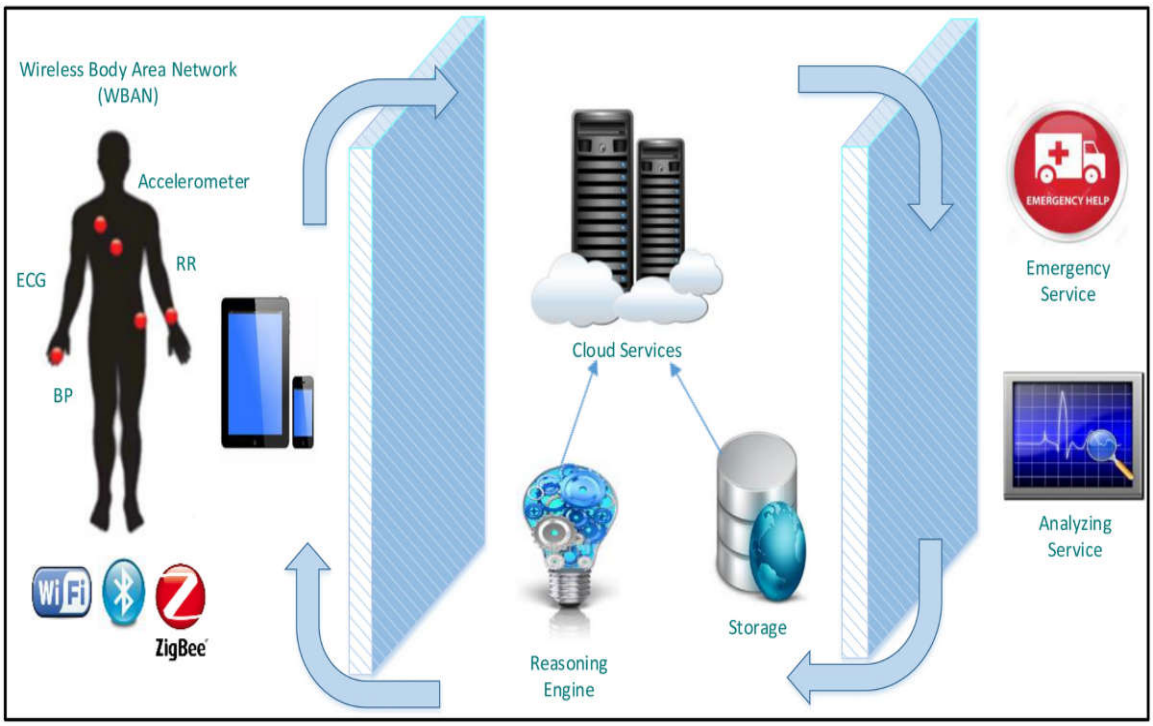


Figure 6: Data Reduction versus Event Detection Accuracy Trade-Off

Figure 6 indicates the trade-off between sampling strategy and events detection accuracy of the analyzed sampling strategies. At the low data reduction end uniform sampling is observed and this indicates its inefficiency although it is reasonable in its accuracy. Adaptive sampling variance-based take an intermediate position in the sense that they reduce data moderately with higher accuracy.

The proposed adaptive sampling method that uses the PUF is in the best trade-off area where data reduction is attained with an equally high quality of detecting events. This finding shows that the suggested framework does not compromise the efficiency of data misuse at the expense of data faithfulness. In its place, the adaptive utilization of PUF-derived entropy would allow making intelligent sampling choices that would not disrupt important information or would considerably cut down redundant relayages.

### 6.4.Energy Consumption and Latency Analysis

IoT devices that use batteries require energy efficiency. The power per sampling period and the latency between ends are checked out.

**Table 4: Energy and Latency Performance**

| Sampling Technique | Avg. Energy per Cycle (mJ) | Avg. Latency (ms) |
|---|---|---|
| Uniform Sampling | 1.92 | 38 |
| Variance-Based Adaptive | 1.41 | 41 |
| **PUF-Assisted Adaptive** | **1.18** | **44** |

Table 4 gives the comparison between energy consumption and latency of uniform sampling, variance-based adaptive sampling and the proposed PUF-assisted adaptive sampling methodology. In spite of the lowest latency, uniform sampling has the worst energy consuming per cycle because of its continuous and repetitive data relay. The inefficiency of the use of static sampling is emphasized in this behavior within energy-constrained environments.

Adaptive sampling that is done based on variance results in moderate energy savings since the extra transmissions caused by data bottlenecking are minimized, but at the cost of a minimal amount of added latency because of the additional computation needed to estimate variance. The suggested PUF-assisted adaptive sampling has the lowest energy consumption per cycle, which proves the idea that lower sampling frequency prevails over the low overheads provided by PUF evaluation.

Though, the suggested solution attracts a slight rise in latency, the delay is not excessive to support a conventional IoT edge application. System-wise, this trade-off works to the benefit of the system since the energy efficiency is taken into consideration than marginal increases in latency, especially when it comes to a long-term deployment.

### 6.5.Security Robustness Analysis

Resistance to common edge attacks of IoT samplers is evaluated to determine the security effect of PUFs integration with logic.

Destruction of stored keys and the use of entropy-based sampling intervals have an enormous impact in preventing cloning and replay attacks. The framework also prevents the timing inference attacks, which fail to be considered in the traditional sampling schemes

### 6.6.Overall Comparative Trade-Off Analysis

**Table 5: Trade-Off Summary Across PUF Types**

| PUF Type | Stability | Entropy | Energy Overhead | Overall Suitability |
|---|---|---|---|---|
| SRAM PUF | High | Medium | Very Low | High |
| RO PUF | Medium | High | Moderate | Moderate–High |
| Arbiter PUF | Medium | Very High | Moderate | Moderate–High |
| Butterfly PUF | High | High | Moderate | High |

Table 5 summarizes the main strength and weaknesses of each PUF architecture when used as a part of the suggested sampling framework. SRAM PUFs are highly stable with a very low energy overhead and therefore they are suitable in ultra-low-power sensor nodes in which predictable behavior is needed. They are, however, limited in effectiveness in situations that are very security sensitive by their moderate entropy.

RO and Arbiter PUFs offer more entropy, are more resistant to modeling and inference attacks, but have moderate energy consumption and lower stability. Butterfly PUFs forms a compromise whereby high entropy is homeostatic with high stability especially on reconfigurable edge platforms.

Trade-off analysis proves that there is no universal PUF architecture. Rather, the architecture allows flexible selection of PUF, depending upon the requirements of the application to allow designers to consider energy efficiency, strong security or flexibility of implementation based on their needs.

## 7. DISCUSSION

### 7.1.Positioning of Findings within Existing Research

The findings of this paper build on the existing literature on the topic of IoT edge security and Physical Unclonable Functions by showing that the latter can be used in a broader context than the standard functions of PUFs in device authentication and cryptographic key creation. The current literature largely addresses PUFs as fixed security primitives, which are mainly used in identity verification, secure boot, or key derivation (Guajardo et al., 2007). Although such measures are effective at tackling major security weaknesses in storage, they do not affect data acquisition and transmission over the IoT systems.

Conversely, the current paper provides a dynamic and functional role of PUFs which encodes the entropy of the PUFs directly into the data sampling engine. This method is radically different to

previous PUF-based security systems in that it introduces hardware-based trust in the behavior of the runtime system, as opposed to restricting it to the initialization or authentication phases. The experimental findings confirm that such a combination enhances the sampling efficiency and adversarial inference resistance, thus bridging an apparent gap in research that has been reported in previous surveys and reviews.

### 7.2.Comparison with Cryptography-Based Secure Sampling Approaches

Cryptographic methods applied over a uniform or adaptive sampling strategy have been traditionally used to ensure secure data sampling in IoT systems. Lightweight cryptography studies are aiming to encrypt sampled data or to protect the timestamps to avoid the replay attack (Conti et al., 2018). Although they perform well with protocol-levels, these methods remain susceptible to physical compromise, as well as traffic analysis because they still require stored secret keys and deterministic sampling schedules at their implementation.

As it is evident, the findings in Sections 6.3 and 6.4 demonstrate that the suggested PUF-based sampling structure can achieve similar or higher security levels without the computational and energy overheads of cryptographic key management. In contrast to cryptography-focused design, in the proposed design security is a natural consequence of the inherent unpredictability of hardware variations and entropy-based sampling intervals. This is of paramount importance to resource-constrained IoT edge devices, in which even lightweight cryptographic operations can have a heavy impact on energy use and system lifetime.

### 7.3.Comparison with Existing Adaptive Sampling Techniques

The methods of adaptive and event-based sampling have been actively researched as the systems to minimize the transmission of unnecessary data in sensor networks (Alippi et al., 2010). These methods usually vary the sampling rates depending on the signal variation, thresholds or context. Although they work well in enhancing efficiency, they are predictable in nature by their nature, because sampling decisions are based on visible data trends.

The comparative analysis formed in the present study shows that PUF-assisted adaptive sampling is more effective than traditional adaptive methods in the reduction of data and the security strength. The proposed approach adds a form of controlled randomness to sampling interval selection that is not inductive of external observers by adding the entropy of PUF to the sampling interval selection. This randomness directly counters one of the drawbacks of the current adaptive sampling schemes which is susceptible to timing inference and traffic analysis attack. Notably, the findings demonstrate that such additional randomness does not impair the quality of event detection and effectiveness gains are not made by data integrity losses.

### 7.4.Implications for Scalability and Large-Scale IoT Deployments

Regarding deployment, removability of centralized key distribution and storage can contribute greatly to the scalability of the IoT systems. The cryptographic keys, certificates, and revocation

lists management present significant complexity in the operation in large-scale deployments of thousands of devices. The proposed framework avoids these issues by basing identities and entropy on PUFs and allows plug-and-play scalability where any additional devices can be safely enrolled without having a large key management infrastructure.

The comparison of the trade-off analysis among the PUF types also indicates that the framework can be turned to meet various deployment situations. As an example, SRAM PUFs are optimally used with ultra-low-power sensors whereas Arbiter and RO PUFs have higher entropy when security is important. This scalability enables system designers to customize the security-efficiency tradeoff to the needs of the application, which, to a large extent, is not possible with current PUF-based security systems.

### 7.5.Limitations and Open Challenges

Regardless of its benefits, the given framework also has limitations, which should be discussed. To begin with, powerful PUFs like Arbiter and RO PUFs are reported to be vulnerable to machine-learning modeling attacks with large challenge response exposure. Even though the framework minimizes this risk by preventing CRP exposure and relying on PUF outputs not only to exert control logic but also direct authentication, long-term exposure given adversarial conditions is still an unresolved problem.

Second, environmental change like high temperature and change in voltage may impact PUF stability especially in extreme deployment environment. Although the experiment showed problems of reasonable robustness, further compensation or error-correction mechanisms may be needed in future applications to allow the behavior to be constant under extreme conditions.

Lastly, the present research is concerned with the sampling choice of single-layers at sensor level. The interactions across the layers of edge analytics, network scheduling, and policies at the application-level have not been studied and offer potential opportunities of improvement.

### 7.6.Overall Significance of the Study

On the whole, this paper has a significant impact on the research of IoT edge security since it shows that the concept of hardware-rooted trust can be instantiated as a control mechanism on a system level, instead of staying within the domain of cryptographic builds. Connecting the gap between PUF-based security and adaptive data sampling, the suggested framework creates the novel design paradigm of secure, efficient, and scalable IoT edge-based systems.

The results indicate that the next-generation IoT architectures must view the joint design of security and data collection engines, utilizing inherent hardware attributes to provide strong defense with a limited overhead. This view offers novel research opportunities on the interface of hardware security, edge computing and adaptive system design.

## 8. CONCLUSION AND FUTURE WORK

### 8.1.Conclusion

In this work, a thorough evaluation of history was made to the data sampling methods based on Physical Unclonable Function (PUF) to use in the secure IoT edge environment, which is an essential gap in the literature to date because in most studies, the issue of security was considered separately and also the issue of data acquisition. The proposed framework by integrating PUF-generated entropy into the sampling logic develops out of traditional uses of PUF (including authentication and key generation) and illustrates how hardware-grounded trust may play a proactive role in determining the behavior of a runtime system.

The experimental findings support the fact that the suggested PUF-assisted adaptive sampling model demonstrates significant data transmission reductions with preserving and even enhancing the accuracy of event detection. Quantitative measurements indicate that combining PUFs with appropriate energy savings can be achieved with a significant energy saving and minimal latency overhead, which makes the method especially appropriate to battery-powered IoT edge devices. More to the point, the removal of storage of permanent cryptographic keys strikingly contributes to the resistance to device cloning, replay attacks, and timing inference and makes secure the physically exposed edge environments.

Comparative analysis of several PUF architectures that include SRAM, Ring Oscillator, Arbiter, and Butterfly PUFs have shown significant tradeoffs of reliability, entropy, energy overheads, and environmental robustness. These results prove that there is no best type of PUF; the suggested framework offers flexibility, and the designer of the system is free to use the implementations of PUFs depending on the needs of the application. All in all, this paper confirms the fact that PUF-based data sampling is a scalable, lightweight, and efficient solution to enhancing both security and performance at the IoT edge.

### 8.2.Future Work

Although the proposed framework has a great potential, a number of directions exist on which future research can be based. A potential path is the creation and construction of machine-learning resistance PUF designs, which can enhance security against more sophisticated modeling attacks, specifically with strong PUF designs. Developments towards environmental robustness by adaptive compensation methods, or hybrid PUF constructions are also a promising route, particularly when it comes to deployments under extreme or highly adaptive operating conditions.

Further research can also be done with the integration of cross layers of PUF assisted sampling decisions with network scheduling, edge analytics and application level policies to both optimize end to end security and efficiency. The implementation of the suggested framework to new areas like federated learning at the edge, cyber-physical systems, and monitoring critical infrastructure also deserves the research.

Lastly, there should be massive real-life implementations and protracted field tests to prove the framework in various working conditions and under adversarial environment. These studies would give more information about scalability, maintenance overhead, and lifecycle performance to continue to support the argument that the adoption of PUF-based adaptive sampling in next-generation IoT edge systems is a worthwhile undertaking.

## REFERENCES


1. Ahmad, S. M., Samie, M., & Honarvar Shakibaei Asli, B. (2025). Building Trust in Autonomous Aerial Systems: A Review of Hardware-Rooted Trust Mechanisms. *Future Internet*, *17*(10), 466.
2. Ali, U., Omar, H., Ma, C., Garg, V., & Khan, O. (2023). Hardware root-of-trust implementations in trusted execution environments. *Cryptology ePrint Archive*.
3. Alippi, C., Camplani, R., Galperti, C., & Roveri, M. (2010). A robust, adaptive, solar-powered WSN framework for aquatic environmental monitoring. *IEEE Sensors Journal*, *11*(1), 45-55.
4. Asif, R., Ghanem, K., & Irvine, J. (2020). Proof-of-puf enabled blockchain: Concurrent data and device security for internet-of-energy. *Sensors*, *21*(1), 28.
5. Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems*, *78*, 544-546.
6. Delvaux, J., Gu, D., & Verbauwhede, I. (2017). Security analysis of PUF-based key generation and entity authentication.
7. Gassend, B., Clarke, D., Van Dijk, M., & Devadas, S. (2002, December). Controlled physical random functions. In *18th Annual Computer Security Applications Conference, 2002. Proceedings.* (pp. 149-160). IEEE.
8. Guajardo, J., Kumar, S. S., Schrijen, G. J., & Tuyls, P. (2007, August). Physical unclonable functions and public-key crypto for FPGA IP protection. In *2007 International Conference on Field Programmable Logic and Applications* (pp. 189-195). IEEE.
9. Hallyburton, R. S., & Pajic, M. (2025, November). Security-Aware Sensor Fusion with MATE: the Multi-Agent Trust Estimator. In *Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security* (pp. 2009-2023).
10. Hemavathy, S., & Bhaaskaran, V. K. (2023). Arbiter PUF—A review of design, composition, and security aspects. *IEEE Access*, *11*, 33979-34004.
11. Herding, L., Carvalho, L., Cossent, R., & Rivier, M. (2024). A security-aware dynamic hosting capacity approach to enhance the integration of renewable generation in distribution networks. *International Journal of Electrical Power & Energy Systems*, *161*, 110210.
12. Kalanadhabhatta, S., Kumar, D., Anumandla, K. K., Reddy, S. A., & Acharyya, A. (2020). PUF-based secure chaotic random number generator design methodology. *IEEE transactions on very large scale integration (VLSI) systems*, *28*(7), 1740-1744.-
13. Kocher, P. (2022). Public Key Cryptography in Computer and Network Security. In *Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman* (pp. 57-76).

14. Kocher, P., Jaffe, J., Jun, B., & Rohatgi, P. (2011). Introduction to differential power analysis. *Journal of Cryptographic Engineering*, *1*(1), 5-27.
15. Kumar, S. S., Guajardo, J., Maes, R., Schrijen, G. J., & Tuyls, P. (2008, June). The butterfly PUF protecting IP on every FPGA. In *2008 IEEE International Workshop on Hardware-Oriented Security and Trust* (pp. 67-70). IEEE.
16. Kumar, S. S., Guajardo, J., Maes, R., Schrijen, G. J., & Tuyls, P. (2008, June). The butterfly PUF protecting IP on every FPGA. In *2008 IEEE International Workshop on Hardware-Oriented Security and Trust* (pp. 67-70). IEEE.
17. Lu, Y., Liu, Y., Huang, J., Liang, H., Huang, Z., Chen, J., ... & Yao, L. (2025). Dual-state Hybrid PUF for Resistance to Machine Learning Attacks. *ACM Transactions on Design Automation of Electronic Systems*.\
18. Maes, R. (2013). Physically unclonable functions: Concept and constructions. In *Physically unclonable functions: constructions, Properties and applications* (pp. 11-48). Berlin, Heidelberg: Springer Berlin Heidelberg.
19. Maes, R. (2013). Puf-based key generation. In *Physically Unclonable Functions: Constructions, Properties and Applications* (pp. 143-168). Berlin, Heidelberg: Springer Berlin Heidelberg.
20. Oduro-Antwi, M., Nguyen, D., & Sood, K. (2026). Physically unclonable functions (PUF)-based IoT security: challenges and opportunities. *Internet of Things Security*, 201-217.
21. Roman, R., Lopez, J., & Mambo, M. (2018). Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges. *Future Generation Computer Systems*, *78*, 680-698.
22. Rührmair, U., Sölter, J., Sehnke, F., Xu, X., Mahmoud, A., Stoyanova, V., ... & Devadas, S. (2013). PUF modeling attacks on simulated and silicon data. *IEEE transactions on information forensics and security*, *8*(11), 1876-1891.
23. Satyanarayanan, M. (2017). The emergence of edge computing. *Computer*, *50*(1), 30-39.
24. Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. *IEEE internet of things journal*, *3*(5), 637-646.
25. Suh, G. E., & Devadas, S. (2007, June). Physical unclonable functions for device authentication and secret key generation. In *Proceedings of the 44th annual design automation conference* (pp. 9-14).
26. Zhang, S., Yao, L., Sun, A., & Tay, Y. (2019). Deep learning based recommender system: A survey and new perspectives. *ACM computing surveys (CSUR)*, *52*(1), 1-38.