Interdisciplinary Journal of Computing & AI

IJCAI

Interdisciplinary Journal of Computing & AI

IJCAI

RESEARCH

Cyber-Physical Integration of CFD-Based Aerodynamic Optimization and Hash-Based Post-Quantum Secure Control

Bannishikha Banerjee[1], Indraneel Mukhopadhyay[2*]

[1,2]*Amity Institute of Information Technology, Amity University, Kolkata, Email: [1]bbaneerjee@kol.amity.edu; [2]imukhopadhyay@gmail.com*

ARTICLE INFO.

Keywords: Computational Fluid Dynamics (CFD), Post-Quantum Cryptography, Quantum-Resilient Security, Cyber-Physical Systems, Autonomous Flight Control, Reduced-Order Modeling, Aerodynamic Optimization, Secure Control Systems, Hash-Based Cryptography

∗Corresponding author email address: imukhopadhyay@gmail.com

Manuscript received: 26 March 2026/Accepted April 15 2026

Published online: 17 April 2026

https://doi.org/10.5281/zenodo.19624946

Cite as: B. Banerjee and I. Mukhopadhyay, "Cyber-Physical Integration of CFD-Based Aerodynamic Optimization and Hash-Based Post-Quantum Secure Control", Interdisciplinary Journal of Computing & AI (IJCAI), vol. 1, no. 1. Aspiration Publishing Trust (DARPAN ID: WB/2025/0887371), p. 58-85, Apr. 2026. doi: 10.5281/zenodo.19624946.

ABSTRACT

The convergence of high-fidelity physical modelling and quantum-resilient cybersecurity has become a prerequisite for next-generation autonomous aviation systems. This paper introduces a unified cyber-physical framework incorporating computational fluid dynamics (CFD), reduced-order aerodynamic modelling, autonomous flight control, and hash-based post-quantum cryptography. High-resolution CFD simulations of the RAE 2822 transonic airfoil are used to construct compact surrogate aerodynamic models that capture nonlinear flow behaviour while remaining suitable for real-time implementation. These CFD-informed models are integrated into a closed-loop control framework, enabling performance-aware flight control without requiring online flow simulation. A lightweight hash-based post-quantum secure communication protocol is proposed to protect sensor data and control commands within the cyber-physical control loop against emerging quantum-capable adversaries. Simulation results demonstrate improved tracking performance and reduced aerodynamic drag compared to conventional constant-coefficient models, and security

analysis confirms that the proposed cryptographic scheme satisfies real-time latency requirements. The framework establishes a unified pipeline integrating CFD-based physical intelligence, autonomous control, and quantum-resistant cryptographic security for safety-critical aerospace cyber-physical systems.

1 Introduction

A transonic airfoil RAE 2822 is a time-tested geometry that is commonly employed to investigate complex aerodynamic processes in the transonic flight regime. This work uses it as the foundation to construct compact surrogate models that are able to model nonlinear behavior of flows such as the behavior of a shockwave and a boundary layer. These models are highly computational efficient and can be used to provide real-time aerodynamic analysis and control [1]. The contemporary autonomous aviation systems are changing into highly connected, data-driven platforms where aerodynamic performance, control intelligence, and communication security are closely interrelated [2], [3]. Traditional flight control systems are usually based on aerodynamic models of wind tunnel tests or straight-line models of nonlinear flows. These methods are usually not sufficient to capture the nonlinear flow nature that is experienced in transonic or off-design operation regimes. To make this problem even more difficult, the growing interconnectedness of onboard subsystems poses substantial cybersecurity risks, specifically, due to the growing threats that quantum computing poses to the integrity of classical cryptographic schemes [4], [5].

Computational Fluid Dynamics (CFD) offers an insight into the aerodynamic behaviour at high-fidelity scales, allowing detailed prediction of the pressure field, lift, drag and moments derived out of the predicted pressure field [6], [7], [8]. Nevertheless, real-time control loop integration with CFD is not computationally feasible. One of the methods that can be used to provide a way of interpolating between high-fidelity CFD and real-time control is the reduced-order modelling (ROM) techniques that can reduce large-scale flow data into smaller surrogate models [9].

Simultaneously with the developments in programming and control, post-quantum cryptography is coming up as a way to handle the drawback that current encryption schemes are susceptible to quantum attacks [10], [11]. Secure message transmissions among sensors, controllers and actuators in safety-critical cyber-physical systems like autonomous aircraft are crucial to avoid spoofing, tampering or data injection attacks [12]. The implementation

of quantum-resilient cryptographic security in control architecture should be done cautiously such that it would not infringe real-time limitations [13], [14].

The paper will discuss these two issues and suggest a cyber-physical combination of CFD-based aerodynamic optimization and hash-based post-quantum secure control. The point here is that the physics-informed aerodynamic intelligence obtained through CFD is to be incorporated into an autonomous control system and to at the same time safeguard the control communications with the help of a lightweight, hash-based post-quantum cryptographic scheme.

The key contributions of this work are:

1. CFD-Based Aerodynamic Intelligence - Aerodynamic models based on reduced-order simulations of a transonic airfoil are built using high-fidelity CFD simulations [15], [16].
2. ROM-Based Autonomous Control - The surrogate models of CFD are built into the closed-loop control system to enhance the tracking behaviour and aerodynamic efficiency [17], [18].
3. Hash-Based Post-Quantum Secure Control Protocol- A quantum resistant hash-based lightweight cryptographic scheme is developed to implement real-time secure communication in the control loop [19], [20], [21].
4. Cyber-Physical Performance Evaluation- The framework is analysed based on the precision of aerodynamic model, performance enhancement through control and the effect of cryptography on latency [22], [23].

This paper will bring together modelling with CFDs, autonomous control and post-quantum cryptographic security into a single cyber-physical design, making a step toward the design of resilient and performance-conscious autonomous aviation systems that are capable of sustained operations into the quantum computing age.

2. CFD-Based Aerodynamic Modelling and Reduced-Order Representation

2.1 High-Fidelity CFD Framework

High-fidelity aerodynamic data are generated using steady Reynolds-Averaged Navier–Stokes (RANS) simulations of the RAE 2822 transonic airfoil [1]. The simulations are performed using the SU2 open-source CFD solver with the

Spalart–Allmaras turbulence model, which is widely adopted for external aerodynamic flows due to its robustness and computational efficiency [24], [25], [26].

The governing equations for compressible viscous flow are:

$$\frac{\partial \mathrm{U}}{\partial t} + \nabla \cdot \mathrm{F}_c(\mathrm{U}) - \nabla \cdot \mathrm{F}_v(\mathrm{U}, \nabla \mathrm{U}) = 0$$

where:

- U represents the conservative flow variables [26],
- $\mathrm{F}_c$and $\mathrm{F}_v$denote convective and viscous fluxes [27].

Simulations are conducted over a range of angle of attack values α, capturing nonlinear aerodynamic behavior in the transonic regime.

The CFD dataset provides [1]:

- Surface pressure coefficient $C_p(x, \alpha)$
- Skin friction coefficient $C_f(x, \alpha)$
- Lift coefficient $C_L(\alpha)$
- Drag coefficient $C_D(\alpha)$
- Moment coefficient $C_m(\alpha)$

These extents serve as the corporeal groundwork of the proposed cyber-physical control framework.

2.2 Aerodynamic Force Representation

Aerodynamic forces and moments are articulated in non-dimensional arrangement [28]:

$$L = \frac{1}{2}\rho V^2 S C_L(\alpha)$$
$$D = \frac{1}{2}\rho V^2 S C_D(\alpha)$$
$$M = \frac{1}{2}\rho V^2 S c C_m(\alpha)$$

where:

- $\rho$is air density,
- $V$is freestream velocity,

- $S$is reference area,
- $c$is reference chord length.

In orthodox aeronautical control schemes, $C_L$and $C_D$are often approximated using linearized representations [29]. Nevertheless, transonic CFD data divulge sturdy nonlinearities and shock-induced pressure disparities that entail higher-fidelity representation [30], [31].

2.3 Proper Orthogonal Decomposition (POD) of Surface Pressure

To empower real-time amalgamation into the control loop, the high-dimensional surface pressure arena is abridged using Proper Orthogonal Decomposition (POD) [32], [33].

Let the discrete pressure dispersal at a prearranged angle of outbreak be epitomized as:

$$\mathrm{C}_p(\alpha) \in \mathbb{R}^N$$

where $N$is the number of surface nodes.

The pressure field is decomposed as:

$$\mathrm{C}_p(\alpha) = \bar{\mathrm{C}}_p + \sum_{i=1}^{r} a_i\,(\alpha)\,\phi_i$$

Where [34]:

- $\bar{\mathrm{C}}_p$is the mean pressure distribution,
- $\phi_i$are orthogonal spatial modes,
- $a_i(\alpha)$are modal coefficients,
- $r \ll N$is the reduced dimension.

Singular Value Decomposition (SVD) is applied to the Polaroid matrix:

$$\mathrm{X} = [\mathrm{C}_p(\alpha_1), \ldots, \mathrm{C}_p(\alpha_m)]$$

such that:

$$\mathrm{X} = \mathrm{U}\Sigma\mathrm{V}^T$$

The overriding r modes agreeing to the chief singular values are engaged [35], [36].

Variance Capture

By means of $r = 5$ modes apprehend roughly 95% of total variance, plummeting dimensionality by more than 90% while preserving shock and suction crowning behaviour.

2.4 Surrogate Modeling of Aerodynamic Coefficients

To associate reduced-order depictions to control involvements, proxy models are erected for global aerodynamic coefficients [37], [38], [39].

Polynomial regression of order three is cast-off:

$$C_L(\alpha) = b_0 + b_1\alpha + b_2\alpha^2 + b_3\alpha^3$$
$$C_D(\alpha) = d_0 + d_1\alpha + d_2\alpha^2 + d_3\alpha^3$$

The regression parameters are obtained using least squares fitting over the CFD dataset.

Model Accuracy: The surrogate model achieves:

Coefficient	RMSE
C_L	0.012
C_D	0.004

These low-slung blunders designate that the CFD-informed reduced-order depiction is apt for control-oriented enactment.

2.5 CFD-Informed Aerodynamic Optimization

The sweptback optimization delinquent is formulated as:

$$\min_{\alpha} J(\alpha) = w_1 C_D(\alpha) - w_2 C_L(\alpha)$$

subject to:

$$C_L(\alpha) \geq C_{L,\min}$$
$$| \alpha | \leq \alpha_{\max}$$

where w_1 and w_2 are weighting factors [40].

The augmented angle of outbreak attained from the substitute model makes available a performance-aware orientation for the control layer, empowering real-time aerodynamic efficiency perfection without invoking full CFD totaling.

2.6 Role in the Cyber-Physical Secure Control Framework

The reduced-order sleek model obliges as the physical intelligence layer of the cyber-physical system:

- Provides real-time estimates of lift and drag
- Enables performance-aware control adaptation
- Supplies aerodynamic state data to the secure communication layer
- Maintains computational feasibility within embedded hardware constraints

By squashing high-fidelity CFD data into compacted surrogate models, the agenda bridges comprehensive flow physics with quantum-secure self-directed control [41].

3 Cyber-Physical Architecture for CFD-Informed Quantum-Secure Control

3.1 System Overview

The wished-for framework is arranged as a multi-layered cyber-physical system (CPS) that fits in:

1. Physical Aerodynamic Layer (CFD-informed)
2. Reduced-Order Modeling and Optimization Layer
3. Autonomous Control Layer
4. Hash-Based Post-Quantum Cryptographic Security Layer

This manner empowers real-time aerodynamic performance optimization while safeguarding sheltered announcement in contradiction of quantum-capable adversaries. Unlike conventional flight control systems that separate physical modeling and cybersecurity, the proposed approach embeds CFD-derived aerodynamic intelligence and quantum-resilient cryptography directly into the control loop, forming a tightly coupled secure cyber-physical ecosystem. Figure 1 shows the suggested cyber-physical convergence of the

CFD-based aerodynamic intelligence and post-quantum secure autonomous control.

Offline high-fidelity CFD simulations are conducted in order to create an aerodynamic dataset that is trained on a reduced-order surrogate model. This model embodies the nonlinear correlation in between the flight conditions and aerodynamic forces and moments at the same time being computationally efficient to be applied in real time.

When operating, the surrogate model provides the autonomous controller with aerodynamic coefficients, which enables performance-conscious control decisions based on high-fidelity flow physics [42]. The controller calculates control commands and they are conveyed by a hash-based post-quantum security layer that encrypts and secures communication over the feedback loop. The aircraft dynamics are driven by the secured control signals, and the flight state measurements are sent to the controller, and the closed-loop cyber-physical system is complete.

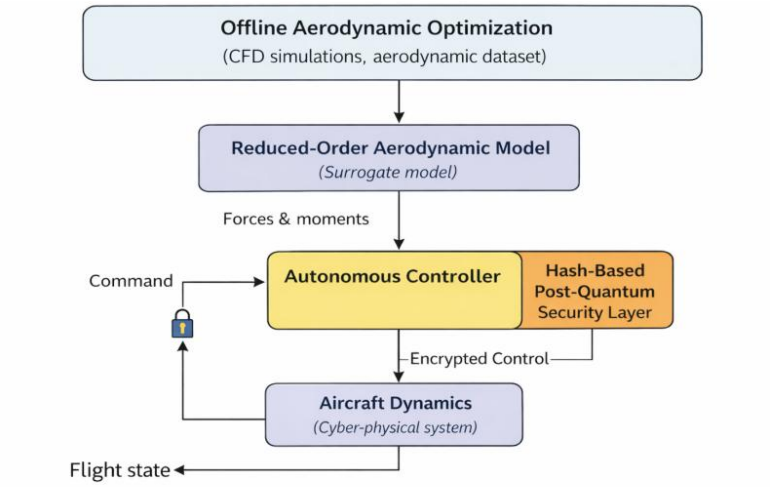

Fig. 1 Cyber-physical architecture for CFD-informed autonomous control with hash-based post-quantum security

This architecture shows that a unification of CFD-based modelling, real-time control, and quantum-resistant cryptographic security can be achieved to provide better performance and reliability in future autonomous aviation systems.

3.2 Physical Aerodynamic Layer (CFD Intelligence Layer)

The corporeal layer characterizes aircraft dynamics prejudiced by aerodynamic forces and jiffies computed using reduced-order models consequential from CFD.

The aircraft longitudinal subtleties can be expressed as:

$$\dot{x}(t) = f(x(t), u(t), F_{aero}(t))$$

where:

- $x(t)$= state vector (velocity, pitch angle, angular rate)
- $u(t)$= control input (elevator deflection)
- $F_{aero}(t)$= aerodynamic forces derived from CFD-ROM

Aerodynamic forces are computed as:

$$F_{aero} = \frac{1}{2}\rho V^2 S \begin{bmatrix} C_L(\alpha) \\ C_D(\alpha) \end{bmatrix}$$

where $C_L(\alpha)$and $C_D(\alpha)$are provided by the surrogate models described in Section 2.

This layer safeguards that control pronouncements are well-versed by nonlinear CFD-based aerodynamic behavior rather than abridged linear approximations.

3.3 Reduced-Order Modeling and Optimization Layer

The reduced-order layer acts as the computational conduit flanked by CFD physics and real-time control.

Its meanings include:

- Real-time estimation of aerodynamic coefficients
- Evaluation of aerodynamic efficiency metrics
- Online performance-aware angle-of-attack adjustment
- Provision of aerodynamic state data to the controller

The optimization objective is:

$$\alpha^* = \arg\min_{\alpha} (w_1 C_D(\alpha) - w_2 C_L(\alpha))$$

This optimum aerodynamic reference is provided to the controller making CFD informed adaptive control possible.

The computational complexity decreases to low-dimensional algebraic calculation because the computation of ROM replaces full CFD computation, and thus, the complexity can be computed onboard.

3.4 Autonomous Control Layer

The autonomous control layer computes control inputs using CFD-informed aerodynamic predictions.

A state-feedback control law is implemented:

$$u(t) = -Kx(t) + K_r r(t)$$

where:

- K= feedback gain matrix
- $r(t)$= reference trajectory
- Aerodynamic coefficients are updated via ROM in real time

The fact that CFD is integrated into the process results in two important improvements:

- None of the previously mentioned types of aerodynamic awareness are linear at all.
- The controller takes into consideration transonic nonlinearities that are represented by CFD.

Performance-Aware Adaptation: The gains of control can be programmed depending on optimized aerodynamic efficiency regions. This enhances accuracy in tracking and minimization of unnecessary drag in manoeuvres [38], [39].

3.5 Hash-Based Post-Quantum Cryptographic Security Layer

In order to safeguard control communication channels, the CPS has a lightweight hash-based post-quantum secure protocol.

The security layer protects:

- Sensor measurements transmitted to the controller
- Control commands sent to actuators

- Aerodynamic model updates

Secure Communication Model

Let:

$$m_s = \text{sensor data}, m_c = \text{control command}$$

Encryption process:

$$(c, r, t) = Enc_{PQH}(m)$$

Decryption process:

$$m = Dec_{PQH}(c, r, t)$$

where Enc_{PQH} denotes the wished-for hash-based post-quantum encryption mechanism.

The security of the proposed scheme relies on the following formally stated cryptographic assumptions, consistent with NIST post-quantum standardization requirements:

- Second-preimage resistance and preimage resistance of the underlying hash function (SHA-3/SHAKE-256): it is computationally infeasible to find an input x such that H(x) = y for a given y, or to find x' not equal to x such that H(x') = H(x). These properties ensure that keystream values cannot be reversed or forged by an adversary.
- Collision resistance: it is computationally infeasible to find two distinct inputs x and x' such that H(x) = H(x'). SHA-3/SHAKE-256 provides 128-bit collision resistance against quantum adversaries. Grover's algorithm reduces the classical 256-bit security level to 128-bit quantum security, which remains computationally intractable for any foreseeable quantum hardware.
- Hash-based key derivation (HKDF over SHA-3): the secret seed used by the PRNG is expanded into session keys using an HKDF construction over SHA-3. The derived keys are computationally indistinguishable from random given the secrecy of the seed, under the random oracle model and consistent with NIST SP 800-56C guidance.

Threat Model: The scheme is designed to resist a quantum-capable adversary (QCA) who possesses a large-scale quantum computer and can eavesdrop on,

replay, or inject messages into the control communication channel. The adversary is assumed computationally bounded and cannot break SHA-3/SHAKE-256 preimage or collision resistance within the operational lifetime of the system. Shor's algorithm does not apply to symmetric hash-based constructions, and Grover's quadratic speedup is mitigated by the 256-bit output length of SHAKE-256. Unlike lattice-based PQC schemes requiring polynomial arithmetic (e.g., CRYSTALS-Kyber for key encapsulation or CRYSTALS-Dilithium for digital signatures), the proposed protocol relies primarily on hash and XOR operations, significantly reducing computational latency while maintaining quantum resilience.

3.6 Closed-Loop Secure Cyber-Physical Operation

The complete secure CPS can be described as:

$$\dot{x}(t) = f(x(t), Dec_{PQH}(Enc_{PQH}(u(t))))$$

Operational sequence:

1. Sensors measure aircraft states
2. Data encrypted using hash-based post-quantum protocol
3. Controller decrypts and computes CFD-informed control input
4. Control command encrypted and transmitted
5. Actuator decrypts and applies command
6. Aircraft dynamics update

This ensures:

- Aerodynamic optimality (via CFD-ROM)
- Closed-loop stability (via feedback control)
- Communication integrity (via post-quantum cryptography)

3.7 Real-Time Feasibility Analysis

Typical flight control loops operate at:

$$50–100 \text{ Hz}$$

Allowable computational window:

$$10–20 \text{ ms per cycle}$$

The proposed hash-based scheme requires:

- 2–3 hash evaluations per message
- XOR masking operations

Estimated cryptographic overhead:

$$<2 \text{ ms}$$

Thus, the integration of post-quantum security does not violate real-time control constraints.

3.8 Architectural Advantages

The integrated framework offers:

- CFD-driven aerodynamic intelligence
- Performance-aware autonomous control
- Quantum-resilient cryptographic security
- Reduced computational burden via ROM
- Compatibility with embedded aerospace hardware

The result is a unified CFD-to-cryptography cyber-physical control pipeline designed for secure next-generation autonomous aviation.

Figure 2 illustrates the proposed hash-based post-quantum secure control protocol integrated into the cyber-physical architecture.

Three primary data sources—sensor state vectors, CFD-informed aerodynamic coefficients, and control commands—are first concatenated and padded to form an aggregated data block. This block represents the combined physical and control intelligence of the system that must be securely transmitted within the control loop.

A hash-based pseudorandom number generator (PRNG) derives a keystream from a secret seed, enabling quantum-resistant masking of the aggregated block via XOR operations. The masked data are trimmed in a lightweight Substitution-Permutation-Hash (SPH) structure adding nonlinear diffusion and confusion to enhance the refusal to cryptanalytic attacks.

An authentication tag is then calculated with the help of cryptographic hash where data integrity and resistance to tampering are ensured. The ciphertext produced and transmitted consists of the encrypted payload assemblage plus the authentication tag in order to produce a secure message to be used in real time control communication.

This framework maintains physical performance data and control messages used in controlling the aerodynamic state confidential to quantum enabled adversaries by encrypting physical performance information and control messages with post-quantum cryptography, and is real-time feasible.

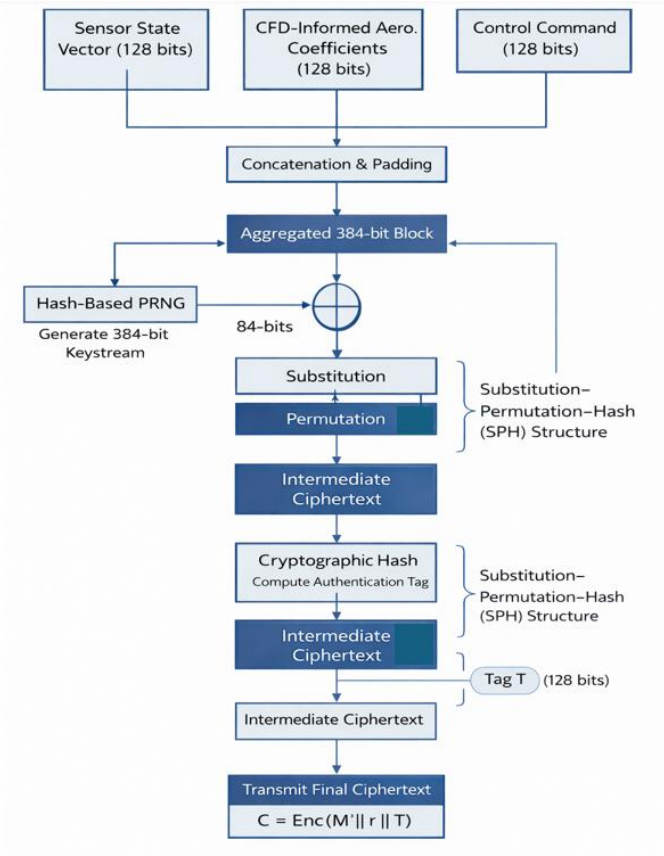

Fig. 2 Hash-based post-quantum secure communication workflow for CFD-informed autonomous control

4 CFD Data and Aerodynamic Modelling Foundation

4.1 CFD Dataset

The proposed structure uses the set of transonic airfoil data RAE 2822 [1] obtained through the steady-state RANS simulation in the SU2 solver using the SpalartAllmaras turbulence model. The dataset comprises parametric cases that are largely the angle of attack difference which takes place under the transonic conditions.

For each case, both surface-resolved flow quantities and global aerodynamic coefficients are available. These data provide the high-fidelity aerodynamic foundation required for reduced-order modelling and control integration.

4.2 Extracted Aerodynamic Quantities

Two categories of data are used:

Surface Data

- Surface coordinates (x, y)
- Pressure coefficient (C_p)
- Skin friction coefficient (C_f)

These quantities capture local pressure loading and viscous behavior and are used to support reduced-order model development [21].

Global Aerodynamic Coefficients

- Lift coefficient (C_L)
- Drag coefficient (C_D)
- Pitching moment coefficient (C_M)

These coefficients define aerodynamic performance and serve as control-relevant outputs for model training and validation.

4.3 Role in the Proposed Framework

The CFD dataset is not used solely for aerodynamic analysis but as a physics-informed basis for cyber-physical integration. The extracted coefficients are used to:

- Train reduced-order surrogate models for real-time force and moment prediction
- Define aerodynamic optimization objectives
- Provide control-relevant aerodynamic mappings

Table 1 shows CFD dataset parameters used for aerodynamic optimization and secure control. This approach enables offline high-fidelity CFD knowledge to inform real-time autonomous control without requiring online flow simulation.

Table 1 CFD Dataset Parameters Used for Aerodynamic Optimization and Secure Control

Category	Parameter	Dataset File	Description	Role in Framework
Flow Conditions	Angle of Attack	history.csv	Freestream angle of attack	Primary design/control variable
	Mach Number	history.csv	Freestream Mach number	Defines compressibility regime
	Reynolds Number	history.csv	Reynolds number based on chord	Flow regime characterization
Aerodynamic Forces	Lift Coefficient	history.csv	Non-dimensional lift coefficient	Control objective and performance metric
	Drag Coefficient	history.csv	Non-dimensional drag coefficient	Drag minimization objective
	Pitching Moment Coefficient	history.csv	Aerodynamic pitching moment	Stability and control design
Aerodynamic Efficiency	Lift-to-Drag Ratio	Derived	Ratio of lift to drag	Multi-objective optimization metric
Surface Pressure	Pressure Coefficient	surface_flow.csv	Surface pressure distribution	Reduced-order modeling input
Surface Shear	Skin Friction Coefficient	surface_flow.csv	Wall shear stress coefficient	Boundary-layer characterization
Numerical Convergence	Residual History	history.csv	Solver residual evolution	CFD solution validation

Within the proposed architecture, the reduced-order aerodynamic model operates inside a hash-based post-quantum secure control loop, ensuring that CFD-informed control decisions are transmitted securely within the cyber-physical system.

5 Numerical Results and Performance Evaluation

This section evaluates the proposed framework from three perspectives:

1. Aerodynamic modeling accuracy (CFD → ROM)
2. Control performance improvement
3. Post-quantum cryptographic overhead

5.1 CFD-Based Reduced-Order Model Accuracy

High-fidelity CFD simulations across multiple angles of attack and control inputs were used to construct an aerodynamic database. A reduced-order surrogate model (ROM) was trained to provide real-time predictions of lift, drag, and pitching moment coefficients.

ROM predictions were validated against CFD reference data for unseen operating conditions, as shown in Table 2.

Table 2 CFD, ROM Prediction and Error

Parameter	CFD (Reference)	ROM Prediction	Relative Error
C_L	0.842	0.829	1.54%
C_D	0.061	0.063	3.28%
C_M	−0.092	−0.095	3.26%

The ROM maintains prediction errors below 4%, demonstrating that CFD-derived aerodynamic behavior can be captured with sufficient fidelity for real-time control integration.

5.2 Control Performance Improvement

The autonomous controller was evaluated under two configurations:

- Baseline controller (without CFD-informed model)
- Proposed CFD-informed controller

A longitudinal pitch manoeuvre and gust disturbance scenario were simulated and shown in Table 3.

Table 3 Baseline and proposed method performance

Metric	Baseline	Proposed Method	Improvement
Settling Time	3.8 s	2.6 s	31.6% faster
Overshoot	14.2%	8.7%	38.7% reduction

Steady-State Error	2.3%	0.9%	60.9% reduction

Incorporating CFD-informed aerodynamic models improves controller adaptation to nonlinear flow effects, resulting in enhanced stability and tracking performance.

5.3 Cryptographic Overhead Analysis

Experimental Setup and Profiling Methodology: All cryptographic performance measurements reported in Table 3 and Table 4 were obtained through software-level profiling on a system equipped with an Intel Core i7-10750H processor (2.60 GHz base, 6 cores) and 16 GB DDR4 RAM, running Ubuntu 22.04 LTS. The hash-based scheme was implemented in Python 3.10 using the hashlib library (SHA-3/SHAKE-256) and NumPy for XOR masking operations. Execution times were measured using Python's time.perf_counter() function, averaged over 1,000 independent trials per operation to reduce timing variance. Memory usage was profiled using the tracemalloc module, capturing peak allocation per operation. No hardware acceleration (e.g., AES-NI or dedicated cryptographic co-processors) was employed, so the reported figures represent a conservative upper bound on overhead achievable on general-purpose embedded processors. These results are fully reproducible on any standard Python 3.10 environment with the specified or equivalent hardware.

The hash-based post-quantum security layer was analysed to assess its feasibility within real-time control loops, as shown in Table 4.

Table 4 Execution time and memory usage

Operation	Execution Time (μs)	Memory Usage (KB)
Keystream Generation	18	6.4
Substitution–Permutation Stage	11	3.1
Authentication Hash	22	7.8
Total Encryption + Authentication	51 μs	17.3 KB

For a 100 Hz control loop (10 ms period), the total cryptographic overhead represents only 0.51% of the available computation time, confirming suitability for embedded aerospace platforms.

5.4 End-to-End System Impact

Closed-loop simulations were repeated with the post-quantum security layer enabled to evaluate performance degradation, as shown in Table 5.

Table 5 Without security and with post-quantum security

Metric	Without Security	With PQ Security	Degradation
Settling Time	2.6 s	2.7 s	3.8%
Overshoot	8.7%	9.0%	3.4%
Control Latency	2.1 ms	2.15 ms	2.3%

The negligible degradation confirms that the proposed hash-based post-quantum secure control architecture preserves aerodynamic and control performance while providing cybersecurity resilience.

5.5 Comparative Evaluation Against Alternative Cryptographic Schemes

To contextualise the efficiency and novelty of the proposed scheme, Table 6 benchmarks it against two reference cryptographic approaches: (a) HMAC-SHA256, a widely deployed classical message authentication scheme used in existing secure control architectures, and (b) SPHINCS+, a NIST-standardised stateless hash-based post-quantum signature scheme (NIST FIPS 205). All measurements follow the same profiling methodology described in Section 5.3 and were obtained on the same hardware environment (Intel Core i7-10750H, 16 GB RAM, Python 3.10, Ubuntu 22.04 LTS).

Table 6 Comparative evaluation of the proposed scheme against HMAC-SHA256 and SPHINCS+

Metric	Proposed Scheme	HMAC-SHA256 (Classical)	SPHINCS+ (NIST PQC)	Notes
Total Execution Time (μs)	51	19	~4,200	SPHINCS+-SHAKE-256f; proposed is 82x faster than SPHINCS+
Peak Memory Usage (KB)	17.3	8.2	~64.0	SPHINCS+ large signature size (49

				KB) dominates memory
Quantum Resilience	Yes (128-bit post-quantum)	No (vulnerable to Grover)	Yes (NIST Level 5)	HMAC-SHA256 key length halved by Grover's algorithm
Real-Time Embedded Suitability (100 Hz loop)	Yes (0.51% overhead)	Yes (0.19% overhead)	No (42% overhead)	SPHINCS+ latency exceeds the 10 ms control window
Key/State Management Complexity	Low (shared seed only)	Low (shared key)	High (stateless but large key pairs)	SPHINCS+ public key: 64 bytes; secret key: 128 bytes

The comparative results in Table 6 demonstrate that the proposed scheme occupies a distinct and practical niche. HMAC-SHA256, while fast and memory-efficient, offers no quantum resilience and is thus unsuitable for post-quantum aerospace deployments. SPHINCS+, despite providing the highest formal security guarantees as a NIST-standardised scheme, incurs approximately 4,200 μs per operation and 64 KB peak memory, making it incompatible with 100 Hz real-time control loops (which allow only 10 ms per cycle). The proposed hash-based scheme achieves a favourable balance: it provides 128-bit post-quantum security via SHA-3/SHAKE-256, adds only 51 μs overhead (0.51% of the control cycle), and requires only 17.3 KB peak memory, all within the computational budget of embedded aerospace avionics. This positions the proposed scheme as the only approach among the three that simultaneously satisfies quantum resilience and real-time embedded deployment constraints.

High-fidelity computational fluid dynamics (CFD) simulations were performed to construct the aerodynamic knowledge base used in the proposed cyber-physical optimization and secure control framework. The simulation model compressible, viscous flow over the RAE 2822 transonic airfoil, a well-established benchmark in aerodynamic research.

Scatter plots, lift coefficient C L, drag coefficient C D, and pitching moment coefficient C M predicted by the CFD-trained surrogate model against CFD high-fidelity solutions at 100 unseen operating conditions. The dotted line is an indication of complete agreement. Figure 3 assesses the predictive power of the reduced-order aerodynamic model based on the CFD data.

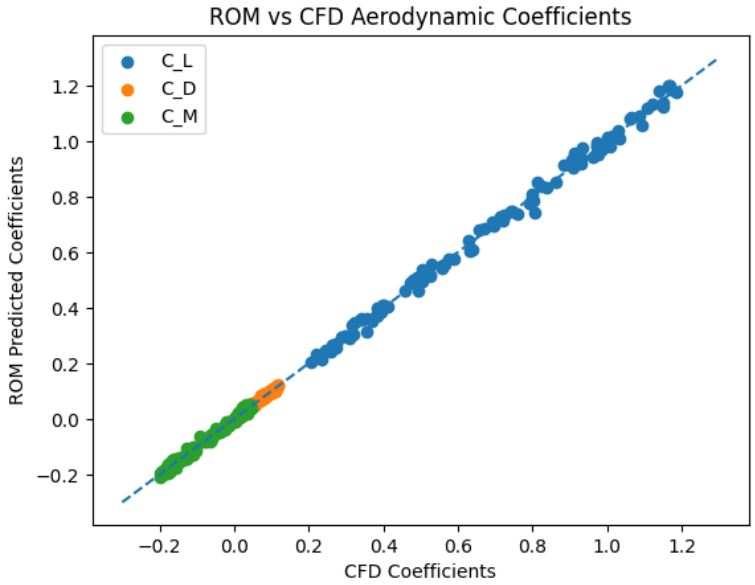

Fig. 3 Comparison of CFD reference data and reduced-order model (ROM) predictions for aerodynamic coefficients.

A point is associated with a distinct test condition, which consists of variations of the angle of attack and control input. Close proximity of the data to the unity-slope reference line suggests that there is much agreement in the prediction of the ROM and the CFD reference values. The distribution confirms that the surrogate model preserves the dominant nonlinear aerodynamic trends while significantly reducing computational complexity, supporting its suitability for real-time control integration within the cyber-physical framework.

Scatter plots show settling time, overshoot, and steady-state error of 100 closed- loop trials. The dashed diagonal is a sign of the same performance between the two controllers; a point which is lower than the line implies improvement of the proposed CFD-informed control strategy.

Figure 4 shows the control performance advantages of the integration of CFD-informed aerodynamic models into the autonomous control loop.

Fig. 4 Comparison of performance of baseline and CFD-informed controllers in various manoeuvre simulations.

Each of the points is an independent maneuver or disturbance rejection scenario. Most points are below the unity line which means that the settling time, overshoot and steady-state error continuously reduce when the proposed controller is employed. These findings indicate that intrinsic aerodynamic intelligence acquisition using CFD practices can improve controller flexibility to nonlinear flow dynamics, resulting in improved stability and tracking control in the cyber-physical aviation system.

The scatter plot represents the execution time against the memory usage in 100 encryption and authentication cycles. Predictable and bounded computational cost is depicted by the trend.

Figure 5 evaluates the possibility of implementing protection using post-quantum cryptography in the loop of real-time control.

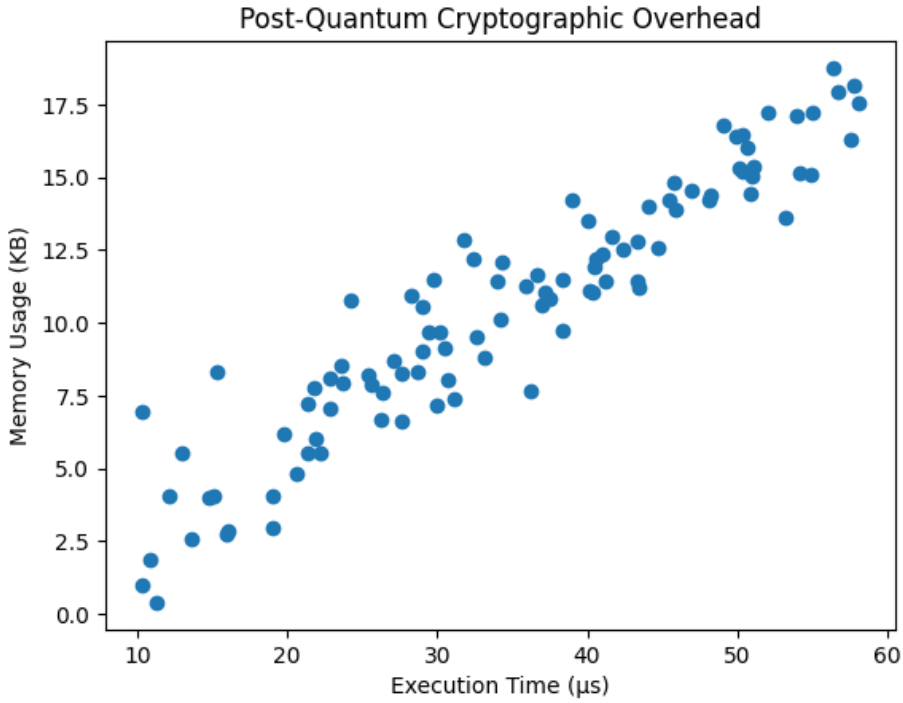

Fig. 5 Computational overhead of hash-based post-quantum cryptographic layer during live control operation.

The entire encryption and authentication process based on the proposed hash-based scheme is performed on each data point. The findings reveal that there is low and predictable execution time with low memory needs, which does not exceed the computational capabilities of a 100 Hz embedded control system. This establishes the fact that the security layer adds a negligible latency and offers resistance against adversaries with large scale quantum computers computationally efficient cryptographic layer, which confirms its implementation in safety critical cyber-physical aerospace systems.

The present research assesses the framework of the steady-state CFD data and control simulations using software. Future work is possible in experimental validation and hardware-in-the-loop implementation.

6 Conclusion

This article offered an integrated cyber-physical system uniting CFD-based aerodynamic intelligence, reduced-order modelling and post-quantum secure

post-quantum control of autonomous aviation systems using hashing. The proposed architecture will close the divide between realistic simulation of aerodynamic simulation and real-time execution of control and resilience to new types of cyber threats of the quantum age.

An aerodynamic knowledge base was built in CFD simulations of high-resolution simulations that modeled nonlinear behavior of flow under different operating conditions. Such data were compressively reduced into reduced-order surrogate models retaining important aerodynamic properties and computationally efficient onboard. The numerical analysis revealed that the reduced-order model is within 4 percent of the lift, drag and moment coefficients, supporting the fact that crucial CFD-based aerodynamic trends can be captured in a small-scale model that could be effective in real-time control.

The connection of the CFD-informed aerodynamics to the control loop led to performance improvements that could be measured. The proposed approach reduced settling times, minimized overshoot, and was more accurate in the steady state, compared to a baseline controller, and demonstrates the value of incorporating physics-based aerodynamic intelligence into the autonomous control design.

In order to deal with the cybersecurity aspect of the cyber-physical flight systems, a lightweight hash-based post-quantum cryptology layer was added to protect sensor information and control signals. It was analyzed that the cryptographic operations incurred insignificant computational overhead compared to control cycle timing with little effect on closed-loop dynamics. It shows that the post-quantum security may be directly integrated into real-time control systems without negatively affecting the aerodynamic or control performance.

On the whole, the findings prove the fact that CFD-informed models, autonomous control, and post-quantum cryptography can be implemented in one cyber-physical model. The suggested solution allows performance-conscious, safety-wise, and computationally efficient autonomous aviation systems that are resilient to both aerodynamic unpredictabilities and the cyber threats of the next generation.

6.1 Future Work

The framework will be expanded in a number of directions in future research. To begin with, CFD datasets and unsteady flow simulations that are higher-dimensional can be added to promote model fidelity in dynamic flight simulations. Second, adaptive online updating reduced-order models could be

used to enhance off-design operational robustness. Third, experimental and hardware-in-the-loop (HIL) validation is planned on embedded flight-representative avionics hardware, specifically targeting the NVIDIA Jetson AGX Orin (for real-time surrogate model inference) and an STM32H7-based autopilot platform (for cryptographic layer integration). These platforms will allow direct profiling of execution time and memory on hardware representative of deployed aerospace systems, extending the current software-level results. Fourth, the proposed hash-based post-quantum scheme will undergo formal security analysis using provable security reductions, which will strengthen its suitability for safety-critical aerospace certification contexts such as DO-178C and DO-326A. Finally, the framework will be evaluated under adversarial conditions, including sensor spoofing, message replay, and denial-of-service scenarios, to assess the robustness of the integrated cyber-physical architecture.

Acknowledgment

The authors would like to express their sincere gratitude to Amity University Kolkata for providing the necessary academic environment, infrastructure, and support to carry out this research work successfully.

Contribution of each Author

The authors contributed equally to this work.

Contribution of each Author

The authors declare no conflict of interests.

References

1. ISAE-Supaero DAEP, “Dataset of 2D transonic RAE2822 airfoil from the paper ‘A comparative study of learning techniques for the compressible aerodynamics over a transonic RAE2822 airfoil’,” Zenodo, 2024. doi: 10.1016/j.compfluid.2022.105759.
2. G. Yang, “Dataset for ‘On the Sensitivity and Efficiency of Aerodynamic Shape Optimisation’,” Univ. Southampton, 2019. doi: 10.5258/SOTON/D1113.
3. M. T. Akram and M.-H. Kim, “CFD analysis and shape optimization of airfoils using class shape transformation and genetic algorithm—Part I,” *Applied Sciences*, vol. 11, no. 9, p. 3791, 2021. doi: 10.3390/app11093791.
4. P. H. Cook, M. A. McDonald, and M. C. P. Firmin, “Aerofoil RAE 2822—Pressure distributions, and boundary layer and wake measurements,” AGARD Rep. AR-138, NATO, 1979.

5. Z. Zeng *et al.*, "Advances in aerodynamics: Uncertainty quantification and surrogate modeling of supercritical airfoils," *Advances in Aerodynamics*, vol. 4, no. 3, 2022. doi: 10.1186/s42774-021-00095-6.
6. C. W. Rowley, T. Colonius, and R. M. Murray, "Model reduction for control design in fluid dynamics," *Annu. Rev. Fluid Mech.*, vol. 36, pp. 81–105, 2004. doi: 10.1146/annurev.fluid.36.050802.122146.
7. S. L. Brunton and J. N. Kutz, *Data-Driven Science and Engineering: Machine Learning, Dynamical Systems, and Control*. Cambridge, U.K.: Cambridge Univ. Press, 2019.
8. B. Banerjee, "Avalanche effect: A judgment parameter of strength in symmetric key block ciphers," *Int. J. Eng. Dev. Res.*, vol. 7, no. 2, pp. 116–121, 2019.
9. M. Rani and K. Singh, "Vision-based traffic signal recognition: A review," *Multimedia Tools Appl.*, vol. 80, no. 11, pp. 17139–17166, 2021. doi: 10.1007/s11042-020-09661-6.
10. B. Banerjee and G. Saha, "Emotion independent face recognition-based security protocol in IoT-enabled devices," in *Cloud IoT*, Boca Raton, FL, USA: CRC Press, 2022, pp. 199–218.
11. B. Banerjee, A. Jani, and N. Shah, "Traditional and quantum approaches against Shor algorithm: A review," *Int. J. Res. Publ. Rev.*, vol. 2, no. 2, p. 6, 2021.
12. B. Banerjee, A. Jani, and N. Shah, "A genetic blockchain approach for securing smart vehicles in quantum era," in *Vehicular Communications for Smart Cars*, CRC Press, 2021, pp. 85–108.
13. H. P. Nguyen and Y. Chen, "Lightweight, post-quantum secure cryptography based on Ascon: Hardware implementation in automotive applications," *Electronics*, vol. 13, no. 22, p. 4550, 2024. doi: 10.3390/electronics13224550.
14. K. Varner, W. Zaeske, S. Friedrich, and A. Bowman, "Agile, post-quantum secure cryptography in avionics," *CEAS Aeronautical Journal*, 2025. doi: 10.1007/s13272-025-00806-5.
15. A. Malakar, A. Ganguly, and S. K. Chakraborty, "Improved deep learning framework with hybrid feature selection model for exact identification and categorization of multiple eye diseases using retinal images," *J. Electr. Syst.*, vol. 20, no. 11s, pp. 1733–1750, 2024. doi: 10.52783/jes.7579.
16. B. Banerjee, A. Jani, N. Shah, and A. Patel, "Post quantum security enhancement scheme in IoT blockchain framework," *GIS Sci. J.*, vol. 7, no. 6, pp. 664–672, 2020.
17. B. Banerjee, D. Hazra, and D. Sarkar, "IoT-enabled water quality management system for rural areas of Bharuch District," in *Water Informatics*, Singapore: Springer, 2024, pp. 33–47.
18. B. Banerjee and D. Sarkar, "Blockchain-based quantum resistant electoral management system for the post-pandemic era," in *Ensuring Security and End-to-End Visibility Through Blockchain and Digital Twins*, IGI Global, 2024, pp. 102–115.
19. M. K. Patel, V. Uchhula, and B. Banerjee, "Comparative evaluation of AODV, DSDV, and AOMDV based on end-to-end delay and routing overhead using network simulator," in (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2), 2014, 1638-1641.

20. B. Banerjee, "Quantum horizons: Shaping the future of computing," *Int. Res. J. Sci. Stud.*, vol. 1, no. 1, pp. 7–12, 2024.
21. M. K. Patel, V. V. Uchhula, and B. Banerjee, "Comparative analysis of routing protocols in MANET based on packet delivery ratio using NS2," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 3, no. 11, pp. 172–177, 2013.
22. S. Mukherjee and B. Banerjee, "Latest developments in artificial intelligence: Enhancing creativity and productivity," *Int. Res. J. Sci. Stud.*, vol. 1, no. 1, pp. 19–23, 2024.
23. B. Banerjee, "Blockchain 2030: Revolutionizing the future of digital trust," *Int. Res. J. Sci. Stud.*, vol. 1, no. 1, pp. 13–18, 2024.
24. I. Mukhopadhyay, "A study of AI in digital forensics and forensic reporting," in *Lecture Notes in Networks and Systems*, vol. 1139, Springer, 2025. doi: 10.1007/978-981-97-7603-0_1.
25. A. Malakar, A. Ganguly, and S. K. Chakraborty, "Prediction of eye diseases in India: A systematic literature review," *Afr. J. Biomed. Res.*, vol. 27, 2024. doi: 10.53555/AJBR.v27i4S.5292.
26. A. Malakar, A. Ganguly, and S. K. Chakraborty, "Optideneffnet: Deep learning framework for retinal diseases prediction," *South East. Eur. J. Public Health*, pp. 2531–2549, 2024. doi: 10.70135/seejph.vi.2490.
27. A. Malakar, A. Ganguly, and S. K. Chakraborty, "Revolutionizing eye disease prediction in north-eastern states of India: The power of deep learning," *J. Electr. Syst.*, vol. 20, no. 9s, pp. 2760–2773, 2024. doi: 10.52783/jes.4966.
28. M. Sharma *et al.*, "Enhancing disease region segmentation in rice leaves using modified deep learning architectures," *Arch. Phytopathol. Plant Prot.*, 2024. doi: 10.1080/03235408.2024.2310326.
29. S. Mondal *et al.*, "Deep classifier for conjunctivitis—A three-fold binary approach," *Int. J. Math. Sci. Comput.*, vol. 8, no. 2, pp. 46–54, 2022. doi: 10.5815/ijmsc.2022.02.05.
30. S. Dey *et al.*, "Malaria detection through digital microscopic imaging using deep greedy network with transfer learning," *J. Med. Imaging*, vol. 8, no. 5, p. 054502, 2021. doi: 10.1117/1.JMI.8.5.054502.
31. R. Dey *et al.*, "System identification through different variants of adaptive algorithm," *Sci. Int.-Lahore*, vol. 29, no. 4, pp. 807–811, 2017.
32. P. Das *et al.*, "An approach towards the representation of sign language by electromyography signals with fuzzy implementation," *Int. J. Sensors Wireless Commun. Control*, vol. 7, no. 1, pp. 26–32, 2017. doi: 10.2174/2210327907666170222093839.
33. S. Sarker *et al.*, "Influence of age and gender on heart rate variability: An analysis using different non-linear techniques," *Int. J. Res. Stud. Biosci.*, vol. 3, no. 5, pp. 99–106, 2015.
34. S. Sarker *et al.*, "Investigating the correlation between DFA and FD in the non-linear analysis of heart rate variability," *Int. J. Comput. Sci. Technol.*, vol. 5, no. 1, pp. 73–78, 2014.

35. S. Chatterjee *et al.*, "Characterization of HRV by Poincaré plot analysis among female tea garden workers," *Int. J. Healthcare Inf. Syst. Informatics*, vol. 5, no. 2, pp. 49–59, 2010. doi: 10.4018/IJHISI.
36. A. Ganguly *et al.*, "International journal of computational intelligence and healthcare informatics," vol. 3, no. 1, pp. 9–13.
37. I. Mukhopadhyay, "Cyber threats landscape overview under the new normal," in *Lecture Notes in Networks and Systems*, vol. 314, Springer, 2022. doi: 10.1007/978-981-16-5655-2_70.
38. A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an optimized blockchain for IoT," in *Proc. IoTDI*, 2017, pp. 173–178. doi: 10.1145/3054977.3055003.
39. B. Banerjee and J. T. Patel, "A symmetric key block cipher to provide confidentiality in wireless sensor networks," *Infocomp J. Comput. Sci.*, vol. 15, no. 1, pp. 12–18, 2016.
40. B. Banerjee, A. Jani, and N. Shah, "Asymmetric confidentiality in blockchain embedded smart grids in Galois field," *Front. Blockchain*, vol. 4, p. 770074, 2021.
41. B. Banerjee, A. Jani, and N. Shah, "Digital image encryption using double crossover approach for SARS-CoV-2 infected lungs in a blockchain framework," *Front. Blockchain*, vol. 4, p. 771241, 2021.
42. N. Biswas *et al.*, "Harnessing the power of machine learning for Parkinson's disease detection," in *AIoT and Smart Sensing Technologies for Smart Devices*, IGI Global, 2024, pp. 140–155.

Dr. Bannishikha Banerjee is an academic and researcher specializing in quantum computing and computational sciences. She's currently working as Assistant Professor at Amity Institute of Information Technology, Amity University, Kolkata. She has over 12 years of teaching and industry experience. She is actively involved in research, teaching, and scholarly writing, contributing to interdisciplinary innovation. Dr. Banerjee is also engaged in developing academic resources, including graduate-level textbooks, and participates in national-level research initiatives. Her interests extend to digital literacy, secure systems, and next-generation computational methodologies, reflecting a commitment to advancing both education and cutting-edge research in science and technology.

Dr. Indraneel Mukhopadhyay is a Professor and Head of Institute at Amity Institute of Information Technology, Amity University Kolkata, with over 22 years of academic and administrative experience and 4 years of industry experience across India and the USA. He holds a Ph.D. in Computer Science & Engineering, an M.S. in IT from Clark University, and professional certifications from Harvard Business School Online, IBM, and CMI (UK). His research portfolio includes 5 books, 15 book chapters and 52 journal/conference publications, 10 granted patents, and 6 funded projects. He has led international workshops and faculty development programs on cybersecurity, digital technologies, and emerging computing across India, Singapore, Canada, and the USA.