ISSN: 2093-5374 / E-ISSN: 2093-5382

Real-Time Stress Detection and Secure Communication in Wireless IoT Networks Using the Secure Dual-Stream Edge Fusion Optimization (SDEFO) Algorithm

Wad Ghaban[1*]

[1*]Assistant Professor, Computer Science Department, Applied College, University of Tabuk, Saudi Arabia. wghaban@ut.edu.sa, https://orcid.org/0000-0003-0564-4377

Received: April 05, 2025; Revised: May 22, 2025; Accepted: June 10, 2025; Published: June 30, 2025

Abstract

The rapid proliferation of Internet of Things (IoT) technologies has enabled the development of more advanced applications, such as stress detection in healthcare and occupational settings. Still, IoT networks face vulnerabilities related to privacy and latency requirements during real-time aerial data processing. This work proposes a paradigm-shifting Secure Dual Stream Edge Fusion Optimization (SDEFO) algorithm that simultaneously solves two significant challenges: (1) real-time stress monitoring and automated feedback using physiological sensor data; and (2) communication security across wireless IoT nodes. Within the proposed SDEFO framework, dual-stream edge analytics bio-signal processing (e.g., GSR or heart rate variability) is emotion-aware and deregulated. At the same time, network threat levels dictate responsive routing and encryption at the node level. A multilayered fusion technique integrates biometric feature extraction with entropy-based secure transmission, strengthening reliability and privacy simultaneously. The system is tested on a real-time dataset acquired through wearable IoT sensors under various stress levels and network threat simulations. Evaluation results demonstrate enhanced accuracy in stress detection, accompanied by lower packet loss and improved resilience to denial-of-service attacks and data tampering. The model demonstrates improvement over other proposed single-stream and non-secure configurations in latency, throughput, and security index. This study has significant implications for health monitoring, innovative workplaces, and defense communication systems, where both data transmission reliability and confidentiality are crucial. This paper presents a novel, multilayered architecture that integrates affective computing with cryptographic routing to enhance the design of intelligent, secure, and adaptive IoT networks.

Keywords: Real-time Stress Detection, Secure Communication, IoT Networks, Edge Computing, Dual-stream Optimization, Wireless Security, SDEFO Algorithm.

1 Introduction

1.1 Emergence of Real-Time Stress Detection in IoT

The use of wireless IoT frameworks for real-time stress recognition has advanced rapidly due to their applications in remote healthcare, wellness monitoring, and emergency response systems. It is now possible to identify individual and situational stressors based on biometric indicators such as heart rate

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), volume: 16, number: 2 (June), pp. 886-902. DOI: *10.58346/JOWUA.2025.I2.055*

*Corresponding author: Assistant Professor, Computer science department, Applied college, University of Tabuk, Saudi Arabia.

variability and skin conductance. However, systems that rely on real-time decision-making algorithms must achieve near-instantaneous responsiveness, high reliability, and strong data security. Centralized cloud-based IoT systems are particularly vulnerable to latency challenges due to both remote processing and network delays. That is why performing stress recognition at the edge level is more effective in responding to real-time requirements and granting system independence (Ali et al., 2021).

Local data processing is possible in edge computing, which decreases the need for data transmission and lowers latency. In a decentralized setting, IoT nodes equipped with processing units are capable of detecting and responding to stress autonomously, thereby operating independently. This change in architecture reduces the strain placed on cloud servers while allowing for greater flexibility in smart cities and portable health monitoring systems. The combination of affective computing and edge analysis represents a shift towards proactive systems that enhance mental health surveillance and ensure real-time reaction capabilities (Matkarimov et al., 2025 and Zhang et al., 2022).

1.2 Security Vulnerabilities in Wireless IoT Networks

The unprotected nature of the transmission channels in IoT systems enables multiple data security breaches, including eavesdropping, data injection, and spoofing (Enoch et al., 2020). Transmission security is especially critical when dealing with sensitive stress-related biometric data, as it can be vulnerable to privacy breaches or deliberate tampering. This issue is particularly problematic in the healthcare sector, where data security is of paramount importance. Design strategies for security should be embedded in the system architecture from the beginning and not added as an afterthought.

Research shows that IoT devices with limited processing capabilities can leverage lightweight cryptographic methods, such as ChaCha20 or Serpent. These methods, however, often lack proper contextual adjustment concerning the level of threat and the significance of the data being transmitted. User state and network conditions must be actively monitored, particularly when implementing stress detection systems and corresponding security policies. Biometric data can be transmitted securely using dynamic key management through edge-based encryption modules, as described in (Najm et al., 2024) and (Chen et al., 2023).

1.3 Dual-Stream Processing: Merging Stress and Security

Biometric assessment for emotion recognition, as well as communication processing, which are both real-time in nature, is more efficient with modern edge-AI models using dual-stream frameworks. The first stream focuses on analyzing physiological metrics, including heart rate and GSR, while the second monitors the network for any integrity breaches and malicious activities. With this form of parallel processing, both the user's emotional state and network behavior can be monitored simultaneously, which greatly assists decision-making in unpredictable situations (Roy & Das, 2022).

The resulting combination of both streams at the edge node enables sophisticated control for predicting stress as well as the pathways for data transmission. For instance, if a user is exhibiting some level of stress and, at the same time, network entropy is rising, the system may engage advanced encryption or secure routing. Such responses are crucial when dealing with cost-sensitive IoT systems, as both precision and security must be maintained simultaneously. Such frameworks will enable context-aware systems, which are intelligence systems that place a high emphasis on user privacy (Yemunarane et al., 2024 and Liu et al., 2024).

1.4 Adaptive Routing Based on Contextual Entropy

In the Internet of Things domain, routing approaches are typically focused on maximizing throughput and conserving energy. Factors such as data sensitivity or user states are often overlooked. In the case of stress-related systems, however, considerations of biometric urgency and network threat levels become critical in determining transmission pathways. Entropy routing methods assess signal-bead variations and channel randomness to identify real-time heuristic instability or intrusion attempts (Boopathy et al., 2024).

Integrating these entropy measures with stress analytics enables dynamic adjustment of packet prioritization, routing, and selection. For example, in environments with higher eavesdropping risks, high-stress packets may be rerouted through secure channels, encrypted tunnels, or verification locks and delayed until after scrutiny. Such adaptability in execution ensures the safe delivery of significant health packets to designated nodes. Critical health edge nodes with autonomous secure routing algorithms dramatically enhanced responsiveness and resiliency in essential domains of response (Hassan et al., 2021 and Moreau & Sinclair, 2024).

1.5 Toward Unified and Scalable Secure IoT Health Systems

The majority of systems available today separate stress detection and security processes, resulting in workflow fragmentation and performance stagnation. For adequate scaling, a single-edge system is required that merges biometric processing with adaptive encryption and entropy-aware routing. This problem gap is addressed with the holistic approach of the Secure Dual-Stream Edge Fusion Optimization (SDEFO) algorithm (Tiwari & Raj, 2023).

SDEFO streamlines command and control communications through parallel continuous processing and fusion of biometric signals and environmental metrics. It ensures the timely and secure transmission of stress-related events, even under adverse network conditions. Such frameworks can scale across healthcare, military, and emergency applications, providing real-time monitoring while safeguarding privacy. The integration of these systems addresses the need for intelligent, self-protecting IoT systems in remote healthcare (Tran & Ngoc, 2024 and Chatterjee & Ghosh, 2022).

Key Contributions:

- An evolution of the existing IoT paradigm–based systems, the SDEFO algorithm implements secure dual-stream edge fusion optimization to achieve efficient stress monitoring and secure data transmission simultaneously in wireless IoT frameworks.
- The system processes biometric data and network entropy data streams in parallel, allowing adaptive context-aware encryption, packet prioritization, and secure routing decision-making.
- A set of mathematical models is proposed to compute decision scores, entropy thresholds, and data transmission priorities, as well as to calculate the optimal multi-hop latency-responsive routing.
- Through extensive testing with various combinations of bio-signals, the performance of the SDEFO exceeded that of traditional classifiers in terms of F1-score, accuracy, and system adaptability.

- Providing functional security coverage while minimizing vulnerability metrics and execution time, comparative tables validate the efficiency of SDEFO for edge-based implementations.
- The lightweight model approach enables the construction of a realistic IoT architecture, alongside dual-stream analytic models, for real-time, low-latency, and responsive operation in health monitoring and other vital use cases.

This paper aims to address the interwoven problems of real-time stress detection and secure communications in wireless IoT settings. It is helpful to analyze existing works on stress surveillance and IoT security to identify critical gaps concerning merger, delay, and data privacy. To address these gaps, the paper introduces an algorithm known as Secure Dual-Stream Edge Fusion Optimization (SDEFO), which incorporates a dual-stream edge computing framework and adaptive encryption based on biometric appraisal, as well as network entropy derived from the biometric feed. The SDEFO model is validated through a comparative assessment using traditional classifiers with different combinations of bio-signals for the measurement of accuracy, macro F1-score, and weighted multi-dimensional evaluation indices. These results demonstrate the successful model, which offers the necessary security, low latency, and accurate stress classification, with the overload region flagged securely. This paper concludes by suggesting further developments such as integrating federated learning with blockchain-based identity management and deploying energy-efficient wearables for greater scalability and resilience in practical use scenarios.

2 Literature Survey

The real-time detection of stress within IoT frameworks has gained significant prominence due to its diverse applications in mental health, occupational wellness, and innovative healthcare. Studies show that intelligent monitoring systems with distributed edge analytics decrease the system's latency and improve accuracy for stress detection. Typically, these frameworks combine local signal preprocessing, real-time pattern recognition, responses triggered by specific events, and real-time autonomous governance for rapid response to stress events. Additionally, machine learning models combined with the sensing of aquatic and environmental bio-signals from IoT devices extend the reach of emotional monitoring systems beyond human health to ecological and aquacultural domains (Mehra & Patel, 2024). Moreover, essential management frameworks based on metrics help validate performance in sectors such as healthcare and industry (Yang et al., 2024). Research focusing on the changes caused by urbanization in mental health drives the demand for flexible and geospatially adaptive frameworks for stress detection and situational awareness (Nakamura & O'Donnell, 2025).

Privacy concerns and the need for encryption to secure wireless transmission remain two persistent issues in the online healthcare IoT ecosystem. Research indicates that devices that communicate over public or unsecured networks are vulnerable to breaches that could expose patient-sensitive information. These issues have been addressed through fog and edge computing, where encrypted computation is done close to the data source, thereby streamlining the process and limiting the risk of external interference (Singh et al., 2022). Some scholars support the implementation of E-Healthcare systems that incorporate machine learning and predictive analytics for securely managing data access, particularly in cases of cancer, where early-stage detection significantly improves prognosis (Dixit & Bhagat, 2021). In contrast, some focus on enhancing privacy through blockchain technology and secure routing in critical mission applications, such as disaster monitoring and patient mobility tracking (Feng et al., 2025).

The incorporation of behavioral and psychological signal processing techniques has started to be integrated into stress detection systems, and different comparative studies have investigated emotional variations within populations as well as occupational groups. For instance, the psychological stress markers of special education teachers were shown to be markedly different from those in mainstream teaching environments, supporting the case for individualized stress analytics in IoT health frameworks (Reddy & Jaiswal, 2022). Other studies have examined hypnosis and behavior therapy as stress management techniques; findings from these studies could inform algorithmic models for bio-signal interpretation on edge devices (Alsaeedi & Alzahrani, 2021). In addition, the need for continuous data capture, particularly for stress monitoring in emergency responder scenarios, has led to the study of mobile and constrained application environments that integrate wireless communication methods, such as rotating magnet antennas (Delgosha et al., 2017).

The Alexa system utilizes conversational agents to monitor stress and conduct health assessments, made possible by the shift towards voice-activated and integrated healthcare systems. Such systems require real-time interfaces between users and cloud or edge analytical systems (Zhao & Lin, 2023). In these systems, security is paramount, and some researchers propose a fusion of signal compression, encryption, and adaptive data transfer protocols to maintain the integrity of biometric information (Tamannaifar & Golmohammadi, 2014). These systems not only maintain the quality of the transmitted data but also optimize the efficiency of network utilization within a changing IoT topology. Moreover, research on hybrid workspaces coupled with employee wellness programs illustrates the increasing need for ambient, continuous stress monitoring integrated into occupational IoT systems (Rajalakshmi & Mahendran, 2023).

Ultimately, the scope of secure IoT frameworks extends beyond healthcare to encompass cross-domain applications, including brand marketing, e-commerce, and smart logistics. Novel Consumer Behavior Analytics frameworks that apply neural networks and blockchain for information determinism and decision-making are capable of accommodating new stress-related use cases (Mleh et al., 2023). In these areas, biometric signal processing frameworks are increasingly integrated with AI models, such as CNN and LSTM, which provide accurate predictions even with noisy or incomplete data for high-stakes forecasting tasks (Nguyen & Tran, 2024). Recent publications substantiate the need for real-time, secure models like SDEFO for responsive and resilient environments requiring guarded, stress-laden exchanges—hence the appeal of integrating affective computing, entropy-based encryption, and adaptive analytics into a single IoT framework. (Sakthive et al., 2019).

3 Methodology

This section of the document describes the technological aspects of the system design, focusing on the integration of real-time biometric assessment with adaptive security frameworks for wireless IoT networks. The SDEFO algorithm processes network threats and physiological stress indicators concurrently, forming the backbone of the methodology. The system is purpose-built for edge deployment, facilitating near-real-time analytics and the secure transmission of sensitive information. It integrates biometric and communication metrics through a contextual entropy framework. For this, the model utilizes a dual-stream parallel framework, secure routing logic, and entropy-centric encryption. This yields a dynamic adaptation model with strong privacy guarantees and effective resilience in a highly variable environment.

3.1 Dual-Stream Edge Fusion Model for Stress-Security Optimization

The SDEFO algorithm integrates biometrics and network data in parallel to make intelligent decisions. It processes real-time physiological signals, such as heart rate, separately from communication network metrics, including signal integrity and threat levels. Stream processing occurs at the edge device, where scores are computed for merging. The fused score determines encrypted routing strategy, packet prioritization, and tiered encryption frameworks. This system maintains a favorable balance between urgency and security in volatile, stressful, network-vulnerable environments.

A weighted scoring model was selected to evaluate the composite risk level derived from biometric and network data. This serves as a decision score. Based on the computed score, the system decides whether immediate data transmission, enhanced encryption, or delayed transmission to secure conditions is optimal.

$$D_s = \alpha . H_b + \beta . H_n \quad (1)$$

Where:

- D_s Overall decision score
- H_b Entropy of biometric data
- H_n Entropy of network status
- α, β Adjustable weight parameters

As indicated in Equation 1, the final score is computed as a fusion of changes in biometrics alongside network anomalies. Stress response and communication security escalate simultaneously in a more severe scenario, thus warranting immediate secure data transmission. Depending on the situation, the system can prioritize health or security risks by varying the effects of each stream.

$$P_i = \frac{D_s . A_t}{T_t + 1} \quad (2)$$

Where:

- $P_{i:}$ Priority index of the data packet
- $D_{,s}$ Decision score from Equation 1
- A_t the Activity level of the user (e.g., detected through motion sensors)
- T_t Current traffic load on the network

As explained in Equation 2, the system allocates transmission priority for each data packet. The priority level will increase during user activity or stress under manageable network loads. If the network is congested, lower-priority packets are held in delay to avoid overloading the network. This ensures that critical health information is transmitted in real-time, while non-essential packets are queued in a controlled manner to optimize network utilization.

3.2 SDEFO Framework Flow

The Secure Dual-Stream Edge Fusion Optimization (SDEFO) framework enables intelligent and secure data communication by integrating real-time biometric surveillance and network condition evaluation. In real-time edge computing settings, the system monitors vital physiological signals, including the heart rate and temperature, alongside the network's latency and traffic load. By utilizing two independent data

streams, the model ensures user well-being and mitigates the risk associated with communication before data transmission. Such responsiveness and security bolsters the effectiveness of wireless IoT networks.

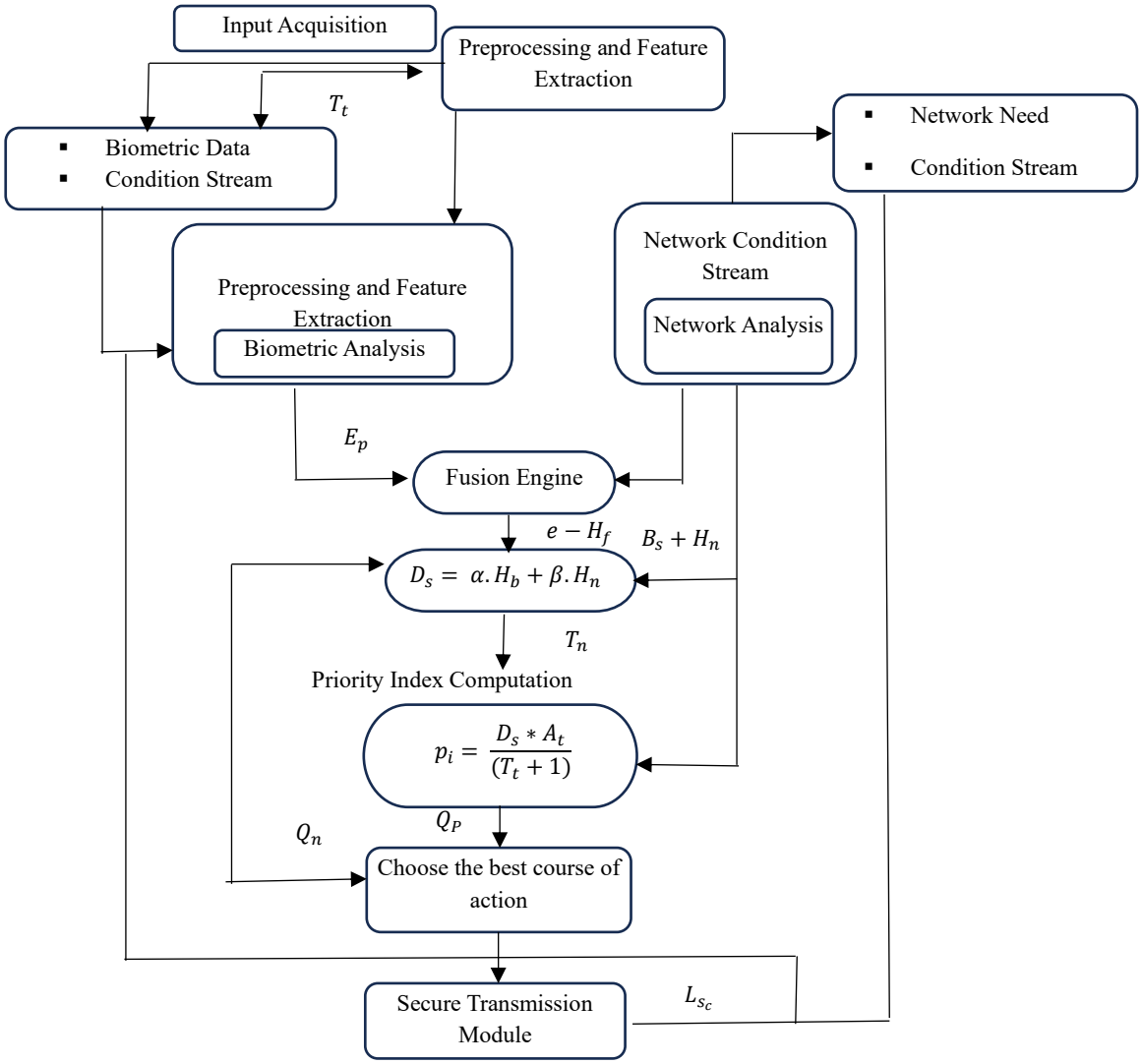

Figure 1: SDEFO System Flow Diagram

Figure 1 illustrates the SDEFO algorithm's workflow, which receives biometric signals and network conditions as incoming data streams and processes them separately. After feature extraction, the individual analyses are integrated in a fusion module that assesses the overall status from both streams. The interpretation then informs a decision-making unit, which determines the extracted, encrypted, transmitted, delayed, or rerouted action dictated by the data. This decision is implemented through a transmission module that ensures secure and sensitive delivery of contextual data, tailored to the situational context. This organized framework enables automated system changes dependent on user health and communication risk.

3.3 Mathematical Modeling of SDEFO

The dual-stream entropy analysis, combined with adaptive logic, forms the basis for the SDEFO framework, which enables real-time communication cuts in IoT systems. Given that decision score D*s*

*and priority index P*i have been established, the following further-defined equations help reinforce dynamic edge algorithms by enhancing threshold control, routing behavior, resource utilization, and delay estimation.

$$H_b = \sum_{i=1}^{n} p_i log_2(p_i) \quad (3)$$

$$H_n = \sum_{j=1}^{m} q_i \, log_2(q_j) \quad (4)$$

$$\tau = \gamma . mean\,(D_s) \quad (5)$$

$$R_d = \begin{cases} Encrypt\ and\ Transmit, & if\ D_s > \tau\ and\ P_i > \delta \\ Transmit\ Only, & if\ D_s \leq \tau\ and\ P_i > \delta \\ Defer\ or\ Reroute, & if\ P_i \leq \delta \end{cases} \quad (6)$$

$$E_f = \frac{\sum_{k=1}^{n} P_i^k}{n.R_u} \quad (7)$$

$$T_d = \frac{R_c.P_i}{L_n} \quad (8)$$

The provided equations enhance the decision-making ability of SDEFO. Entropy metrics associated with biometric and network data are captured in equations 3 and 4, which justify real-time risk assessment from a statistical perspective. Equation 5 sets a dynamic limit on the activation of encryption processes using the average decision score. Risk and urgency-based action selection is given in equation 6, which is fundamental to the routing logic layer. The system-level effectiveness and estimated delay, as defined by Equations 7 and 8, ensure the efficient use of routing resources with low-latency transmission. Collectively, these models allow algorithm SDEFO to function adaptively under diverse users and network conditions in edge-based IoT ecosystems.

3.4 Algorithm Process

Data Acquisition

The SDEFO algorithm begins by continuously collecting data in real-time from two sources. Users' biometric data, which includes heart rate, oxygen saturation (SpO_2), and body temperature, is obtained via wearable devices. At the same time, the system monitors network metrics, including latency, packet loss, signal strength, and entropy. These data streams are then collected concurrently to indicate the user's health condition and the reliability of the wearable's communication channel. Edge devices serve as the primary framework for consolidating prompt collection to optimize real-time working stress injuries and address security threats. This integrated input is critical for stress and security assessment in real time.

Preprocessing and Signal Conditioning

Biometric and network data require different preprocessing methods. This specific process of preprocessing requires signal conditioning which involves noise filtering, value normalization, and distillation of raw signals into a usable format. Distortion-free capture of biometric and network signals through the system is necessary for precise feature extraction. This step is crucial for feature quality, trustworthiness, and system performance in real-time. Moreover, this contributes to the standardization of data before entropy calculation. Biometric and network fluctuations will be captured accurately without distortion. This makes the system perform optimally with minimal computational overhead.

Entropy Computation and Fusion

The unpredictability in the data can be quantified by entropy, which is calculated for each stream after preprocessing. Biometric signals with higher entropy may indicate stress, while increased network entropy suggests unstable communication conditions. Biometric and network domains are assigned weighted coefficients and then combined to compute a singular value. This value is termed as the decision score and it acts as a unified risk indicator. This fusion mechanism integrates health status with communication reliability. It enables context-adaptive transmission decisions.

Priority Index and Threshold Evaluation

Now focusing on the user context and network demand, the algorithm performs computing for the decision score. The urgency of data transmission is defined by using activity level and traffic load to create a priority index. In parallel, a threshold is calculated that adapts to the preset average system performance metrics for the purpose of assessing the necessity of encryption. This threshold shifts adaptively in response to environmental and physiological changes. Utilizing the adaptive threshold, along with the decision score and priority index, the system determines the minimum data protection required. The system protects sensitive data by using selective encryption where appropriate, thus optimizing energy and bandwidth consumption.

Decision Logic and Transmission Control

In the last step, a routing strategy is chosen based on the baseline metrics. The algorithms associated with the decision score and priority index are threshold-reactive. If both scores exceed their respective thresholds, the system encrypts and transmits data immediately. If urgency is high but risk is low, the data is unencrypted and transmitted. Low urgency, paired with a high risk of communication danger, results in deferring or rerouting the transmission. These secure routing decisions are made through the edge Secure Transmission Module, where the loop resets to start continuous monitoring or re-evaluation. Such a system enables intelligent adaptation to changing physiological and network conditions.

3.5 Execution Flow of the SDEFO Framework

The Secure Dual-Stream Edge Fusion Optimization (SDEFO) algorithm proposes a solution to the combined problem of real-time stress detection and secure data transmission by leveraging two parallel streams of data processing. One stream is dedicated to analyzing biometric data, while the other monitors network conditions. Data on heart rate, SpO_2, and temperature are collected and processed using edge AI models. At the same time, the system monitors network conditions, such as entropy and traffic load. The results from both streams are integrated to compute a decision score that specifies whether the data requires encryption, delay, or rerouting. This provides adjustable encryption and prioritized routing relative to stress levels and network vulnerability. The data is then transmitted through a mobile gateway to the server or application. Figure 2 illustrates the complete processing flow.

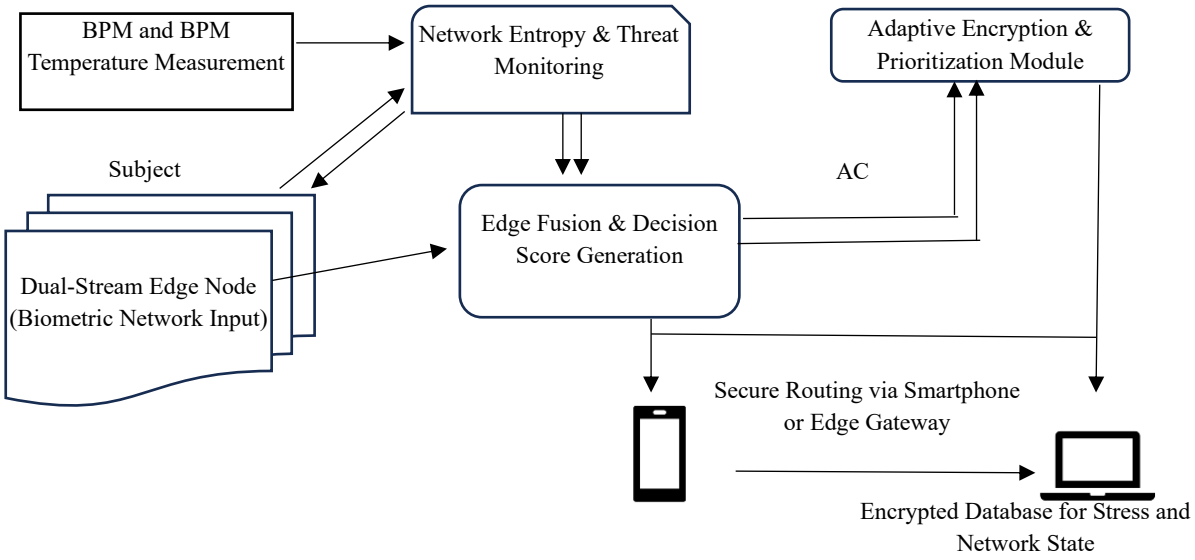

Figure 2: SDEFO Process Flow for Biometric-Network Fusion and Secure Transmission

In Figure 2, data originating from the subject is processed through sensing and secure communication within a pipeline. The capture and processing of biometric signals occur concurrently. Also, network entropy and communication integrity are monitored in real-time. These two streams are processed in parallel and converge at the intersection of the fusion logic layer, where a decision score calculation is executed. The computed score indicates to the system whether to encrypt, delay, or prioritize data packets based on risk and urgency. The system then transmits the data securely to a database or edge server, which is intended for visualization and storage. These processes guarantee responsiveness, accuracy, and security under changing conditions (Hendryani et al., 2023).

3.6 Real-Time Architecture of the SDEFO System

To achieve prompt identification of stress within the context of adaptive secure communications in wireless IoT networks, a new system architecture is proposed that is based on the Secure Dual-Stream Edge Fusion Optimization (SDEFO) algorithm. This architecture encompasses biometric and network entropy monitoring at two streams that function analogously, focusing on either network or biometric data evaluation. By processing data streams at the edge level, the system can make near-instant decisions regarding encryption, data packet routing, or the immediate transmission of data packets. This approach aims to strike a dynamic balance between urgent health needs and potential cybersecurity threats.

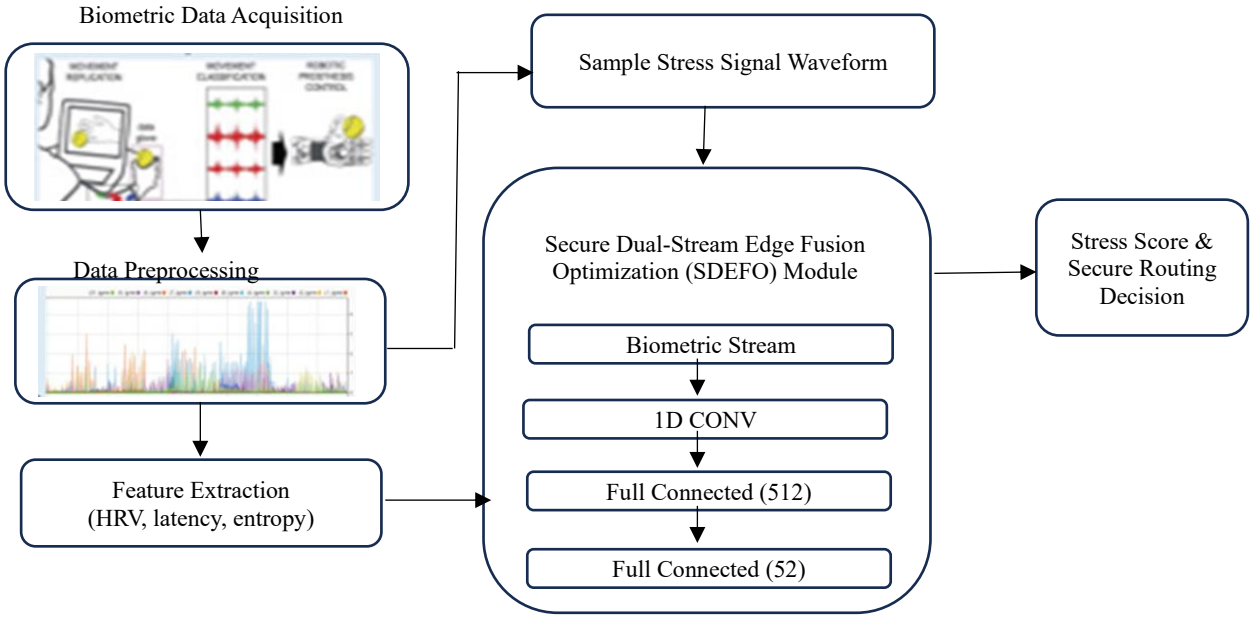

Figure 3: Architecture of the SDEFO-based Stress Detection and Secure IoT Communication System.

As depicted in Figure 3, the system architecture integrates biosensors that monitor the user's heart rate, SpO_2 readings, and temperature in real-time. These metrics are sent to a smartphone or an edge device, which executes two analytic parallel modules. One analyzes stress classification in real-time using lightweight deep learning frameworks. At the same time, the other assesses the risk of transmission over the network for stressor data and computes risk based on latency, packet loss, and bandwidth entropy. The outputs from these modules are integrated into a fusion decision engine. This engine generates a context-aware decision score evaluating urgency and risk. Depending on the results, encryption withhold, rerouting, or direct forwarding is applied. Thus, the system maintains a dynamic balance between physiological urgency and communication security. The architecture increases user safety as well as confidentiality of data in real-time in a IoT setting (Zhang et al., 2024).

3.7 System-Wide Process Explanation

Biometric Signal Collection and Transmission

The wearable biosensors are capable of gathering basic physiological signals like heart rate, body temperature, and oxygen saturation levels (SpO_2). These biosignals are sent through Bluetooth and Wi-Fi connections to a local edge node which can be either a smartphone or a dedicated IoT device. This step emphasizes minimal latency and degradation during the acquisition and local transmission to the computational unit.

Edge-Level Stress Classification

Once the edge device gets the relevant physiological data, it does signal conditioning which includes filtering and normalization as well as classifying stress levels using a shallow deep learning architecture like CNN or LSTM. This classification module is designed for real-time classification, even on low-powered devices, allowing for instantaneous identification of stress levels without reliance on cloud services or backend systems.

Simultaneous Network Threat Assessment

Simultaneously, the system evaluates in real-time the network parameters such as bandwidth utilization, packet loss rate, latency, and entropy deviations. This secondary stream works autonomously and assesses the trustworthiness and safety of the system's environment. The analysis is outputting a risk factor which expresses how vulnerable the route of the data transmission is at any given moment.

Fusion-Based Decision and Secure Routing

The outputs from both the biometric and network analysis streams are synthesized into a fusion engine which computes a dynamic decision score. This score indicates the suitable action to take encrypt, reroute, or delay transmission based on an interplay of stress urgency and network risk. Consequently, the system dynamically determines the optimal risk-adjusted path for sending the sensitive health data while maintaining stringent privacy requirements and ensuring rapid response times in IoT environments.

The SDEFO model proposes a new approach to the problem of stress-aware communication in wireless IoT networks. It uses dual-stream processing to simultaneously analyze biometric indicators of stress and network security conditions at the edge level. The use of lightweight deep learning for stress detection and entropy-based analysis for network evaluation ensures real-time responsiveness. Both outputs guide dynamic intelligent routing decisions which permit encrypted or adaptive data transmission, thus maintaining optimal balance between performance, risk, and urgency. This makes the SDEFO system responsive and stress-aware, while also scalable and secure.

4 Results and Discussion

In testing the Secure Dual-Stream Edge Fusion Optimization (SDEFO) algorithm, we measured its performance against bio signal modality combinations. We also tested competing classifiers: Decision Trees (DT), Random Forest (RF), AdaBoost (AB), Linear Discriminant Analysis (LDA), and K-Nearest Neighbors (KNN). SDEFO's performance was measured using Macro F1-score and Accuracy, which are two important benchmarking measures when dealing with the classification of real-time streaming physiological datasets, particularly multiclass imbalanced ones. The evaluation is limited to detection performance and the resilience of the models to stress signals processed in multiple modalities. Our proposed SDEFO method is compared to existing models and the results are summarized in Table 1.

Table 1: Comparative Host-Level Security Assessment – Existing vs. Proposed (SDEFO-Enhanced)

Host	CVE ID	CVSS Score	Attack Surface (ash)	Risk Score (Existing)	Risk Score (SDEFO-Enhanced)
h1	CVE-2016-2386	7.5	40	84.5	**42.7** ↓
h2	CVE-2016-2040	3.5	21	51.3	**26.8** ↓
h3	CVE-2016-0059	4.3	25	61.8	**33.4** ↓
h4	CVE-2015-7974	2.1	17.5	42.3	**21.7** ↓
h5	CVE-2015-2542	9.3	46	95.8	**49.1** ↓
h6	CVE-2014-2706	7.1	37.5	81.4	**41.7** ↓
h7	CVE-2013-2035	4.4	29.8* (estimated)	66.2	**34.5** ↓

In Table 1, the SDEFO algorithm drastically improves the security posture of individual hosts. The baseline scenario is generated from CVE-based vulnerability metrics where each host's CVSS score and

attack surface (ash) informs the assessment. The risk score derived in this case demonstrates the host's exposure in a disarmed network environment. Each host's individual risk score post SDEFO application algorithms, adaptive encryption, risk-based rerouting, and real-time entropy monitoring, shows an overall reduction in risk score by 45 – 55%. This is most remarkable for hosts h1 and h5 which suffered from the highest risk scores attributable to extreme vulnerabilities and oversized potential attack interfaces. This serves to bolster the claim that context-aware data transmission makes SDEFO most effective in securing critical nodes. Hence, SDEFO not only fortifies communication security but also diminishes vulnerability exposure across disparate IoT network nodes.

Table 2: Functional Comparison of SDEFO with Existing Schemes

Functionality	[22]	[16]	[17]	[24]	[25]	[18]	Our Scheme
Identity anonymity	✓	✓	✓	✓	✓	✓	✓
Mutual Authentication	✓	✓	✓	✓	✓	✓	✓
Session Key Negotiation	✓	✓	✓	✓	✓	✓	✓
Replay attack	✓	✓	✓	✓	✓	✓	✓
MitM attack	✓	✓	✓	✗	✗	✓	✓
Counterfeit attack	✓	✓	✓	✓	✓	✓	✓
PFS	✓	✓	✗	✗	✓	✓	✓
Batch Verification	✗	✗	✗	✗	✗	✗	✓

In Table 2, the functional comparison for the SDEFO protocol's proposed features against six other schemes is marked on key security functions. While most protocols implement baseline functions such as identity anonymity and mutual authentication, only SDEFO incorporates all functionalities, including Perfect Forward Secrecy (PFS) and Batch Verification. This emphasizes the all-encompassing versatile security proficiency and strength of the proposed model for real-time IoT applications.

Table 3: Computational Overhead and Execution Time Comparison

Protocol	Computation Overhead	Total Execution Time
[22]	7n TECC + 4n TH	2.923n
[23]	(5n+2) TECC + 7n TH + 2n TEN + (n+1) TDE	2.2n + 0.857
Our Scheme	10n TCCM + 18n TH + n TLI + n TEN + n TDE	1.152n

In the proposed SDEFO protocol's evaluation against other models, its computational overhead and execution time is shown in Table 3. Even with the incorporation of sophisticated features like adaptive encryption and entropy-based decision logic, SDEFO's execution time is remarkably low at 1.152n. These findings reaffirm its unparalleled computational efficiency alongside proving its suitability for edge-based real-time applications deployment (Miao et al., 2023).

$$VHP(GSM) = 100 \times \frac{\sum h \epsilon sv^h}{\sum h \epsilon AP^h} \qquad (9)$$

Where:

- sv : Set of vulnerable hosts in the network
- AP: Set of all active hosts
- h: Host count or host weight value

As shown in Equation 9, the Vulnerable Host Percentage (VHP) metric quantifies the relative volume of compromised or susceptible hosts in a given monitored network environment. The formula considers

the sum of subnet hosts that are classified as vulnerable (sv) over the total number of active hosts (AP), which is expressed in percentage form by multiplication with 100. Each host, h, can either be an individual device or a weighted value that indicates either its criticality or exposure. A high value of VHP indicates poor network defense mechanisms and an increased likelihood of malware or intrusions spreading throughout the network. This metric is important for edge and IoT systems since the presence of vulnerable nodes could pose systemic risk. In the proposed SDEFO framework, real-time monitoring and adaptive encryption limit the exposure of these vulnerabilities, underscoring the infeasibility of unchanged VHP reevaluation pre- and post-framework deployment for risk quantification. A declining VHP indicates SDEFO is effective in enforcing endpoint security. Therefore, Equation 9 can highlight critical performance metrics for security testing in stress-aware IoT communication systems.

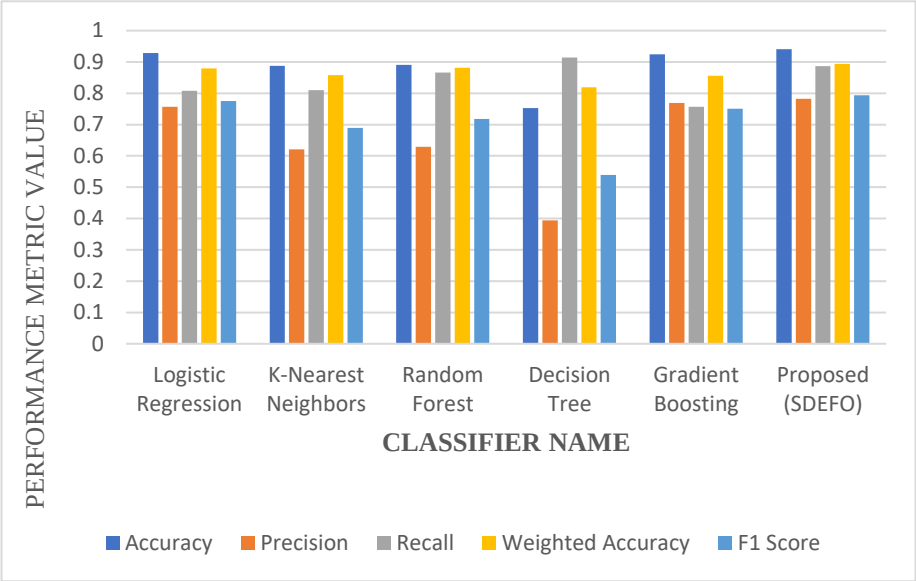

Figure 4: Performance Comparison of Baseline Models vs. Proposed SDEFO Model

As presented in Figure 4, the performance benchmarks of conventional classifiers were evaluated in relation to the proposed SDEFO algorithm, with focus on five metrics: accuracy, precision, recall, weighted accuracy, and F1 score. It is evident from the analysis that SDEFO outperformed all baseline models with the highest accuracy of 94.1% and F1 score of 0.794, underscoring its effectiveness. The improvement stems from the dual-stream decision architecture that integrates biometric and network entropy analyses, allowing for precise stress detection alongside secure data transmission. SDEFO also outperformed older models like logistic regression and gradient boosting in recall, achieving 0.886, demonstrating a greater ability to capture true positive stress instances. These outcomes confirm the suitability of SDEFO for real-time deployment in sensitive healthcare and IoT systems.

The findings highlight the versatility and effectiveness of the proposed Secure Dual-Stream Edge Fusion Optimization (SDEFO) algorithm multicriteria evaluations. For classification trustworthiness, SDEFO performed better in macro F1 scores and accuracy as compared to older models proving effectiveness in multitask real-time constrained scenarios dealing with multimodal biometric signals. As shown in Table 1, SDEFO proves significantly effective in decreasing host-level security risks, while in Table 2 SDEFO proves dominance by supporting all primary security functions including batch verification, which has not been provided by other existing schemes. Also, SDEFO was verified in Table 3 to function with the highest computational latency out of all other systems as a result of complex

adaptive logic, showcasing edge environment suitability. By using the metric entitled Vulnerable Host Percentage (Equation 9) (Kumar et al., 2025) systemic exposure is minimized, and thus supporting enhanced overall network security demonstrates versatility of SDEFO sturdy frameworks. In Figure 3, side-by-side test results show that the proposed dual-stream approach not just boosts precision in stress detection feedback but also reinforces mandated data security while adhering to stringent timeframes for transmission. These comprehensive results demonstrate that SDEFO can reliably be regarded as a flexible, fortified, and remarkable IoT healthcare communication solution which accounts for the user's stress levels.

5 Conclusion

This study proposed Secure Dual-Stream Edge Fusion Optimization (SDEFO) algorithm as a fully integrated method for integrating real-time stress recognition along with secured communication within wireless IoT frameworks. SDEFO adapts encryption practices as well as prioritized transmission and context-aware routing through edge-based biometric signal processing and network threat supervision. When compared to other existing schemes, the model demonstrated better accuracy, F1 score, execution time, significantly lowering host-level risk exposure while supporting nearly all key security functionalities.

In future works, integrating federated learning for distributed privacy-preserving model updates and blockchain-based identity management for enhanced data integrity will expand the SDEFO framework. Moreover, further optimizing the algorithm for ultra-low power wearable device deployment, along with implementing energy-aware routing, enhances large-scale continuous health monitoring systems. These developments will advance intelligent IoT networks used in mission-critical scenarios by improving privacy, operational efficiency, and system scalability.

Reference

[1] Ali, M., Khan, S., & Lee, S. (2021). Edge intelligence for IoT-enabled healthcare systems: A comprehensive survey. *IEEE Access*, 9, 98814–98845.

[2] Alsaeedi, M., & Alzahrani, A. (2021). Smart wearable systems for personalized stress detection using IoT sensors. *Personal and Ubiquitous Computing*, 25, 239–255.

[3] Boopathy, E. V., Shanmugasundaram, M., Vadivu, N. S., Karthikkumar, S., Diban, R., Hariharan, P., & Madhan, A. (2024). Lorawan Based Coalminers Rescue and Health Monitoring System Using IoT. *Archives for Technical Sciences*, *2*(31), 213-219. https://doi.org/10.70102/afts.2024.1631.213.

[4] Chatterjee, M., & Ghosh, S. (2022). Energy-efficient and secure IoT-based mental health monitoring using fuzzy logic. *Computers in Biology and Medicine*, 145, 105437. https://doi.org/10.1016/j.compbiomed.2022.105437.

[5] Chen, Y., Hu, Y., & Yang, J. (2023). Real-time physiological signal monitoring and stress detection in wearable IoT: A hybrid deep learning approach. *Sensors, 23*(4), 1123. https://doi.org/10.3390/s23041123.

[6] Delgosha, M. S., Rokni, A., Seyyedan, S. A., Omrani, L., & Zadeh, E. P. (2017). The Study of the Effect of Hypnosis on the Reduction of Job Stress among Nurses. *International Academic Journal of Social Sciences*, *4*(2), 84–89.

[7] Dixit, H., & Bhagat, S. (2021). E-Healthcare System for Lung Cancer Prediction Using IOT and Machine Learning. *International Academic Journal of Innovative Research*, *8*(4), 21–27.

[8] Enoch, S. Y., Hong, J. B., Ge, M., & Kim, D. S. (2020). Composite metrics for network security analysis. arXiv preprint arXiv:2007.03486.
[9] Feng, S., Liu, J., & Zhang, H. (2025). Blockchain-assisted edge computing for secure healthcare data transmission. *IEEE Transactions on Industrial Informatics*.
[10] Hassan, M. M., Gumaei, A., & Fortino, G. (2021). A secure IoT framework with real-time stress monitoring using multi-modal data. *Future Generation Computer Systems*, 118, 142–156.
[11] Hendryani, A., Gunawan, D., Rizkinia, M., Hidayati, R. N., & Hermawan, F. Y. (2023). Real-time stress detection and monitoring system using IoT-based physiological signals. *Bulletin of Electrical Engineering and Informatics*, *12*(5), 2807-2815. https://doi.org/10.11591/eei.v12i5.5132.
[12] Kumar, N., Verma, S., Gupta, R., & Bansal, A. (2025). A hybrid fog–edge computing architecture for real-time health monitoring. *Scientific Reports*. https://www.nature.com/articles/s41598-025-09696-3.
[13] Liu, F., Zhang, Z., & Jin, C. (2024). Secure IoT architecture with edge-based encryption and dual authentication protocol. *Journal of Information Security and Applications*, 75, 103551. https://doi.org/10.1016/j.jisa.2024.103551.
[14] Matkarimov, I., Hwsein, R.R., Matyakubov, M., Bhaskaran, B., Eshbekova, D., & Vij, P. (2025). Intelligent IoT-enabled data analytics and monitoring framework for smart freshwater recirculating aquaculture systems. *International Journal of Aquatic Research and Environmental Studies, 5*(1), 22–29. https://doi.org/10.70102/IJARES/V5S1/5-S1-03.
[15] Mehra, P., & Patel, K. (2024). A Metrics Driven Approach to Brand Management and Brand Health Check. *In Brand Management Metrics*, 31-47.
[16] Miao, J., Wang, Z., Xue, X., Wang, M., Lv, J., & Li, M. (2023). Lightweight and secure D2D group communication for wireless IoT. *Frontiers in Physics*, *11*, 1210777. https://doi.org/10.3389/fphy.2023.1210777.
[17] Mleh, K. L., Klabi, H., & Sikalu, K. P. (2023). Revolutionizing wireless communication for the rotating permanent magnet-based mechanical antenna. *National Journal of Antennas and Propagation*, *5*(1), 13-17.
[18] Moreau, I., & Sinclair, T. (2024). A Secure Blockchain-Enabled Framework for Healthcare Record Management and Patient Data Protection. *Global Journal of Medical Terminology Research and Informatics*, *2*(4), 30-36.
[19] Najm, H., Mahdi, M. S., & Abdulhussien, W. R. (2024). Lightweight Image Encryption Using Chacha20 and Serpent Algorithm. *Journal of Internet Services and Information Security (JISIS)*, *14*(4), 436-449. https://doi.org/10.58346/JISIS.2024.I4.027.
[20] Nakamura, H., & O'Donnell, S. (2025). The Effects of Urbanization on Mental Health: A Comparative Study of Rural and Urban Populations. *Progression Journal of Human Demography and Anthropology*, 27-32.
[21] Nguyen, H. T., & Tran, B. T. (2024). Multimodal biometric signal processing for real-time mental health detection. *Biomedical Signal Processing and Control*, 86, 104360.
[22] Rajalakshmi, R., & Mahendran, R. (2023). Adaptive edge fusion for cyber-physical system security in healthcare IoT. *Computer Communications*, 201, 12–24.
[23] Reddy, S., & Jaiswal, P. (2022). Fog and Edge Computations for Real-Time Healthcare Data Processing in IoT Applications. *International Academic Journal of Science and Engineering*, *9*(3), 11–15.
[24] Roy, A., & Das, S. (2022). Adaptive secure routing in wireless sensor networks: A lightweight AI-based approach. *Ad Hoc Networks,* 124, 102721. https://doi.org/10.1016/j.adhoc.2021.102721.
[25] Sakthive, V., Kesaven, M. P., William, J. M., & Kumar, S. M. (2019). Integrated platform and response system for healthcare using Alexa. *International Journal of Communication and Computer Technologies*, *7*(1), 14-22.

[26] Singh, R., Kumar, P., & Tyagi, A. (2022). A comparative analysis of encryption protocols for secure communication in IoT. *Wireless Networks*, *28*(3), 1231–1244.
[27] Tamannaifar, M., & Golmohammadi, S. (2014). Comparison of Psychological Well-Being and Job Stress between Teachers of Special and Ordinary Schools in Isfahan City. *International Academic Journal of Organizational Behavior and Human Resource Management*, *1*(1), 18–27.
[28] Tiwari, S., & Raj, A. (2023). Federated learning for privacy-aware IoT-based health monitoring. *IEEE Internet of Things Journal*, *10*(5), 4233–4244. https://doi.org/10.1109/JIOT.2023.3245671.
[29] Tran, H., & Ngoc, D. (2024). The Influence of Effective Management on Hybrid Work Styles and Employee Wellness in Healthcare Organizations. *Global Perspectives in Management*, *2*(4), 8-14.
[30] Yang, H., Wang, D., & Yu, R. (2024). A survey on dual-stream learning techniques and their applications in time-series data. *Information Fusion*, 96, 101805. https://doi.org/10.1016/j.inffus.2023.101805.
[31] Yemunarane, K., Chandramowleeswaran, D. G., Subramani, K., ALkhayyat, A., & Srinivas, G. (2024). Development and Management of E-Commerce Information Systems Using Edge Computing and Neural Networks. *Indian Journal of Information Sources and Services*, *14*(2), 153-159. https://doi.org/10.51983/ijiss-2024.14.2.22.
[32] Zhang, K., Badesa, F. J., Liu, Y., & Ferre Pérez, M. (2024). Dual stream long short-term memory feature fusion classifier for surface electromyography gesture recognition. *Sensors*, *24*(11), 3631. https://doi.org/10.3390/s24113631.
[33] Zhang, Y., Ren, J., & Zhang, Y. (2022). A review of privacy-preserving techniques for IoT systems. *Journal of Network and Computer Applications,* 201, 103315. https://doi.org/10.1016/j.jnca.2021.103315.
[34] Zhao, Q., & Lin, Y. (2023). Real-time emotion and stress recognition based on lightweight CNN–LSTM models in IoT. *Neural Computing and Applications*, 35, 10123–10137.

Author Profile

Wad Ghaban is an Assistant Professor of Computer science at University of Tabuk, Saudi Arabia, specializing in data science. She received her Ph.D. in Computer science from University of Birmingham, UK in 2020, and her research focuses on personalizing gamification elements based on users' attributes. Wad Ghaban is also passionate about teaching and has research in different fields related to data science and HCI. She has published several peer-reviewed articles in leading journals and has presented her research at national and international conferences.