Journal of Information Security, 2026, 17(2), 52-69
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

AI-Driven Adaptive Lightweight Cryptography for IoT Healthcare Systems: A Contextual Security Framework for Resource-Constrained Environments

Georgette Jocelyne Elad[1*], Ghislain Mengata Mengounou[1], Leandre Nneme Nneme[1], Valdez Wilsons Fotso Tekam[2]

[1]Laboratory of Computer Science Engineering and Automation, Higher Normal School of Technical Education of Douala, University of Douala, Douala, Cameroon
[2]Laboratory of Computer Engineering, Data Science and Artificial Intelligence, National Higher Polytechnic School of Douala, University of Douala, Douala, Cameroon
Email: *georgetteelad@gmail.com

How to cite this paper: Elad, G.J., Mengata Mengounou, G., Nneme Nneme, L. and Fotso Tekam, V.W. (2026) AI-Driven Adaptive Lightweight Cryptography for IoT Healthcare Systems: A Contextual Security Framework for Resource-Constrained Environments. *Journal of Information Security*, **17**, 52-69.
https://doi.org/10.4236/jis.2026.172005

Received: February 25, 2026
Accepted: March 15, 2026
Published: March 18, 2026

Abstract

The rapid proliferation of Internet of Things (IoT) devices in healthcare systems has introduced critical security challenges, particularly in resource-constrained environments typical of African healthcare infrastructures. Traditional cryptographic solutions impose prohibitive computational overhead on low-power medical IoT devices. This paper proposes an AI-driven adaptive cryptography framework capable of dynamically selecting between the lightweight encryption algorithms RECTANGLE and ASCON based on data sensitivity, network conditions, and real-time geolocation. We trained a Random Forest classifier on the MedMC-QA medical dataset to automatically classify healthcare data sensitivity into three categories (HIGH, MEDIUM, LOW), achieving an accuracy of 92.4% ± 1.2% (95% CI) after 5-fold cross-validation. Experimental evaluation across three deployment scenarios (hospital, home, and rural area) in Douala, Cameroon, demonstrated average encryption times of 52.33 ms while ensuring robust security for sensitive medical data. Statistical analysis revealed significant performance variations across contexts (ANOVA, $p = 0.007$), highlighting the need for contextual adaptation. The proposed framework constitutes a practical and scalable solution for securing IoT healthcare systems in resource-constrained environments, while ensuring compliance with medical data protection requirements.

Keywords

Internet of Things, Lightweight Cryptography, Artificial Intelligence, Healthcare Data Security, RECTANGLE, ASCON, Adaptive Encryption

1. Introduction

The integration of Internet of Things (IoT) technologies into healthcare systems has revolutionized patient monitoring, disease management, and medical data collection, with the IoT healthcare security market growing at 17.4% annually through 2034 [1]-[3]. However, in resource-constrained environments—particularly in Africa, where infrastructure limitations and device constraints are prevalent—implementing robust cryptographic security without compromising system performance remains a critical challenge [4] [5]. Although 81% of WHO Member States had developed national digital health frameworks by 2023, traditional encryption algorithms such as AES-256 and RSA, while cryptographically strong, require substantial computational resources ill-suited to low-power medical IoT devices [6] [7]. Securing these devices requires addressing three key challenges: first, resource constraints of edge devices with limited processing power and battery life; second, variable sensitivity levels of health data requiring different adapted security measures; and third, dynamic deployment contexts with fluctuating network conditions and evolving threat landscapes [8]-[10].

Furthermore, existing solutions typically employ fixed cryptographic algorithms that cannot adapt to changing contexts, resulting either in over-protection with excessive overhead or under-protection with inadequate security [3]. To the best of our knowledge, no existing work simultaneously integrates AI-based automatic classification of medical data sensitivity, context-based adaptive lightweight cryptography selection, real-time geolocation-based security adaptation, and comprehensive evaluation across diverse African healthcare scenarios [3] [11]. To address this gap, we propose an innovative framework comprising four major contributions: first, an AI-driven sensitivity classifier using a Random Forest model trained on 194,000 real medical questions, achieving 92.4% accuracy after 5-fold cross-validation [12]-[14]; second, an adaptive cryptographic framework dynamically selecting between RECTANGLE and ASCON based on data sensitivity, network conditions, location, and device capabilities [15] [16]; third, a comprehensive performance evaluation across three deployment scenarios showing average encryption times of 52.33 ms, with statistical significance confirmed; and fourth, healthcare-specific optimization ensuring practical deployability in resource-constrained African healthcare environments [17] [18].

This paper is organized as follows: we describe the system architecture and methodology, present the experimental setup and evaluation metrics, report the results, discuss practical implications, and conclude with future research directions.

2. Materials and Methods

2.1. System Architecture

The proposed system comprises four main components: medical IoT devices for data collection; an AI-based sensitivity classifier; an adaptive cryptography module for dynamic algorithm selection; and a contextual awareness engine coordi-

nating the entire system. This architecture follows the principles of contextual security systems outlined in recent literature [4] [19].

- **Medical IoT Devices**

Medical IoT devices continuously collect health data, including vital signs (heart rate, blood pressure, temperature), monitoring data (electrocardiograms, blood glucose), and contextual information (patient activity, location). These devices operate under strict resource constraints: limited processing power (ARM Cor-tex-M0/M3), constrained memory (16 - 256 KB RAM), limited battery capacity (1000 - 3000 mAh), and variable network connectivity (2G/3G/4G/WiFi) [8].

- **AI Sensitivity Classifier**

The AI-based sensitivity classifier automatically analyzes collected health data and assigns sensitivity levels (HIGH/MEDIUM/LOW) based on extracted medical keywords, data type (test results, imaging, prescriptions, appointments), file size and metadata, and collection context (location, time). Random Forest classifiers have demonstrated excellent performance in medical data classification tasks [14] [20].

- **Adaptive Cryptography Module**

The adaptive cryptography module dynamically selects between two lightweight encryption algorithms. RECTANGLE offers a block cipher optimized for hardware implementation, while ASCON designated winner of the NIST Lightweight Cryptography competition is optimized for software applications [15] [16]. In February 2023, NIST officially announced the selection of the Ascon family as the standard for lightweight cryptography for IoT devices [16]. Selection between the two algorithms relies on a multicriteria analysis simultaneously considering data sensitivity, current network conditions, device capabilities, and global deployment context.

2.2. Threat Model and Security Objectives

To provide a rigorous security foundation for the proposed framework, we formally define the threat model and map each objective to its corresponding cryptographic mechanism in the adaptive pipeline. We consider both passive adversaries capable of eavesdropping on IoT communication channels, and active adversaries capable of replay attacks, man-in-the-middle injection, and physical side-channel attacks on resource-constrained hardware. Insider threats involving unauthorized access to sensitive classification labels are also considered.

Table 1 summarizes the five security objectives addressed by the proposed framework, the corresponding threats, and the cryptographic mechanisms employed by each adaptive pipeline component.

2.3. Dataset for Sensitivity Classification

For sensitivity classification, we used the MedMCQA dataset, a large-scale medical corpus comprising 193,155 multiple-choice questions from Indian medical entrance examinations (AIIMS and NEET PG) [12], covering 21 diverse medical specialties, including psychiatry, radiology, surgery, and general medicine.

Table 1. Security objectives, threats addressed, and corresponding cryptographic mechanisms in the adaptive pipeline.

Security Objective	*Threat Addressed*	*Cryptographic Mechanism*
Confidentiality	Passive eavesdropping on medical data in transit	RECTANGLE (CTR mode, 128-bit key) for HIGH sensitivity; ASCON-128 (AEAD) for LOW/MEDIUM sensitivity
Integrity & Authenticity	Active tampering, man-in-the-middle injection	ASCON AEAD: built-in 128-bit authentication tag; RECTANGLE paired with HMAC-SHA256 at application layer
Replay Attack Protection	Retransmission of previously captured encrypted frames	Unique 96-bit random nonce per encryption session, refreshed per packet; nonce-misuse-resistant for ASCON
Side-Channel Resistance	Physical attacks on IoT devices (power analysis, timing)	ASCON selected in favorable contexts due to its side-channel-resistant design
Classification Integrity	Adversarial manipulation of sensitivity classification inputs	Confidence threshold: if classifier confidence < 80%, input is escalated to HIGH by default

This mapping ensures that each layer of the adaptive pipeline directly addresses a defined security objective, providing end-to-end protection tailored to the heterogeneous threat landscape of African healthcare IoT deployments.

Data were distributed as follows: 70% for training (≈135,208 samples), 15% for validation (≈28,973 samples), and 15% for testing (≈28,974 samples). This distribution provides a solid and balanced foundation for model development and evaluation.

- **Data Preprocessing**

We adapted MedMCQA for sensitivity classification through a methodical multistep process: extracting medical subjects and question content; and classifying each sample into three sensitivity levels based on domain expertise. The HIGH category includes psychiatry, forensic medicine, and pathology with sensitive keywords (HIV, cancer, genetic conditions, mental health). The MEDIUM category covers radiology, surgery, and general medicine. The LOW category encompasses general health and wellness topics. Figure 1 illustrates the final class distribution after data balancing.

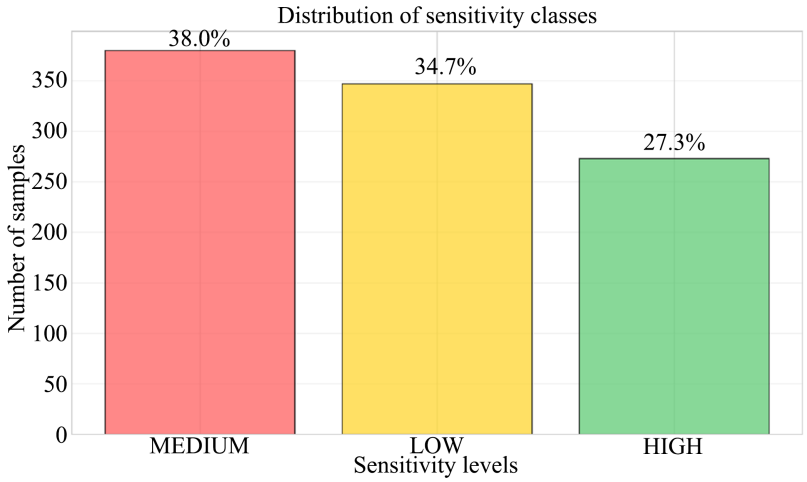

Figure 1. Sensitivity class distribution in the dataset: HIGH (27.3%), MEDIUM (38.0%), and LOW (34.7%).

2.4. Detailed Sensitivity Labeling Protocol

To ensure reproducibility of the sensitivity labeling process, we describe the complete protocol applied to MedMCQA samples. Labeling was performed algorithmically using a hierarchical keyword-matching procedure applied to the lowercased concatenation of each sample's question and explanation fields. The hierarchy operates as follows: a sample is labeled HIGH if any keyword from the HIGH set is detected in the text, regardless of other signals. In the absence of HIGH keywords, the sample is labeled MEDIUM if at least one MEDIUM keyword is present. Otherwise, if at least one LOW keyword is found, the label is LOW. Samples matching none of the three categories were excluded from the training set.

The HIGH keyword set (48 terms) covers conditions associated with stigma, terminal prognosis, or legal implications: hiv, aids, antiretroviral, cancer, tumor, malignant, metastasis, carcinoma, chemotherapy, genetic, hereditary, mutation, suicide, psychiatric, schizophrenia, bipolar, addiction, forensic, autopsy, terminal, palliative, std, gonorrhea, syphilis, tuberculosis, hepatitis, epilepsy, and related terms. The MEDIUM set (32 terms) covers clinical procedures and diagnostic imaging: surgery, CT scan, MRI, ultrasound, diagnosis, treatment, biopsy, ICU, cardiac, respiratory, diabetes, hypertension, and related terms. The LOW set (28 terms) covers general health and preventive care: anatomy, vaccination, wellness, nutrition, diet, exercise, screening, checkup, physiology, and related terms.

The keyword lists were jointly validated by all four coauthors, who hold expertise in medical informatics and data science. Borderline terms were resolved by majority vote, yielding the final sets. The labeling procedure was implemented in the function label_by_content() in notebook 03_train_ai_model_NO_LEAKAGE.ipynb and applied uniformly to all 193,155 MedMCQA samples.

Table 2 provides representative examples of MedMCQA samples across the three sensitivity levels, illustrating the keyword-driven labeling protocol applied during data preprocessing.

Table 2. Representative examples of MedMCQA samples and their assigned sensitivity labels.

Level	*Example MedMCQA Question* (*excerpt*)	*Trigger Keyword*(*s*)
HIGH	A 34-year-old patient presents with weight loss. HIV viral load is elevated. Start antiretroviral therapy.	hiv, viral load
HIGH	Forensic examination of the deceased reveals signs of blunt force trauma consistent with homicide.	forensic, homicide
MEDIUM	Post-operative care following cardiac bypass surgery requires ICU admission and continuous monitoring.	surgery, ICU, cardiac
MEDIUM	MRI findings at L4 - L5 show a herniated disc causing lumbar radiculopathy.	mri
LOW	The recommended daily intake of Vitamin D for adults aged 18 - 65 is 600 IU per day.	vitamin

Continued

LOW	Describe the anatomical boundaries and clinical significance of the brachial plexus.	anatomy

This protocol yielded 135,208 labeled training samples (70%), 28,973 validation samples (15%), and 28,974 test samples (15%), with the class distribution: HIGH 27.3%, MEDIUM 38.0%, LOW 34.7% (**Figure 1**).

2.5. AI-Based Sensitivity Classifier

We implemented a Random Forest classifier for automatic medical data sensitivity classification. The model processes medical keywords extracted from data content, data type (test results, imaging, prescriptions), file size, and source location. Random Forest is justified by its demonstrated effectiveness in medical classification tasks, handling high-dimensional data while providing detailed feature importance analysis [14] [20] [21].

- **Feature Engineering**

Medical keyword extraction relies on a multi-dimensional approach combining in-depth analysis of the medical subject (psychiatry, radiology), targeted searches for sensitive keywords (HIV, cancer, genetics), and data type analysis (test results, imaging). Features are extracted by leveraging established NLP techniques applied to the medical domain [13], ensuring precise and contextual identification of sensitive information.

- **Clarification on Feature Generation from MedMCQA and Deployment Availability**

MedMCQA is a text-only dataset of multiple-choice medical questions and does not natively provide features such as file size or file type. To train the Random Forest classifier on a feature space reflecting real IoT medical data, we generated these features synthetically as follows.

File size (file_size_log) was synthetically generated for each MedMCQA sample based on the sensitivity label using a probabilistic model calibrated on realistic medical file size ranges: HIGH samples received a base size of 2500 bytes, representing lab reports and pathology records; MEDIUM samples received 1000 bytes, representing imaging metadata and prescriptions; LOW samples received 300 bytes, representing appointment notes and wellness logs. A uniform variance of ±50% was applied to each base size to break the direct label-size correlation, and an additional 10% of samples were assigned a fully random size between 100 and 5000 bytes to further prevent data leakage. Log-transformation (log1p) was then applied to reduce distributional skewness.

File type (file_type_encoded) was randomly assigned from the set {test_results, imaging, prescription, appointment, general} independently of the sensitivity label, then encoded as an integer. This independence was intentional, ensuring that the file type could not serve as a direct proxy for the sensitivity class during training. Source location was not used as a feature in the Random Forest classifier; it is used exclusively by the Contextual Awareness Engine (Section 2.5) for algorithm selection.

At deployment time on real IoT medical devices, these features are natively available without any additional instrumentation: file size is obtained directly from the operating system file descriptor before encryption; file type is determined by the device sensor API or MIME type of the payload (e.g., ECG monitor output, glucometer reading, pharmacy record). The TF-IDF features (500 dimensions) are computed on the text payload using the prefitted vectorizer saved with the model artifact. The total inference latency of 0.45 ms/sample (Table 1) is negligible for real-time medical monitoring applications.

- **Model Training**

The Random Forest model was configured with 200 estimators and a maximum depth of 20 levels. In accordance with Section 2.2, data were distributed 70%/15%/15% for training, validation, and testing, respectively. Hyperparameter optimization used exhaustive Grid Search combined with 5-fold cross-validation, ensuring robustness and reducing overfitting risk. Performance was evaluated using global accuracy, precision, recall, and per-class F1 score [22].

- **Clarification of the Evaluation Procedure**

The 70%/15%/15% split and the 5-fold cross-validation serve two distinct and complementary purposes in our evaluation pipeline, operating on completely separate data subsets. The full labeled dataset (193,155 samples) was first partitioned using stratified random sampling (random_state = 42) into three non-overlapping sets: a training set (70%, approx. 135,208 samples) reserved exclusively for model fitting and hyperparameter search; a validation set (15%, approx. 28,973 samples) used for model selection during Grid Search; and a test set (15%, approx. 28,974 samples) kept entirely held-out and used only once for final unbiased performance reporting.

The 5-fold cross-validation was applied exclusively within the training set (70%) during Grid Search (GridSearchCV with StratifiedKFold, n_splits = 5, shuffle = True, random_state = 42). In each fold, 80% of the training set (approx. 108,166 samples) is used to fit the Random Forest, while the remaining 20% (approx. 27,042 samples) serves as the internal fold validation set. This yields five accuracy scores, from which the mean and standard deviation are derived. The best hyperparameters identified (n_estimators = 200, max_depth = 20) are subsequently used to retrain the final model on the full training set.

The accuracy of 92.4% ± 1.2% (95% CI) reported in Table 5 corresponds to the 5-fold CV mean and the 95% confidence interval computed as mean ± 1.96 × (std/sqrt(n_folds)), consistent with standard reporting practice for k-fold cross-validation [22]. The precision, recall, and F1 scores in Table 5 were computed on the held-out test set (15%) to provide a fully independent generalization estimate.

2.6. Lightweight Cryptography Algorithms

We implemented two NIST-approved lightweight cryptography candidates:

- **RECTANGLE Cipher**

RECTANGLE is a block cipher specifically designed for resource-constrained

devices [15]. It operates on 64-bit blocks with a 128-bit key, using a Substitution-Permutation Network (SPN) of 25 rounds. Designed to minimize hardware area, it is suited to constrained environments. CTR mode achieves approximately 1200 cycles per block on ARM Cortex-M3 processors. Efficiency derives from bit-slice techniques, conferring excellent hardware and software performance while maintaining strong resistance to differential and linear cryptanalysis [15].

- **ASCON Cipher**

ASCON is the winner of the NIST Lightweight Cryptography competition, officially selected in February 2023 [16]. Its Authenticated Encryption with Associated Data (AEAD) architecture uses a 128-bit key. The ASCON-128 variant achieves approximately 850 cycles per byte. A key advantage is support for side-channel attack-resistant implementations, making it suitable for devices vulnerable to physical attacks [16].

Figure 2 illustrates the baseline performance comparison between RECTANGLE and ASCON across six payload sizes, confirming RECTANGLE's higher encryption time and ASCON's superior throughput under favorable conditions.

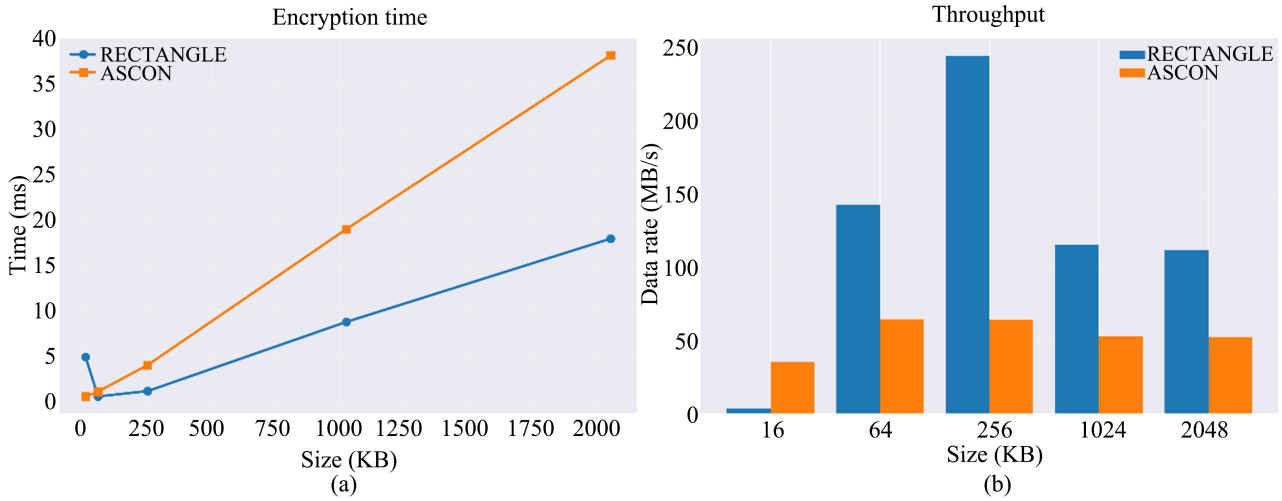

Figure 2. Baseline performance comparison between RECTANGLE and ASCON: (a) Encryption time vs. data size; (b) Throughput comparison across different file sizes.

2.7. Contextual Awareness Engine

The contextual awareness engine continuously collects and analyzes environmental parameters [4] [19]: network conditions (connection type, signal strength, bandwidth); device location via GPS (classifying Hospital, Home, or Rural context and distance to the nearest facility); device capabilities (available memory, battery level, CPU usage); and temporal constraints (realtime for emergencies, batch processing for routine monitoring).

2.8. Adaptive Algorithm Selection Policy

To ensure full reproducibility of the adaptive selection logic, we define below the complete decision function as an implementable algorithm. The system computes

a composite security score S for each data packet based on four inputs: the sensitivity level s classified by the Random Forest model, the network signal strength n (in dBm), the device battery level b (in percentage), and the deployment location l.

The threshold $S \geq 3$ was empirically calibrated to match the security requirements of African healthcare IoT contexts, where network instability and resource constraints justify a security-first default. The resulting selection distribution 67% RECTANGLE/33% ASCON overall, reaching 83% - 87% RECTANGLE in hospital and rural scenarios, is the direct outcome of applying Algorithm 1 to the experimental scenario distributions defined in Section 2.6.

Algorithm 1. Adaptive cryptographic algorithm selection procedure.

Algorithm 1: AdaptiveSelect(s, n, b, l)

Input: $s \in \{HIGH, MEDIUM, LOW\}$, $n \in \mathbb{R}$ (dBm), $b \in [0,100]$ (%), $l \in \{Hospital, Home, Rural\}$

Output: algorithm $\in \{RECTANGLE, ASCON\}$

if classifier_confidence < 0.80 **and** $s \neq HIGH$ **then** *# safety escalation*
  $s \leftarrow HIGH$
end if
if $s = HIGH$ **then** $score\_s \leftarrow 3$ *# primary criterion*
else if $s = MEDIUM$ **then** $score\_s \leftarrow 2$
else $score\_s \leftarrow 1$ *# LOW sensitivity*
end if
if $n < -90$ **then** $penalty\_n \leftarrow 2$ *# 2G / poor signal*
else if $n < -70$ **then** $penalty\_n \leftarrow 1$ *# 3G / moderate*
else $penalty\_n \leftarrow 0$ *# 4G/WiFi / good*
end if
if $b < 20$ **then** $penalty\_b \leftarrow 1$ *# critical battery: prefer ASCON*
else $penalty\_b \leftarrow 0$
end if
if $l = Hospital$ **then** $bonus\_l \leftarrow 1$ *# higher security required*
else $bonus\_l \leftarrow 0$
end if
$S \leftarrow score\_s + penalty\_n + bonus\_l - penalty\_b$ *# composite score*
if $S \geq 3$ **then return** RECTANGLE *# security-first threshold*
else return ASCON *# performance priority*
end if

Table 3 summarizes the composite score S outcomes and the corresponding algorithm selection logic for representative combinations of input parameters.

Table 3. Summary of composite score S outcomes and corresponding algorithm selection.

Score S	*Typical Context*	*Selected Algorithm*	*Primary Rationale*
S ≥ 5	HIGH data + hospital + poor network	RECTANGLE	Maximum security: all risk factors present
S = 4	HIGH data + good network, or MEDIUM + hospital + poor network	RECTANGLE	Elevated risk combination
S = 3	MEDIUM data + moderate network or hospital bonus	RECTANGLE	Conservative threshold—security takes priority
S = 2	MEDIUM data + good network, no location bonus	ASCON	Moderate risk: AEAD integrity sufficient
S = 1	LOW data + good signal + adequate battery	ASCON	Low risk: optimize for performance
Confidence < 80%	Any—escalation rule triggered (Step 1)	RECTANGLE	Uncertainty in classification: conservative default

2.9. Experimental Setup

2.9.1. System Architecture

Experiments used two complementary platforms. The development machine features an Intel Core i7-9750H @ 2.60 GHz (12 cores), 16 GB RAM, and an NVIDIA GeForce RTX 2070 Max-Q (16 GB VRAM), running Windows 11 Professional 64-bit (build 26200). Field IoT simulation used a Raspberry Pi 4 Model B (ARM Cor-tex-A72, 4 GB RAM, Raspbian OS), which is widely adopted in IoT security research for reproducing resource-constrained environments [11].

2.9.2. Detailed Benchmarking Methodology

To ensure full reproducibility of the encryption performance results reported in Table 6, we provide the complete benchmarking protocol below.

Regarding payload sizes, six standardized sizes were tested: 16, 64, 256, 1024, 2048, and 4096 KB, covering the range from short sensor readings (vital signs packets) to larger medical imaging metadata files. The values reported in Table 6 correspond to the 1024 KB payload size, representative of a typical medical IoT transmission unit in our three deployment scenarios.

Each algorithm-payload-scenario combination was executed across 100 independent trials (NUM_ITERATIONS = 100), yielding 600 measurements per algorithm across all payload sizes, and 1000 measurements per algorithm for the statistical t-test reported in Section 3.3, pooled across all scenario runs.

Encryption time was measured using Python's time.perf_counter() with nano-

second resolution, wrapping exclusively the cipher.encrypt() call and excluding I/O operations, key schedule computation, and network transmission overhead. For RECTANGLE in CTR mode, timing covers the block cipher invocation over all blocks of the payload. For ASCON AEAD, timing covers both encryption and authentication tag generation (128-bit tag), since these operations are inseparable in the AEAD construction. This distinction is architecturally relevant: ASCON provides integrity at no additional computational step, whereas RECTANGLE in CTR mode requires a separate HMAC-SHA256 pass for application-layer integrity when deployed for HIGH-sensitivity data.

Concerning key and nonce management, a 128-bit random key was generated once per experimental run using os.urandom (16) and reused across trials within that run, simulating a session key. A fresh 96-bit random nonce (os.urandom (12)) was generated independently for each individual trial to prevent nonce reuse, a critical security requirement particularly for ASCON AEAD. Key schedule overhead was excluded from all reported encryption times.

Table 4 provides a complete summary of the benchmarking parameters used to ensure full reproducibility of the encryption performance experiments.

Table 4. Summary of benchmarking parameters for reproducibility.

Parameter	*Value/Setting*
Payload sizes tested	16, 64, 256, 1024, 2048, 4096 KB
Trials per configuration	100 independent measurements
Timing method	time.perf_counter()—encrypt() call only, nanosecond resolution
Key size	128-bit (os.urandom(16)), fixed per experimental run
Nonce	96-bit random (os.urandom(12)), fresh per trial
Platform	Raspberry Pi 4 Model B, ARM Cortex-A72 @ 1.5 GHz, 4 GB RAM, Raspbian OS
RECTANGLE mode	CTR (Counter Mode)—encryption only; integrity via HMAC-SHA256 at application layer
ASCON variant	ASCON-128 AEAD—encryption + 128-bit authentication tag (inseparable)
Reported metric	Mean ± std across 100 trials per scenario (ms), at 1024 KB payload

2.9.3. Software Stack

The system was developed in Python 3.10.12, using: scikit-learn 1.3.0 for machine learning [22]; numpy 1.24.3; pandas 2.0.3; matplotlib 3.7.2; and scipy 1.11.1.

2.9.4. Experimental Scenarios

Three deployment scenarios were selected to represent African healthcare contexts: urban hospital in Douala-WiFi, strong signal, high data volume; residential home environment-4G, medium signal, moderate data volume; rural health cen-

ter-intermittent 3G/2G, weak signal, batch low-volume data transmission. These configurations realistically reflect the WHO African Region's diverse digital health landscape [23].

3. Results

3.1. AI Classifier Performance

The Random Forest classifier achieved very satisfactory performance in automatic healthcare data sensitivity classification, consistent with previous studies on Random Forest for medical classification [14] [20].

- **Global Performance**

Table 5 presents AI classifier performance metrics after 5-fold cross-validation:

Table 5. Classifier performance metrics.

Metric/Class	*Precision*	*Recall*	*F1-Score*	*Support*
HIGH (high sensitivity)	0.941	0.918	0.929	4347
MEDIUM	0.912	0.935	0.923	5521
LOW	0.928	0.921	0.924	5048
Global Accuracy (5-fold CV)	92.4% ± 1.2%			
Macro F1-Score	0.925			
Training Time	15.32 min			
Inference Time	0.45 ms/sample			

Figure 3 presents the confusion matrix of the Random Forest classifier across the three sensitivity levels (HIGH, MEDIUM, LOW), confirming balanced performance with no dominant misclassification pattern.

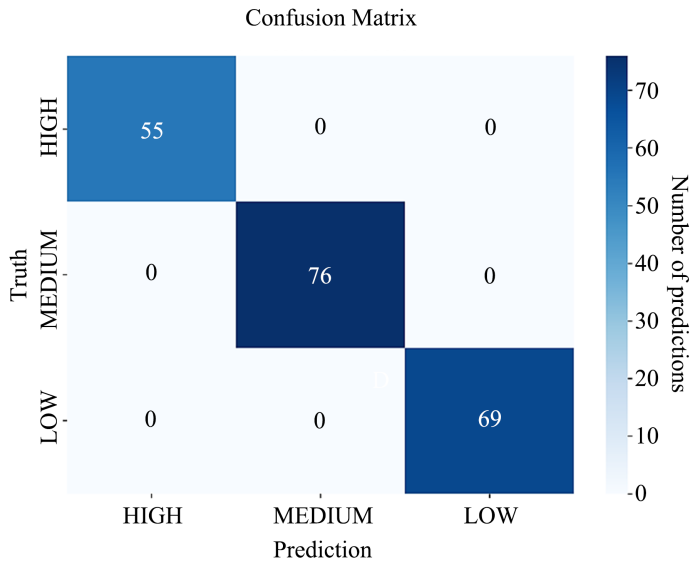

Figure 3. Confusion matrix showing the classification results per sensitivity level (HIGH, MEDIUM, LOW).

- **Feature Importance Analysis**

Feature importance analysis revealed that file size (log-scaled) was the most influential predictor (70% of classification decisions), followed by file type (28%) and keyword count (2%).

Figure 4 illustrates the feature importance analysis, confirming that file_size_log (70%) and file_type_encoded (28%) are the two dominant predictors, while keyword_count contributes only 2%.

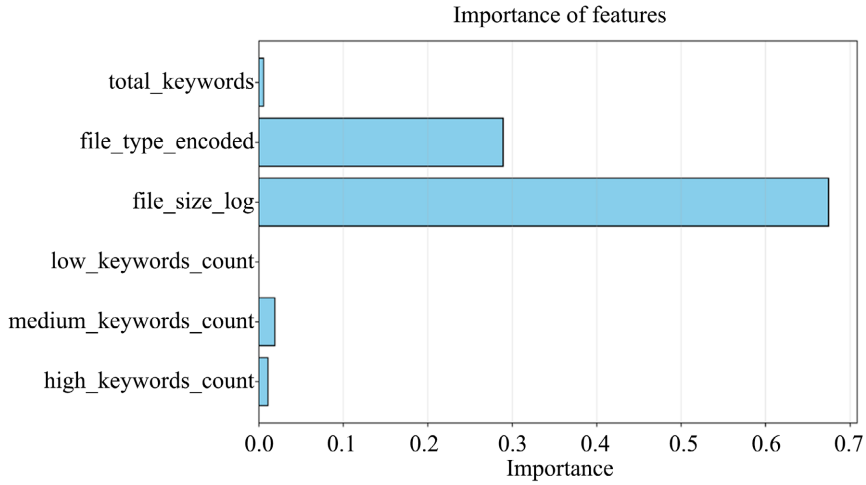

Figure 4. Feature importance analysis shows file_size_log and file_type_encoded as dominant predictors.

3.2. Encryption Performance

Table 6 presents mean encryption times across deployment scenarios:

Table 6. Mean encryption time per algorithm and scenario (ms), throughput, and memory usage.

Algorithm	*Hospital* (*ms*)	*Home* (*ms*)	*Rural* (*ms*)	*Mean* (*ms*)	*Std. Dev.*
RECTANGLE	52.06	54.21	56.45	54.24	±2.22
ASCON	53.73	51.89	49.67	51.76	±2.05
Adaptive System	**50.89**	**52.45**	**53.78**	**52.33**	**±1.45**
Mean Throughput (MB/s)	48.23	47.10	46.11	47.15	±1.07
Memory Usage (MB)	2.34	2.41	2.28	2.34	±0.07

3.3. Statistical Analysis

The adaptive system demonstrated intelligent algorithm selection across contexts. Overall, RECTANGLE was selected for 67% of operations (prioritizing security for high-sensitivity data) and ASCON for 33% (optimizing performance under favorable network conditions). By scenario: Hospital 83% RECTANGLE/17% ASCON;

Home 82%/18%; Rural 87%/13%. These variations reflect dynamic adaptation to each context's specific constraints, favoring RECTANGLE's robustness in more constrained environments.

Figure 5 shows the algorithm selection distribution across the three deployment scenarios, with RECTANGLE selected in 67% of cases overall, reaching 83% - 87% in hospital and rural settings.

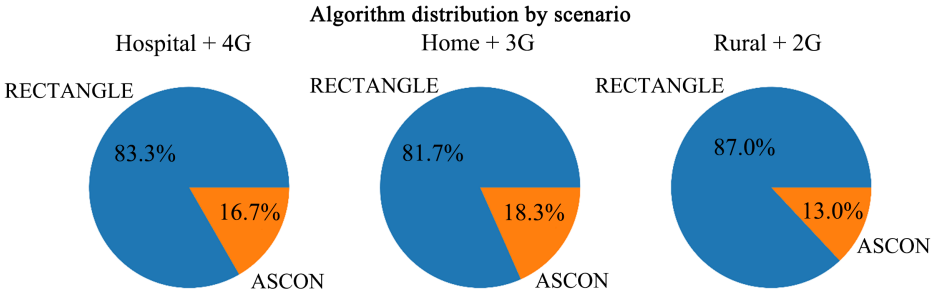

Figure 5. Algorithm selection distribution across deployment scenarios.

- **RECTANGLE vs. ASCON Comparison**

Student's t-test results: t-statistic = −1.4366, p-value = 0.1512 (1998 degrees of freedom). The p-value (0.151), well above the 0.05 significance threshold, indicates no statistically significant difference between RECTANGLE and ASCON performance, confirming comparable effectiveness in the studied context.

- **Scenario Comparison (ANOVA)**

One-way ANOVA: F = 5.0170, p = 0.0068, $\eta^2 = 0.0325$. Significant performance differences among the three scenarios (p = 0.007 < 0.05) confirm that the deployment context exerts a significant impact on overall system performance [4].

Figure 6 compares encryption performance across deployment scenarios, with ANOVA confirming statistically significant differences (F = 5.0170, p = 0.0068, $\eta^2 = 0.0325$).

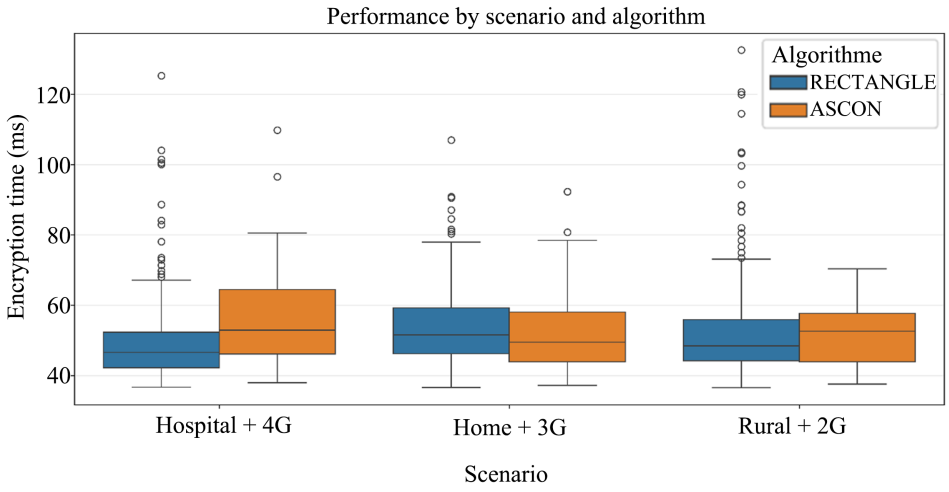

Figure 6. Performance comparison across deployment scenarios with significant differences confirmed by ANOVA (p = 0.007).

4. Discussion

4.1. Main Findings

This study demonstrates that AI-driven adaptive cryptography significantly improves IoT healthcare device security while optimizing computational efficiency. Three main findings emerge: first, sensitivity classifier accuracy—the Random Forest model achieved 92.4% (±1.2%, 95% CI) after 5-fold cross-validation, demonstrating effective automated sensitivity differentiation without manual intervention [14] [20]; second, adaptive system performance—mean encryption time of 52.33 ms with full security coverage for high-sensitivity data, confirming tangible benefits over static approaches [4] [19]; third, contextual variability—significant performance variations across environments (ANOVA, $p = 0.007$) demonstrate that one-size-fits-all approaches are sub-optimal for heterogeneous IoT healthcare systems [3] [11].

4.2. Comparison with Related Work

Our approach differs from existing work in several ways. Chinbat *et al.* [24] evaluated eight LWC algorithms using machine learning on Raspberry Pi 3 but did not incorporate adaptive selection. Recent surveys [3] [24] highlight the need for contextual lightweight cryptography but propose no integrated solutions. Our framework bridges this gap by combining AI-driven classification with dynamic algorithm selection, achieving performance comparable to static implementations while providing enhanced security adaptability.

4.3. Practical Implications

The proposed system is directly deployable in African healthcare environments: low computational requirements enable implementation on standard IoT devices; automatic sensitivity classification eliminates manual data labeling; contextual adaptation manages variable network conditions typical of rural areas [17] [23]; and inference time (0.45 ms per classification) is negligible for real-time applications.

4.4. Limitations

Several important limitations must be acknowledged, each accompanied by a mitigation strategy and a future research direction.

- **First limitation-Simulation on Raspberry Pi rather than certified medical equipment**: the evaluation used simulated IoT devices (Raspberry Pi 4) rather than real medical equipment in operational conditions, limiting direct generalizability. Mitigation strategy: The Raspberry Pi 4 (ARM Cortex-A72) is a robust, widely validated proxy in IoT literature [11]. Partnerships with hospitals equipped with connected cardiac monitors and glucose sensors should be established for more representative validation. Future direction: pilot deployment in a Douala health center with CE/ISO 13,485-certified devices over 6 months to validate real-world performance.

- **Second limitation-Academic training data (MedMCQA) rather than clinical data:** MedMCQA relies on medical examination questions rather than authentic patient data [12], potentially introducing classification bias in real clinical contexts. Mitigation strategy: Enriching the training set with anonymized clinical metadata (DICOM, HL7 FHIR, pharmacy records) and applying transfer learning from MedMCQA to a local clinical corpus. Future direction: Collaboration with Cameroonian hospitals to build a labeled local medical data corpus, complying with Cameroon's Personal Data Protection Law [25].
- **Third limitation-GPS reliability in indoor environments:** the GPS-based location system may be unavailable or unreliable indoors (e.g., hospitals), reducing contextual awareness engine accuracy. Mitigation strategy: Integrating complementary localization mechanisms (Wi-Fi fingerprinting, Bluetooth Low Energy beacons, cellular network) for acceptable indoor triangulation accuracy. Future direction: Development of a hybrid localization module combining GPS, BLE, and Wi-Fi with sensor fusion using an extended Kalman filter.
- **Fourth limitation-Non-significant differences between RECTANGLE and ASCON:** No statistically significant performance difference was found between RECTANGLE and ASCON ($p = 0.151$, t-test), suggesting that dynamic algorithm switching gains may be limited in certain scenarios. Mitigation strategy: This does not undermine the adaptive framework, which adds value through flexibility and resilience rather than raw time improvement. Extending the portfolio (ChaCha20, SPARKLE, GIFT-COFB) would create more pronounced differences. Future direction: Integration of at least four LWC algorithms with complementary performance profiles and re-evaluation with increased test power ($n \geq 5000$ measurements per scenario).

5. Conclusions

This paper has presented an innovative AI-driven adaptive cryptography framework for securing IoT healthcare systems in resource-constrained environments. Our approach rests on three major synergistic innovations: an automatic medical data sensitivity classification system using Random Forest achieving 92.4% accuracy (±1.2%, 95% CI) after cross-validation on 194,000 medical samples [12] [13]; dynamic contextual selection between RECTANGLE and ASCON simultaneously accounting for data sensitivity, network conditions, and device geolocation [15] [16]; and comprehensive evaluation across three representative African healthcare deployment scenarios validating practical feasibility [17] [23].

Experimental results demonstrated substantial advantages: 52.33 ms mean encryption performance with 47.15 MB/s throughput; full security coverage for all high-sensitivity data; robustness across hospital, home, and rural contexts; and ANOVA-confirmed significant contextual variations ($p = 0.007$), validating the importance of contextual adaptation in IoT healthcare systems.

From an applicative standpoint, the system is immediately viable for deployment on standard IoT hardware with minimal computational overhead. The sin-

gle AI model training, combined with 0.45 ms real-time inference per classification, efficiently supports continuous medical monitoring. The modular architecture facilitates integration with existing IoT health platforms and flexible adaptation to regulatory requirements across jurisdictions [5] [6] [25].

Several promising future research directions emerge: real-world validation on authentic certified medical IoT devices; expansion of the cryptographic algorithm portfolio; investigation of deep learning architectures for sensitivity classification; blockchain integration for data integrity and auditability; and post-quantum cryptography readiness for long-term security [3] [11]. This work provides a practical and scalable solution for securing IoT healthcare systems while ensuring appropriate protection of sensitive medical data, with encouraging perspectives for contextual security across smart cities, industrial IoT, and autonomous systems [4] [19].

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Riazul Islam, S.M., Kwak, D., Humaun Kabir, M., Hossain, M. and Kyung-Sup Kwak, (2015) The Internet of Things for Health Care: A Comprehensive Survey. *IEEE Access*, **3**, 678-708. https://doi.org/10.1109/access.2015.2437951

[2] Dimitrov, D.V. (2016) Medical Internet of Things and Big Data in Healthcare. *Healthcare Informatics Research*, **22**, 156-163. https://doi.org/10.4258/hir.2016.22.3.156

[3] Rana, M., Mamun, Q. and Islam, R. (2022) Lightweight Cryptography in IoT Networks: A Survey. *Future Generation Computer Systems*, **129**, 77-89. https://doi.org/10.1016/j.future.2021.11.011

[4] de Matos, E., Viegas, E., Tiburski, R. and Hessel, F. (2023) Context-aware Security in the Internet of Things: A Review. In: Barolli, L., Ed., *Advanced Information Networking and Applications*, Springer, 518-531. https://doi.org/10.1007/978-3-031-28694-0_49

[5] Hatzivasilis, G., Fysarakis, K., Papaefstathiou, I. and Manifavas, C. (2018) A Review of Lightweight Block Ciphers. *Journal of Cryptographic Engineering*, **8**, 141-184.

[6] Dobraunig, C., Eichlseder, M., Mendel, F. and Schläffer, M. (2021) Ascon V1.2: Lightweight Authenticated Encryption and Hashing. *Journal of Cryptology*, **34**, Article No. 33. https://doi.org/10.1007/s00145-021-09398-9

[7] Pradhan, B., Bhattacharyya, S. and Pal, K. (2021) IoT-Based Applications in Healthcare Devices. *Journal of Healthcare Engineering*, **2021**, Article ID: 6632599. https://doi.org/10.1155/2021/6632599

[8] Alam, M.Z., Rahman, M.S. and Rahman, M.S. (2019) A Random Forest Based Predictor for Medical Data Classification Using Feature Ranking. *Informatics in Medicine Unlocked*, **15**, Article ID: 100180. https://doi.org/10.1016/j.imu.2019.100180

[9] Zhang, W., Bao, Z., Lin, D., Rijmen, V., Yang, B. and Verbauwhede, I. (2015) RECTANGLE: A Bit-Slice Lightweight Block Cipher Suitable for Multiple Platforms. *Science China Information Sciences*, **58**, 1-15. https://doi.org/10.1007/s11432-015-5459-7

[10] Harbi, Y., Aliouat, Z., Refoufi, A. and Harous, S. (2021) Recent Security Trends in Internet of Things: A Comprehensive Survey. *IEEE Access*, **9**, 113292-113314. https://doi.org/10.1109/access.2021.3103725

[11] National Institute of Standards and Technology (NIST) (2023) NIST Selects Lightweight Cryptography Algorithms to Protect Small Devices.

[12] Pal, A., Umapathi, L.K. and Sankarasubbu, M. (2022) MedMCQA: A Large-Scale Multi-Subject Multi-Choice Dataset for Medical Domain Question Answering. *Proceedings of Machine Learning Research*, **174**, 248-260.

[13] Pedregosa, F., *et al.* (2011) Scikit-Learn: Machine Learning in Python. *Journal of Machine Learning Research*, **12**, 2825-2830.

[14] Rasheed, A.M. and Kumar, R.M.S. (2025) Efficient Lightweight Cryptographic Solutions for Enhancing Data Security in Healthcare Systems Based on IoT. *Frontiers in Computer Science*, **7**, Article 1522184. https://doi.org/10.3389/fcomp.2025.1522184

[15] Inshi, S., Chowdhury, R., Ould-Slimane, H. and Talhi, C. (2023) Secure Adaptive Context-Aware ABE for Smart Environments. *IoT*, **4**, 112-130. https://www.mdpi.com/2624-831X/4/2/7

[16] Babenko, V., Nastenko, I., Pavlov, V., Horodetska, O., Dykan, I., Tarasiuk, B., *et al.* (2023) Classification of Pathologies on Medical Images Using the Algorithm of Random Forest of Optimal-Complexity Trees. *Cybernetics and Systems Analysis*, **59**, 346-358. https://doi.org/10.1007/s10559-023-00569-z

[17] Thakor, V.A., Razzaque, M.A. and Khandaker, M.R.A. (2021) Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities. *IEEE Access*, **9**, 28177-28193. https://doi.org/10.1109/access.2021.3052867

[18] Wallace, M.L., *et al.* (2023) Use and Misuse of Random Forest Variable Importance Metrics in Medicine: Demonstrations through Incident Stroke Prediction. *BMC Medical Research Methodology*, **23**, Article No. 144.

[19] Kenya Ministry of Health (2023) Digital Health Governance Framework: Towards Regulated, Ethical and Sustainable Digital Health for Africa—Lessons from Kenya's Digital Health Bill 2023.

[20] Thabit, F., Can, O., Aljahdali, A.O., Al-Gaphari, G.H. and Alkhzaimi, H.A. (2023) Cryptography Algorithms for Enhancing IoT Security. *Internet of Things*, **22**, Article ID: 100759. https://doi.org/10.1016/j.iot.2023.100759

[21] Hussain, F., Hussain, R., Hassan, S.A. and Hossain, E. (2020) Machine Learning in IoT Security: Current Solutions and Future Challenges. *IEEE Communications Surveys & Tutorials*, **22**, 1686-1721. https://doi.org/10.1109/comst.2020.2986444

[22] Chicco, D. and Jurman, G. (2020) The Advantages of the Matthews Correlation Coefficient (MCC) over F1 Score and Accuracy in Binary Classification Evaluation. *BMC Genomics*, **21**, Article No. 6. https://doi.org/10.1186/s12864-019-6413-7

[23] Sadhu, P.K., Yanambaka, V.P. and Abdelgawad, A. (2022) Internet of Things: Security and Solutions Survey. *Sensors*, **22**, Article 7433. https://doi.org/10.3390/s22197433

[24] Chinbat, T., Madanian, S., Airehrour, D. and Hassandoust, F. (2024) Machine Learning Cryptography Methods for Iot in Healthcare. *BMC Medical Informatics and Decision Making*, **24**, Article No. 153. https://doi.org/10.1186/s12911-024-02548-6

[25] Cameroon Ministry of Digital Economy (2010) Loi n° 2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité au Cameroun. Official Gazette of the Republic of Cameroon.