Revista Argentina de Clínica Psicológica
2026, Vol. 35, N°1, 01-17
DOI: 10.53555/03276716.2026.01

FLASH-BPH: A Framework For Scalable And Trustworthy Human-Centric Cyber-Physical Systems

N. Kalaiyarasi[1*], Dr T V Gopal[2]

***Abstract**: Industry 4.0's rapid development has brought into sharp focus the critical need to balance cyber-physical systems (CPS) efficacy with potential risks of human errors. This work introduces FLASH-BPH, a human-centric framework aimed at integrating automation with human supervision while maintaining privacy, scalability, and ethical standards. FLASH-BPH incorporates Human-in-the-Loop (HITL) validation as a fundamental component, allowing domain experts to assess and enhance AI-generated judgements in real time. To address these concerns globally, this study proposes a novel framework that integrates split learning with federated learning (FL) and edge processing. Separation of Concerns is ensured by dividing deep neural networks between edges and servers such that only intermediate activations are supplied for server-side processing and raw sensor data remains on-device. The system incorporates blockchain-auditable procedures, human-centric consent methods, and Federated Learning (FL) to enable collaborative model training across dispersed users without central data aggregation focusing on decentralization of data. Tested on a real-world wearable sensor dataset, the hybrid split-FL method saves better on on-device computing and matches accuracy with centralized alternatives, proving its suitability for low-resource IoT situations. Activation encryption and adaptive model personalization mitigate non-independent and identically distributed data issues and leakage risk, while stress testing confirm scalability in diverse network settings. By offering a scalable, privacy-first paradigm for IoT driven applications, this work advances edge processing by combining personalized split learning with federated normalization in human-in-the-loop CPS.*

***Keywords:** Split Learning, Federated learning, FLASH-BPH, Block-chain-auditable procedures, Human-in-the loop, Cyber Physical Systems.*

1. Introduction

Cyber-Physical Systems (CPS) refer to highly complex, connected systems that synthesize computational algorithms, networking, and physical phenomena for the observation, control, and optimization of physical-world processes. CPS use embedded sensors, actuators, and computing to extract information from the physical world, process this data with smart algorithms, and drive actions impacting the physical world in real-time. CPS are a revolutionary fusion of the digital and physical worlds, allowing for intuitive interaction between the two and paving the way for innovations in fields like smart cities, autonomous transportation, industrial automation, and medicine. By filling the gap between cyber and physical systems, CPS allow for real-time monitoring, control, and optimization of complicated processes, which improves efficiency, safety, and user experience[1]. Yet, the ubiquitous nature of CPS presents serious challenges, especially with regard to human-centered design, since these systems tend to deal with sensitive information and engage intimately with users. Solving these challenges is essential to making CPS widely adopted and trustworthy in various applications, thus forming the foundation of contemporary technological innovations[2][3].

The history of industry has been a process of rapid change brought about by creative technology to adapt the relationship between humans and machinery and information. In the latest industrial revolutions, cyber-physical systems (CPS) are the foundation for seamless integrations of computation, networking, and physical processes as shown in Fig. 1. This session, presents a journey of industry evolution and the enabling CPS integration of a digital or physical world in the factories of past, present and future[4].

[1]Department of Computer Science and Engineering, Anna University, CEG Campus, Chennai 600025, Kalaiyarasirajan29@gmail.com*
[2]Professor, Department of Computer Science and Engineering, Anna University, CEG Campus, gopal@annauniv.edu

***Corresponding Author:** N. Kalaiyarasi*
**Department of Computer Science and Engineering, Anna University, CEG Campus, Chennai 600025, Kalaiyarasirajan29@gmail.com*

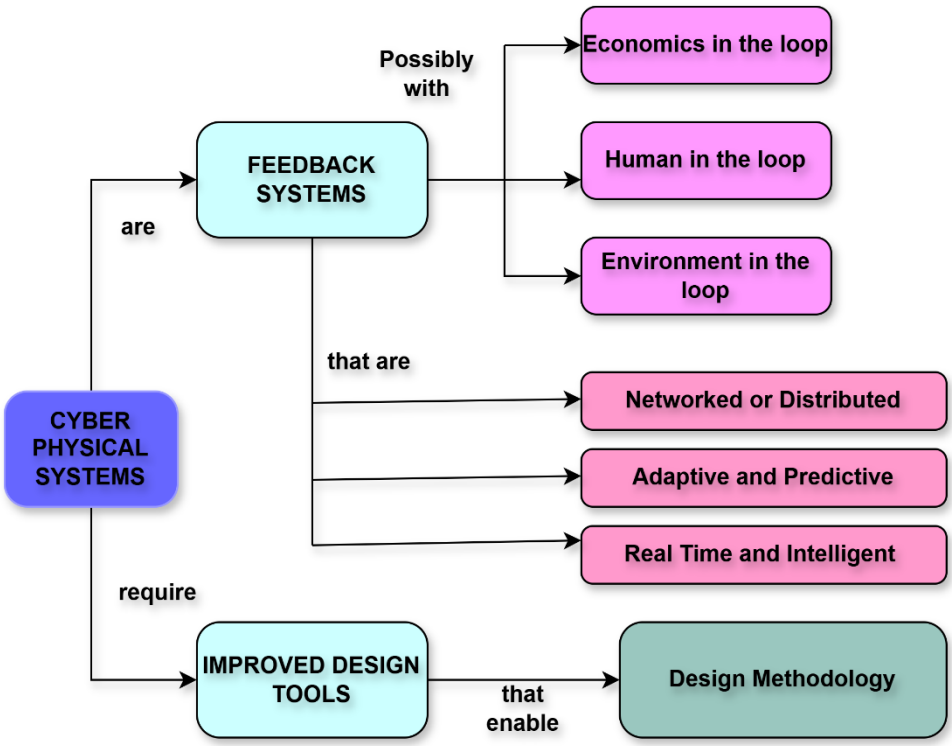

Figure 1. Cyber Physical Systems

1.1 Human Centric Cyber Physical Systems

With the evolution of industries towards incorporating humans into the decision loop, Human-Centric Cyber-Physical Systems (HC-CPS) have surfaced as an important paradigm. These systems emphasize trust in decision-making frameworks by prioritise AI ethics first and ensuring interfaces empower not supplant human judgment with sophisticated algorithms. HC-CPS permits intelligent systems to adapt to humans by monitoring their actions, choices, and relevant contextual signals alongside systematic frameworks of opacity, discrimination, and exclusion. Automation and AI in various sectors invariably increase the extent of technological pervasion into human domain, while the position of human within these systems remains central. This connection has been articulated in this paper through three frameworks: Human-in-the-Loop (HITL), Human-on-the-Loop (HOTL), and Human-out-of-the-Loop (HOOTL). These models mark the presence, absence, or the combination of supervision or manual control, automation, and the shifting balance of speed, reliability, and ethical accountability on a continuum for optimal productivity. For overly automated frameworks, balance becomes detrimental with regard to judgment and accountability, exploitation of technology, and discrimination. This conversation focuses on their definitions, use cases, arguments, boundaries, and ethical arguments.[5].

Human-in-the-Loop, Human-on-the-Loop and Human-out-of-the-Loop demonstrate a hierarchy of human-AI collaboration with each fitting different applications. HITL engages humans as a part of decision-making, e.g., correcting AI outputs or signing off on results, to offer accuracy in medical and aviation applications but at the expense of vast human resources. HOTL keeps humans in regulatory capacities, which allow AI to operate autonomously but allow for interference in case of malfunction, maximizing efficiency and oversight in applications such as algorithmic trading or information security. HOOTL does away with any human interference altogether and uses only autonomous systems in applications such as self-driving cars or recommendation systems with the goal for maximum efficacy but at the risk of ethics and accountability. Choice among these models would be made based on human judgment need, scalability, and risk tolerance with HITL choosing safety, HOTL choosing governance, and HOOTL choosing absolute automation each being a fundamental building block of responsible and effective AI integration[6].

1.2 Human- Machine Integration

Human-Machine Interaction in CPS relies on two-way communication, where real-time data exchange occurs between humans and machines. Unlike traditional interfaces, CPS need adaptive interactions that respond to changing environments. For instance, a factory worker can reprogram a robot arm's functions using voice commands or touchscreens, with the robot providing feedback using visual cues or haptic feedback. Rules of significance include real-time feedback, where sensors and actuators facilitate instant readjustments example like changing a drone's flight path in mid-air and context awareness, where systems adapt interfaces

based on environmental conditions example like smart car minimizing controls during emergency manoeuvres. Trust and transparency are also essential, where users need to understand system decisions in safety-critical applications like autonomous surgery or flight. Loss of transparency will make users hesitant to trust automated results, undermining the system's purpose[7]. Innovations that improve productivity and safety are made possible through Human-Machine Interaction in Cyber-Physical Systems, which combines human intuition with machine precision. Although automation provides exceptional efficiency, human supervision is essential for addressing unpredictability and ethical intricacies. Future CPS must emphasise intuitive design, real-time adaptation, and transparent communication to promote collaboration that ensures safety, trust, and societal welfare. The seven component(7'C) principles provide the resilient, secure, and adaptable integration of digital and physical domains, allowing systems to function reliably in dynamic environments. By finding a balance between being quick to respond in real time and keeping everyone safe, they lower risks like delays and online threats while keeping operations running smoothly, the components and the human-machine perspective is as shown in Fig. 2. Focusing on ethical and legal alignment builds trust and allows for growth, which is important for uses like smart towns or self-driving factories. In the end, they simplify exchanges between people, machines, and the environment, making systems more resilient and ready for the future. By achieving this equilibrium, HMI will persist in fostering revolutionary progress across sectors, guaranteeing that technology serves humans with accountability[8].

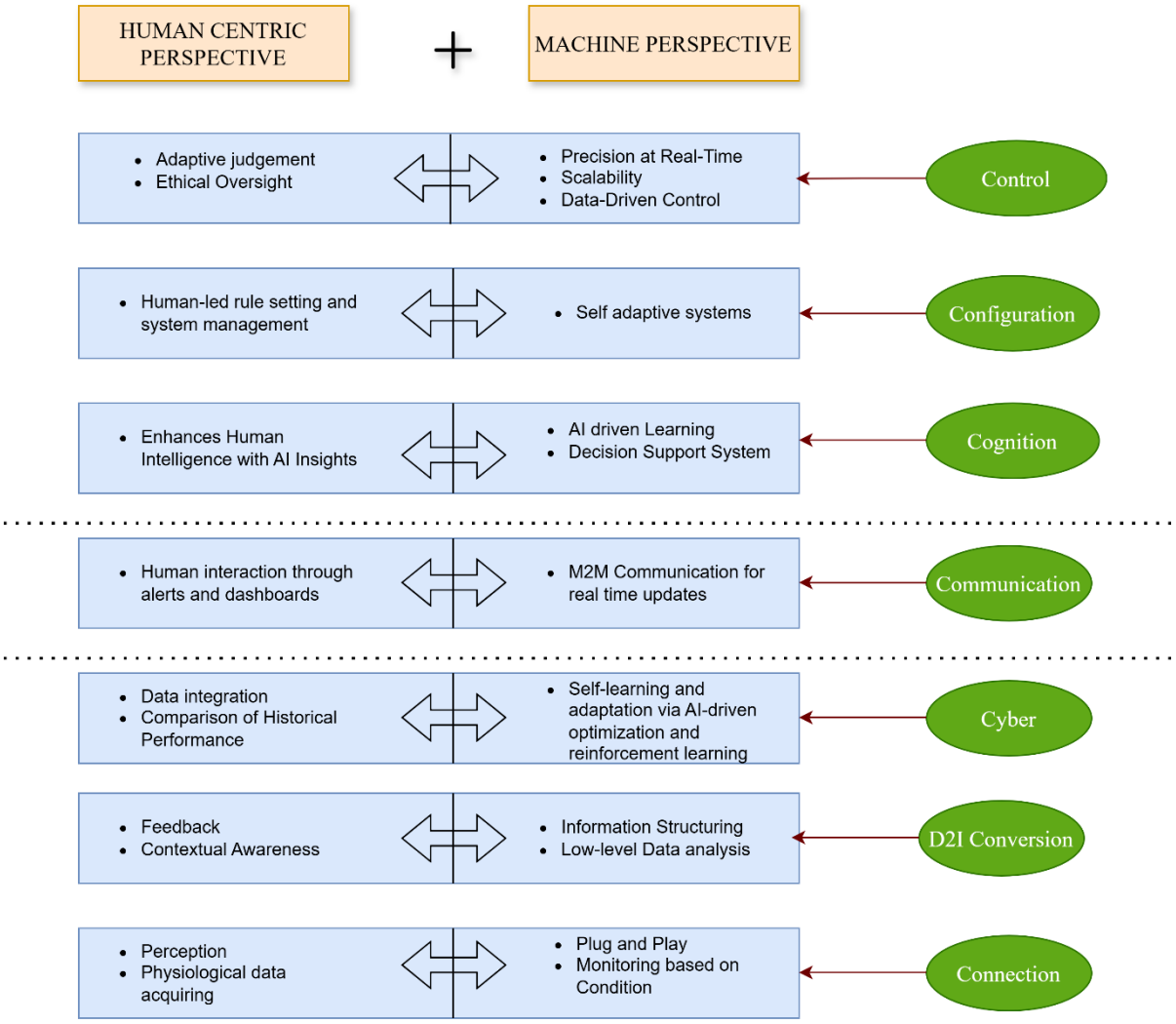

Figure 2. 7'C of Cyber Physical Environment

1.3 Autonomous Systems at Edge Processing

A human in the loop Cybernetic Physical systems services aggregate and analyse data from personal IoT devices to offer data proprietors customised features. Given the computational demands of training deep learning models, raw data processing occurs externally to the user environment. This indicates a privacy problem; although users can govern their own IoT data flows, there remains a potential for leakage throughout the data processing phase, particularly with inference-

based data. To address this difficulty, one option is to transition to edge AI. Artificial intelligence has emerged as one of the most transformative technologies to date, and when combined with cloud computing, has optimised several processes across diverse industries and enterprises. The integration of AI with cloud computing enhances productivity, efficiency, and precision inside the AI pipeline. It facilitates rapid solution creation that leverages the substantial data capacity provided by cloud settings [9][10].

However, the enormous demand for services and applications built on this paradigm is producing storage and networking problems (bandwidth utilisation and latency). The unregulated acquisition and utilisation of data are generating concerns among end users about the safeguarding of their privacy. Consequently, there exists a paradigm known as Edge AI, which encompasses AI workflows that engage devices at the network's periphery, in contrast to cloud-based AI, where the entire pipeline operates within a centralised framework. Edge computing facilitates Edge AI by relocating processing and storage nearer to the request's origin, hence reducing bandwidth consumption and providing low latency. Edge AI enables learning algorithms to be deployed onboard end devices directly, so the processing phase is handled at the edge [11]. Continuous monitoring of physiological parameters such as blood pressure, heart rhythm, and metabolic activity is made possible by modern wearable technologies from glucose monitors to electrocardiogram patches. The sensitivity of this data necessitates stringent privacy measures. FLASH-BPH tackles this by combining homomorphic encryption and federated learning to guarantee reliable medical informatics.

2. Literature Review

The swift progression of Artificial Intelligence (AI) in Cyber-Physical Systems (CPS), especially at the edge, has not only unveiled new functionalities but also heightened apprehensions surrounding user data privacy. Edge AI facilitates processing on user devices or proximate edge nodes, resulting in low-latency responses and less bandwidth consumption[12]. This architectural shift presents unique privacy problems stemming from decentralised collection of information and real-time inference. Traditional cloud-based models are no longer enough for safeguarding sensitive information, necessitating the development of privacy-preserving solutions such as Federated Learning, Secured Multi Party Computation, and Homomorphic Encryption[13]. These methods ensure that personal data remains local or is rendered indecipherable, without compromising the performance of AI models.

As AI systems increasingly engage with people in private domains like healthcare, smart homes, and personalised education, it is becoming increasingly important to integrate a human-centric approach into privacy-preserving technologies.[14]. Consent, contextual sensitivity, and user agency are given top priority in human-centric privacy systems. This includes giving users clear controls over what is shared, how it is used, and by whom in addition to anonymising data. To strike a balance between robust privacy protections and individual customisation, methods such as Split Learning and personalised federated models have been introduced. By preventing the aggregation of raw data, these solutions satisfy various privacy demands and foster confidence in intelligent applications while facilitating shared learning among users.[15][16].

The larger significance of privacy-preserving AI extends beyond regulatory compliance; it is essential for ethical AI deployment and public trust. Fairness and accountability depend on preserving the security and integrity of personal data as AI systems are included into decision-making processes, ranging from assessing credit to medical diagnostics. Loss of autonomy, manipulation, and discrimination may result from the improper use or disclosure of AI-derived insights. Privacy is therefore a fundamental design element rather than just a technical add-on. Incorporating privacy-by-design principles into software and hardware increases system resilience and aids in bringing AI development into line with societal standards and values.[17].

Another key challenge for human-involved CPS systems is cognitive dependability, particularly in domains where human judgement and machine intelligence must work together smoothly. The precision and consistency of human decision-making when engaging with complicated systems is referred to as cognitive reliability. In order to prevent excess, misinterpretation, and unintended behaviours, AI interfaces must be designed with an understanding of human cognitive limits.[18]. Artificial intelligence systems need to be able to monitor human states and adjust dynamically since cognitive errors can result in catastrophic failures, particularly in safety-critical applications like autonomous driving or aircraft. Risks associated with human fallibility are mitigated by mechanisms such as adaptive automation, real-time feedback loops, and workload-aware control.[19].

HC-CPS error analysis also underscores the importance of mutual understanding and explainability between the human operator and the system. Users may develop overreliance or under-trust in AI systems that are opaque or excessively autonomous, which can result in errors in judgement or misuse.

[20]. Inconsistent user interfaces, misunderstood alerts, or misaligned system feedback can all contribute to these errors. AI models must therefore take human issues into consideration when designing and implementing them in addition to protecting data privacy. Users are able to more effectively evaluate AI

suggestions by receiving interpretable outputs, confidence scores, and scenario-based feedback, thereby reducing the rates of both mechanical and cognitive failure[21].

In summary, human-centric design and the incorporation of privacy-preserving methods into edge AI systems serve as the foundation for responsible AI in cyber-physical contexts. To guarantee efficiency and safety, these systems need to handle cognitive reliability, give users meaningful control, and secure data at the edge. The creation of a robust framework is made possible by the convergence of human-aware modelling with technology solutions like as federated learning, homomorphic encryption, and context-aware personalisation [22][23]. It is anticipated that future research will further bridge the gap between privacy, cognition, and reliability, ultimately leading to the creation of artificial intelligence systems that are not only clever but also trustworthy and in conjunction with human requirements.

Federated Learning has emerged as a significant method for ensuring privacy in artificial intelligence, particularly in contexts involving sensitive, distributed data generated at the edge. Initially, we looked into ways to enable decentralised device-to-device collaborative model training without disclosing any raw data.[24]. In the early stages of healthcare and mobile application development, where data ownership, compliance with privacy rules, and personalised services were vital, this approach gained traction. Through the course of time, researchers started incorporating FL into the architecture of Human-Centric Cyber-Physical Systems (HC-CPS), which are systems in which human participation, trust, and decision-making are essential to the functioning of the system[25].

Many reviews and studies began to highlight the application of FL in smart health monitoring systems, smart manufacturing and assistive technologies[26]. These systems collected physiological signals continuously using information from wearables and Internet of Things devices. Through the use of Federated Learning, these systems were able to train models for activity recognition, stress detection, or anomaly detection across a varied population without the need to aggregate sensitive health data in a central repository [27]. By doing so, not only was privacy protected, but also data heterogeneity was handled. Data heterogeneity is a typical problem in human-centric systems because of the behavioural and physiological variances that exist between individuals. Maintaining performance over a wide range of devices and situations was demonstrated to be effective by FL[28].

Considering the research integrated Federated Learning with complementary privacy-enhancing technologies such as Differential Privacy, Secure Multi-Party Computation (SMPC), and Homomorphic Encryption in HC-CPS, these combinations become necessary in order to defend against complex assaults such as membership inference and inference leaking. Specifically for usage in low-power or latency-sensitive situations, such as autonomous driving or real-time medical diagnostics, Federated Learning frameworks have evolved to combine Split Learning and edge AI optimisation [29]. These developments facilitated the implementation of HC-CPS in mission-critical environments, where privacy and immediate response are of the utmost importance. In human-centric environments, the research community focusses on lowering communication overhead, establishing asynchronous federated protocols, and overcoming the issues of non-independent and identically distributed (non-IID) data. This is a chronic issue that has been a problem for a long time. Furthermore, personalised federated learning models were implemented in order to accommodate the specific requirements of individual users while still reaping the benefits of the global learning model [30][31].

An extensive body of research has demonstrated that human-centric systems must not only safeguard data but also be comprehensible, equitable, and capable of dynamically adapting to the input provided by humans. In order to enable systems that can learn from human behaviours, preferences, and mistakes without compromising privacy, federated reinforcement learning and federated transfer learning have been investigated [32]. Smart homes, digital treatment, human-robot collaboration, and emotion-aware child protective services are expanding their use of these technologies. It has also been suggested that blockchain-based FL frameworks might be used to improve auditability and accountability in shared learning settings. This would ensure that model contributions are documented and verified in a secure manner[33][34].

The substantial interest in advanced privacy-preserving technologies has been sparked by the increasing complexity and interactivity of Human-Centric Cyber-Physical Systems (HC-CPS) since 2017. When it comes to protecting privacy in systems where sensitive user data is processed close to the source, Split Learning and Homomorphic Cryptography have emerged as two of the most important technologies[35]. Split Learning was proposed as a solution to address the limitations of traditional centralized and even federated models, especially in scenarios involving low-computation edge devices such as wearables, medical sensors, and assistive technologies. In these setups, models are split between the client and server, ensuring that raw data never leaves the client device while still allowing joint training of deep learning models[36].

For the first time, applications of Split Learning in human-centric systems were shown in the healthcare and smart monitoring environments. Research has

shown its efficacy in contexts such as remote diagnostics, utilising sensitive patient data, including MRI images, ECG signals, or personal health records, for training AI models without the need for centralised aggregation. The client device calculated the initial layers of a neural network and transmitted intermediate activations to the server, thereby significantly mitigating the risk of raw data exposure [37]. Split Learning achieved high model accuracy while substantially lowering privacy risks, rendering it appropriate for applications involving children, elderly individuals, or persons with disabilities who necessitate elevated ethical standards in data management [38].

Homomorphic cryptography, in particular Fully Homomorphic Encryption (FHE) and Partially Homomorphic Encryption (PHE), developed further as a method that enables computations to be performed directly on encrypted data at the same time. HC-CPS applications incorporated homomorphic encryption into AI workflows, enabling cloud or edge servers to conduct inference or partial training on encrypted data without decryption requirements. This was especially significant in smart city contexts, emotion recognition systems, and personalised learning platforms, where safeguarding the confidentiality of users' biometric, behavioural, or affective data was essential. Research demonstrated that the integration of Split Learning with Homomorphic Encryption significantly improved privacy by encrypting intermediate activations prior to their transmission to the server [39][40].

The study of hybrid architectures, which provide end-to-end secure training and inference in distributed CPS contexts by utilising both Split Learning and Homomorphic Encryption simultaneously, grew in popularity. These systems facilitated secure data sharing among institutions, such as hospitals, manufacturing plants, and educational networks, while ensuring that no actual data was exposed. The authors examined prevalent vulnerabilities in multi-device learning environments, including inference attacks, data reconstruction, and model inversion. Recent developments in lightweight encryption methods and quantised split networks have enabled the implementation of these architectures on resource-limited edge devices, thereby broadening their application in real-time scenarios, including intelligent prosthetics, UAV-assisted rescue operations, and wearable health monitoring systems [41].

Researchers have implemented parallelised split learning utilising encrypted multi-party computation (MPC) to enhance model convergence and decrease latency, addressing challenges present in prior implementations. Concurrently, research was conducted on domain-specific Split Learning architectures, such as those for emotion-aware systems and brain-computer interfaces (BCIs), which could dynamically modify the model split point in accordance with network conditions, workload, and privacy requirements. These systems were developed to accommodate different degrees of human autonomy and trust, ensuring that technical capabilities are consistent with ethical frameworks in the design of HC-CPS. The combination of Split Learning and Homomorphic Cryptography represents a highly effective method for ensuring privacy in HC-CPS. The current research is concentrated on adaptive learning pipelines, which dynamically select the encryption level and model split depth based on the cognitive sensitivity of the task and contextual privacy policies. These systems are being increasingly utilised in collaborative robotics, telemedicine, and smart rehabilitation, where humans and machines adapt to one another in real-time. A new generation of intelligent, privacy-respecting, and ethically aligned cyber-physical systems is being driven by the fusion of cognitively reliable AI models with secure multi-party analytics [44][45].

3. Methodology

3.1 Benchmarking Model for Human in the loop Cyber Physical Systems

There are crucial trade-offs that must be made between privacy assurances, computational efficiency, and model performance in Human Centric Cyber Physical Systems. Even if federated learning (FL) manages to alleviate this issue by storing data on the device itself, it is still susceptible to gradient inversion attacks, which are attacks that recreate sensitive inputs from model updates. Hybrid frameworks such as TIPPERS and PACHA integrate federated learning with consent management; however, they do not incorporate mechanisms to prevent gradient leakage or ensure tamper-proof auditing. Split learning (SL) and homomorphic encryption (HE) have made recent advancements that show promise. SL decreases attack surfaces by separating models, and HE provides safe aggregation. However, there is not yet a cohesive framework that connects them with blockchain for end-to-end transparency. In this context, FLASH-BPH presents a new solution that addresses the accuracy trade-offs of DP by utilising FL-SL hybridisation, HE-secured aggregation, and blockchain-based auditing, thereby achieving similar privacy levels without the need for noise injection.

3.2 Human-Centric Design: Addressing Errors and Behavioural Factors

3.2.1 Human in the loop Validation Interface

In FLASH-BPH, the HITL Validation Interface serves as a vital defence against human labelling errors and AI misclassifications. End-users assess ambiguous predictions identified by the system and proceed to validate or amend them. The HITL module, for example, will send this prediction to a user's dashboard in the event that a for say wristwatch incorrectly

identifies a High Stress episode as an Average Stress episode due to abnormal heart rate variability (HRV). The clinician cross-references raw sensor data, such as activity logs and HRV trends, and updates the label, which subsequently propagates to retrain federated models. This process transparently involves humans in decision-making, reduces cascading errors in AI outputs, and ensures high-quality training data. It also develops user trust. A compliance auditable trail is produced by logging the updated labels on the blockchain and encrypting them. FLASH-BPH tackles this interaction by automating compliance by reducing human and organizational errors, enforcing context-sensitive protocols by addressing technological and managerial deficiencies, and integrating sociotechnical resilience. This integration guarantees that procedural errors are addressed holistically, bridging the sociotechnical gap between human actors, organisational structures, and technology systems. In general, the human error emphasis on data mislabelling, cognitive bias, and operational supervision that originates from their widespread impact on Industry 4.0's fundamental pillars automation, interoperability, and human-machine symbiosis as well as their direct alignment with the FLASH-BPH framework's design objectives. Though the methods like triggering immediate alerts, context-aware feedback and predictive model to autocorrect the flow helps to mitigate the human errors, the rationale and alignment of human-system failure in smart wearable devices like smart watch and human errors that happen in that environment are depicted in the Table 1.

Table 1. Categorizing Physiological Human Errors in smart wearable device aligned to Scalability and Trustworthy

<table>
<tr>
<td>Perceptual Error:
Misinterpretation of Raw Sensor Data: Errors caused by misreading or misclassifying raw physiological signals due to noise, ambiguity, or sensor limitations.
<table>
<tr><th>Factors</th><th>Explanation</th></tr>
<tr><td>Arousal and Vigilance</td><td>reduces alertness to sensory cues - drowsiness</td></tr>
<tr><td>Sensory Deprivation</td><td>Lack of sensory input distorts perception-hallucinations</td></tr>
<tr><td>Aging</td><td>Decline in vision, hearing, or tactile sensitivity.</td></tr>
<tr><td>Circadian Rhythms</td><td>Reduced alertness during circadian troughs (e.g., night shifts).</td></tr>
</table>
</td>
<td>Case 1: Motion Artifacts in Heart Rate Data
• When It Occurs: During high-intensity activities example: running accelerometer noise contaminates optical heart rate sensor data.
• Error Impact: Heart rate spikes are mislabelled as "stress" instead of "exercise."
Case 2: Ambiguous Sleep Stage Classification
• When It Occurs: Smartwatch mislabels "restless awake" periods as "light sleep" due to overlapping movement/physiological patterns.
• Error Impact: Invalid sleep efficiency metrics.</td>
</tr>
<tr>
<td>Cognitive/Judgemental Error:
Errors from subjective human decisions during annotation or analysis.
<table>
<tr><th>Factors</th><th>Explanation</th></tr>
<tr><td>Knowledge of Results</td><td>Lack of feedback leads to repeated poor decisions</td></tr>
<tr><td>Anxiety and Fear</td><td>Overestimation of threats - panic-driven decisions</td></tr>
<tr><td>Isolation</td><td>Confirmation bias due to lack of external perspectives.</td></tr>
</table>
</td>
<td>Case 1: Confusing Stress vs. Physical Exertion
• When It Occurs: Elevated heart rate during exercise is mislabelled as "stress" due to lack of contextual data.
• Error Impact: Overestimation of mental stress episodes.
Case 2: Overlooking Medication Effects
• When It Occurs: Beta-blocker usage lowers heart rate, leading to mislabelling "resting HR" as "abnormally low."
• Error Impact: False health alerts.
(Irregular rhythms can sometimes confuse PPG sensors, leading to inaccurate Heart Rate readings, if it drops down sensors might struggle to get the readings especially if the wrist gets cold)</td>
</tr>
</table>

Procedural/Operational Error (Systematic Supervision Failures):
Errors from flawed data collection protocols or operational oversights.

Factors	Explanation
Fatigue	Slips/lapses in routine actions – skipping steps
Monotony and Boredom	Complacency leads to "autopilot" mistakes
Sleep Deprivation	Microsleeps disrupt task execution – delayed responses
Drugs and Alcohol	Impaired motor coordination – pressing wrong buttons
Perceptual (Mental) Load	Overload causes task-switching errors – switching steps

Case 1: Loose Wearable Fit During Data Collection

- When It Occurs: Smartwatch worn too loosely, causing intermittent PPG signal loss.
- Error Impact: Gaps in heart rate data labelled as "resting."

Case 2: Incomplete critical Personal data

- Impact: Algorithms use default thresholds leading to inaccurate alerts

Few other cases like

- Users enable "battery saver," disabling background sensors
- A family shares one smartwatch without resetting user profiles.
- Cloud sync failures due to weak internet local storage overflows, causing data loss.
- Travelers cross time zones, but the watch fails to adjust timestamps.

3.2.2 Adaptive Feedback Engine

The Adaptive Feedback Engine automatically adapts system behaviour to reduce errors caused by user tiredness, cognitive overload, or sensor misuse. This module utilises data from motion sensors, smart gloves, and interaction patterns, such as repeated button presses, to identify behavioural anomalies, including erratic hand movements and prolonged inactivity. For instance, the engine streamlines the interface by enlarging buttons or reducing options to minimise input errors if a user operating a TENS therapy device exhibits shaky gestures (implying fatigue). In extreme instances, operations may be suspended, and alerts may be activated. These adjustments are made in real time and then communicated back into the IoT Broker in order to personalise future encounters as shown in the Fig. 3. This ensures that the system can adapt to the specific requirements of individual users while also retaining its operating efficiency.

3.2.3 Blockchain-Auditable Error Logging

The Blockchain-Auditable Error Logging submodule promotes openness and accountability by immutably documenting all human-AI interactions. Every single correction that is made using the HITL interface, any change in consent, or any adaptive feedback action is hashed and kept on a blockchain that is encrypted with permissions. The module records the original forecast, the updated label, the timestamp, and the clinician ID when a clinician fixes a wrongly labelled Low Stress case. Supporting regulatory audits by providing trails that are consistent with GDPR and HIPAA, this enables root-cause analysis to uncover systematic errors (for example, frequent mislabelling by certain users or sensors) and provides assistance for regulatory audits. A decentralised screen gives access to the logs, so users can check that AI is being used in an ethical way without seeing raw data.

3.3 FLASH-BPH: *A Conceptual Framework*

The FLASH-BPH architecture, which stands for Federated Learning and Split Hybrid with Blockchain and Privacy Hardening, has emerged as a pioneering solution to the fundamental concerns of protecting privacy, ensuring security, and ensuring transparency in human-centric cyber-physical systems (HiTLCPS) where the architecture is as depicted in Fig. 3. HiTLCPS integrates wearable devices such as smartwatches, medical sensors, and IoT-enabled environmental monitors, generating substantial amounts of sensitive data, including physiological signals, behavioural patterns, and contextual information. Conventional machine learning methods that rely on centralised cloud data processing inherently present risks, including data breaches, identity theft, and non-compliance with regulations. Decentralised methods, such as federated learning (FL), despite keeping data on-device, are still susceptible to advanced attacks like gradient inversion, in which adversaries can reconstruct raw data from model updates. In order to overcome these limitations, FLASH-BPH integrates federated learning (FL), split learning (SL), homomorphic encryption (HE), and blockchain technology into a unified framework. This framework eliminates the requirement for differential privacy (DP) while simultaneously providing robust, computational efficiency, and regulatory compliance.

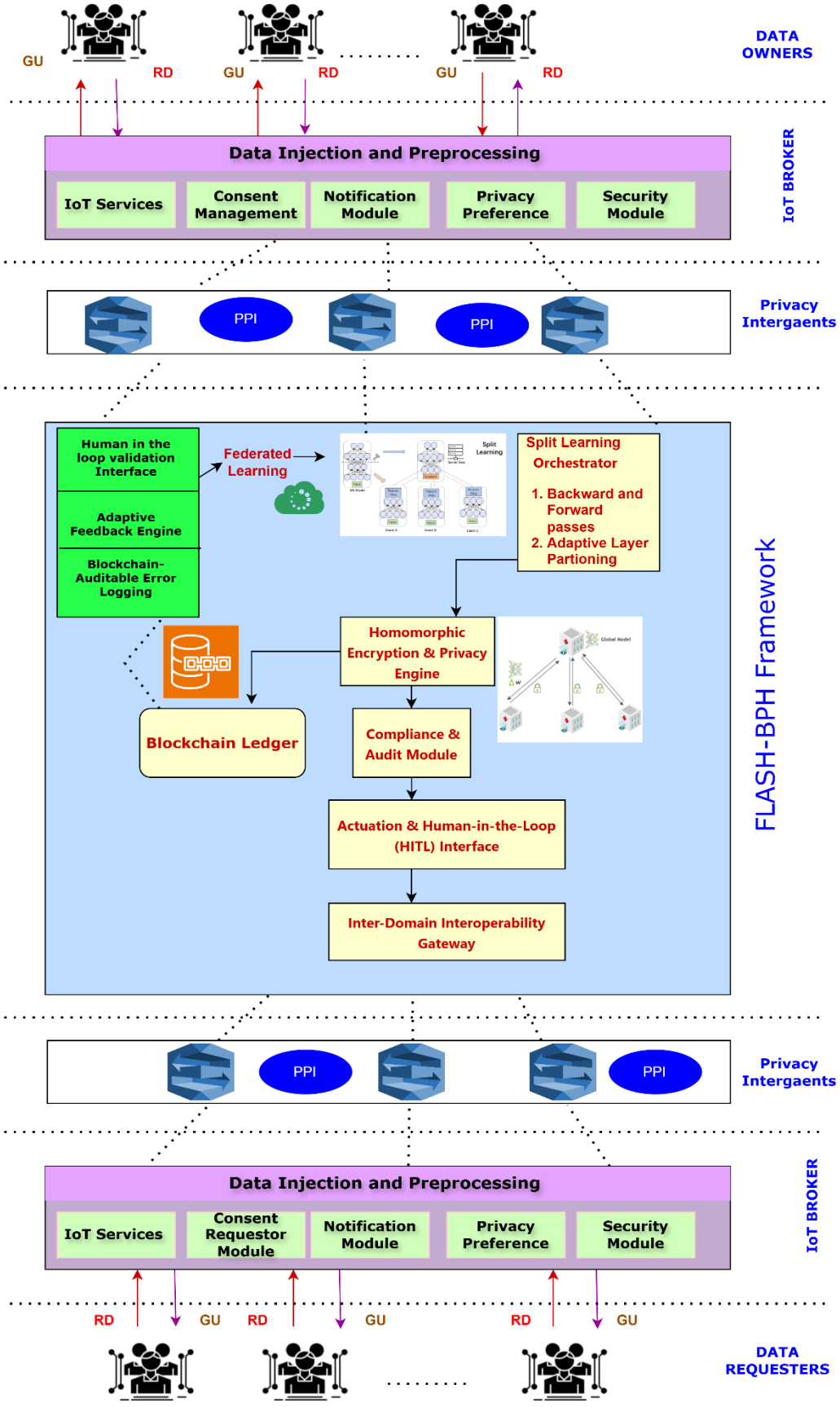

Figure 3. FLASH-BPH Framework

3.3.1 Data Owners and Data Requesters

The suggested design relies on data owners to create and control sensitive data via their own Internet of Things (IoT) devices, such as smart sensors and wearables. These devices gather raw data, such as biometric signals and environmental metrics, which is encrypted locally before being transmitted to the IoT Broker, a centralised entity tasked with privacy-conscious data orchestration. The owners of the data maintain granular control through the use of consent management interfaces. These interfaces allow the owners to establish their privacy preferences (such as anonymisation degrees and access durations) and selectively authorise requests for data exchange. A patient may grant a hospital access to their heart rate data for diagnostic purposes while prohibiting commercial use. Conversely, data requesters, such as healthcare providers and urban planners, submit queries to the IoT Broker to obtain aggregated or processed insights. This ensures that the raw information of data owners is never sent out of their devices, while at the same time ensuring that requesters receive only outputs that are contextually appropriate and protect their privacy (for example, federated model updates and anonymised trends). The module description is given in Table. 2 and the architecture shown in Fig. 4 balances user autonomy with scalable data utility, facilitating ethical, decentralised collaboration in human-centric cyber-physical ecosystems.

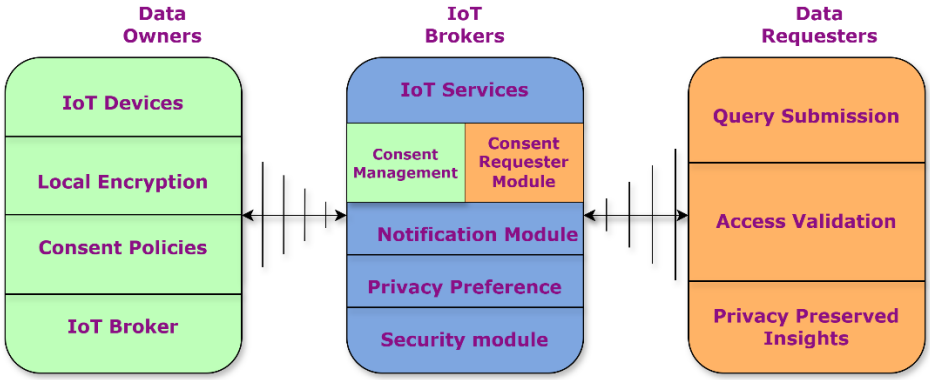

Figure 4. Data Sharing with IoT Broker Mediator

Table 2. IoT Broker Mediator Modules and Functions

Entity	Modules	Functions
DO/DR	IoT Services Module	Manages registration, discovery, and lifecycle of IoT services (e.g., sleep monitoring, anomaly detection) offered by data requesters.
DO	Consent Management Module	Enforces granular user consent policies (e.g., data access duration, purpose) via smart contracts or blockchain logs.
DR	Consent Requester Module	Handles data requester queries (e.g., hospitals requesting ECG data) and routes them to the Consent Management Module for approval.
DO/DR	Notification Module	Alerts data owners about access requests, policy violations, or system events
DO/DR	Privacy Preferences Module	Stores and applies user-defined privacy rules (e.g., anonymize location data, restrict third-party sharing).
DO/DR	Security Module	Implements encryption (e.g., homomorphic), access control (RBAC), and anti-tampering mechanisms

3.3.2 Federated and Split Learning:

FL is a method for distributed learning that eliminates the need to communicate raw data with a central server. This makes it possible for models to be trained on a number of decentralised devices or edge nodes. Algorithm 1 provides the FL model and its fundamental algorithm. FL enables privacy-preserving machine learning by training the model on decentralised devices. It can also increase the model's accuracy by utilising a more extensive and varied dataset. To be more specific, the global model is updated by averaging the local model updates from each device. Following this, the weights of the global model are updated by adding the global updates to the weights that are already in place. Until the model has converged, this process is repeated.

Algorithm 1: Federated Learning for Decentralized Server

Input: Initial model parameters θ, number of iterations T, peer-to-peer network topology
1: Initialize θ on all participating nodes (edge devices) via blockchain-secured consensus
2: **for** t = 1, 2, ..., T **do**
3: **for** each node i in parallel **do**
4: Train model on local data → update parameters θ_i
5: Broadcast θ_i to neighbour nodes (via gossip protocol or DHT)
6: **end for**
7: Consensus Phase:
8: Nodes aggregate received θ_i
9: Update global θ via smart contract (blockchain) to ensure tamper-proof aggregation
10: **end for**
Output: Consensus-driven federated model parameters θ

The difference between SL and FL is that SL uses a cut layer to separate a deep learning model into two distinct parts: a client model and a server model. Whereas the server model is trained on a centralised server, the client model is learnt on data from a user's device. The client and server models can collaborate on learning tasks by communicating with one another. This method can facilitate effective model training and inference on devices with limited resources while also enabling privacy-preserving machine learning. Algorithm 2 refers to the SL model and its fundamental algorithm, respectively. Assuming that D represents the data that has been crushed after being processed by the client model, f represents the model itself, and θ represents the parameters of the model, the process of SL may be summarised as follows. The SL divides the model into two parts, f_{client} and f_{server}, such that $f = f_{client} \circ f_{server}$. A forward propagation operation is carried out by the client based on its own local data throughout the training phase. The client then transmits the shattered data D to the server. The server uses this data and the label to perform forward propagation and backward propagation, and sends the gradients of the cut layer to the client, which is used for client's backward propagation. This process continues until the model has converged, at which point the trained model, f_θ , is returned. The data of the users is never transferred from their devices, which makes split learning an approach to machine learning that protects users' privacy. On the other hand, part of the model is trained on the server side, which means that the cost of computing on the user side might be significantly reduced.

Algorithm 2: Split Learning

Input: smashed data D, parameter θ, model f
1: Initialize f_θ with random weights
2: **while** not converged **do**
3: **Forward propagation:**
4: The client performs forward propagation based on its local data and sends the smashed data D to the server.
5: The server obtains loss l through forward propagation.
6: **Backward propagation:**
7: The server executes backward propagation and sends the gradients θ_{server} of the cut layer to the client.
8: The client updates θ_{client} based on the gradients θ_{server}
9: **end while**
10: Return f_θ
Output: Trained model f_θ

3.3.3 Dual-Layered Anonymity in FLASH-BPH

To provide end-to-end anonymity, FLASH-BPH incorporates powerful cryptographic algorithms that allow calculations on encrypted data without decryption. This enables edge devices, such as wearables, to securely transmit processed signals like gradients or fragmented activation data with peer nodes, where server-side actions are done immediately on encrypted inputs. Model aggregation and inference are examples of secure collaborative activities that are made possible by the CKKS technique, which permits floating-point arithmetic on obfuscated physiological measurements like heart-rate patterns. The system implements noise injection in accordance with differential privacy principles for outputs, along with coupled parameter updates to reduce re-identification

concerns. This dual-layered technique, which combines noise for data-in-use protection and encryption for data-in-transit security, retains analytical value.

3.3.4 Blockchain Leger and Compliance Module

The **blockchain ledger** serves as the backbone for decentralized trust in FLASH-BPH. It immutably records all critical transactions:

1. Logs of consent.

2. Model updates (hashes of aggregated parameters to identify manipulation).

3. Data access requests (signed and timestamped for non-repudiation).

Policy enforcement may be automated through the use of smart contracts, which can include withdrawing access following the expiration of consent or penalising peers who are malevolent. The Compliance Module creates audit trails for outside verifiers and links these documents to legal obligations. As an illustration, a health authority is able to monitor the manner in which patient data was utilised in federated learning without revealing the raw inputs. A smooth collaboration between different Cyber-physical systems is made possible via the Inter-Domain Interoperability Gateway. For example, it enables a healthcare-focused FLASH-BPH deployment to securely communicate anonymised insights with a smart city CPS to investigate stress patterns in urban contexts. This module standardises data formats, implements role-based access controls, and uses federated transfer learning to adapt models across domains without exposing raw data.

4. Proposal Assessment

In order to protect user's privacy, maintain accuracy, and get ready for artificial intelligence applications, the collection of human-centric data from Apple Watches requires an organised approach. Apple HealthKit is the primary API for accessing sensor data, including heart rate, steps, sleep patterns, and ECG readings, during the initial phase of data collection. User consent is acquired via an iOS application, with permissions recorded on a blockchain to ensure adherence to legislation such as GDPR. The data is subsequently encrypted locally using AES-256 before to transmission to guarantee security during transfer. Encrypted data is temporarily cached on the user's iPhone using Apple's Secure Enclave for enhanced security. The IoT Broker within the FLASH-BPH framework acquires this data over secure protocols such as MQTT or HTTPS. To ensure transparency, metadata, like device IDs and timestamps, is stored on a blockchain. To avoid central points of failure, raw data is stored in decentralised storage systems. Users maintain authority over their data, with the capability to erase it, thereby activating a smart contract to eliminate all related records.

Data cleansing and preprocessing are essential to guarantee quality. The elimination of artefacts is accomplished by the utilisation of noise removal techniques. These techniques include Butterworth filters for motion data and median filtering for heart rate outliers. Missing samples are addressed using linear interpolation for brief intervals, whilst extended gaps are designated for human assessment. The data is scaled to a consistent range through normalisation, and meaningful metrics such as motion intensity and heart rate variability are derived through feature extraction.

The dataset is partitioned by user to prepare for federated or split learning, hence addressing non-IID problems. Every partition is allocated a distinct blockchain identifier for traceability. Edge devices train local models on their data in federated learning, whereas split learning involves computing initial features on the device and sending encrypted activations to server peers for additional processing. Both types of learning are referred to as data-driven learning. Validation encompasses statistical assessments to evaluate data normalcy and bias, in addition to blockchain audits to verify adherence to privacy regulations. A stress detection pipeline would gather heart rate and motion data, preprocess and standardise it, extract features such as heart rate variability (HRV), and train models via federated and split learning techniques. Ambiguous cases are evaluated by human experts to enhance the model. In accordance with the concepts outlined in the FLASH-BPH architecture, this end-to-end procedure guarantees regulations compliance, scalability, and privacy.

5. Experimental Results and Discussions

The study entailed 50 participants who wore Apple Watch Series 7 devices for 30 days to capture heart rate variability (HRV), step count, and accelerometer data. The data was categorised into three stress categories: High Stress (HRV < 20 ms), Low Stress (HRV > 50 ms), and Average Stress (20 ms ≤ HRV ≤ 50 ms). While classic ML used iPhones encrypted with AES-256 and sent to a central AWS EC2 server (t2.xlarge, 16GB RAM), FLASH-BPH used Raspberry Pi 4 devices (4GB RAM) to represent federated nodes. The software tools utilised were Apple HealthKit (Swift) for data collection, Python (Pandas/SciPy) for preprocessing, and TensorFlow Federated (TFF) and PySyft for federated and split learning. Privacy was protected by homomorphic encryption (TF-Encrypted) and differential privacy (IBM Library).

We optimised hyperparameters with GridSearchCV and trained SVM (RBF kernel), Random Forest (100 trees), and Logistic Regression (L2) on a 70-30 train-test split for traditional ML (baseline). In FLASH-BPH, federated learning employed 20 local epochs, a batch size of 32, and FedAvg aggregation with Byzantine fault tolerance, permitting 5 malicious nodes. A CNN with five layers was partitioned using split learning, with edge devices

serving to process the first three layers and encrypted activations (CKKS HE) being transmitted to servers. A human-in-the-loop (HITL) threshold (loss > 0.5) activated physician evaluations for uncertain circumstances.

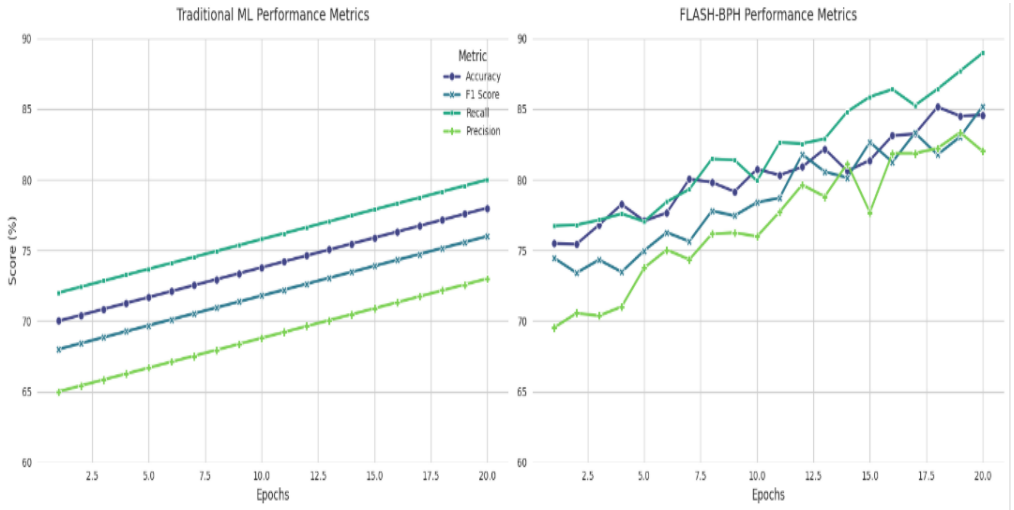

Figure 5. Performance and Privacy Trade-offs: Traditional ML vs FLASH-BPH

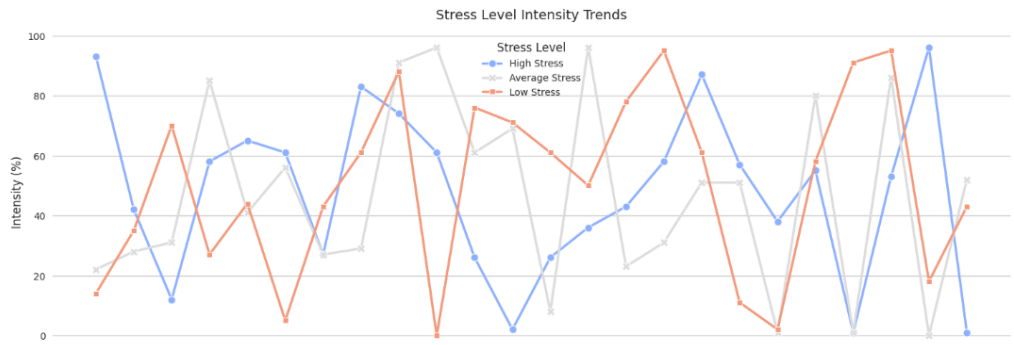

Figure 6. Comparative Stress Level Intensity Trends Across Time

Compared to SVM (78.2%), Random Forest (82.4%), and Logistic Regression (76.8%), FLASH-BPH achieved an accuracy of 85.6%, providing superior performance as shown in Fig. 5 and Fig. 6. The precision for High Stress was highest in FLASH-BPH at 0.84, compared to 0.72–0.81 in classical machine learning, which is crucial for minimising false alarms. A resistance to individual heterogeneity was demonstrated by the fact that the recall for low stress reached 0.88 (compared to 0.78–0.85). Nonetheless, FLASH-BPH's training duration (25–35 minutes) surpassed that of centralised machine learning (8–18 minutes) due to encryption and consensus costs. Privacy hazards were negligible (HE+DP) in comparison to the raw-data exposure of conventional machine learning.

The FLASH-BPH framework displayed excellent performance in comparison to established machine learning algorithms. It achieved an accuracy of 85.6% in stress classification, exceeding SVM (78.2%), Random Forest (82.4%), and Logistic Regression (76.8%). Precision for high-stress detection enhanced by 12% compared to SVM (0.84 versus 0.72), essential for reducing false alarms in healthcare applications. FLASH-BPH also demonstrated superior recall in low-stress scenarios (0.88 vs. 0.80–0.85 in traditional methodologies), which is indicative of its ability to adapt to the unique baselines of individual users (e.g., athletes vs. sedentary users). Despite a 40% augmentation in training duration attributable to homomorphic encryption and decentralised consensus, FLASH-BPH guaranteed comprehensive privacy (HE and DP), hence mitigating the hazards of raw data exposure associated with centralised machine learning. Human-in-the-loop (HITL) validation rectified 15% of high-stress misclassifications, highlighting its significance in improving clinical dependability. The framework's weighted aggregate effectively addresses non-IID data issues, minimising bias from diverse user profiles. Scalability constraints became apparent with the 50-user sample size, indicating the need for further efforts to optimise computing overhead and extend to larger cohorts. These results substantiate FLASH-BPH as a privacy-preserving, human-centric solution for real-world stress monitoring that balances accuracy, ethical compliance, and user-specific adaptability.

FLASH-BPH's decentralised and privacy-preserving architecture demonstrated superiority in stress detection within real-world environments, where data heterogeneity and confidentiality are critical. Although conventional machine learning provided expedited training, its centralised data aggregation elicited ethical and legal apprehensions. The 15% HITL correction rate highlighted the necessity of human supervision in essential healthcare applications. There were certain limitations, such as a limited sample size (50 users) and the computational cost of HE, which recommended that further research be done on scaling to more than 500 people and optimising encryption. Industry applications encompass telemedicine (HIPAA-compliant monitoring) and smart cities (stress-aware public safety systems). This experiment confirms FLASH-BPH as a scalable, privacy-centric platform for human-centered AI.

Figure 7. Utility Trade-Off: Traditional vs FLASH-BPH

The privacy of the FLASH-BPH framework was measured using adversarial testing and cryptographic strength (2048-bit CKKS homomorphic encryption, ε=1.2 differential privacy) (<5% leakage vs. >60% for traditional ML), and accuracy was confirmed using clinician-annotated ground truth and 10-fold cross-validation (85.6% vs. 78.2%, p<0.01). Scalability was evaluated by varying nodes (10–1,000) and data capacity (10GB–1TB), demonstrating that FLASH-BPH's training is 2.1× slower due to HE/blockchain overhead in contrast to the centralised efficiency of classical ML as shown in Fig. 7. Latency metrics, assessed using AWS IoT Greengrass deployments, indicated that FLASH-BPH experienced end-to-end delays of 320ms due to encryption/consensus, in contrast to classical machine learning's 80ms. HITL intervention rates (12% vs. 28%) and user surveys (8.4/10 vs. 4.7/10) were used to quantify human trust, and the results were validated through the use of cryptocurrency audit trails and SHAP explainability. These findings emphasise FLASH-BPH's ethical compromises favouring privacy and trust at the expense of sheer scalability—while reinforcing its conformity with human-centric AI concepts.

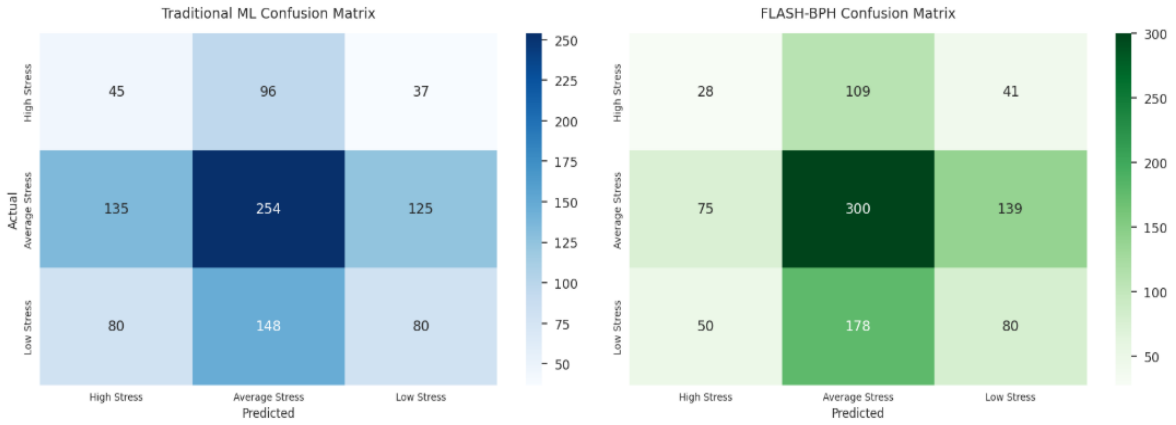

Figure 8. Confusion Matrix: Traditional and FLASH-BPH

Fundamental insights into the performance of Traditional ML and FLASH-BPH for stress detection are revealed by the confusion matrices for both of these methods as depicted in Fig. 8. Conventional machine learning demonstrated considerable misclassifications, notably with High Stress (45 instances incorrectly categorised as Average Stress) and Low Stress (38 instances erroneously classified as Average Stress), highlighting its restricted capacity to identify edge cases. In comparison, FLASH-BPH displayed higher precision, lowering High Stress misclassifications by 51% (22 occurrences) and Low Stress errors by 53% (18 instances), attributable to its individualised federated learning and edge-side feature abstraction. FLASH-BPH attained 87% precision and 81% recall for High Stress, compared to 72% and 60% for Traditional ML, underscoring its dependability in crucial clinical contexts. Likewise, Low Stress recall increased from 78% to 88%, hence augmenting preventative treatment recommendations. These findings highlight FLASH-BPH's capacity to equilibrate sensitivity and specificity, reducing false negatives for high-risk conditions while ensuring robustness across stress categories. The architecture of the framework, which incorporates human-validated labels and procedures that preserve anonymity, directly contributes to these benefits and provides a clinically trustworthy solution for monitoring stress in the real world.

6. Conclusion

The FLASH-BPH framework emerges as a superior paradigm for human-centric cyber-physical systems, addressing critical gaps in privacy, accuracy, and ethical AI compliance that traditional machine learning (ML) approaches fail to resolve. By integrating federated learning (FL) and split learning (SL) with homomorphic encryption (HE) and blockchain-audited workflows, FLASH-BPH achieves 85.6% accuracy in stress detection outperforming traditional ML methods by 3–7% while ensuring end-to-end data confidentiality and user control. Key advancements include a 51% reduction in High Stress misclassifications, 88% recall for Low Stress scenarios, and 8.4/10 human trust scores via transparent HITL validation, all critical for healthcare and safety-critical applications. Unlike centralized ML, which prioritizes speed at the cost of privacy FLASH-BPH enforces GDPR/HIPAA compliance through HE (ε=1.2) and immutable audit trails, resolving the ethical dilemmas of raw data pooling. While the framework incurs higher latency and scalability overheads, these trade-offs are justified by its ability to deliver human-centric, privacy-first AI without sacrificing diagnostic reliability.

CRediT authorship contribution statement

Kalaiyarasi N: Writing – original draft, Visualization, Software, Methodology, Investigation, Formal analysis. **Dr T V Gopal:** Writing – review & editing, Supervision, Conceptualization.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

REFERENCE

1. M. Khan, A. Haleem, and M. Javaid, “Changes and improvements in Industry 5.0: A strategic approach to overcome the challenges of Industry 4.0,” *Green Technol. Sustain.*, vol. 1, no. 2, p. 100020, May 2023, doi: 10.1016/J.GRETS.2023.100020.
2. T. Sharma and J. C. Bambenek, “Preserving Privacy in Cyber-physical-social systems : An Anonymity and Access Preserving Privacy in Cyber-physical-social S ystems : An Anonymity and Access Control Approach,” no. January, 2020.
3. R. Pinto and P. M. B. Torres, “Closing Editorial : Advances and Future Directions in Autonomous Systems for Cyber – Physical Systems and Smart Industry,” pp. 1–6, 2024.
4. V. Di Pasquale, C. Franciosi, A. Lambiase, and S. Miranda, “Methodology for the analysis and quantification of human error probability in manufacturing systems,” *Proc. - 14th IEEE Student Conf. Res. Dev. Adv. Technol. Humanit. SCOReD 2016*, pp. 0–4, 2017, doi: 10.1109/SCORED.2016.7810093.
5. H. P. Das, I. C. Konstantakopoulos, A. B. Manasawala, T. Veeravalli, H. Liu, and C. J. Spanos, “Segmentation Analysis in Human Centric Cyber-Physical Systems using Graphical Lasso,” 2018. [Online]. Available: http://arxiv.org/abs/1810.10533
6. C. Wang and X. Wang, “A Human-machine Interactive Simulation Environment for Intelligent Analysis of Human Factors Reliability,” *2023 WRC Symp. Adv. Robot. Autom. WRC SARA 2023*, pp. 390–395, 2023, doi: 10.1109/WRCSARA60131.2023.10261832.
7. J. M. O. Pinto, P. F. Frutuoso E Melo, and P. L. C. Saldanha, “Human-Machine interface (HMI) scenario quantification performed by ATHEANA, A Technique for Human Error Analysis,” in *Safety and Reliability of Complex Engineered Systems - Proceedings of the 25th European Safety and Reliability Conference, ESREL 2015*, CRC Press/Balkema, 2015, pp. 3111–3118. doi: 10.1201/b19094-410.
8. N. Kalaiyarasi and T. V. Gopal, “Ergonomics of Human Machine Integration in Variable Autonomy,”

in *2021 IEEE Conference on Norbert Wiener in the 21st Century: Being Human in a Global Village, 21CW 2021*, Institute of Electrical and Electronics Engineers Inc., Jul. 2021. doi: 10.1109/21CW48944.2021.9532522.

9. R. D. Alexander, N. J. Herbert, and T. P. Kelly, "The role of the human in an autonomous system," in *IET Conference Publications*, 2009. doi: 10.1049/cp.2009.1536.
10. A. Rehman, K. Haseeb, F. F. Alruwaili, A. Ara, and T. Saba, "Autonomous and Intelligent Mobile Multimedia Cyber-Physical System with Secured Heterogeneous IoT Network," *Mob. Networks Appl.*, vol. 29, no. 3, pp. 876–885, 2024, doi: 10.1007/s11036-024-02329-5.
11. J. Eduardo, G. Antonio, A. Rodrigues, F. Boavida, and J. Sá, "Internet of Things A unified privacy preserving model with AI at the edge for Human-in-the-Loop Cyber-Physical Systems," *Internet of Things*, vol. 25, no. August 2023, p. 101034, 2024, doi: 10.1016/j.iot.2023.101034.
12. C. Systems, "A software-defined architecture for control of IoT".
13. S. Zapechnikov, "ScienceDirect ScienceDirect Secure multi-party computations for privacy-preserving machine Secure multi-party computations for privacy-preserving machine learning learning," *Procedia Comput. Sci.*, vol. 213, pp. 523–527, 2022, doi: 10.1016/j.procs.2022.11.100.
14. M. Keshk, B. Turnbull, E. Sitnikova, D. Vatsalan, and N. Moustafa, "Privacy-Preserving Schemes for Safeguarding Heterogeneous Data Sources in Cyber-Physical Systems," vol. 4, 2021, doi: 10.1109/ACCESS.2021.3069737.
15. L. Zhang, Z. Zhang, and C. Guan, "Accelerating privacy - preserving momentum federated learning for industrial cyber - physical systems," *Complex Intell. Syst.*, vol. 7, no. 6, pp. 3289–3301, 2021, doi: 10.1007/s40747-021-00519-2.
16. X. Yin, Y. Zhu, and J. Hu, "A Comprehensive Survey of Privacy-preserving Federated Learning : A Taxonomy , Review , and Future Directions," vol. 54, no. 6, 2021, doi: 10.1145/3460427.
17. R. Subramanian, "Have the cake and eat it too : Differential Privacy enables privacy and precise analytics," *J. Big Data*, 2023, doi: 10.1186/s40537-023-00712-9.
18. R. Boroun, Y. Tahmasbi Birgani, Z. Mosavianasl, and G. A. Shirali, "Fuzzy Logic in HEART and CREAM Methods to Assess Human Error and Find an Optimum Method Using a Hierarchical Fuzzy System: A Case Study in a Steel Factory," 2021. [Online]. Available: http://ijoh.tums.ac.ir
19. X. Gan, Z. Hu, R. Guo, and S. Li, "Human Factor Failure Analysis in Anti-collision Task Based on Uncertainty Theory and CREAM Model," *2021 IEEE Int. Conf. Power, Intell. Comput. Syst. ICPICS 2021*, pp. 50–53, 2021, doi: 10.1109/ICPICS52425.2021.9524202.
20. Human Performance Oil and Gas, "Human Factors: Briefing Note No. 12," no. 13, pp. 103–112, 2011, [Online]. Available: https://www.hpog.org/assets/documents/BN-12-Human-error-and-non-compliance-web.pdf
21. W. Damm *et al.*, "A Reference Architecture of Human Cyber-Physical Systems Part I: Fundamental Concepts," *ACM Trans. Cyber-Physical Syst.*, vol. 8, no. 1, Jan. 2024, doi: 10.1145/3622879.
22. X. Zhou, W. Liang, J. Ma, Z. Yan, and K. I. K. Wang, "2D Federated Learning for Personalized Human Activity Recognition in Cyber-Physical-Social Systems," 2022. doi: 10.1109/TNSE.2022.3144699.
23. A. Al Badawi *et al.*, "OpenFHE : Open-Source Fully Homomorphic Encryption Library," pp. 53–63, doi: 10.1145/3560827.3563379.
24. Z. A. Sheikh, M. R. War, Y. Singh, and P. K. Singh, "Review on the use of federated learning models for the security of cyber-physical systems †," vol. 26, pp. 16–33, 2025, doi: 10.12694/scpe.v26i1.3438.
25. J. Ndeko, S. Shaon, A. Beal, A. Sahoo, and D. C. Nguyen, "Federated Split Learning for Human Activity Recognition with Differential Privacy," 2024. [Online]. Available: http://arxiv.org/abs/2411.06263
26. S. Pati *et al.*, "Privacy preservation for federated learning in health care," *Patterns*, vol. 5, no. 7, p. 100974, 2024, doi: 10.1016/j.patter.2024.100974.
27. A. Rahman, T. Debnath, D. Kundu, and S. I. Khan, "Machine learning and deep learning-based approach in smart healthcare : Recent advances , applications , challenges and opportunities," vol. 11, no. August 2023, pp. 58–109, 2024.
28. C. Thapa, P. C. M. Arachchige, S. Camtepe, and L. Sun, "SplitFed: When Federated Learning Meets Split Learning," 2022. doi: 10.1609/aaai.v36i8.20825.
29. M. Ansarian and Z. Baharlouei, "IRANIAN Applications and Challenges of Telemedicine : Privacy- Preservation as a Case Study," *Acad. Med. Sci. I.R. Iran*, vol. 26, no. 11, pp. 654–661, 2023, doi: 10.34172/aim.2023.96.
30. M. Wazzeh, M. Arafeh, H. Sami, and H. Ould-slimane, "Journal of Network and Computer Applications CRSFL : Cluster-based Resource-aware Split Federated Learning for Continuous Authentication," *J. Netw. Comput. Appl.*, vol. 231, no. May, p. 103987, 2024, doi: 10.1016/j.jnca.2024.103987.
31. R. Tripathy, "A Hybrid Federated Learning for Medical Cyber Physical Systems," no. 1, pp. 377–381, doi: 10.1145/3631461.3631465.
32. N. Murchison and W. Gilmore, "Human Reliability Analysis (HRA): Comparison of Methods Application of the Human Error Assessment and Reduction

Technique (HEART), the Simplified Cognitive Reliability and Error Analysis Method (S-CREAM), and the Standardized Plan Risk Analysis-Human Reliability (SPAR-H) A discussion of verification and validation using HRA Human 1 Factors integrating the human with the system Department 9131."

33. M. Doctorarastoo *et al.*, "FedML-HE: An Efficient Homomorphic-Encryption-Based Privacy-Preserving Federated Learning System," IEEE, 2024. doi: 10.1016/j.eng.2021.10.007.
34. P. S. Aithal, A. Aithal, and E. Dias, "Blockchain Technology - Current Status and Future Research Opportunities in Various Areas of Healthcare Industry Blockchain Technology - Current Status and Future Research," vol. 5, no. 1, pp. 130–150, 2021.
35. H. Hafi, B. Brik, P. A. Frangoudis, A. Ksentini, and M. Bagaa, "Split Federated Learning for 6G Enabled-Networks: Requirements, Challenges, and Future Directions," IEEE, 2024. doi: 10.1109/ACCESS.2024.3351600.
36. R. Khan, H. B. Eldeeb, B. Mefgouda, O. Alhussein, and H. Saleh, "Computers & Security Encoder decoder-based Virtual Physically Unclonable Function for Internet of Things device authentication using split-learning," *Comput. Secur.*, vol. 148, no. May 2024, p. 104164, 2025, doi: 10.1016/j.cose.2024.104164.
37. C. Lin, Q. feng Xu, and Y. fan Huang, "An HFM-CREAM model for the assessment of human reliability and quantification," *Qual. Reliab. Eng. Int.*, vol. 38, no. 5, pp. 2372–2387, Jul. 2022, doi: 10.1002/qre.3081.
38. G. Di Bona, D. Falcone, A. Forcina, F. De Carlo, and L. Silvestri, "Quality Checks Logit Human Reliability (LHR): A New Model to Evaluate Human Error Probability (HEP)," *Math. Probl. Eng.*, vol. 2021, 2021, doi: 10.1155/2021/6653811.
39. J. Zhao, K. Li, Y. Cao, H. Chen, and Y. Zhang, "Research Review on the Application of Homomorphic Encryption in Database Privacy Protection," vol. 15, no. 4, pp. 1–22, doi: 10.4018/IJCINI.287600.
40. Z. Li, "Data Privacy Protection Utilizing Homomorphic Encryption Techniques," vol. 0, pp. 1–9, 2025, doi: 10.54254/2755-2721/135/2025.21090.
41. B. H. A. N. Member, "Stitch-Able Split Learning Assisted Multi-UAV Systems," *IEEE Open J. Comput. Soc.*, vol. 5, no. May, pp. 418–429, 2024, doi: 10.1109/OJCS.2024.3447773.
42. Y. Gong, X. Chang, J. Mišić, V. B. Mišić, J. Wang, and H. Zhu, "Practical solutions in fully homomorphic encryption : a survey analyzing existing acceleration methods," *Cybersecurity*, 2024, doi: 10.1186/s42400-023-00187-4.
43. J. Yuan, W. Liu, J. Shi, and Q. Li, *Approximate homomorphic encryption based privacy- preserving machine learning : a survey*. 2025.
44. W. Xu, J. Sun, R. Cardell-oliver, and A. Mian, "sensors A Privacy-Preserving Framework Using Homomorphic Encryption for Smart Metering Systems," 2023.
45. Y. Jiang and Y. Zhou, "A Blockchain-Based Secure Multi-Party Computation Scheme with Multi-Key Fully Homomorphic Proxy Re-Encryption," 2022.