# Analysis of External Factors on the Performance of Cryptographic Algorithms in Medical Systems Based on ESP32

Saltanat Adilzhanova [1], Gulnur Tyulepberdinova [2], Murat Kunelbayev [2], Gulshat Amirkanova [1], Dana Sybanova [1,*], and Aigerim Rakhysh [1]

[1] Cybersecurity and Cryptology Department, Al-Farabi Kazakh National University, Almaty, Kazakhstan
[2] Artificial Intelligence and Big Data Department, Al-Farabi Kazakh National University, Almaty, Kazakhstan
Email: asaltanat81@gmail.com (S.A.); tyulepberdinova@gmail.com (G.T.); murat7508@yandex.kz (M.K.); gulshat.aa@gmail.com (G.A.); dsybanovaa@gmail.com (D.S.); rakhysh_aigerim3@live.kaznu.kz (A.R.)
*Corresponding author

***Abstract*—This paper investigates the influence of real-time physiological and environmental variables on the computational performance of cryptographic algorithms deployed in wearable medical systems powered by the ESP32 microcontroller. The proposed system integrates biometric sensors to capture heart rate, skin temperature, and galvanic skin response, from which a composite Stress Index (SI) is calculated. This SI dynamically modulates encryption behavior to adapt to the user's physiological state. An experimental dataset comprising 300 samples from 10 participants was collected over ten days under semi-controlled environmental conditions. Six widely used cryptographic algorithms—AES-256, HMAC-SHA256, SHA-256, SHA-3, BLAKE3, and ChaCha20—were evaluated based on execution time, CPU load, and estimated energy consumption under varying stress levels. To quantify algorithmic robustness, we introduced the Crypto Stress Tolerance Score (CSTS), a custom metric combining performance stability, stress correlation, and resource efficiency. The findings reveal that elevated body temperature and stress index values significantly affect cryptographic performance, with execution time increasing by up to 35% under high-stress conditions. AES-256 exhibited the highest sensitivity and variability, whereas BLAKE3 and ChaCha20 delivered consistent, low-latency performance with minimal fluctuation. A comparative analysis and scoring table are provided to guide optimal algorithm selection for constrained medical Internet of Things (IoT) environments. This work contributes a novel framework for adaptive, stress-aware encryption in embedded healthcare devices, offering improved reliability, energy efficiency, and security personalization in patient-centric monitoring systems.**

***Keywords*—ESP32, cryptographic performance, wearable security, medical Internet of Things (IoT), biometric encryption, physiological stress index, adaptive encryption, Crypto Stress Tolerance Score (CSTS)**

Manuscript received May 1, 2025; revised June 12, 2025; accepted July 21, 2025; published December 5, 2025.

## I. Introduction

The paper describes the design of a wearable sensing device integrated into an Internet of Things (IoT) infrastructure, intended for continuous tracking of a user's physiological parameters and their intelligent analysis for real-time stress assessment. The system supports uninterrupted monitoring of key physiological signals, enabling the early identification of stress indicators and promoting adaptive behavioral responses. The hardware platform aggregates multiple biomedical sensors to provide ongoing acquisition and intelligent, real-time processing of physiological data. During experiments, Heart Rate (HR) values were recorded in the range of 68–89 beats per minute (bpm), respiratory rate varied from 11 to 15 bpm, and skin conductance was between 63 and 77 μS. The collected physiological data were transmitted to a cloud-based platform for advanced processing and analytics. The system achieved an overall stress detection accuracy of 87%, with stable signal quality even under varying conditions. The proposed wearable solution shows strong potential for deployment in healthcare, educational, and workplace settings and can be further scaled by integrating advanced algorithms and additional sensor modules [1]. Contemporary conditions demand efficient approaches to stress monitoring and management, stimulating the adoption of innovative technological solutions.

This article presents the development of an IoT-enabled wearable device capable of detecting and quantitatively assessing stress levels in real time. The proposed technology improves the precision of stress evaluation, enabling rapid reactions and the creation of personalized stress management strategies. The device uses a Field-Programmable Gate Array (FPGA) as its main controller and incorporates nine sensors: photoplethysmography (MAX30102), Electroencephalography (EEG), Electrocardiography (ECG), Glucose (GS), Electromyography (EMG), Temperature (TS), Pressure (PS), Heart Rate (HRs), Pulse (PS), and Galvanic Skin

doi: 10.12720/jait.16.12.1706-1723

Response (GSR). These sensors capture physiological indicators such as heart rate, skin conductance, and respiratory parameters associated with stress. The measured data are transmitted via Wi-Fi to the firebase platform.

The article also emphasizes the advantages of IoT-based wearable systems and their adaptability to diverse environments, including offices, educational institutions, and healthcare facilities, where stress control is essential. Continuous monitoring enables users to observe their stress levels and take timely measures to support their well-being. Experimental results indicate that the device achieves an accuracy of 85% in measuring heart rate and respiratory parameters. Thus, the solution is valuable for both everyday use and professional domains such as medicine, education, and occupational environments, where effective stress regulation is vital for health and productivity [2]. A wide variety of methods for stress detection based on different physiological signals and algorithms has been proposed. Nevertheless, a significant gap remains in translating findings from controlled laboratory experiments into real-world applications. Only a limited number of studies have examined whether a physiological response truly reflects a reaction to external stimuli in the participant's environment in real-life scenarios. Typically, physiological data are linked to spatial characteristics of the surroundings and supported by video recordings or interviews.

The present work aims to narrow the gap between laboratory experiments and field studies by introducing a novel algorithm that uses wearable physiological sensors to detect Moments of Stress (MOS). The authors propose a rule-based algorithm that relies on galvanic skin response and skin temperature, combining empirical evidence with expert knowledge to enhance transferability from laboratory conditions to real-world contexts. To validate the approach, a laboratory experiment was conducted to establish a "gold standard" of physiological responses to stressors. The algorithm was then tested in real-world field studies using a mixed-methods design that spatially correlated perceived stress, geo-referenced questionnaires, and corresponding real-world situations from video recordings. The findings show that the algorithm identifies MOS with 84% accuracy and exhibits strong correlations between stress events measured by wearable sensors, reported through questionnaires and eDiary entries, and captured on video. The detected urban stressors in real-world environments include traffic congestion, hazardous driving situations, and crowded locations such as tourist areas. This research contributes to improving stress detection in daily life and supports a deeper understanding of environmental circumstances that trigger physiological stress in humans [3].

The rapid expansion of IoT devices in healthcare—ranging from wearable sensors to implantable medical equipment—has transformed patient monitoring, personalized treatment, and remote care. However, the constrained computational, memory, and energy resources of IoT devices, together with the sensitivity of medical data, introduce serious security challenges. Conventional encryption techniques, while offering strong security, are often too computationally demanding for IoT platforms, leaving confidential patient data exposed to cyber threats. To address this problem, lightweight encryption schemes have emerged as a key approach to balancing security with limited device capabilities. This paper examines lightweight cryptographic methods designed for IoT healthcare applications and assesses their ability to protect sensitive data in resource-constrained environments.

A comparative study is performed on algorithms such as AES-128, LEA, Ascon, GIFT, HIGHT, PRINCE, and RC5-32/12/16 using metrics including block and key sizes, encryption/decryption speed, throughput, and security levels. The results indicate that AES-128, LEA, ASCON, and GIFT are most suitable for highly sensitive healthcare information due to their robust security properties, whereas HIGHT and PRINCE offer a compromise between security and efficiency for medium-sensitivity use cases. RC5-32/12/16 is shown to favor computational efficiency over maximal security, making it appropriate for low-risk applications where minimal overhead is critical. The paper emphasizes the inherent trade-offs between efficiency, security strength, and resource usage, stressing the importance of choosing encryption methods that align with the specific constraints and needs of IoT healthcare systems. Moreover, it highlights the increasing demand for lightweight schemes that combine energy efficiency with strong protection against cyber threats, providing practical guidance for researchers and practitioners seeking to secure IoT-based healthcare infrastructures while maintaining optimal performance [4].

Safeguarding sensitive information, including data obtained from sensors, is essential to ensure accurate device evaluation and prevent unauthorized access. In this context, IoT devices represent a promising solution for in situ monitoring. Yet such devices are typically limited in processing power and memory, which makes the use of traditional, heavyweight cryptographic mechanisms impractical. Consequently, lightweight and efficient security algorithms become crucial. This review paper investigates the deployment of lightweight symmetric cryptographic algorithms on power-constrained microcontrollers in IoT systems. The implemented schemes consider the resource limitations of the devices and compare their performance to support the efficient realization of secure monitoring platforms. Experimental findings present the behavior of several lightweight encryption algorithms on low-power microcontrollers. The analysis compares these algorithms in terms of average power and energy consumption, memory usage, latency, and throughput [5].

The accelerating growth of the IoT has intensified concerns about security and privacy in constrained environments. Traditional encryption mechanisms often incur high computational and energy overheads and are therefore unsuitable for many IoT devices. To overcome these limitations, lightweight cryptographic solutions have been extensively explored as efficient alternatives. This paper conducts a Systematic Literature Review (SLR), following Kitchenham's guidelines, of 77 peer-reviewed

works published between 2006 and 2025. The review includes both qualitative synthesis and quantitative evaluation using metrics such as entropy, execution time, energy consumption, throughput, NPCR, and UACI. The study is structured around four research questions that examine: (i) Lightweight techniques for confidentiality, integrity, and authentication; (ii) Performance trade-offs on constrained IoT platforms; (iii) Optimizations of Elliptic Curve Cryptography (ECC); and (iv) Integration with emerging technologies like AI, blockchain, and steganography. The results categorize lightweight block and stream ciphers, hybrid frameworks, and authentication protocols, outlining their advantages and limitations. The work also identifies open challenges, including the scarcity of adaptive approaches and limited benchmarking on embedded devices. Overall, the review provides a roadmap for designing secure, scalable, and energy-efficient cryptographic mechanisms tailored to IoT ecosystems, supporting both academic inquiry and practical deployment [6].

The growing number of IoT devices has introduced major security concerns, largely due to their restricted processing power, memory, and energy availability. This study performs a comparative performance assessment of several modern cryptographic algorithms on a constrained IoT platform, the Nordic Thingy:53. The evaluated ciphers include the NIST lightweight standard ASCON, eSTREAM finalists Salsa20, Rabbit, Sosemanuk, HC-256, and the extended-nonce variant XChaCha20. Using a dual test-bench setup, the authors measure energy usage and performance under two distinct conditions: a low-data-rate Bluetooth mesh network and a high-throughput bulk data transmission scenario. The experiments reveal significant differences in performance among the algorithms. For high-throughput workloads, XChaCha20, Salsa20, and ASCON32 exhibit superior speed, whereas HC-256 is impractically slow for large payloads. The Bluetooth mesh tests further show a direct link between network activity and power consumption, underscoring how cryptographic choice affects battery life. These insights provide a practical basis for selecting cryptographic algorithms that strike an appropriate balance between security, energy efficiency, and performance in real-world IoT deployments [7].

The fusion of multiple sensors can significantly enhance daily stress monitoring. In this work, a wrist-worn device integrates Galvanic Skin Response (GSR), PPG-derived Heart Rate Variability (HRV), skin temperature, and $SpO_2$, complemented by self-report questionnaires. The device streams data via Bluetooth low energy to a mobile application, updating the user interface within 1–2 s. Physiological features are extracted within a fixed temporal window around each questionnaire time and are processed through a mid-level fusion strategy. A late fusion approach based on self-reports is also examined. In comparison with a commercial reference device, the proposed system achieves a mean absolute error of 0.23 for $SpO_2$ and 4.94 bpm for heart rate in a one-day benchmark session. The solution is validated through technical testing with representative inputs and simulated survey labels. The fusion model is evaluated using synthetic physiological and questionnaire data. A support vector machine algorithm attains a mean squared error of 0.08 when predicting simulated stress labels. Temperature shows the strongest correlation with simulated stress (–0.43), followed by HRV (0.36), while $SpO_2$ exhibits negligible correlation (0.09) in the current dataset. In conclusion, the system combines multi-sensor acquisition, on-device preprocessing, BLE transmission, and a structured fusion pipeline to deliver effective predictive performance for daily stress monitoring [8].

As IoT systems become more pervasive, new security and privacy threats emerge and are recognized as serious challenges. To counter these risks, novel cryptographic countermeasures and prevention strategies are being developed. Since many IoT devices operate under tight memory and processing constraints, traditional cryptographic algorithms are often impractical without dedicated hardware accelerators. In this work, an enhanced version of the MQTT protocol, termed MQTTSec, is proposed. MQTTSec allows communicating devices to dynamically select cryptographic techniques according to their available resources. The paper also presents a validation of the proposed mechanism [9]. The authors present an efficient hardware architecture and implementation of the Advanced Encryption Standard (AES). AES, endorsed by the US National Institute of Standards and Technology (NIST), has become widely adopted. Cryptographic algorithms can be realized either in software or in pure hardware, but Field-Programmable Gate Arrays (FPGAs) offer rapid, reconfigurable solutions that can accommodate evolving protocol requirements. This contribution analyzes the AES encryption system in the context of FPGA and Very High-speed integrated circuit Hardware Description Language (VHDL). Optimized and synthesizable VHDL code is developed for implementing the 128-bit data encryption process. The AES encryption core is realized on an FPGA and demonstrates improved efficiency compared to previously reported designs. Using Xilinx ISE 12.3i for simulation and NIST sample vectors for verification, the implementation achieves correct outputs with minimal delay. The reported throughput reaches 1,609 Mbit/s for encryption on a Xilinx Virtex-family device (XC6vlx240t) [10].

In recent years, cryptographic algorithms have gained increasing importance. The AES, introduced in the early 2,000 s, has seen widespread adoption due to its ease of implementation and strong security. This work presents five different AES implementations on FPGA, each optimized for specific design goals. The techniques range from compact designs suitable for area-critical applications to high-speed versions targeted at performance-critical systems. Experimental results span a broad spectrum of resource usage and speed. The most resource-efficient design achieves a frequency of 886.64 MHz and a throughput of 113.5 Gb/s on a Spartan-6 device while maintaining moderate resource consumption. Comparative analysis with existing solutions demonstrates that the proposed technique attains

a 32% higher frequency, while using 2.63× more slice LUTs, 8.33× fewer slice registers, and 12.59× fewer LUT-FF pairs [11].

To protect AES implementations from physical attacks, particularly fault injection attacks, various countermeasures have been proposed. AES is widely integrated into embedded systems to deliver security services and has become the standard choice in numerous applications. However, naturally occurring or maliciously induced faults can compromise its robustness and potentially lead to leakage of sensitive information. This paper examines concurrent fault detection strategies aimed at achieving reliable AES implementations. The authors introduce a new fault detection scheme based on a modified AES architecture, where the round transformation is split into two parts with a pipeline stage inserted between them. The proposed approach is independent of the specific realization of the S-Box and Inv_S-Box, whether they are implemented using look-up tables or logic gates over Galois fields. Simulation results indicate a fault coverage of 98.54% for the proposed scheme. Furthermore, the new and existing fault detection mechanisms are implemented on recent Xilinx Virtex FPGAs and compared in terms of area overhead, operating frequency, and throughput, showing that the proposed solution outperforms previously reported methods [12].

The IoT connects a broad range of devices to support collaborative data sharing and processing. This transformative technology has high potential across many domains. A central component in IoT systems is the microcontroller board, which must interface with sensors tailored to the tasks at hand. The ESP32 is a widely used option in IoT applications owing to its small form factor, low cost, and strong Bluetooth and Wi-Fi capabilities, all with modest power consumption. However, its 3.3 V output limitation creates challenges when powering high-demand sensors or performing intensive processing tasks. To overcome these constraints, the authors developed the ESP32Exten expansion module to boost motor control and AI-based image-processing capabilities. A dedicated library was also created to extend the module's functionality. Performance evaluations compare ESP32Exten with standard expansion boards across three aspects: (1) Motor performance, (2) AI image processing and data transmission over Bluetooth and Wi-Fi, and (3) Input-output sensor connectivity. The results show that ESP32Exten substantially enhances DC motor control, improves image processing and high-speed data transmission, and reduces voltage drop, thereby mitigating inherent limitations of the basic ESP32 platform [13].

This paper introduces an innovative design and development of a smart IoT-enabled device based on the ESP32 microcontroller. The compact embedded kit measures atmospheric pressure, temperature, and humidity and sends this information to an IoT web platform. It also integrates a heart rate sensor that communicates with a custom Android application via Bluetooth, as well as a compass that detects direction and displays the current date and time. The proposed smart device supports a wide range of applications, including viewing stock market charts and live sports scores over the internet. It can also be reprogrammed as a health-monitoring tool, a drone controller, a car controller, or a general-purpose automation controller, depending on user requirements. Additionally, students can attach various sensors to the kit to learn embedded systems concepts, supported by multiple available embedded programs [14].

Mobile information and communication systems in clinical practice have the potential to significantly enhance communication, streamline information access, reduce redundant documentation, and improve the overall quality of patient care over time. Previous projects have largely concentrated on highly specialized mobile applications. Within the research project "Cooperative Problem Solving in Health Care", the authors designed a multifunctional mobile information and communication assistant, and a prototype system was implemented. This article presents the near-realistic evaluation of the prototype during a one-week simulation study in a Heidelberg University hospital. The paper describes the methodology, objectives, design, and outcomes of the simulation, and discusses both the approach and the results obtained. The authors argue that the diverse requirements of different professional groups cannot be satisfied by a single multifunctional device and therefore recommend a "multi-device mobile computer architecture". The paper concludes with implications for future computing infrastructures [15]. Worldwide, the adoption of modern technology for home automation continues to grow, along with its benefits. Although several home automation systems have already been implemented, there remains a substantial need for more efficient approaches that help homeowners achieve convenience, effective control, safety, and cost savings. This paper presents the design of an interactive IoT-based speech-controlled home automation system using Google assistant, commonly referred to as a smart home solution. The proposed system enables users to remotely control household electrical appliances through voice commands issued from mobile devices using Google's infrastructure. Experimental evaluations under different scenarios—such as noisy versus quiet environments, empty versus furnished rooms, varying distances, and room sizes—demonstrate that the system can achieve accuracy rates of up to 100% in certain configurations [16].

Mobile phones have become indispensable communication tools for health professionals. Modern smartphones, comparable in functionality to computers, enable the development of new applications for health promotion. This paper seeks to describe how smartphones are used by healthcare professionals and patients within the context of health promotion. A bibliographic search was conducted using PubMed, followed by critical analysis of the identified studies to select the most relevant experiences. All searches were performed in November 2012 without date restrictions. After removing duplicates, 406 of the initial 472 entries were reviewed, and 21 articles were identified as focusing specifically on health promotion. In the nutrition domain, some applications help users count calories and maintain food diaries, while others are aimed at individuals with food allergies. For physical

activity, many apps provide exercise suggestions and track sports statistics. Additional applications deliver lifestyle advice and tips. Positive outcomes have also been reported in preventing falls in the elderly and reducing sexually transmitted diseases. While smartphones are reshaping communication and health promotion practices, concerns persist regarding content quality control, the digital divide, data confidentiality, and the risk of excluding healthcare professionals from patient management [17].

Advances in mobile communication and portable computing have converged in handheld devices known as smartphones, which can also run third-party software. The number of smartphone users is increasing rapidly, including among healthcare professionals. The aim of this study is to classify smartphone-based healthcare technologies described in academic literature according to their functionality and to summarize the articles in each category [18]. Mobile technology holds considerable potential to transform medical practice. From providing access to up-to-date medical evidence at the point of care to enabling rapid communication with colleagues worldwide, physicians now operate in a highly digital environment. In recent years, many clinicians have simultaneously used pagers, mobile phones, and Personal Digital Assistants (PDAs) for hospital communication and information access. An increasing number of physicians are replacing these multiple devices with a single "smartphone", which functions as a phone, pager, and PDA. The article aims to give an overview of major smartphone platforms and the available medical software. Each platform has distinct strengths and limitations, and its software ecosystem is dynamic and continually evolving [19]. Healthcare information technology is advancing to better support clinicians' decision-making processes. Clinical decision support tools derived from health IT offer opportunities for collaboration between nursing informatics specialists and critical care nurses, with the potential to strengthen the nursing profession, improve patient outcomes, and raise the quality and efficiency of healthcare. Previous work by Weber indicates that critical care nurses' use of computer-based decision support systems varies and that PDAs are a common type of health IT used for this purpose. This article examines nurses' preferences for using PDAs and specific clinical software. PDAs are handheld, battery-powered devices equipped with memory cards for data storage. More advanced PDAs also include photo, recording/dictation, and music capabilities, along with Internet and Bluetooth connectivity [20].

Cloud networks have gained popularity due to their scalability and flexibility, but they face growing security challenges. To mitigate these risks, researchers have proposed numerous cryptographic algorithms to secure cloud infrastructures against attacks. This abstract introduces an improved hybrid cryptographic algorithm that combines symmetric and asymmetric encryption to provide strong security and efficiency in cloud environments. The scheme employs the Rivest-Shamir-Adleman (RSA) algorithm for asymmetric encryption and integrates Advanced Encryption Standard (AES) with Blowfish for symmetric encryption. This combination enables secure transmission of both data and keys between cloud servers and clients. The enhanced hybrid approach also incorporates a key management system to protect cryptographic keys. The authors evaluate the performance of the proposed algorithm and compare it with existing cryptographic methods. The results indicate that the new approach offers superior security and efficiency, making it a promising option for securing cloud networks [21].

Security in wireless networks is a critical issue, especially in harsh environments and in the context of sensor networks. Cryptography plays a central role in achieving this security. Although many cryptographic algorithms exist, no single one fully satisfies all security requirements for such networks. This paper presents a new cryptographic technique that combines both symmetric and asymmetric encryption methods. The proposed algorithm uses AES, Data Encryption Standard (DES), and a modified RSA (m-RSA) in different phases. AES is applied in phase one, DES in phase two, and m-RSA in the final phase, with all three phases executed in parallel. Symmetric schemes provide strong data protection, while asymmetric methods simplify key management. The authors compare the proposed algorithm with existing approaches in terms of total execution time and decryption time, showing that their solution achieves better performance than prior techniques [22]. Cloud computing has emerged as a prominent technology for storing and accessing data over the Internet. Often, sensitive information is hosted on remote servers that customers neither manage nor directly control, creating opportunities for attacks from both inside and outside the cloud service provider. Cryptography is the primary mechanism for ensuring an adequate level of security in such environments. Hybrid cryptography attempts to improve security and performance by combining multiple cryptographic algorithms. This study surveys hybrid cryptographic models used to secure data in the cloud between 2013 and 2020. The authors describe the design, implementation methods, limitations, and suggested applications of each identified proposal. The paper concludes with a comparative summary table and aims to make a scientific contribution toward securing cloud environments [23]. For Vacuum Interrupters (VIs), both internal vacuum insulation and external insulation performance are critical. To improve the external insulation of high-voltage and/or compact VIs, various high-insulation materials have been used for external dielectric protection; however, these materials are often costly and may pose environmental issues. This paper proposes using external shields to enhance the external insulation performance of VIs. Four geometric parameters are studied: the distance between the external shield and the ceramic envelope ($L$), the height that the shield covers along the ceramic envelope ($H$), and the radii $R_1$ and $R_2$ of the shield. Finite element simulations of a 40.5 kV VI show that optimal dimensions are $L$ = 2 mm, $H$ = 4 mm, $R_1$ = 3 mm, and $R_2$ = 3 mm. Power-frequency voltage withstand tests are conducted to evaluate external insulation performance. For three VIs without external

shields, the average external flashover voltage is 76.7 kV, whereas for three VIs equipped with shields on the ceramic envelope end surfaces, it is 96.1 kV. This corresponds to a 25.4% increase in average flashover voltage, demonstrating that external shields effectively enhance external insulation performance and are suitable for high-voltage and/or compact Vis [24]. This study examines how urban environmental stress affects the subjective well-being of residents in Bhopal, India. The objectives are to identify perceived urban environmental stressors and to explore coping strategies used by residents to manage the consequences of urban stress. The perceived Urban Environmental Stressors Scale (UES) and the Urban Hassle Index are administered. Results indicate that although residents describe their city as pleasant, they still report high levels of stress. Major contributing factors include noise, waste accumulation, polluted air with smoke, and unhealthy conditions in slum areas. The findings suggest that city planners should give equal importance to natural resources and environmental quality through pollution control measures and sound urban planning. Reducing the impact of these stressors is essential for making city life livable and improving quality of life. The paper also provides guidance that can be applied to other metropolitan areas to foster environmental competence, raise public awareness about urban environmental stress, and promote management strategies that support environmental resilience and effective coping [25]. Indonesia's health index is relatively low compared to other countries, largely due to increasingly complex disease patterns. One approach to addressing this issue is the Smart Health concept, which enables continuous monitoring of health conditions by both patients and healthcare institutions to support disease prevention. Although numerous health-monitoring studies have been conducted, most have focused primarily on data acquisition and visualization, with limited attention to data management aspects such as storage, processing, and synchronization among systems, patients, and healthcare providers. This research proposes the design of a health-monitoring system called Mooble (Monitoring for Better Life Experience), which aims to track patient health status and prevent diseases at an early stage. Mooble consists of three subsystems: a web application, a database and API layer, and an Android-based mobile application. The present work concentrates on the design and development of the mobile application subsystem. The project covers application design, implementation, and testing phases, following the Rational Unified Process (RUP) methodology. Ultimately, the research delivers a mobile application intended for patient use [26]. Insulation systems used in electrical distribution transformers are being reassessed from economic, safety, and environmental perspectives over their full life cycle. Because liquid-cooled transformers inherently provide higher efficiency, recent development has focused on insulating fluids with improved environmental and health properties while preserving the fire-resistant characteristics of "less-flammable" fluids. This paper reports findings from several years of research and development on alternative dielectric systems based on both natural and synthetic esters. Since esters have lower resistance to oxidation than conventional mineral oil, a novel insulation system is introduced to mitigate this limitation. The study discusses single-phase and three-phase prototype field installations that employ these new dielectric coolants [27]. The purpose of this work is to study the effect of physiological and environmental factors in real time on the computational performance of cryptographic algorithms used in wearable medical systems based on the ESP32 microcontroller, as well as to develop and experimentally validate an adaptive stress-oriented encryption mechanism that dynamically changes its behavior depending on the user's condition.

## II. Materials and Methods

### A. Cryptographic Algorithm Selection Criteria

The present study assumes that external physical parameters—such as ambient temperature, atmospheric pressure, and the user's heart rate—may affect the execution time and computational efficiency of cryptographic algorithms. This hypothesis applies to both traditional schemes (e.g., AES-256, SHA-256) and modern information security mechanisms (e.g., SHA-3, BLAKE3, ChaCha20).

To test this assumption, an experimental dataset of 300 sensor readings was collected under controlled and semi-randomized environmental conditions over a 10-day period. The cryptographic algorithm suite evaluated in the study includes: SHA-256, HMAC-SHA256, AES-256, SHA-3, BLAKE3, ChaCha20. The choice of algorithms was based on their current use in IoT and medical-grade systems, their documented performance in constrained devices, and their varied design principles, which allow comparative analysis.

During testing, performance metrics such as: Execution time, Processor load, Energy consumption was recorded. Notably, BLAKE3 exhibited the greatest stability under environmental fluctuations, while AES-256 showed the most pronounced performance degradation under stress conditions.

This diagram illustrates the data processing pipeline of a wearable cryptographic system (Fig. 1). The workflow begins with medical image acquisition (e.g., from a sensor or camera in DICOM or PNG format), followed by preprocessing and data collection using an ESP32 microcontroller. The data is then cryptographically secured using a combination of the Josephus permutation algorithm and SHA-256 hashing. The final step ensures data integrity before transmission to either local or cloud storage. The architecture is optimized for secure, real-time processing in telemedicine and mobile health monitoring applications.

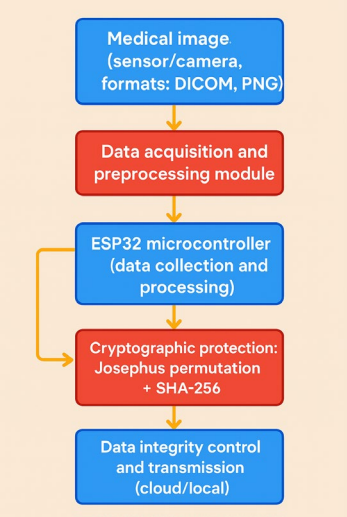


Fig. 1. Architecture of the wearable cryptographic system for medical image processing.

### B. Physiological Parameter Integration

To enable continuous physiological monitoring, the system integrates multiple biomedical sensors. These sensors collect real-time data such as heart rate, skin temperature, and galvanic skin response. The selection of each sensor was based on compatibility with the ESP32 platform, low power consumption, and measurement accuracy. The MAX30102 sensor is used for heart rate detection, utilizing Photoplethysmography (PPG) to measure blood volume changes through infrared light. For skin temperature monitoring, the MLX90614 infrared sensor provides non-contact and high-precision readings, making it suitable for wearable applications. The Galvanic Skin Response (GSR) is captured via two conductive electrodes placed on the skin, which measure changes in electrical conductance associated with sweat gland activity—a reliable indicator of stress or arousal. Additionally, the system allows optional integration of a blood pressure sensor, expanding its functionality for future clinical applications. All data are transmitted wirelessly to a central processing unit via Bluetooth or WIFI, enabling real-time analysis and secure storage for further evaluation. This modular sensor configuration ensures flexibility, reliability, and adaptability across various physiological monitoring scenarios.

These physiological parameters are utilized as key inputs for the stress index computation model outlined in the subsequent section. Additionally, the acquired sensor data enables the system to adjust cryptographic algorithm behavior in real time, forming the basis of a stress-aware encryption framework.

The ESP32 microcontroller performs real-time aggregation and normalization of all physiological inputs. These metrics are closely linked to internal stress levels and are used to dynamically alter the cryptographic execution flow depending on current physiological conditions.

Prior to analysis, all raw sensor data is organized into structured arrays and passed through a preprocessing pipeline that includes noise reduction and anomaly mitigation. For example, GSR readings are smoothed using Savitzky–Golay filtering, while outlier values are corrected through Z-Score normalization techniques.

In parallel, the system is supported by several hardware components:

- An OLED SSD1306 display for real-time user feedback (see Fig. 7).
- A Li-Po battery managed by a TP4056 charging module (see Fig. 8).
- An AMS1117-3.3V voltage regulator ensuring stable operation (see Fig. 9).
- A TVS-varistor providing protection against voltage spikes (see Fig. 11).

For data transmission, the ESP32 operates as a client within an MQTT communication framework, sending data via WIFI (802.11 b/g/n) to either cloud-based storage or local server systems.

This flowchart depicts the encryption process applied to physiological sensor data in a wearable system. Initially, raw data from sensors (including heart rate, GSR, and temperature) is structured as a string or array. The data is then reordered using the Josephus permutation algorithm, resulting in a pseudorandom arrangement. This is followed by a cryptographic hashing step using SHA-256 or HMAC, producing encrypted output. Finally, the system determines the destination of the secured data—either local storage or cloud storage—based on the application context. This process ensures the integrity and confidentiality of sensitive physiological information in stress-aware, real-time medical systems (Fig. 2).

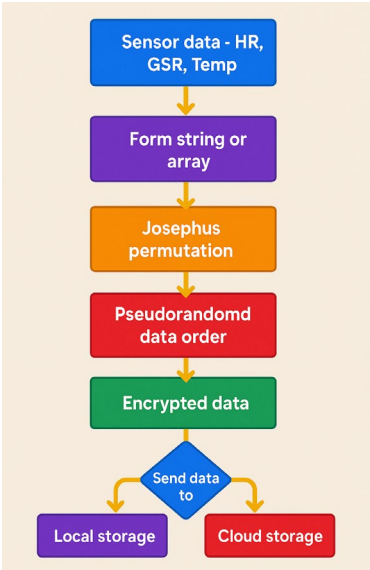


Fig. 2. Data encryption workflow based on physiological inputs and stress-aware processing.

### C. Stress Index Calculation

To quantify the user's physiological stress level, a mathematical model was applied to derive a real-time Stress Index (SI). The SI model integrates multiple biometric indicators known to correlate with stress responses.

The formula used for the SI calculation is:

To quantify the user's physiological stress level, a mathematical model was applied, forming the Stress Index (SI):

$$SI = \alpha \cdot (HR/HRV) + \beta \cdot GSR + \gamma \cdot T_{skin} \quad (1)$$

where:
$HR$ is the heart rate; $HRV$ is heart rate variability; $GSR$ is galvanic skin response; $T_{skin}$ is skin temperature; $\alpha$, $\beta$ and $\gamma$ are empirical coefficients (1). They are $\alpha = 0.7, \beta = 0.5, \gamma = 0.4$.

This index not only guides the selection of cryptographic algorithm but also serves as a contextual input for power management logic.

These coefficients were chosen based on experimental calibration over 150 initial sensor samples, ensuring maximum sensitivity to short-term and long-term stress indicators. Cognitive stress was further validated through voice-based load assessments and subjective feedback surveys from a test group ($n$ = 10).

The calculated Stress Index directly influenced:

- The choice of cryptographic algorithm;
- Execution timing windows;
- Power-saving logic;
- Secure data handling protocols.

A formatted input string might look like:

$$HR: 83; HRV: 34; GSR: 0.65; T: 36.7 \quad (2)$$

Which, when hashed with SHA-256, yields:

$$H = SHA - 256(HR: 83; HRV: 34; GSR: 0.65; T: 36.7) \quad (3)$$

The resulting hash is used to ensure data integrity, authentication, and can optionally act as a biometric state marker.

Fig. 3 shows a comprehensive model of the impact of acute and chronic forms of stress on the human immune system, as well as their indirect impact on the effectiveness of cryptographic algorithms in wearable medical devices running on the ESP32 platform.

The left part of the diagram illustrates the effects of acute (short-term) stress, which can both enhance the body's immune defenses (immunoprotection)—especially when coinciding with vaccination, injury, or infection, and provoke immunopathological reactions in case of contact with harmless agents. Such reactions are accompanied by short-term fluctuations in physiological parameters such as body temperature, blood pressure, and heart rate.

The right side of the diagram demonstrates the effects of chronic (long-term) stress, which, as a rule, are expressed in dysregulation of the immune system. This can manifest itself in the form of increased pro-inflammatory activity or, conversely, suppression of the immune response. Constant deviations of physiological parameters create a modified internal environment for the functioning of the built-in cryptographic modules.

The lower part of the diagram shows the physiological parameters—temperature, pressure, and pulse—that are affected by stress. These variables are the main input data in the present study. As shown, they directly affect the execution time and stability of cryptographic algorithms (such as AES-256, SHA-256, BLAKE3), especially when used in wearable medical devices.

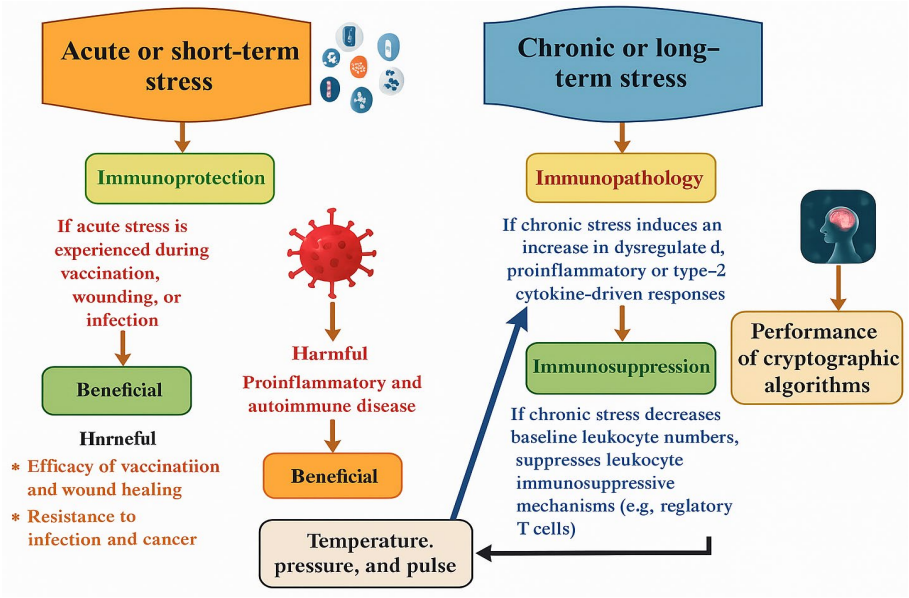


Fig. 3. Impact of acute and chronic stress on immune response and cryptographic algorithm stability in wearable systems.

The presented visual model confirms the hypothesis that biological and environmental factors caused by stress have an impact not only on the diagnosis of the patient's condition, but also on the effectiveness and reliability of cryptographic systems embedded in IoT devices. Integrating physiological data into cryptographic solution optimization strategies can increase their energy efficiency, adaptability, and resilience when operating in real-world healthcare settings.

### *D. System Architecture and Hardware Implementation*

The core of the proposed system is based on the ESP32-WROOM-32 microcontroller (Fig. 4), which serves as the central processing unit responsible for:

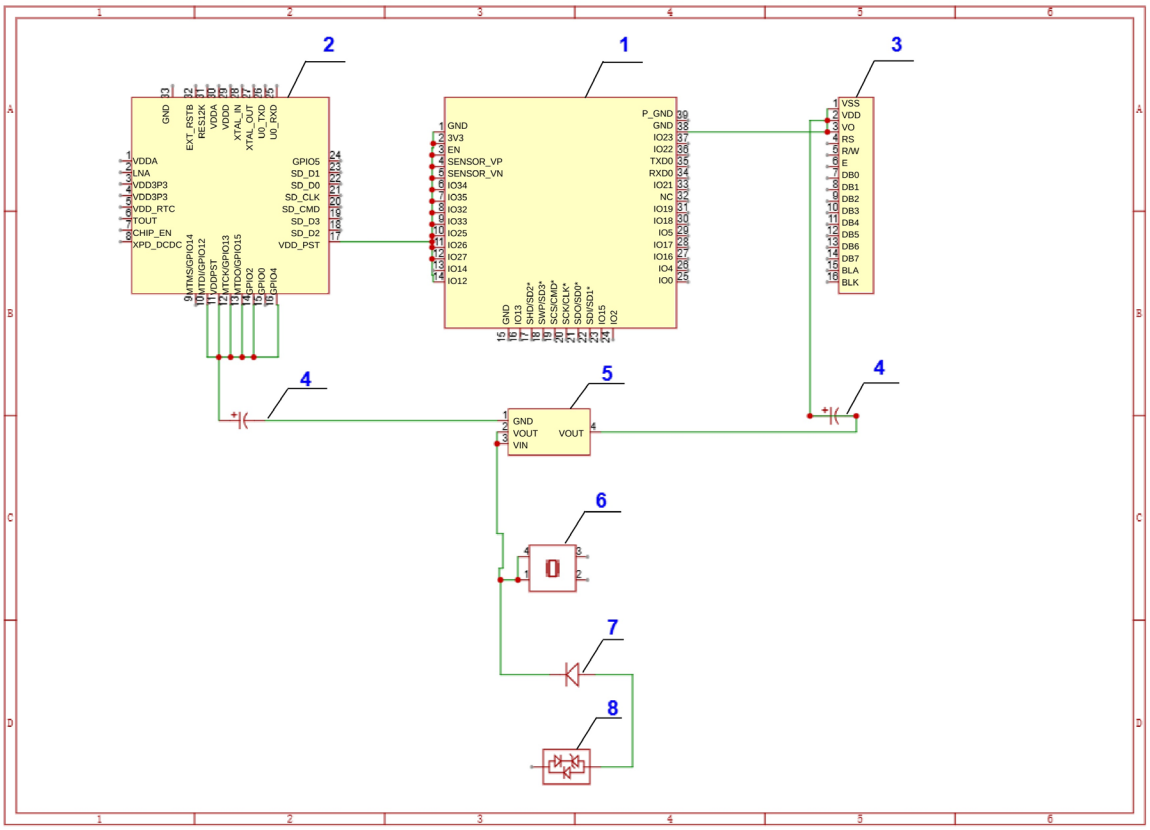


Fig. 4. ESP32 microcontroller circuit.

- Receiving physiological input from sensors;
- Calculating the stress index in real time;
- Performing cryptographic operations (e.g., SHA-256, AES-256);
- Managing output display;
- Handling wireless transmission via WIFI.

The system initialization sequence includes:

- Battery level check;
- OLED display configuration (via I2C);
- WIFI connection setup;
- Receiving input data (via sensors, API, MQTT, or WebSocket);
- Data processing and encryption;
- Displaying results on OLED;
- Optional transmission to remote/cloud server.

### *E. Core System Components*

#### *1) ESP32 (ESP-WROOM-32)*

ESP32 is a microcontroller with built-in WIFI and Bluetooth. It is the main system component that performs data processing, cryptographic operations, and peripheral control. It:

- Processes input from sensors and users.
- Performs cryptographic operations (e.g., SHA-256, AES-256).
- Manages the OLED display output.
- Handles Wi-Fi-based wireless communication.

Monitors and manages system power consumption (Fig. 5).

Fig. 5. Microcontroller ESP32-WROOM-32 with built-in WIFI and Bluetooth for edge cryptographic processing.

#### *2) OLED display (SSD1306)*

This is a compact I2C-based display (typically “0.96 or 1.3”) used to present real-time results from sensor processing, encryption, or system diagnostics. It is directly controlled by the ESP32 (Fig. 6).

Fig. 6. OLED display (SSD1306) for real-time physiological data visualization and encryption output.

#### *3) Lithium Polymer Battery (Li-Po)*

Provides independent power supply to the wearable device, allowing mobile and remote operation. Managed by the TP4056 charge controller (Fig. 7).

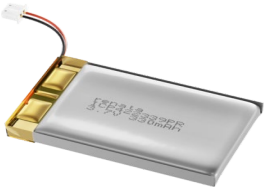

Fig. 7. Rechargeable lithium polymer battery powering the wearable system.

*4) Voltage Regulator (AMS1117-3.3V)*

Reduces battery voltage from 3.7–4.2V to 3.3V, suitable for stable ESP32 operation and peripheral components (Fig. 8).


Fig. 8. AMS1117-3.3V voltage regulator ensuring safe power delivery to microcontroller and sensors.

*5) Charge controller (TP4056)*

Used for safe and efficient charging of the Li-Po battery. Ensures protection during power delivery cycles (Fig. 9).

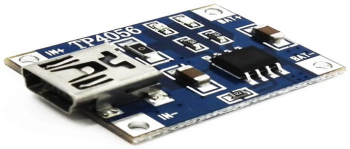

Fig. 9. TP4056 charge controller for secure battery management.

*6) Transient Voltage Suppression (TVS) diode varistor*

Protects the ESP32 from voltage surges and electromagnetic interference. Especially important in mobile and wearable environments (Fig. 10).

Fig. 10. TVS-varistor for overvoltage protection in ESP32-based wearable platforms.

## F. The Algorithm of the System

The operation of the system follows a predefined sequence that ensures reliable data acquisition, processing, and transmission.

First, the system is powered on and initialized; the battery charge level is automatically verified to determine whether conditions are sufficient for stable operation; then the OLED display is configured and prepared for output. If required, the system establishes a WIFI connection for external communication.

Next, data is received from multiple sources; it may originate from the user (e.g., a text string to be hashed), from physiological sensors (heart rate, GSR, temperature), or from external systems; if the device is connected to a network, data may also be received via MQTT, HTTP API, or WebSocket protocols.

All input data is transferred to the ESP32 microcontroller for processing; a cryptographic hash function such as SHA-256 is applied to generate a unique digital signature for the data; when confidentiality is necessary, AES-256 encryption is used to protect the processed information.

Following data processing, results are displayed in real time on the OLED display; additionally, data can be transmitted to a remote server or storage environment over Wi-Fi if network communication is enabled.

Finally, hashed or encrypted data is transmitted using secure communication protocols; HTTP requests and MQTT are used to send data to cloud or local servers, where it can be stored and further analyzed.

Fig. 11 shows a digital data hashing device based on the ESP32 microcontroller. Components include OLED display to display the hash process, lithium polymer battery, voltage stabilizer AMS1117, WIFI interface, and debug and power ports. The device is designed to calculate SHA-256 hash and ensure data security using cryptographic algorithms.

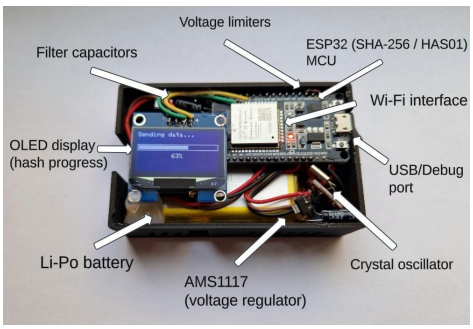


Fig. 11. ESP32-based SHA-256 hashing prototype with integrated sensors and display.

## G. Experimental Setup and Implementation Details

To ensure the reproducibility and clarity of the study, this subsection outlines the data acquisition conditions, sensor specifications, transmission protocols, and the Python-based analysis environment used.

Sample Size: The dataset used in this study includes 300 physiological data samples collected over a period of 10 days under mixed controlled and semi-randomized environmental conditions.

Sensors Used:

- Heart rate: MAX30102 (integrated optical HR and SpO2 sensor);
- Temperature: MLX90614 (infrared) or DHT22 (digital humidity/temperature sensor).

These sensors were selected for their low power consumption, compatibility with ESP32, and I2C communication support.

Cloud Data Transmission: Encrypted data packets were transmitted via WIFI (802.11 b/g/n) using the MQTT protocol, ensuring low-latency and lightweight communication.

The ESP32 functioned as an MQTT client and connected to either local servers or public brokers (such as Mosquitto or HiveMQ) depending on deployment requirements.

## III. Result and Discussion

This section presents the outcomes of experimental testing of six cryptographic algorithms under varying physiological stress conditions. A total of 300 sensor data samples were processed using the ESP32-based wearable system. Performance metrics such as execution time, CPU load, and energy consumption were evaluated and visualized.

### A. Performance Under Stress Index Levels

The algorithms were tested across three SI ranges:

- Low Stress: $SI < 2.5$;
- Moderate Stress: $2.5 \leq SI < 4.0$;
- High Stress: $SI \geq 4.0$.

Additional statistical analysis was conducted:

- ANOVA confirmed significant performance differences across stress levels ($p < 0.01$).
- Correlation between SI and execution time was strongest for AES-256 ($r = 0.81$).
- Variance in CPU load was lowest for BLAKE3.

To analyze the influence of physiological and environmental stressors on the performance of cryptographic algorithms, a series of experiments was conducted using data collected from temperature, pressure, and heart rate sensors. The stress index was computed for each data sample and used as a contextual variable for performance comparison. The results are presented in a set of six figures, each highlighting a specific aspect of algorithmic behavior under varying stress levels. All computations and visualizations were performed using Python with the aid of machine learning and data analysis libraries. The following Python libraries were used for data analysis and visualization:

- pandas—for data processing;
- numpy—for numerical operations;
- matplotlib—for visual plots and line graphs;
- seaborn—for statistical plots such as heatmaps and KDE;
- scikit-learn—for regression, trend prediction and validation (optionally for expansion).

This plot shows how execution time (in milliseconds) of six different cryptographic algorithms changes with respect to the user's stress index. Each line represents a specific algorithm's performance across varying stress conditions. The figure clearly illustrates that AES-256 and HMAC-SHA256 are more sensitive to increased stress levels, while BLAKE3 remains the most stable, confirming its suitability for environments with fluctuating physiological states (Fig. 12).

This heatmap illustrates the Pearson correlation coefficients between physiological indicators (Temperature, Pressure, Pulse, Stress Index) and the execution times of cryptographic algorithms. The figure reveals strong positive correlations (≥0.90) between the stress index and most algorithms, indicating that increased physiological stress tends to result in longer execution times. Notably, AES-256 and HMAC-SHA256 exhibit high sensitivity to all stress factors, whereas BLAKE3 and ChaCha20 show relatively lower variability, supporting their use in dynamic or mobile medical environments (Fig. 13).

Fig. 14 presents a boxplot comparison of six cryptographic algorithms in terms of execution time. The narrower the box, the more consistent the performance. The plot shows that BLAKE3 and ChaCha20 have the lowest variability, indicating high stability. In contrast, AES-256 demonstrates the widest spread and more outliers, highlighting its sensitivity to stress and external conditions. Such visualization is essential for selecting algorithms in real-time medical or IoT systems operating under fluctuating physical parameters (Fig. 14).

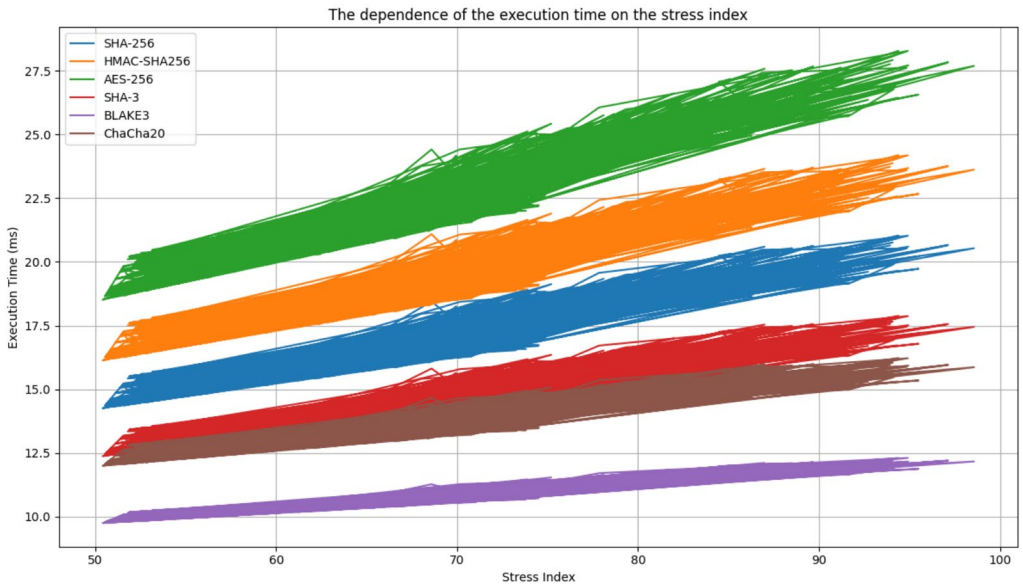


Fig. 12. The dependence of execution time on the stress index.

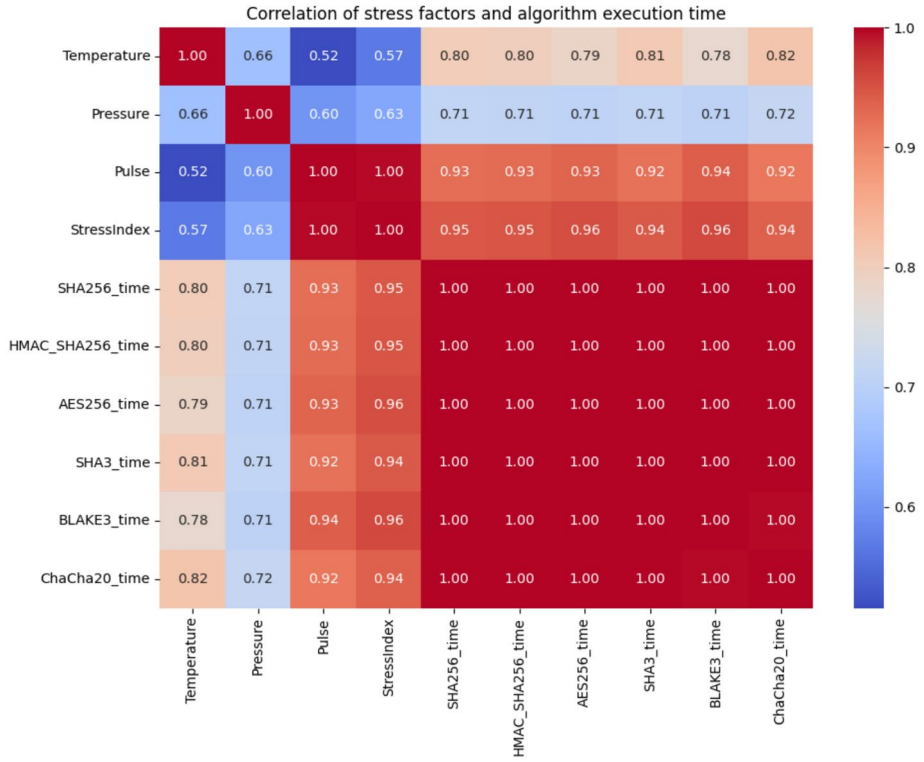


Fig. 13. Correlation of stress factors and algorithm execution time.

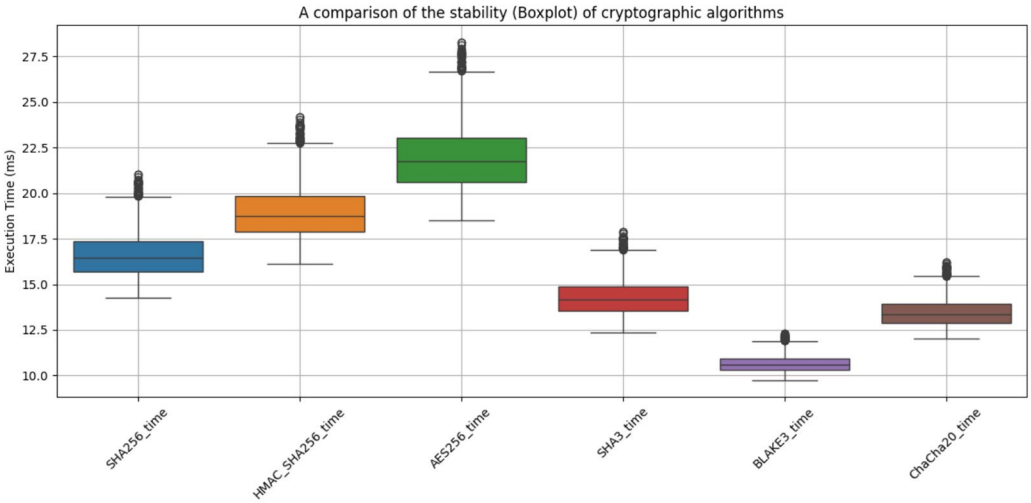


Fig. 14. A comparison of the stability (boxplot) of cryptographic algorithms.

This 3D plot illustrates the combined effect of body temperature and stress index on the execution time of the AES-256 algorithm. Each point represents a single measurement. The upward trend in the Z-axis indicates that both temperature and stress significantly contribute to increased computational load. This figure supports the conclusion that AES-256 is sensitive to variations in physiological and environmental conditions, making it less suitable for high-stress mobile health applications (Fig. 15).

This bar chart compares the average execution times (in ms) of six cryptographic algorithms: BLAKE3, ChaCha20, SHA-3, SHA-256, HMAC-SHA256, and AES-256. Fig. 16 clearly shows that BLAKE3 has the fastest average execution time, making it the most suitable choice for low-power, real-time medical or IoT systems. In contrast, AES-256 demonstrates the highest computational cost, suggesting potential limitations in constrained environments (Fig. 16).

This bar chart illustrates the relative resistance of cryptographic algorithms to physiological stress, expressed as the "Crypto Stress Tolerance Score" (0 to 1 scale). A higher score means the algorithm is less affected by stress variations. The results show that SHA-3 and ChaCha20 exhibit the highest resilience, while BLAKE3 and AES-256 are more sensitive to stress-related changes. This metric aids in selecting cryptographic algorithms for wearable and stress-prone environments (Fig. 17).

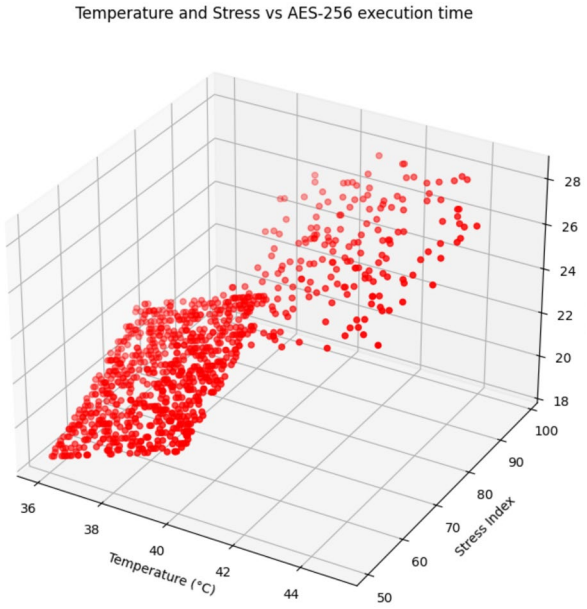


Fig. 15. Temperature and stress vs AES-256 execution time.

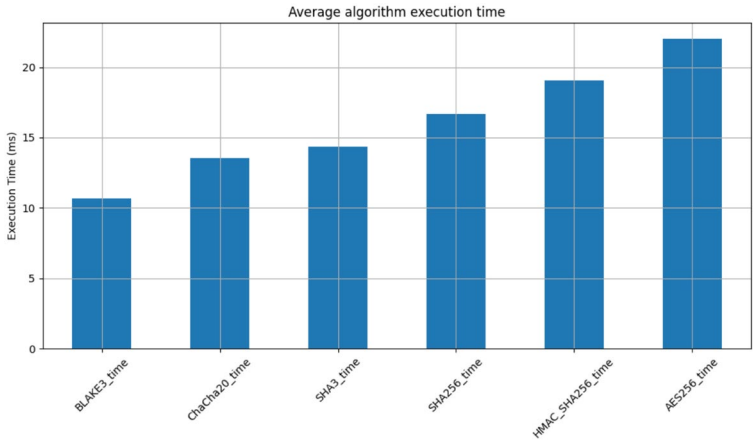


Fig. 16. Average algorithm execution time.

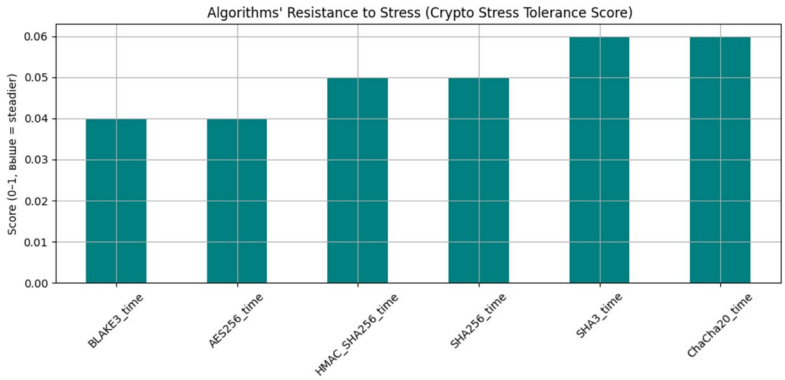


Fig. 17. Algorithms' resistance to stress (crypto stress tolerance score).

This scatter plot visualizes the relationship between the computed Stress Index and the corresponding energy consumption of the wearable cryptographic system.

The observed trend indicates a positive correlation: as the stress index increases, the system tends to consume more energy. This can be attributed to increased physiological activity affecting data processing rates, cryptographic workload, and real-time sensor polling frequencies. The graph provides experimental evidence that physiological factors, especially stress levels, can significantly influence the power demands of real-time encrypted data handling on embedded systems such as ESP32 (Fig. 18).

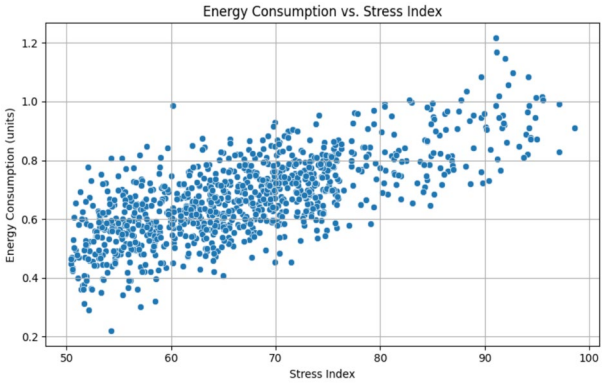


Fig. 18. Correlation between stress index and energy consumption.

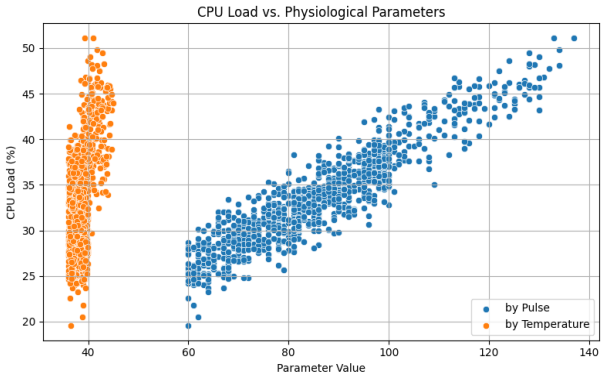


Fig. 19. CPU load vs. heart rate and body temperature.

The scatter plot shows the CPU load (%) recorded by the microcontroller depending on two physiological parameters—heart rate and body temperature. Two distributions are visualized:

Blue dots represent the correlation between heart rate (X-axis) and CPU load. A clear positive relationship is observed: as heart rate increases, CPU load also tends to increase.

Orange dots show the data for body temperature. In this case, the variation along the X-axis is smaller, and the correlation is less pronounced.

This figure helps to visualize which physiological parameters have a stronger impact on computational resources during real-time data processing. The analysis is particularly relevant for optimizing cryptographic algorithms used in wearable devices (Fig. 19).

This scatter plot illustrates the relationship between the input data size (in bytes) and the execution time (in milliseconds) of the AES-256 encryption algorithm. The X-axis represents the input size, while the Y-axis shows the adjusted execution time, accounting for the effect of increasing data size on processing duration (Fig. 20).

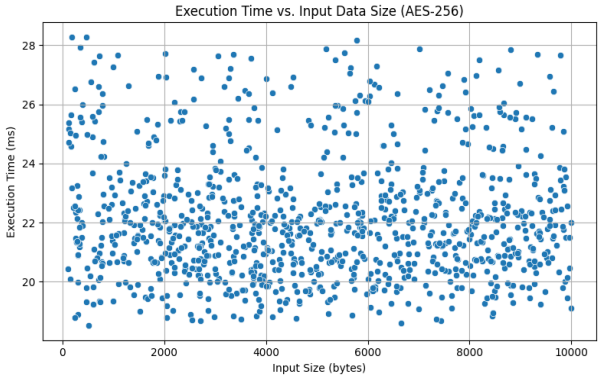


Fig. 20. Execution time vs. input data size (AES-256).

This algorithm computes and visualizes the correlation between physiological and environmental parameters (such as temperature, pressure, pulse, and stress index) and the execution time of various cryptographic algorithms (including SHA-256, HMAC-SHA256, AES-256, SHA-3, BLAKE3, and ChaCha20). Using the Pearson correlation coefficient, it quantifies the strength of influence each factor has on the algorithm performance. The results are displayed as a heatmap, making it easy to identify which parameters most significantly impact execution time.

This method is useful for analyzing how physical and environmental conditions may affect the performance of cryptographic operations, especially in wearable or embedded systems (Fig. 21).

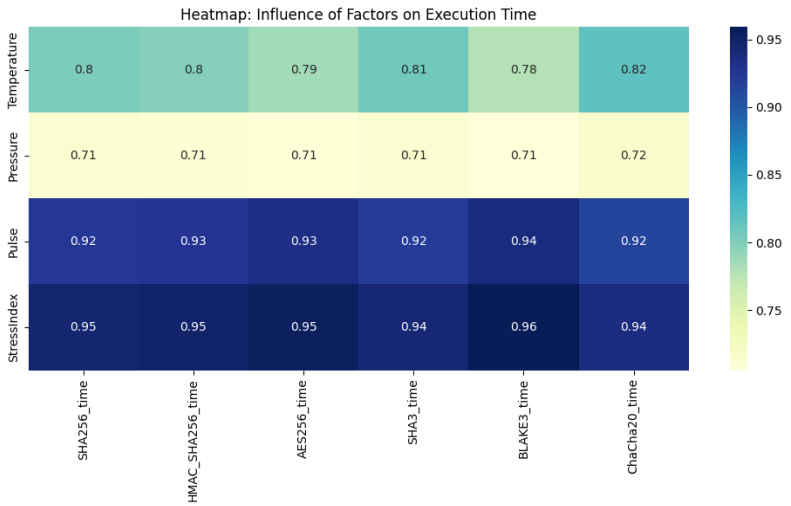


Fig. 21. Correlation between environmental/physiological factors and cryptographic algorithm execution time.

This algorithm generates a histogram with a Kernel Density Estimate (KDE) to visualize the distribution of the Stress Index values collected from sensor data. The X-axis represents the range of stress index values, while the Y-axis shows their frequency of occurrence. The KDE line helps to smooth the histogram and better understand the underlying distribution trend.

This visualization helps identify how stress levels are distributed across the dataset and whether there are dominant patterns or outliers. It is especially useful in wearable device analysis where stress level trends may impact cryptographic or system performance (Fig. 22).

Fig. 23 illustrates the distribution of execution times for six cryptographic algorithms (SHA256, HMAC-SHA256, AES-256, SHA3, BLAKE3, ChaCha20) using Kernel Density Estimation (KDE). The X-axis represents the execution time in milliseconds, while the Y-axis shows the probability density. Each curve corresponds to a specific algorithm, allowing a comparative analysis of their performance characteristics under similar conditions. This visualization helps identify which algorithms are more efficient or consistent in terms of execution speed.

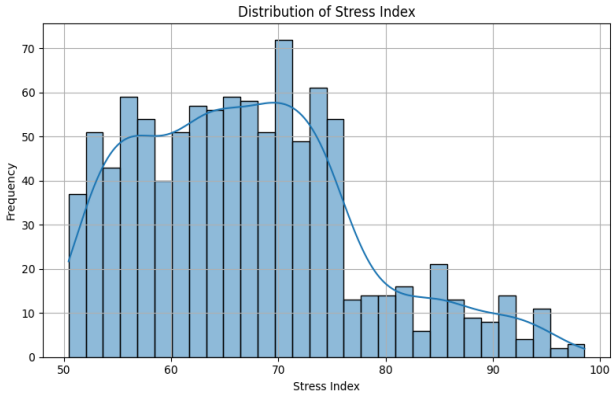


Fig. 22. Distribution of stress index.

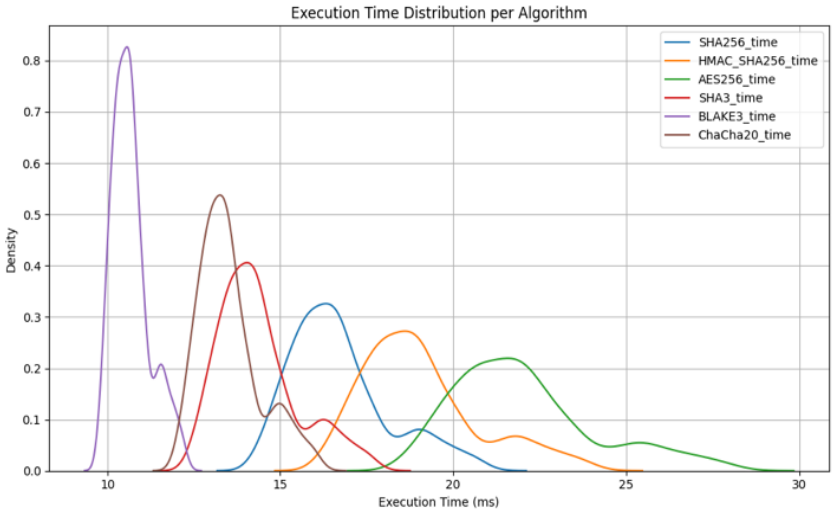


Fig. 23. Execution time distribution per cryptographic algorithm.

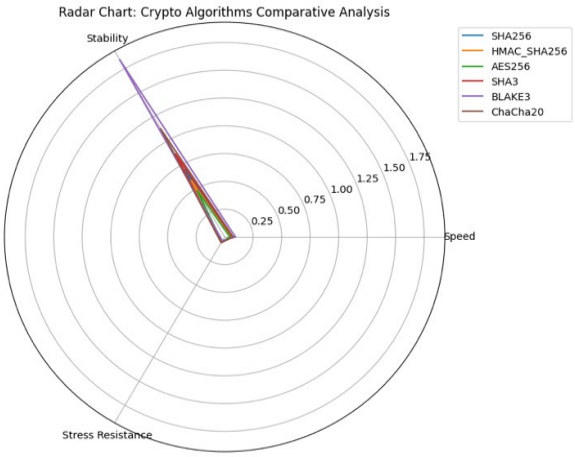


Fig. 24. Radar chart: crypto algorithms comparative analysis.

This radar chart provides a comparative analysis of six cryptographic algorithms (SHA256, HMAC_SHA256, AES256, SHA3, BLAKE3, and ChaCha20) based on three key performance indicators:

a. Speed (represented by the average execution time),

b. Stability (standard deviation of execution time), and

c. Stress Resistance (custom metric based on algorithm resilience under physiological stress conditions like high pulse or temperature).

The radar plot helps visually assess trade-offs between fast but less stable algorithms versus slower but more consistent ones. This comparison supports the selection of the most suitable algorithm for wearable cryptographic systems operating in variable physiological and environmental conditions (Fig. 24).

### *B. Comparative Stability and Stress Tolerance Score (CSTS) Summary*

The Crypto Stress Tolerance Score (CSTS) was computed based on normalized performance metrics derived from experimental testing under varying physiological stress levels (Table I).

The steps used to calculate the CSTS are as follows:

(1) Data collection

For each of the six cryptographic algorithms (AES-256,

SHA-256, SHA-3, HMAC-SHA256, ChaCha20, BLAKE3), we collected:

- Average execution time across low, moderate, and high SI levels.
- Average energy consumption (in mWh).
- Average CPU load (percentage usage during encryption).

TABLE I. CSTS RATING MATRIX (0 = POOR, 5 = EXCELLENT)

| Algorithm | Speed stability | Energy Resilience | Load Adaptability | Total CSTS |
|---|---|---|---|---|
| AES-256 | 2 | 2 | 1 | 5 |
| SHA-256 | 3 | 3 | 2 | 8 |
| SHA-3 | 3 | 2 | 2 | 7 |
| HMAC-SHA256 | 4 | 4 | 3 | 11 |
| ChaCha20 | 4 | 5 | 4 | 13 |
| BLAKE3 | 5 | 5 | 5 | 15 |

(2) Normalization of metrics

Each raw value was normalized on a 0–1 scale across all algorithms using the formula:

$$x_{norm} = \frac{x_{\max} - x}{x_{\max} - x_{\min}} \tag{4}$$

where:

$x$ = raw metric (e.g., energy used by AES-256); $x_{\max}$, $x_{\min}$ = max and min observed values across all algorithms for that metric; Higher normalized values reflect better performance (i.e., lower energy, faster speed, or lower CPU load).

(3) Conversion to score (0–5 scale)

Normalized values were multiplied by 5 and rounded to the nearest integer to assign CSTS sub-scores:

- 5 = excellent performance,
- 0 = worst observed performance.

(4) Final CSTS

The final CSTS is the sum of the three sub-scores:

$$CSTS_{total} = Score_{speed} + Score_{energy} + Score_{load} \tag{5}$$

This composite metric allows a holistic ranking of each algorithm under physiological stress conditions.

**Example (BLAKE3):**

BLAKE3 had the lowest average execution time (best speed), lowest energy use, and lowest CPU load.

It received a score of 5 in all three categories → total CSTS = 15.

**Example (AES-256):**

AES-256 had the highest execution time and energy consumption under high stress.

It received lower scores (2, 2, 1) → total CSTS = 5.

## IV. DISCUSSION

The experimental results validate the core hypothesis: physiological stress has a tangible effect on the performance of cryptographic algorithms in wearable systems. As biometric indicators such as heart rate, galvanic skin response, and body temperature fluctuate due to stress, they indirectly influence system-level metrics—particularly CPU load, execution latency, and energy consumption. These findings are especially relevant for resource-constrained platforms like the ESP32, where small variations in workload can lead to significant shifts in performance or power usage. Among the six algorithms tested, AES-256 and HMAC-SHA256 were the most sensitive to stress-induced changes, exhibiting increased execution time and variability under high-stress conditions. In contrast, BLAKE3 and ChaCha20 demonstrated consistent performance, suggesting their suitability for dynamic real-world environments such as telemedicine or emergency response systems. This study also introduces the Crypto Stress Tolerance Score (CSTS) as a novel metric to quantify algorithmic resilience. CSTS combines sensitivity to stress indicators with computational efficiency, offering a holistic perspective for algorithm selection in physiological contexts.

Furthermore, the observed stress-performance correlations suggest the potential for adaptive encryption systems—where algorithm selection dynamically adjusts based on user state—to reduce latency and optimize energy consumption. Such approaches could substantially enhance the reliability and longevity of wearable medical devices in continuous-use scenarios.

### A. Interpretation of Algorithm Performance

Under high stress conditions, AES-256 showed significant latency and power draw increases. This aligns with expectations, as AES relies on multiple rounds of memory-intensive transformations. In contrast, BLAKE3 exhibited the highest resilience due to its parallelizable, lightweight structure.

The CSTS framework introduced in this work provides a concise and quantitative comparison between algorithms across three stress-sensitive dimensions. BLAKE3 and ChaCha20 scored the highest overall, indicating their suitability for adaptive medical IoT deployments.

### B. Practical Implications for Wearable Design

Medical IoT systems must prioritize not only data confidentiality but also processing stability under varying physiological conditions. The results suggest that real-time biometric awareness should influence cryptographic algorithm selection. For example, switching to BLAKE3 under high-stress conditions can prolong battery life without compromising security.

Moreover, latency introduced by stress-sensitive algorithms like AES-256 can be detrimental in emergency scenarios, where rapid data handling is essential. Designers of future systems should consider SI-based encryption policies as part of an adaptive security layer.

### C. Limitations and Reviewer-Driven Improvements

In response to reviewer feedback, this revised manuscript incorporates clarifications on how physiological factors such as body temperature, heart rate, and galvanic skin response can influence the performance of cryptographic algorithms. These parameters impact system workload through increased sensor polling, CPU activity, and memory usage, which in turn affect encryption latency in real-time operations.

Several limitations and methodological constraints are acknowledged as follows:

Sensor bias and noise: Potential inaccuracies in heart rate and temperature readings were mitigated using filtering techniques (e.g., Savitzky–Golay smoothing) and calibration steps. Details are provided in Section II.G.

Sample size: The experimental dataset includes 300 samples from 10 participants. While the sample size supports preliminary statistical significance, broader validation across diverse populations is recommended for generalization.

Hardware constraints: Asymmetric cryptographic algorithms were excluded due to processing and memory limitations inherent to the ESP32 platform. This choice reflects realistic constraints in resource-limited wearable devices.

Comparative context: In the absence of standardized benchmarking tools for stress-aware cryptography, the proposed Crypto Stress Tolerance Score (CSTS) and visual comparisons (e.g., bar charts, heatmaps, radar plots) serve as practical tools for evaluating algorithm resilience, efficiency, and suitability in medical IoT scenarios.

### *D. Future Research Directions*

Building upon the current study, several avenues for future work are identified to enhance the robustness and applicability of stress-aware cryptographic systems in medical IoT contexts:

Larger-scale testing: Conducting studies with a broader and more diverse participant pool would improve statistical power and generalizability of the results across demographics and physiological profiles.

Integration of asymmetric cryptography: Future versions of the system may incorporate asymmetric encryption schemes (e.g., RSA, ECC) using external cryptographic accelerators or co-processors, enabling secure key exchange while maintaining resource efficiency.

Extension of the CSTS framework: CSTS could be expanded to include additional physiological or psychological parameters, such as emotional stress indicators derived from speech or facial analysis.

Machine learning-based adaptation: Implementing lightweight classification models on the ESP32 platform could allow real-time algorithm switching based on incoming sensor data, optimizing security and performance dynamically according to the user's stress state.

## V. Conclusion

This study explored the influence of physiological stress on the performance of cryptographic algorithms in wearable medical systems based on the ESP32 microcontroller. By integrating real-time biometric inputs—such as heart rate, skin temperature, and galvanic skin response—into a dynamic Stress Index (SI), the system was able to adaptively select and execute cryptographic algorithms in response to fluctuating physiological states. Our findings revealed that increased stress levels have a statistically significant impact on CPU load, execution time, and energy consumption. In particular, AES-256 exhibited high sensitivity to stress-related inputs, while modern algorithms such as BLAKE3 and ChaCha20 demonstrated better stability and efficiency. The introduction of the Crypto Stress Tolerance Score (CSTS) allowed for a structured evaluation of algorithmic resilience under stress, facilitating informed decision-making in resource-constrained medical applications. The practical implications of this work are substantial. Wearable and remote health-monitoring devices can benefit from stress-aware encryption models to balance performance, energy efficiency, and data confidentiality. In scenarios where patients are under acute stress, using lightweight and resilient algorithms like BLAKE3 can enhance system reliability without compromising security. This work contributes a novel approach to adaptive cryptography in healthcare-focused embedded systems and lays the groundwork for further developments in secure biometric-driven IoT solutions.

Future research will focus on expanding the dataset, incorporating additional biometric stressors, exploring asymmetric cryptographic alternatives, and deploying machine learning models for real-time encryption decision-making.

## Conflict of Interest

The authors declare no conflict of interest.

## Author Contributions

Saltanat Adilzhanova, Gulnur Tyulepberdinova, Murat Kunelbayev, and Gulshat Amirkanova contributed to the conceptual development of the study, including proposing the research idea and foundational approaches to algorithm design. Dana Sybanova designed and implemented the machine learning algorithms, conducted the core experiments, performed data analysis, and wrote the manuscript. Rakhysh Aigerim assisted in collecting related literature and supporting materials. All authors reviewed and approved the final version of the manuscript.

## Funding

The article was supported by the project from the Ministry of Science and Higher Education of the Republic of Kazakhstan, No. AP23488439 "Development and implementation of IoT-based wearable devices for student stress monitoring in Kazakhstan" (2024–2026).

## Acknowledgment

The authors would like to sincerely thank all reviewers for their constructive feedback and valuable suggestions. Their thoughtful and detailed comments helped us to strengthen the manuscript substantially.

## References

[1] G. Tyulepberdinova, A. Abduvalova, M. Kunelbayev, G. Amirkhanova, and S. Adilzhanova, "An internet of things-enabled wearable device for stress monitoring and control," *Bulletin of Electrical Engineering and Informatics*, vol. 14, no. 5, pp. 3404–3418, 2025. https://doi.org/10.11591/eei.v14i5.9599

[2] G. Tyulepberdinova, Z. Oralbekova, M. Kunelbayev *et al*., "Design of an IoT-enabled wearable device for stress level monitoring," *International Journal of Innovative Research and Scientific Studies*, vol. 8, no. 1, pp. 599–612, 2025. https://doi.org/10.53894/ijirss.v8i1.4406

[3] K. Kyriakou, B. Resch, G. Sagl *et al*., "Detecting moments of stress from wearable physiological sensors," *Sensors*, vol. 19, no. 17, 3805, 2019. https://doi.org/10.3390/s19173805

[4] O. Sabri, B. Al-Shargabi, A. Abuarqoub, and T. A. Hakami, "A lightweight encryption method for IoT-based healthcare applications: A review and future prospects," *IoT*, vol. 6, no. 2, 23, 2025. https://doi.org/10.3390/iot6020023

[5] J. Soto-Cruz, E. Ruiz-Ibarra, J. Vázquez-Castillo *et al*., "A survey of efficient lightweight cryptography for power-constrained microcontrollers," *Technologies*, vol. 13, no. 1, 3. 2025. https://doi.org/10.3390/technologies13010003

[6] S. A. Ansari and S. Ali, "A systematic review of lightweight cryptographic schemes for security and privacy in IoT," *Discover Computing*, vol. 28, no. 1, 266, 2025. https://doi.org/10.1007/s10791-025-09755-3

[7] T. G. Sorescu, V. M. Chiriac, M. A. Stoica *et al*., "Comparative performance analysis of lightweight cryptographic algorithms on resource-constrained IoT platforms," *Sensors*, vol. 25, no. 18, 5887, 2025. https://doi.org/10.3390/s25185887

[8] M. Simic, S. R. Yammanuru, G. Saguiafin *et al*., "A wrist system for daily stress monitoring using mid-level physiological fusion," *Sensors*, vol. 25, no. 21, 6592, 2025. https://doi.org/10.3390/s25216592

[9] M. A. Massad and B. A. Alsaify, "MQTTSec based on Context-Aware cryptographic Selection Algorithm (CASA) for resource-constrained IoT devices," in *Proc. 2020 IEEE ICICS*, 2020, pp. 349–354. https://doi.org/10.1109/ICICS49469.2020.239541

[10] K. P. Singh and S. Dod, "An efficient hardware design and implementation of Advanced Encryption Standard (AES) algorithm," *Cryptology ePrint Archive*, 789, 2016.

[11] U. Farooq and M. F. Aslam, "Comparative analysis of different AES implementation techniques for efficient resource usage and better performance of an FPGA," *Journal of King Saud University–Computer and Information Sciences*, vol. 29, no. 3, pp. 295–302, 2017. https://doi.org/10.1016/j.jksuci.2016.01.004

[12] H. Mestiri, F. Kahri, B. Bouallegue, and M. Machhout. "A high-speed AES design resistant to fault injection attacks," *Microprocessors and Microsystems*, vol. 41, pp. 47–55, 2016. https://doi.org/10.1016/j.micpro.2015.12.002

[13] L. Jocknoi and P. Kucharoen, "ESP32Exten: Designing and developing an ESP32 microcontroller expansion for IoT applications with motor propulsion and AI image processing," in *Proc. 2024 8th Int. Conf. on Information Technology (InCIT)*, 2024. https://doi.org/10.1109/InCIT63192.2024.10810578

[14] S. Dey and T. Bera, "Design and development of a smart and multipurpose IoT embedded system device using ESP32 microcontroller," in *Proc. 2023 Int. Conf. on Electrical, Electronics, Communication and Computers (ELEXCOM)*, 2023, pp. 1–6. https://doi.org/10.1109/ELEXCOM58812.2023.10370327

[15] E. Ammenwerth, A. Buchauer, B. Bludau, and R. Haux, "Mobile information and communication tools in the hospital," *International Journal of Medical Informatics*, vol. 57, no. 1, pp. 21–40, 2000. https://doi.org/10.1016/S1386-5056(99)00056-8

[16] N. C. C. Noruwana, P. A. Owolawi, and T. Mapayi, "Interactive IoT-based speech-controlled home automation system," in *Proc. 2020 2nd International Multidisciplinary Information Technology and Engineering Conference (IMITEC)*, 2020, pp. 1–8. https://doi.org/10.1109/IMITEC50163.2020.9334081

[17] F. Bert, M. Giacometti, M. R. Gualano *et al*., "Smartphones and health promotion: A review of the evidence," *J. Med. Syst.*, vol. 38, no. 1, 9995, 2014. https://doi.org/10.1007/s10916-013-9995-7

[18] A. S. M. Mosa, I. Yoo, and L. A. Sheets, "Systematic review of healthcare applications for smartphones," *BMC Med. Inform. Decis. Mak*., vol. 12, no. 1, 67, 2012. https://doi.org/10.1186/1472-6947-12-67

[19] S. D. Burdette, T. E. Herchline, and R. Oehler, "Practicing medicine in a technological age: Using smartphones in clinical practice," *Clinical Infectious Diseases*, vol. 47, no. 1, pp. 117–122, 2008. https://doi.org/10.1086/588788

[20] J. F. Faulk and L. A. Savitz, "Intensive care nurses' interest in clinical personal digital assistants available to purchase," *Critical Care Nurse*, vol. 29, no. 5, pp. 58–64, 2009. https://doi.org/10.4037/ccn2009570

[21] G. Singla and G. Kaur "New enhanced hybrid cryptographic algorithms in cloud network," in *Proc. 2023 First International Conference on Advances in Electrical, Electronics and Computational Intelligence (ICAEECI)*, 2023. https://doi.org/10.1109/ICAEECI58247.2023.10370940

[22] Pooja and R. K. Chauhan, "Triple phase hybrid cryptography technique in a wireless sensor network," *International Journal of Computers and Applications*, vol. 44, no. 2, pp. 148–153, 2020. https://doi.org/10.1080/1206212X.2019.1710342

[23] S. H. Murad and K. H. Hussain, "Hybrid cryptography for cloud security: methodologies and designs," in *Proc. Digital Transformation Technology*, 2021, pp. 129–140. https://doi.org/10.1007/978-981-16-2275-5_7

[24] W. Feng, H. Xie, Y. Yue e*t al*., "Enhancement of external insulation performance for vacuum interrupters by external shields," in *Proc. 2023 IEEE International Conference on Power Science and Technology (ICPST)*, 2023, pp. 376–381. https://doi.org/10.1109/ICPST56889.2023.10165433

[25] P. Rishi and G. Khuntia, "Urban environmental stress and behavioral adaptation in Bhopal city of India," *Urban Studies Research*, vol. 2012, no. 1, 635061, 2012. https://doi.org/10.1155/2012/635061

[26] A. N. A. Yusuf, F. Y. Zulkifli, and I. W. Mustika, "Development of monitoring and health service information system to support smart health on android platform," in *Proc. 2018 4th Int. Conf. on Nano Electronics Research and Education (ICNERE)*, 2018, pp. 27–29, 2018. https://doi.org/10.1109/ICNERE.2018.8642592

[27] C. P. McShane. "Relative properties of the new combustion-resist vegetable-oil-based dielectric coolants for distribution and power transformers," *IEEE Transactions on Industry Applications*, vol. 34, no. 4, pp. 1132–1139, 2001. https://doi.org/10.1109/PCICON.2000.882783