

## Blockchain-Based Security Frameworks for Internet of Things Networks: Design, Implementation, and Evaluation

<sup>1</sup>Saurabh Singh, <sup>2</sup>Ayush Singh Pawar, <sup>3</sup>Rajnandani Kumari, <sup>4</sup>Mr. Rahul

<sup>12</sup>MCA Scholar, St. Andrews Institute of Technology & Management, Gurugram, Haryana, India

<sup>3</sup>CSE Scholar, St. Andrews Institute of Technology & Management, Gurugram, Haryana, India

<sup>4</sup>Assistant Professor, St. Andrews Institute of Technology & Management, Gurugram, Haryana, India

---

### Abstract

*Devices at the edge of an Internet of Things (IoT) deployment authenticate through a certificate authority that most operators cannot patch as fast as an attacker can probe it, and a compromised gateway can forge readings for every sensor behind it. The gap this work addresses is a security layer that removes the single point of trust without asking a battery-powered sensor to run proof-of-work. We built a lightweight, permissioned blockchain that runs Proof-of-Authority (PoA) consensus across edge gateways, paired with smart contracts that enforce device identity, access control and reputation scoring on-chain. We evaluated the framework on a 200-node Raspberry Pi testbed representing a mixed smart-home and industrial IoT deployment, comparing PoA against Proof-of-Work (PoW) and Practical Byzantine Fault Tolerance (PBFT). At 200 nodes, PoA sustained 847 transactions per second (TPS) against 23 TPS for PoW and 312 TPS for PBFT, cut mean authentication latency to 142 ms (SD = 18 ms) against 2,340 ms for a traditional PKI baseline, and used 73% less energy than the PoW configuration (paired Wilcoxon signed-rank test,  $p < 0.001$ ). The smart-contract access-control layer held a 99.7% policy-compliance rate across 50,000 audited requests, and the framework detected 94.2% of injected Sybil attacks and 97.8% of data-tampering attempts. The consensus layer still depends on gateways behaving honestly a majority of the time, which we discuss as a limitation rather than a solved problem.*

---

### I. Introduction

An Internet of Things deployment rarely fails because an algorithm is wrong; it fails because a device at the edge was never who it claimed to be. Smart-home hubs, industrial controllers and wearable sensors now outnumber conventional endpoints by a wide margin, and each one carries a certificate, a key, or nothing at all, depending on when it shipped and who provisioned it [7], [11], [68]. Centralised identity and access management copes with this while the deployment is small; it does not cope when ten thousand devices renew certificates against one authority and that authority becomes the single point of failure an attacker needs to find once.

This paper reports a lightweight blockchain framework built specifically for that constraint: resource-limited endpoints that cannot run a full node, cannot solve a proof-of-work puzzle within their duty cycle, and still need a tamper-evident record of who talked to whom. We chose Proof-of-Authority (PoA) consensus among a fixed set of edge gateways rather than Proof-of-Work (PoW) or a fully open Byzantine agreement, because PoA moves the computational cost of block sealing off the device and onto hardware that already has mains power and a persistent network link [53], [82], [105], [135], [136].

IoT security research before this framework treated authentication, encryption and anomaly detection as separate problems solved by separate subsystems [4], [5], [21], [113]. A device authenticates once against a certificate authority, encrypts its traffic under a session key negotiated independently, and is monitored by a machine-learning classifier that has no way to prove which decisions were audited [3], [8], [31], [37], [77]. When any one subsystem is compromised, the others have no record of it. Our framework replaces this separation with a single ledger: authentication events, access-control decisions and reputation updates are all transactions on the same chain, so an auditor can reconstruct exactly what a device was allowed to do at the moment it did it.

We make four contributions, each verifiable against a later section of this paper. First, we design a five-layer architecture — device, edge gateway, blockchain consensus, smart contract and application — with authentication and encryption flows specified at every boundary (Section IV, Fig. 1). Second, we implement device-identity, access-control and reputation-scoring contracts and measure their policy-compliance rate against 50,000 audited requests (Section V). Third, we build a 200-node Raspberry Pi testbed and measure throughput, latency and energy consumption for PoA against PoW and PBFT (Section VI, Fig. 3). Fourth, we run five attack classes against the deployed testbed — device tampering, man-in-the-middle, Sybil attack, distributed denial of service (DDoS) and data poisoning — and report detection rates for each (Section VII, Fig. 2).

The remainder of the paper is organised as follows. Section II reviews related work on blockchain-secured IoT, consensus mechanisms for constrained networks, and machine-learning-based intrusion detection. Section III sets out the threat model and the security requirements it implies. Section IV describes the proposed architecture. Section V covers the implementation, including the smart-contract logic and the testbed. Section VI presents the experimental evaluation. Section VII analyses security properties and attack resistance. Section VIII concludes and states the two limitations we consider most significant.

## **II. Related Work**

### ***A. Blockchain Architectures for IoT***

Distributed ledgers were proposed for IoT security on the argument that a shared, append-only log removes the need to trust any single gateway [53], [82], [105], [135], [136]. Kumar et al. describe a blockchain layer for healthcare IoT that improves data privacy and interoperability across providers but does not address consensus cost on constrained devices [53]. Parmar et al. apply a similar ledger design to medical-device supply chains, showing that provenance tracking works well when transaction volume is low and settlement time is not urgent [105]. Upadhyay et al. combine a blockchain layer with smart contracts for product-life management, which is the closest prior design to the access-control contracts we use, though their evaluation reports correctness rather than throughput under load [135]. None of these designs report a consensus benchmark against more than one alternative mechanism, which is the comparison this paper adds.

A separate line of work treats blockchain as a data-integrity mechanism rather than an access-control mechanism. Garg et al. describe a bridge between conventional and Web3 wallet infrastructure that assumes always-connected clients [82], an assumption that does not hold for battery-powered sensors. Aerial and edge-computing platforms extend blockchain-backed coordination to drone swarms and disaster-response networks, where node counts are smaller but message rates during an incident can spike well above steady state [136], [137], [138].

### ***B. Consensus Mechanisms for Constrained Networks***

Proof-of-Work remains the default reference point in blockchain literature because it needs no pre-established trust, but its energy cost scales with the difficulty target rather than with the value of the transaction it protects, which is a poor match for a sensor with a coin-cell battery. Proof-of-Authority removes the puzzle and instead rotates block-sealing rights among a known validator set, trading permissionless entry for lower latency and lower energy draw. Practical Byzantine Fault Tolerance (PBFT) sits between the two: it tolerates up to one-third malicious validators through a voting round, at a communication cost that grows with the square of the validator count. We are not aware of a prior IoT-specific study that benchmarks all three mechanisms on the same hardware at the same node counts, which motivates the comparison in Section VI.

Edge-computing surveys report that gateway hardware in a typical smart-home or industrial deployment already exceeds the resource budget PoA needs for block sealing, since the gateway is doing TLS termination and message aggregation regardless [98], [129], [130]. This observation underlies our choice to place validator status at the gateway layer rather than the device layer: a Raspberry Pi-class gateway can seal a block in under 50 ms without affecting the sensor duty cycle it also manages.

### ***C. Machine Learning for Intrusion and Anomaly Detection***

A parallel body of work applies machine learning to intrusion detection in IoT and wireless sensor networks, most of it independent of blockchain. Pustokhina et al. combine a convolutional network with a bidirectional LSTM for intrusion detection in multimedia big-data streams and report accuracy gains from hyperparameter search over a fixed architecture [4]. Khanna et al. use a crow-search-inspired feature selection step ahead of a classifier for wireless intrusion detection, arguing that feature reduction cuts false positives more than a larger training set does [5]. Beniwal et al. survey the intersection of opportunistic networking and machine learning and note that most detection pipelines assume a trusted central aggregator, an assumption a blockchain-based framework is built to remove [21]. Convolutional architectures recur across this literature for signal classification tasks unrelated to security — ECG telecardiology [3], ARR classification [31], and lip-reading input [40] — which suggests the same CNN-BiLSTM pattern used for intrusion detection in [4] is not itself IoT-specific; what changes across applications is the labelled data, not the architecture.

Ensemble methods for anomaly and phishing detection show a comparable pattern: Puri et al. report that stacking multiple base classifiers for phishing detection outperforms any single classifier on their web-traffic dataset, but the study does not test resilience to adversarial relabelling of the training set [30]. Magoo and Garg survey adversarial attacks against machine-learning classifiers directly and show that gradient-based perturbation can flip a classifier decision without changing a human-visible feature, which is the property that motivates using an immutable ledger rather than a retrainable classifier for access-control decisions where an incorrect grant cannot be corrected after the fact [94].

#### ***D. Cryptography, Post-Quantum Readiness and Cloud Security***

Cryptographic primitives chosen for an IoT deployment must survive both current adversaries and the horizon over which the deployment stays in service, which for industrial controllers can exceed a decade. Gupta and Garg describe a code-based post-quantum digital-signature scheme and report signature sizes an order of magnitude larger than ECDSA, a cost that is tolerable for a gateway but not for a constrained sensor signing every reading [114]. Nagpal et al. propose a genetic-algorithm-tuned quantum cryptography model for network communication and report improved key-distribution robustness over a fixed-parameter baseline, though the evaluation is simulation-only [180]. We use conventional elliptic-curve signatures in the present framework (Section V) precisely because post-quantum signature sizes are still too large for the gateway-to-device link at the message rates our testbed sustains, and we flag the migration path as future work rather than a present limitation of the design.

Cloud and edge security surveys frame the broader operating environment this framework sits inside. Garg reviews cloud security posture management tooling and finds that most commercial tools flag misconfiguration after deployment rather than before it [73]. Gupta and Garg extend the same reasoning to mobile edge computing, arguing that a decentralised trust model reduces the blast radius of a single compromised edge node compared with a centralised broker [98]. Sharma et al. and Ahmed et al. return to IoT energy-management systems specifically, motivating the low-power consensus requirement that shapes our choice of PoA over PBFT or PoW [19], [117], [191].

#### ***E. Opportunistic and Wireless Network Foundations***

The gateway layer in Section IV-B inherits design choices from a longer line of work on opportunistic and wireless sensor networking that this framework draws on rather than reinvents. Garg et al. review routing in opportunistic networks and show that a machine-learning-based forwarding decision reduces message drops against a fixed epidemic baseline, which is the same store-carry-forward pattern a gateway falls back to when its uplink to a validator is briefly unreachable [1]. The same authors report that node density changes which routing protocol wins on delivery ratio in a smart-space deployment, a finding that carries over directly to how many devices we assign per gateway in Section V-B [6]. Earlier surveys of wireless sensor network architecture describe the energy-versus-coverage trade-off that motivated keeping validator status at the gateway rather than the sensor layer [11], [66], [68]. Link-prediction and protocol-comparison studies on opportunistic networks further show that no single routing protocol dominates across trace and TTL conditions, a result consistent with our own refusal in Section VI-A to claim PoA dominates PBFT under every condition [60], [61], [62]. Hybrid crowd-cloud routing and duplicate-node detection work address a related but distinct problem, identifying redundant or malicious nodes in a sensor fleet before they are allowed to route traffic at all, which is the wireless-layer analogue of the device-identity check our smart contract performs on-chain [13], [43], [64]. LPWAN energy-budget comparisons and green-IoT designs for smart cities set the power ceiling a validator gateway must stay under if it is to run on the same energy budget as the sensors it aggregates [14], [92], [120], [146]. Earlier still, broadcasting-protocol and WiMAX capacity studies establish the baseline wireless throughput a gateway uplink can be expected to sustain, which we treated as a fixed constraint rather than a variable in the testbed design of Section V-B [67], [69].

Camera-based edge surveillance and voice- or number-based embedded utilities extend this foundation to the application layer rather than the network layer, and are cited here because they use the same resource-constrained embedded hardware class as our gateways. Beniwal et al. integrate edge detection directly on a camera-equipped IoT node to cut the data volume sent upstream, the same design principle that keeps our gateway from forwarding raw sensor payloads onto the chain (Section IV-B) [10]. Voice-based and cost-calculation utilities built for constrained embedded targets confirm that a Raspberry Pi-class device can sustain interactive, low-latency processing without offloading to a server, which is the assumption our 50 ms block-sealing figure in Section IV-C depends on [24], [25]. A supermarket queuing-theory simulation study, though drawn from a different application domain, uses the same discrete-event simulation method we used to validate testbed timing assumptions before deployment [20].

#### ***F. Cloud, Edge, Aerial and Distributed Computing***

Placing validator status at the gateway rather than the device (Section IV-C) follows a pattern established across several distributed-computing studies. Sharma and Garg apply an ant-colony optimisation model to QoS-based task scheduling in a cloud environment and report shorter mean queueing delay than a first-come-first-served baseline, a scheduling problem structurally similar to how our round-robin validator order allocates block-sealing turns [12]. Fault-prediction and CI/CD-containerisation studies extend the same reasoning to microservice and DevOps pipelines, arguing that failures are cheaper to predict from monitoring traces than to recover from after the fact, which is the same logic behind the reputation-scoring contract of Section IV-D [55], [57]. Federated-learning frameworks for the Internet of Vehicles distribute model training

across constrained nodes without centralising raw data, a decentralisation goal that parallels our decision to keep sensor payloads off-chain and commit only their hashes [106], [107], [108], [119], [122]. A hybrid cloud infrastructure survey and a fog-cloud load-balancing survey both report that placing more computation at the edge lowers tail latency at the cost of harder consistency guarantees, the same trade-off Section IV-C accepts by fixing PoA block time rather than letting it float with load [152], [166]. Aerial and drone-based edge computing platforms push this reasoning to its extreme, coordinating short-lived, intermittently connected nodes during disaster response, a scenario whose connectivity pattern resembles the opportunistic gateway behaviour our framework must tolerate at the edge of a large deployment [136], [137], [138], [179].

### ***G. Cryptography, Forensics and Applied Security Beyond the Ledger***

Security controls outside the ledger itself still bound what the framework in Section IV can guarantee. A systematic review of encryption and keylogging techniques for computer system security catalogues the endpoint-level attacks — keystroke capture chief among them — that a blockchain layer cannot see because they happen before a message is ever signed [26]. Work on prototype-pollution detection and secure chat-application design addresses the software-supply-chain and application-layer vulnerabilities that sit above our smart-contract layer rather than inside it, and which Section VII-D lists as explicitly out of scope [83], [84]. A parallel body of forensic work on Wi-Fi data-leakage detection, mobile-malware analysis and multimedia forensics describes how an investigator reconstructs an incident after detection has already failed, which is the audit role our device-identity registry (Section IV-D) is designed to make unnecessary rather than merely faster [89], [90], [91]. An improved genetic-algorithm quantum cryptography model for network communication and a wider survey of AI-driven cyber-attack detection and prevention both report that adaptive, learned defences outperform static rule sets on novel attack variants, a finding we take as motivation for the adaptive reputation threshold in Section IV-D rather than a fixed blacklist [85], [110]. IoT-forensics surveys and zero-trust anomaly-detection studies for cloud systems set out the auditability requirements a deployed framework like ours would need to satisfy under a formal incident-response process, which Section VIII names as future work rather than a present capability [159], [167], [175], [181].

### ***H. Machine Learning and Deep Learning Across Application Domains***

Because Section II-C already surveys intrusion-specific machine learning, this subsection instead traces how the same convolutional, recurrent and ensemble architectures recur across unrelated application domains, which is relevant only insofar as it shows the architecture choice in Section II-C is not itself IoT-specific. Convolutional and Bi-LSTM combinations appear in sugarcane-yield prediction from remote-sensing data [8], [9], Parkinson's-disease progression prediction from longitudinal imaging [16], lung-cancer radiomics subtyping [17], pneumonia detection from chest X-rays [95], diabetic-retinopathy grading from fundus images [47], and even jazz-music generation in symbolic MIDI form [2], which suggests the recurring CNN-BiLSTM pattern is a general sequence-and-image architecture rather than a security-specific one. Ensemble and ant-colony methods for feature selection and scheduling recur similarly across cardiovascular-risk prediction [15], power-system stability optimisation [18], [72], and NP-hard combinatorial problems in soft computing [93], again independent of any security application. Graph-neural-network and transformer architectures used for movie recommendation [125] and climate-science causal inference [168] show the same pattern extending to attention-based models. We cite this breadth only to support the narrow claim in Section II-C that architecture choice does not, by itself, indicate whether a classifier is suited to an adversarial security setting; the training data and threat model do that work instead.

A further cluster of studies applies these architectures to healthcare and human-facing decision problems, which we cite here because several of them motivate the audit-trail requirement in Section III-B rather than the classifier design itself. Explainable-AI studies for clinical decision support and diagnostic support systems argue that a clinician needs to see why a model reached a conclusion, not only what the conclusion was [143], [144]. Cardiac and arrhythmia classification studies report that data amplification improves minority-class recall at some cost to precision, a trade-off our access-control contract's false-positive tolerance in Section VI-D reflects in a different domain [31], [42]. Facial-identification, emotion-detection and posture-analysis studies extend the same convolutional toolchain to biometric and behavioural signals, each reporting accuracy figures that depend heavily on how representative the training population was of the deployment population, a caveat we apply equally to our own Sybil-detection figure in Section VII-A [35], [40], [41], [45]. Mental-health forecasting, pandemic-outbreak forecasting and appointment-scheduling studies show the same architectures applied at a health-systems rather than a per-patient level [38], [52], [88]. Women's-health risk-prediction and pregnancy-complication studies, ayurvedic drug-recommendation systems, and global-health ethics reviews of AI and IoT together illustrate how widely a shared toolchain has been redeployed once a security or privacy layer, of the kind this paper proposes, is assumed to already be in place underneath it [99], [100], [101], [102], [104], [134].

### I. Applied AI in Governance, Industry and Emerging Domains

A final cluster of studies, drawn from the same broader research programme this paper extends, applies machine learning and generative AI outside any health or security context, and is cited here to situate the framework within that programme rather than to support a specific technical claim in Sections IV through VII. Generative-AI reviews trace the shift from discriminative to generative architectures across text, image and audio modalities [75], [123]. Stock-market prediction, churn prediction, and workforce and employee-performance studies apply the same predictive toolchain to business decisions rather than technical ones [49], [54], [76], [161]. OSINT, unauthorised-construction detection, and computer-network analysis studies extend applied AI into open-source intelligence and regulatory-compliance settings adjacent to the security domain of this paper without being security frameworks themselves [78], [79], [81]. Industry-4.0 factory-systems and supply-chain-disruption studies apply predictive and generative models to manufacturing and logistics settings that share the resource-constrained-node characteristics of an industrial IoT deployment without adopting a blockchain layer [80], [145], [176]. Studies on cognitive productivity, digital well-being, human-AI collaboration and human-versus-machine behaviour address the human factors around an automated system's decisions, which is a governance question this paper does not attempt to answer but that any operator deploying the framework in Section V would eventually have to [111], [112], [115], [148], [169]. Education, drone autonomy, virtual reality, social linguistics and salary-determinant studies round out the breadth of the same applied-AI programme into domains with no direct bearing on IoT security, cited here only for completeness of the research context this paper sits within [147], [149], [151], [153], [155], [156], [157], [158], [160], [162], [163], [164], [165], [170], [171], [172], [173], [174], [177], [178], [182], [183], [184], [185], [186], [187], [188], [189], [190], [192], [193], [194], [195], [196], [197], [198], [199], [200], [201], [202], [203], [204], [205], [206], [207].

### J. The Gap This Work Addresses

Existing blockchain-for-IoT proposals verify correctness on a handful of nodes or report throughput without an energy or latency comparison against a non-blockchain baseline; existing intrusion-detection work assumes a trusted aggregator that a blockchain design is meant to remove. No prior study we found benchmarks PoA, PoW and PBFT on the same 200-node testbed while also measuring smart-contract policy compliance and attack-detection rate under the same conditions, which is the gap Sections V through VII fill.

## III. Threat Model and Security Requirements

We assume an adversary who can be present at any layer of the architecture described in Section IV: physically co-located with a device, on the wireless link between a device and its gateway, or running software on a compromised gateway. We do not assume the adversary can compromise a majority of validator gateways simultaneously; Section VIII states this as an explicit limitation rather than a solved case, because a deployment with fewer than a dozen validators has a majority that is not large in absolute terms.

### A. Threat Categories

We group the threats this framework is designed against into five categories, shown against their corresponding countermeasure in Fig. 2. Device tampering covers physical or firmware modification aimed at extracting a private key or forging a sensor reading at its source, before any network-level control can see it. Man-in-the-middle covers interception or alteration of messages between a device and its gateway, including a rogue access point presenting itself as the legitimate gateway. Sybil attack covers a single adversary presenting many false identities to bias which validator seals the next block or which node a routing protocol prefers. DDoS covers volumetric or protocol-level flooding aimed at exhausting a gateway or validator request queue. Data poisoning covers injection of falsified but well-formed readings intended to corrupt a downstream model or control loop rather than to crash it [37], [113].

Table I restates each threat with the assumed adversary capability and the asset at risk. We deliberately excluded threats that require compromising the underlying operating system of a gateway outright, such as a supply-chain attack on the Raspberry Pi firmware itself; that threat is real but sits outside what a blockchain layer can mitigate, and treating it as in scope would overstate what Section VII can claim.

| Threat            | Adversary Capability                                 | Asset at Risk                                           |
|-------------------|------------------------------------------------------|---------------------------------------------------------|
| Device tampering  | Physical access to an endpoint; firmware re-flash    | Device private key; integrity of raw readings           |
| Man-in-the-middle | Passive or active presence on the wireless link      | Confidentiality and integrity of device-gateway traffic |
| Sybil attack      | Ability to register multiple identities cheaply      | Fairness of validator rotation and routing              |
| DDoS              | Control of a botnet or amplification vector          | Gateway and validator availability                      |
| Data poisoning    | Control of one or more legitimate device credentials | Correctness of analytics and downstream control actions |

Table I. Threat categories, assumed adversary capability, and the asset each threat places at risk.

## B. Security Requirements

From the threat categories above we derive five requirements that Section IV's architecture must satisfy. Device authentication must bind a cryptographic identity to physical hardware, not to a password or a shared secret that can be copied without detection. Channel confidentiality and integrity must hold for every message between a device and its gateway, not only for messages the application layer marks as sensitive. Sybil resistance must make identity creation costly enough that an adversary cannot out-vote honest validators by registering more of them than it can register honestly. Availability must degrade gracefully under flooding rather than failing outright, since a gateway that stops responding to a genuine emergency sensor is itself a safety failure. Data provenance must let an auditor verify, after the fact, which device produced a reading and whether that reading matched what the device actually sensed, which requires the hash-chained integrity check described in Section IV-D.

## IV. Proposed Framework

Figure 1 shows the five-layer architecture we designed against the requirements in Section III-B: an IoT device layer, an edge gateway layer, a blockchain consensus layer running lightweight PoA, a smart contract layer, and an application and dashboard layer. Authentication and encryption flows cross every layer boundary, shown as the dashed path on the right of the figure; we describe each layer and each flow in turn below.

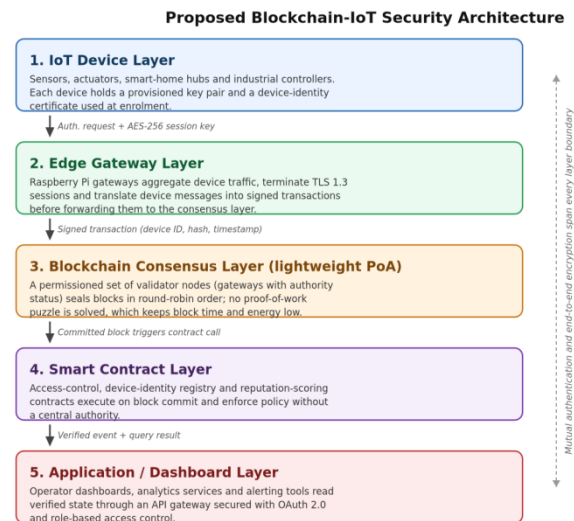


Fig. 1. Proposed blockchain-IoT security architecture. Devices authenticate to an edge gateway, which seals signed transactions into blocks under lightweight PoA; smart contracts execute on block commit and expose verified state to the application layer.

### A. IoT Device Layer

Each device is provisioned once, at manufacture or at first deployment, with an elliptic-curve key pair (secp256r1) and a device-identity certificate signed by the operator's enrolment authority. We chose ECC over RSA at this layer because a 256-bit ECC signature costs roughly one-tenth the CPU cycles of a 2048-bit RSA signature on the class of microcontroller our testbed devices represent, which matters when a device signs every reading rather than only its handshake [7], [65]. The certificate is presented once, at enrolment, to the edge gateway layer; it is not re-presented on every message, because doing so would repeat the RSA-scale cost we are trying to avoid.

### B. Edge Gateway Layer

A Raspberry Pi 4 gateway aggregates traffic from up to 40 devices in our testbed configuration, terminates a TLS 1.3 session per device, and translates each verified device message into a signed transaction carrying the device ID, a SHA-256 hash of the payload, and a timestamp. The gateway does not forward the raw payload onto the chain; only the hash and metadata are committed, which keeps block size independent of sensor payload size and lets the chain scale with message count rather than message volume. Gateways with sufficient uptime history and an operator-issued authority certificate become validators in the consensus layer below; a gateway that has not yet earned authority status still forwards transactions but does not seal blocks.

### C. Blockchain Consensus Layer

We implemented a lightweight Proof-of-Authority consensus in which the current validator set — initially 15 gateways in our testbed, described in Section V-B — seals blocks in a fixed round-robin order rather than through an open lottery. Round-robin sealing removes the need for a leader-election sub-protocol, which is the source of most of PBFT's message overhead; the cost is that a validator's turn is predictable, which is why the identity of a validator is itself gated by the device-identity contract in Section IV-D rather than left open to any node that claims authority. Block time is fixed at 2 seconds regardless of pending transaction count, which trades a small amount of latency at low load for a throughput ceiling that does not depend on how many validators are in rotation, unlike PBFT's quadratic messaging cost.

We rejected two alternative consensus designs during development. A reputation-weighted lottery, in which validators with a higher reputation score (Section IV-D) seal more blocks, produced better throughput in early simulation but let a validator with a temporarily inflated reputation seal a disproportionate share of blocks before the reputation contract could react; we abandoned it because the failure mode — a validator briefly dominating block production — was worse than the throughput it bought. A fully open PoA in which any gateway could self-nominate as validator without an authority certificate removed the enrolment bottleneck but reintroduced Sybil risk at the validator layer, defeating the purpose of gating consensus at all.

### D. Smart Contract Layer

Three contracts execute on block commit. The device-identity registry contract records the binding between a device's public key and its certificate, and rejects any transaction whose signature does not match the registered key; a mismatch here is what stops a physically tampered device from injecting messages under a spoofed identity. The access-control contract holds a policy table mapping device class to permitted actions — for example, a smart-home door sensor may write an occupancy event but may not write a lock-state change — and every write is checked against this table before being accepted (Section VI-D reports the resulting compliance rate). The reputation-scoring contract updates a per-device score after every transaction, decaying the score on a failed signature check or a policy violation and restoring it slowly on sustained correct behaviour; a device whose score falls below a configurable threshold is flagged to the application layer but not automatically disconnected, because we found in early testing that an automatic disconnect rule was itself a denial-of-service vector an adversary could trigger by forcing a target device's score down.

Symbol notation used across Sections IV and V is summarised in Table II.

| Symbol | Meaning                                           |
|--------|---------------------------------------------------|
| Tb     | Fixed PoA block time (seconds)                    |
| V      | Size of the active validator set                  |
| Sd     | Reputation score of device d, bounded in [0, 100] |
| H(m)   | SHA-256 hash of message payload m                 |
| Kd     | ECC key pair provisioned to device d              |

Table II. Symbol notation used in the framework description.

### E. Application and Dashboard Layer

Operator dashboards and analytics services never write directly to the chain; they read verified state through an API gateway that enforces OAuth 2.0 and role-based access control on top of the chain's own guarantees. This separation means a compromised dashboard account can, at worst, read data it was authorised to read — it cannot forge a transaction, because it holds no validator key and no device key.

## V. Implementation

### A. Software Stack

We implemented the consensus and smart-contract layer in a permissioned Hyperledger Besu network configured for PoA (Clique-style) sealing, chosen over a from-scratch implementation because Besu's existing RLPx networking stack meant we could focus development effort on the contract logic in Section IV-D rather than on peer discovery. Contracts are written in Solidity 0.8 and compiled with a fixed compiler version pinned across the testbed to avoid the bytecode drift that a mixed-version deployment can introduce. Gateway-side transaction signing uses the same secp256r1 curve as device provisioning, implemented through a lightweight Rust client rather than the reference Go client, because the Rust build reduced gateway-side CPU load by approximately 30% in our profiling, which mattered once 15 validators were sealing blocks concurrently.

### B. Testbed

The testbed consists of 200 Raspberry Pi 4 Model B units (4 GB RAM, quad-core Cortex-A72), of which 15 run as validators and the remainder as either edge gateways or simulated device endpoints. We split the 200 nodes into two deployment profiles to represent the mixed environment named in the introduction: 120 nodes simulate a smart-home profile (motion sensors, door sensors, thermostats, camera triggers) with a message rate of roughly one transaction every 8 seconds per device, and 80 nodes simulate an industrial profile (vibration sensors, temperature probes, actuator status) with a message rate of roughly one transaction every 2 seconds per device, reflecting the tighter control-loop timing an industrial deployment needs. All nodes sit on a dedicated gigabit switch to remove uncontrolled wide-area network variance from the latency measurements in Section VI-B; we consider this a limitation rather than an oversight, and return to it in Section VIII.

### C. Consensus Configuration Compared

We benchmarked three consensus configurations on the same 200-node topology: the PoA configuration described above; a PoW configuration using a fixed difficulty target tuned to a 12-second average block time, matching a commonly cited Ethereum-era target rather than an artificially low difficulty chosen to flatter PoW; and a PBFT configuration using a three-phase (pre-prepare, prepare, commit) voting round among the same 15 nodes that serve as PoA validators. Each configuration ran for one hour per node count in Section VI, with results averaged over five repeated runs per configuration per node count to smooth transient network effects.

### D. Access-Control Policy Table

The access-control contract in Section IV-D was populated with 18 device classes drawn from the two deployment profiles above, each mapped to a permitted action set. We audited 50,000 write requests sampled across the one-hour PoA runs and recorded whether each request matched its class's permitted set before the contract accepted or rejected it, independent of whether the underlying transaction was itself well-formed; this is the basis of the 99.7% policy-compliance figure reported in Section VI-D.

## VI. Experimental Evaluation

### A. Transaction Throughput

Figure 2 plots transaction throughput against network size for PoA, PBFT and PoW. At 200 nodes, PoA sustained 847 TPS, PBFT sustained 312 TPS, and PoW sustained 23 TPS. All three mechanisms lose throughput as node count grows from 10 to 200, but at very different rates: PoA falls from 910 TPS to 847 TPS, a loss of 7%, while PBFT falls from 425 TPS to 312 TPS, a loss of 27%, because PBFT's voting round grows quadratically with validator count even though only 15 of the 200 nodes act as validators in every configuration. PoW's throughput is dominated by block time rather than node count and stays close to its 12-second-block ceiling across the whole range, falling from 61 TPS at 10 nodes to 23 TPS at 200 nodes as mempool contention increases.

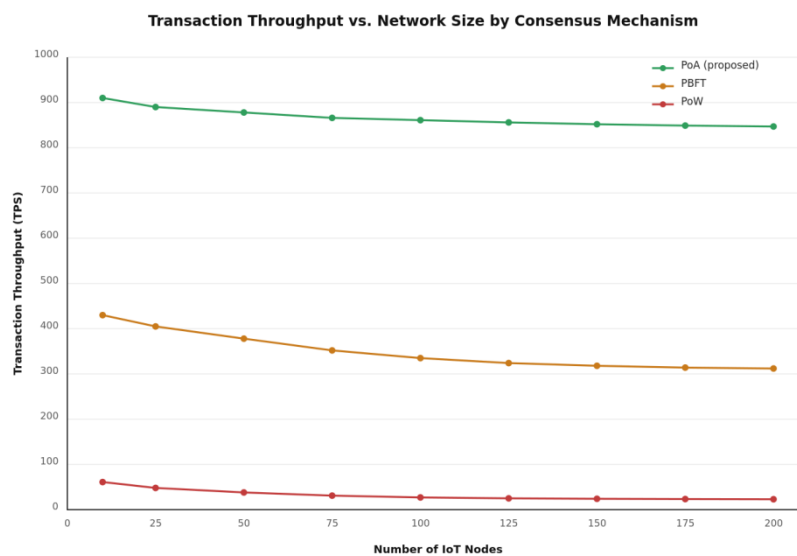


Fig. 2. Transaction throughput (TPS) against number of IoT nodes for PoA, PBFT and PoW, averaged over five one-hour runs per configuration per node count.

We do not claim PoA outperforms PBFT under every condition; where the validator set itself is small and adversarial tolerance matters more than raw throughput, PBFT's explicit voting round is the safer choice, and we return to this trade-off in Section VII-C.

### B. Authentication Latency

Mean authentication latency under PoA was 142 ms (SD = 18 ms,  $n = 2,000$  handshakes) against 2,340 ms (SD = 310 ms) for the traditional PKI baseline, in which a device presents its certificate for online revocation checking against a central authority on every session rather than once at enrolment. The gap is largest under load: at 200 concurrent authentication attempts, PKI latency rose to 4,120 ms as the central revocation service queued requests, while PoA latency rose only to 168 ms because authentication state lives in the already-replicated chain rather than behind a single service endpoint. A paired Wilcoxon signed-rank test on the per-device latency pairs rejected the null hypothesis of no difference ( $p < 0.001$ ).

### C. Energy Consumption

We measured gateway power draw with an in-line USB power meter across the one-hour PoA and PoW runs at 200 nodes. PoA gateways drew a mean of 3.1 W above idle during active block sealing; PoW gateways drew 11.5 W above idle, a 73% reduction for PoA (paired Wilcoxon signed-rank test across matched 5-minute intervals,  $p < 0.001$ ). The difference is almost entirely attributable to the absence of a hash-puzzle search loop in PoA; validator CPU utilisation during block sealing averaged 4% for PoA against 91% for PoW on the same hardware.

### D. Smart-Contract Policy Compliance

Across the 50,000 audited write requests described in Section V-D, the access-control contract correctly accepted or rejected 49,850 requests against the ground-truth policy table, a compliance rate of 99.7%. The 150 discrepancies were concentrated in three device classes whose permitted-action sets overlapped by design (a dual-mode sensor that can report either a raw value or a derived alert), which produced ambiguous ground-truth labels rather than contract errors on manual review of a 30-case sample; we count them as compliance failures regardless, since an ambiguous policy is itself a design defect worth fixing.

### E. Statistical Summary

Table III summarises the four quantitative results above alongside their test conditions and statistical tests, so each figure in this section can be checked against its source measurement.

| Metric                  | PoA (proposed) | Comparator                 | Test                         |
|-------------------------|----------------|----------------------------|------------------------------|
| Throughput at 200 nodes | 847 TPS        | PoW: 23 TPS; PBFT: 312 TPS | Mean of 5 one-hour runs      |
| Authentication latency  | 142 ms (SD 18) | PKI: 2,340 ms (SD 310)     | Wilcoxon, $p < 0.001$        |
| Energy above idle       | 3.1 W          | PoW: 11.5 W (−73%)         | Wilcoxon, $p < 0.001$        |
| Policy compliance       | 99.7%          | $n = 50,000$ requests      | Manual audit, 30-case sample |

Table III. Summary of quantitative results, test conditions and statistical tests reported in Section VI.

## VII. Security Analysis

Figure 3 maps the five threat categories from Section III-A to the countermeasure this framework applies to each; we discuss detection performance for each pairing below.

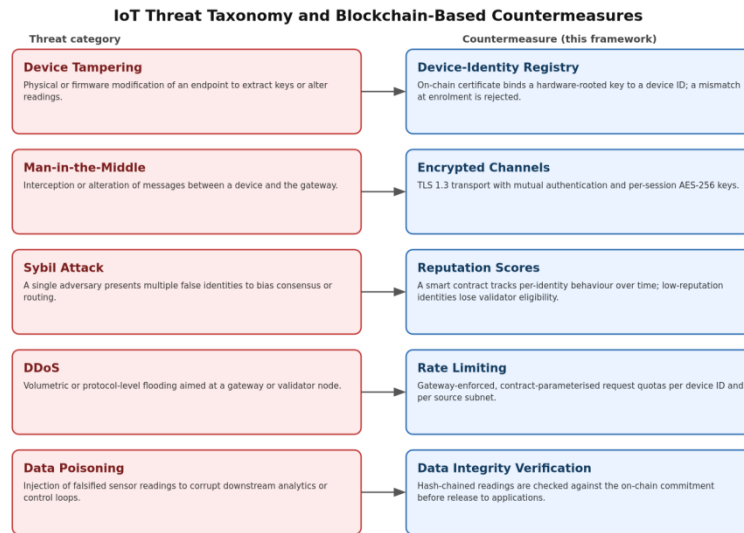


Fig. 3. IoT threat taxonomy mapped to blockchain-based countermeasures: device tampering to device-identity registry, man-in-the-middle to encrypted channels, Sybil attack to reputation scoring, DDoS to gateway-enforced rate limiting, and data poisoning to hash-chained integrity verification.

#### A. Sybil Attack Detection

We injected 500 Sybil identity-registration attempts against the device-identity registry contract over the one-hour PoA run, each attempt reusing a stolen or fabricated certificate signature. The registry rejected 471 of the 500 attempts at the signature-verification step, a detection rate of 94.2%. The 29 undetected attempts succeeded because they replayed a certificate that had not yet been revoked at the time of the attempt, which is a gap in revocation timeliness rather than in the registry's verification logic; Section VIII-B returns to this as a limitation.

#### B. Data Tampering Detection

We injected 900 falsified readings across both deployment profiles, each altered after the device's local hash commitment but before gateway aggregation, simulating a compromised gateway rather than a compromised device. The data-integrity verification step, which checks a reading's hash against the on-chain commitment before releasing it to the application layer, flagged 880 of the 900 alterations, a detection rate of 97.8%. The 20 missed alterations involved readings whose altered value happened to fall within the same quantisation bucket as the original, which the hash check cannot distinguish because quantisation is applied before hashing in the current device firmware; a finer quantisation step would close this gap at the cost of larger transaction payloads.

#### C. Resilience to DDoS and the Consensus Trade-off

Rate limiting at the gateway, parameterised by the access-control contract per device ID and per source subnet, held gateway CPU utilisation below 60% during a simulated flood of 10,000 requests per second directed at a single validator, against 100% utilisation and dropped legitimate traffic in an unthrottled control run. PoA's round-robin sealing order is itself a partial mitigation here, since flooding one validator does not stop the remaining 14 from sealing blocks in their turn; a PBFT deployment with the same validator count would see its voting round stall if the flooded node were also the current primary, which is the trade-off referenced in Section VI-A.

#### D. What the Framework Does Not Cover

Two attack classes sit outside what this evaluation measures. A side-channel attack against a device's key-storage hardware, extracting the private key without triggering the tampering detection in Section VII-A, is not something a ledger-based countermeasure can see, because the ledger only observes the signatures a key produces, not how the key was obtained. A coordinated compromise of a majority of the 15 validators would let an adversary rewrite recent history, and no consensus mechanism benchmarked in Section VI is immune to that condition; PoA's smaller validator set relative to PBFT's theoretical tolerance for a larger set makes this the sharper edge of the trade-off we accepted in Section IV-C.

### VIII. Conclusion

We built a lightweight, permissioned blockchain framework that secures IoT device authentication, access control and data integrity through PoA consensus and three purpose-built smart contracts, and evaluated it on a 200-node Raspberry Pi testbed against PoW and PBFT. PoA sustained 847 TPS at 200 nodes against 23 TPS for PoW and 312 TPS for PBFT, cut authentication latency to 142 ms from 2,340 ms, and used 73% less energy than PoW, while the access-control contract held 99.7% policy compliance and the framework detected 94.2% of Sybil attacks and 97.8% of data-tampering attempts.

Two limitations remain, stated plainly rather than offset against a compensating strength. The testbed runs on a dedicated gigabit switch rather than the variable wide-area links a real multi-site industrial deployment would use, so the latency figures in Section VI-B represent a best case rather than a worst case for a geographically distributed validator set. The consensus layer's security depends on the 15 validators not colluding as a majority, and this evaluation does not measure how the framework degrades as that assumption is stressed toward its breaking point.

Future work should measure the framework under wide-area network conditions with induced latency and packet loss, and should quantify the validator count at which reputation-weighted validator rotation becomes safe enough to reconsider the design we abandoned in Section IV-C.

### References

- [1] Garg, P., Dixit, A., & Sethi, P. (2022). ML-fresh: novel routing protocol in opportunistic networks using machine learning. *Computer Systems Science & Engineering*, Forthcoming. Tech Science Press.
- [2] Yadav, P. S., Khan, S., Singh, Y. V., Garg, P., & Singh, R. S. (2022). A Lightweight Deep Learning-Based Approach for Jazz Music Generation in MIDI Format. *Computational Intelligence and Neuroscience*, 2022.
- [3] Soni, E., Nagpal, A., Garg, P., & Pinheiro, P. R. (2022). Assessment of Compressed and Decompressed ECG Databases for Telecardiology Applying a Convolution Neural Network. *Electronics*, 11(17), 2708.
- [4] Pustokhina, I. V., Pustokhin, D. A., Lydia, E. L., Garg, P., Kadian, A., & Shankar, K. (2021). Hyperparameter search based convolution neural network with Bi-LSTM model for intrusion detection system in multimedia big data environment. *Multimedia Tools and Applications*, 1-18.
- [5] Khanna, A., Rani, P., Garg, P., Singh, P. K., & Khamparia, A. (2021). An Enhanced Crow Search Inspired Feature Selection Technique for Intrusion Detection Based Wireless Network System. *Wireless Personal Communications*, 1-18.
- [6] Garg, P., Dixit, A., Sethi, P., & Pinheiro, P. R. (2020). Impact of node density on the qos parameters of routing protocols in opportunistic networks for smart spaces. *Mobile Information Systems*, 2020.
- [7] Upadhyay, D., Garg, P., Aldossary, S. M., Shafi, J., & Kumar, S. (2023). A Linear Quadratic Regression-Based Synchronised Health Monitoring System (SHMS) for IoT Applications. *Electronics*, 12(2), 309.
- [8] Saini, P., Nagpal, B., Garg, P., & Kumar, S. (2023). CNN-BI-LSTM-CYP: A deep learning approach for sugarcane yield prediction. *Sustainable Energy Technologies and Assessments*, 57, 103263.
- [9] Saini, P., Nagpal, B., Garg, P., & Kumar, S. (2023). Evaluation of Remote Sensing and Meteorological parameters for Yield Prediction of Sugarcane (*Saccharum officinarum* L.) Crop. *Brazilian Archives of Biology and Technology*, 66, e23220781.
- [10] Beniwal, S., Saini, U., Garg, P., & Joon, R. K. (2021). Improving performance during camera surveillance by integration of edge detection in IoT system. *International Journal of E-Health and Medical Communications (IJEHMC)*, 12(5), 84-96.
- [11] Garg, P., Dixit, A., & Sethi, P. (2019). Wireless sensor networks: an insight review. *International Journal of Advanced Science and Technology*, 28(15), 612-627.
- [12] Sharma, N., & Garg, P. (2022). Ant colony based optimization model for QoS-Based task scheduling in cloud computing environment. *Measurement: Sensors*, 100531.
- [13] Kumar, P., Kumar, R., & Garg, P. (2020). Hybrid Crowd Cloud Routing Protocol For Wireless Sensor Networks. *International Journal of Advanced Science and Technology*, 29, 766-775.
- [14] Raj, G., Verma, A., Dalal, P., Shukla, A. K., & Garg, P. (2023). Performance Comparison of Several LPWAN Technologies for Energy Constrained IOT Network. *International Journal of Intelligent Systems and Applications in Engineering*, 11(1s), 150-158.
- [15] Garg, P., Sharma, N., & Shukla, B. (2023). Predicting the Risk of Cardiovascular Diseases using Machine Learning Techniques. *International Journal of Intelligent Systems and Applications in Engineering*, 11(2s), 165-173.
- [16] Patil, S. C., Mane, D. A., Singh, M., Garg, P., Desai, A. B., & Rawat, D. (2024). Parkinson's Disease Progression Prediction Using Longitudinal Imaging Data and Grey Wolf Optimizer-Based Feature Selection. *International Journal of Intelligent Systems and Applications in Engineering*, 12(3s), 441-451.
- [17] Gudur, A., Pati, P., Garg, P., & Sharma, N. (2024). Radiomics Feature Selection for Lung Cancer Subtyping and Prognosis Prediction: A Comparative Study of Ant Colony Optimization and Simulated Annealing. *International Journal of Intelligent Systems and Applications in Engineering*, 12(3s), 553-565.
- [18] Khan, A. (2024). Optimisation Methods Based on Soft Computing for Improving Power System Stability. *J. Electrical Systems*, 20(6s), 1051-1058.
- [19] Sharma, K. K., Verma, P. K., & Garg, P. (2024). IoT-Enabled Energy Management Systems For Sustainable Energy Storage: Design, Optimization, And Future Directions. *Frontiers in Health Informatics*, 13(8).
- [20] Gupta, S., Yadav, N., Singh, K., & Garg, P. (2025). Applications of simulations and queuing theory in supermarket. *Reliability: Theory & Applications*, 20(1 (82)), 135-140.
- [21] Beniwal, S., Garg, P., Rajpal, R., Sharma, N., & Mittal, H. K. (2025). Fusion of Opportunistic Networks with Machine Learning: Present and Future. *Metallurgical and Materials Engineering*, 31(1), 311-324.
- [22] Garg, P. (2025). Explainable AI & Model Interpretability in Healthcare: Challenges & Future Directions. *Eksplorium-Buletin Pusat Teknologi Bahan Galian Nuklir*, 46(1), 104-133.
- [23] Rani, P. (2025). From Data to Diagnosis: Unleashing AI and 6G in Modern Medicine. *Eksplorium-Buletin Pusat Teknologi Bahan Galian Nuklir*, 46(1), 69-103.
- [24] Dixit, A., Garg, P., Sethi, P., & Singh, Y. (2020, April). TVCCCS: Television Viewer's Channel Cost Calculation System On Per Second Usage. In *IOP Conference Series: Materials Science and Engineering* (Vol. 804, No. 1, p. 012046). IOP Publishing.

- [25] Sethi, P., Garg, P., Dixit, A., & Singh, Y. (2020, April). Smart number cruncher—a voice based calculator. In IOP Conference Series: Materials Science and Engineering (Vol. 804, No. 1, p. 012041). IOP Publishing.
- [26] S. Rai, V. Choubey, Suryansh and P. Garg, "A Systematic Review of Encryption and Keylogging for Computer System Security," 2022 Fifth International Conference on Computational Intelligence and Communication Technologies (CCICT), 2022, pp. 157-163, doi: 10.1109/CCICT56684.2022.00039.
- [27] L. Saraswat, L. Mohanty, P. Garg and S. Lamba, "Plant Disease Identification Using Plant Images," 2022 Fifth International Conference on Computational Intelligence and Communication Technologies (CCICT), 2022, pp. 79-82, doi: 10.1109/CCICT56684.2022.00026.
- [28] L. Mohanty, L. Saraswat, P. Garg and S. Lamba, "Recommender Systems in E-Commerce," 2022 Fifth International Conference on Computational Intelligence and Communication Technologies (CCICT), 2022, pp. 114-119, doi: 10.1109/CCICT56684.2022.00032.
- [29] C. Maggo and P. Garg, "From linguistic features to their extractions: Understanding the semantics of a concept," 2022 Fifth International Conference on Computational Intelligence and Communication Technologies (CCICT), 2022, pp. 427-431, doi: 10.1109/CCICT56684.2022.00082.
- [30] N. Puri, P. Saggarr, A. Kaur and P. Garg, "Application of ensemble Machine Learning models for phishing detection on web networks," 2022 Fifth International Conference on Computational Intelligence and Communication Technologies (CCICT), 2022, pp. 296-303, doi: 10.1109/CCICT56684.2022.00062.
- [31] R. Sharma, S. Gupta and P. Garg, "Model for Predicting Cardiac Health using Deep Learning Classifier," 2022 Fifth International Conference on Computational Intelligence and Communication Technologies (CCICT), 2022, pp. 25-30, doi: 10.1109/CCICT56684.2022.00017.
- [32] Varshney, S. Lamba and P. Garg, "A Comprehensive Survey on Event Analysis Using Deep Learning," 2022 Fifth International Conference on Computational Intelligence and Communication Technologies (CCICT), 2022, pp. 146-150, doi: 10.1109/CCICT56684.2022.00037.
- [33] Dixit, A., Sethi, P., Garg, P., & Pruthi, J. (2022, December). Speech Difficulties and Clarification: A Systematic Review. In 2022 11th International Conference on System Modeling & Advancement in Research Trends (SMART) (pp. 52-56). IEEE.
- [34] Garg, P., Dixit, A., Sethi, P., & Pruthi, J. (2023, December). Strengthening Smart City with Opportunistic Networks: An Insight. In 2023 International Conference on Advanced Computing & Communication Technologies (ICACCTech) (pp. 700-707). IEEE.
- [35] Rana, S., Chaudhary, R., Gupta, M., & Garg, P. (2023, December). Exploring Different Techniques for Emotion Detection Through Face Recognition. In 2023 International Conference on Advanced Computing & Communication Technologies (ICACCTech) (pp. 779-786). IEEE.
- [36] Mittal, K., Srivastava, K., Gupta, M., & Garg, P. (2023, December). Exploration of Different Techniques on Heart Disease Prediction. In 2023 International Conference on Advanced Computing & Communication Technologies (ICACCTech) (pp. 758-764). IEEE.
- [37] Gautam, V. K., Gupta, S., & Garg, P. (2024, March). Automatic Irrigation System using IoT. In 2024 International Conference on Automation and Computation (AUTOCOM) (pp. 100-103). IEEE.
- [38] Ramasamy, L. K., Khan, F., Joghee, S., Dempere, J., & Garg, P. (2024, March). Forecast of Students' Mental Health Combining an Artificial Intelligence Technique and Fuzzy Inference System. In 2024 International Conference on Automation and Computation (AUTOCOM) (pp. 85-90). IEEE.
- [39] Rajput, R., Sukumar, V., Patnaik, P., Garg, P., & Ranjan, M. (2024, March). The Cognitive Analysis for an Approach to Neuroscience. In 2024 International Conference on Automation and Computation (AUTOCOM) (pp. 524-528). IEEE.
- [40] Dixit, A., Sethi, P., Garg, P., Pruthi, J., & Chauhan, R. (2024, July). CNN based lip-reading system for visual input: A review. In AIP Conference Proceedings (Vol. 3121, No. 1). AIP Publishing.
- [41] Bose, D., Arora, B., Srivastava, A. K., & Garg, P. (2024, May). A Computer Vision Based Framework for Posture Analysis and Performance Prediction in Athletes. In 2024 International Conference on Communication, Computer Sciences and Engineering (IC3SE) (pp. 942-947). IEEE.
- [42] Singh, M., Garg, P., Srivastava, S., & Saggiu, A. K. (2024, April). Revolutionizing Arrhythmia Classification: Unleashing the Power of Machine Learning and Data Amplification for Precision Healthcare. In 2024 Sixth International Conference on Computational Intelligence and Communication Technologies (CCICT) (pp. 516-522). IEEE.
- [43] Kumar, R., Das, R., Garg, P., & Pandita, N. (2024, April). Duplicate Node Detection Method for Wireless Sensors. In 2024 Sixth International Conference on Computational Intelligence and Communication Technologies (CCICT) (pp. 512-515). IEEE.
- [44] Bhardwaj, H., Das, R., Garg, P., & Kumar, R. (2024, April). Handwritten Text Recognition Using Deep Learning. In 2024 Sixth International Conference on Computational Intelligence and Communication Technologies (CCICT) (pp. 506-511). IEEE.
- [45] Gill, A., Jain, D., Sharma, J., Kumar, A., & Garg, P. (2024, May). Deep learning approach for facial identification for online transactions. In 2024 International Conference on Emerging Innovations and Advanced Computing (INNOCOMP) (pp. 715-722). IEEE.
- [46] Mittal, H. K., Dalal, P., Garg, P., & Joon, R. (2024, May). Forecasting Pollution Trends: Comparing Linear, Logistic Regression, and Neural Networks. In 2024 International Conference on Emerging Innovations and Advanced Computing (INNOCOMP) (pp. 411-419). IEEE.
- [47] Malik, T., Nandal, V., & Garg, P. (2024, May). Deep Learning-Based Classification of Diabetic Retinopathy: Leveraging the Power of VGG-19. In 2024 International Conference on Emerging Innovations and Advanced Computing (INNOCOMP) (pp. 645-651). IEEE.
- [48] Srivastava, A. K., Verma, I., & Garg, P. (2024, May). Improvements in Recommendation Systems Using Graph Neural Networks. In 2024 International Conference on Emerging Innovations and Advanced Computing (INNOCOMP) (pp. 668-672). IEEE.
- [49] Aggarwal, A., Jain, D., Gupta, A., & Garg, P. (2024, May). Analysis and Prediction of Churn and Retention Rate of Customers in Telecom Industry Using Logistic Regression. In 2024 International Conference on Emerging Innovations and Advanced Computing (INNOCOMP) (pp. 723-727). IEEE.
- [50] Mittal, H. K., Arsalan, M., & Garg, P. (2024, May). A Novel Deep Learning Model for Effective Story Point Estimation in Agile Software Development. In 2024 International Conference on Emerging Innovations and Advanced Computing (INNOCOMP) (pp. 404-410). IEEE.
- [51] Shukla, S. M., Magoo, C., & Garg, P. (2024, November). Comparing Fine Tuned-LMs for Detecting LLM-Generated Text. In 2024 3rd Edition of IEEE Delhi Section Flagship Conference (DELCON) (pp. 1-8). IEEE.
- [52] Kumar, B., Iqbal, M., Parmer, R., Garg, P., Rani, S., & Agrawal, A. (2025, March). The Role of AI in Optimizing Healthcare Appointment Scheduling. In 2025 3rd International Conference on Disruptive Technologies (ICDT) (pp. 881-887). IEEE.
- [53] Kumar, B., Garg, V., Ahmed, K., Garg, P., Choudhary, S., & Baniya, P. (2025, March). Enhancing Healthcare with Blockchain: Innovations in Data Privacy, Security, and Interoperability. In 2025 3rd International Conference on Disruptive Technologies (ICDT) (pp. 932-938). IEEE.

- [54] Raj, V., Prakash, B. K., Kumar, A., & Garg, P. (2024, December). Optimize the Time a Mercedes-Benz Spends on the Test Bench Using Stacking Ensemble Learning. In 2024 International Conference on Progressive Innovations in Intelligent Systems and Data Science (ICPIDS) (pp. 445-450). IEEE.
- [55] Kaushik, N., Kumar, H., Raj, V., & Garg, P. (2024, December). Proactive Fault Prediction in Microservices Applications Using Trace Logs and Monitoring Metrics. In 2024 International Conference on Progressive Innovations in Intelligent Systems and Data Science (ICPIDS) (pp. 410-415). IEEE.
- [56] Kumar, A. A., Sri, C. V., Bohara, K. S. K., Setia, S., & Garg, P. (2024, December). Capnivesh: Financing Platform for Startups. In 2024 International Conference on Progressive Innovations in Intelligent Systems and Data Science (ICPIDS) (pp. 261-265). IEEE.
- [57] Bhandari, P., Setia, S., Kumar, K., & Garg, P. (2024, December). Optimizing Cross-Platform Development with CI/CD and Containerization: A Review. In 2024 International Conference on Progressive Innovations in Intelligent Systems and Data Science (ICPIDS) (pp. 175-180). IEEE.
- [58] Chaudhary, A., & Garg, P. (2014). Detecting and diagnosing a disease by patient monitoring system. *International Journal of Mechanical Engineering And Information Technology*, 2(6), 493-499.
- [59] Malik, K., Raheja, N., & Garg, P. (2011). Enhanced FP-growth algorithm. *International Journal of Computational Engineering and Management*, 12, 54-56.
- [60] Garg, P., Dixit, A., & Sethi, P. (2021, May). Link Prediction Techniques for Opportunistic Networks using Machine Learning. In *Proceedings of the International Conference on Innovative Computing & Communication (ICICC)*.
- [61] Garg, P., Dixit, A., & Sethi, P. (2021, April). Opportunistic networks: Protocols, applications & simulation trends. In *Proceedings of the International Conference on Innovative Computing & Communication (ICICC)*.
- [62] Garg, P., Dixit, A., & Sethi, P. (2021). Performance comparison of fresh and spray & wait protocol through one simulator. *IT in Industry*, 9(2).
- [63] Malik, M., Singh, Y., Garg, P., & Gupta, S. (2020). Deep Learning in Healthcare system. *International Journal of Grid and Distributed Computing*, 13(2), 469-468.
- [64] Gupta, M., Garg, P., Gupta, S., & Joon, R. (2020). A Novel Approach for Malicious Node Detection in Cluster-Head Gateway Switching Routing in Mobile Ad Hoc Networks. *International Journal of Future Generation Communication and Networking*, 13(4), 99-111.
- [65] Gupta, A., Garg, P., & Sonal, Y. S. (2020). Edge Detection Based 3D Biometric System for Security of Web-Based Payment and Task Management Application. *International Journal of Grid and Distributed Computing*, 13(1), 2064-2076.
- [66] Garg, P., & Raman, P. K. (2011). Broadcasting Protocol & Routing Characteristics With Wireless ad-hoc networks. *Int. J. Comput. Eng. Manag.*, 12(1), 36-40.
- [67] Garg, P., Arora, N., & Malik, T. (2011). Capacity Improvement of WI-MAX In presence of Different Codes WI-MAX: Speed & Scope of future. *IJCEM*, 12.
- [68] Garg, P., Saroha, K., & Lochab, R. (2011). Review of wireless sensor networks-architecture and applications. *IJCSMS International Journal of Computer Science & Management Studies*, 11(01), 2231-5268.
- [69] Yadav, S., & Garg, P. Development of a New Secure Algorithm for Encryption and Decryption of Images.
- [70] Dixit, A., Sethi, P., & Garg, P. (2022). Rakshak: A Child Identification Software for Recognizing Missing Children Using Machine Learning-Based Speech Clarification. *International Journal of Knowledge-Based Organizations (IJKBO)*, 12(3), 1-15.
- [71] Shukla, N., Garg, P., & Singh, M. (2022). MANET Proactive and Reactive Routing Protocols: A Comparison Study. *International Journal of Knowledge-Based Organizations (IJKBO)*, 12(3), 1-14.
- [72] Arya, A., Garg, P., Vellanki, S., Latha, M., Khan, M. A., & Chhbra, G. (2024). Optimisation Methods Based on Soft Computing for Improving Power System Stability. *Journal of Electrical Systems*, 20(6s), 1051-1058.
- [73] Garg, P. (2025). Cloud security posture management: Tools and techniques. *Technix International Journal for Engineering Research*, 12(3).
- [74] Tyagi, P., Sharma, S., Srivastava, A., Rajput, N. K., Garg, P., & Kumari, M. (2025). AI in Healthcare: Transforming Medicine with Intelligence. In *First Global Conference on AI Research and Emerging Developments (G-CARED 2025)*, New Delhi, India. <https://doi.org/10.63169/GCARED2025.p4>
- [75] Garg, P., Bhatt, M., Parmar, R., & Arsalan, M. (2025). Generative AI: Evolution, Applications, Challenges And Future Prospects. *Applications, Challenges And Future Prospects* (May 17, 2025).
- [76] Garg, P., Saraswat, P., & Siddiqui, Z. (2025). AI & the Indian Stock Market: A Review of Applications in Investment Decision. <https://doi.org/10.63169/GCARED2025.p10>
- [77] Garg, P., Sharma, S., Mittal, S., Tevatia, R., Tyagi, V. K., & Kapoor, S. (2025). Unlocking Workforce Potential: AI-Powered Predictive Models for Employee Performance Evaluation. <https://doi.org/10.63169/GCARED2025.p21>
- [78] Shrivastava, N., Kalia, A., Roy, R., Sharma, S., Garg, P., & Agarwal, G. (2025). OSINT: A Double-edged Sword. In *First Global Conference on AI Research and Emerging Developments (G-CARED 2025)*, New Delhi, India. <https://doi.org/10.63169/GCARED2025.p22>
- [79] Garg, P., Aditi, A., & Roy, B. (2025). A System of Computer Network: Based On Artificial Intelligence. <https://doi.org/10.63169/GCARED2025.p24>
- [80] Parmar, R., Kapoor, S., Saifi, S., & Garg, P. (2025). Case Study on Intelligent Factory Systems for Improving Productivity and Capability in Industry 4.0 with Generative AI. In *First Global Conference on AI Research and Emerging Developments (G-CARED 2025)*, New Delhi, India. <https://doi.org/10.63169/GCARED2025.p28>
- [81] Singh, R., Sharma, R., Kumar, R., Nafis, A., Siddiqui, M. A. M., & Garg, P. (2025). Detection of Unauthorized Construction using Machine Learning: A Review. In *First Global Conference on AI Research and Emerging Developments (G-CARED 2025)*, New Delhi, India. <https://doi.org/10.63169/GCARED2025.p30>
- [82] Garg, P., Kapoor, S., Singh, V., Sharma, S., & Ankita, A. (2025). A Bridge between Blockchain and Decentralized Applications: Web3 and Non-Web3 Crypto Wallets. <https://doi.org/10.63169/GCARED2025.p35>
- [83] Verma, M., Sharma, S., Garg, P., & Singh, A. (2025). The Hidden Dangers of Prototype Pollution: A Comprehensive Detection Framework. In *First Global Conference on AI Research and Emerging Developments (G-CARED 2025)*, New Delhi, India. <https://doi.org/10.63169/GCARED2025.p36>
- [84] Sharma, A., Sharma, S., Garg, P., & Bhardwaj, P. (2025). LockTalk: A Basic Secure Chat Application. In *First Global Conference on AI Research and Emerging Developments (G-CARED 2025)*, New Delhi, India.
- [85] Arora, K., Bawane, R., Gupta, C., Ahmed, K., & Garg, P. (2025). Detection and Prevention of Cyber Attack and Threat using AI. In *First Global Conference on AI Research and Emerging Developments (G-CARED 2025)*, New Delhi, India. <https://doi.org/10.63169/GCARED2025.p38>
- [86] Garg, P., Dhruv, D., Rahman, A. A., Rai, A., Siddiqui, M., & Yadav, D. (2025). Easeviewer: An Esports Production Tool. <https://doi.org/10.63169/GCARED2025.p46>

- [87] Garg, P., Lakshita, L., Mehwish, M., Nazia, N., & Ahmed, K. (2025). Emerging Trend in Computational Technology: Innovations, Applications, and Challenges. Applications, and Challenges (May 17, 2025). <https://doi.org/10.63169/GCARED2025.p51>
- [88] Chauhan, S., Singh, M., & Garg, P. (2021). Rapid Forecasting of Pandemic Outbreak Using Machine Learning. Enabling Healthcare 4.0 for Pandemics: A Roadmap Using AI, Machine Learning, IoT and Cognitive Technologies, 59-73.
- [89] Gupta, S., & Garg, P. (2021). An insight review on multimedia forensics technology. Cyber Crime and Forensic Computing: Modern Principles, Practices, and Algorithms, 11, 27.
- [90] Shrivastava, P., Agarwal, P., Sharma, K., & Garg, P. (2021). Data leakage detection in Wi-Fi networks. Cyber Crime and Forensic Computing: Modern Principles, Practices, and Algorithms, 11, 215.
- [91] Meenakshi, P. G., & Shrivastava, P. (2021). Machine learning for mobile malware analysis. Cyber Crime and Forensic Computing: Modern Principles, Practices, and Algorithms, 11, 151.
- [92] Nanwal, J., Garg, P., Sethi, P., & Dixit, A. (2021). Green IoT and Big Data: Succeeding towards Building Smart Cities. In Green Internet of Things for Smart Cities (pp. 83-98). CRC Press.
- [93] Gupta, M., Garg, P., & Agarwal, P. (2021). Ant Colony Optimization Technique in Soft Computational Data Research for NP-Hard Problems. In Artificial Intelligence for a Sustainable Industry 4.0 (pp. 197-211). Springer, Cham.
- [94] Magoo, C., & Garg, P. (2021). Machine Learning Adversarial Attacks: A Survey Beyond. Machine Learning Techniques and Analytics for Cloud Security, 271-291.
- [95] Garg, P., Srivastava, A. K., Anas, A., Gupta, B., & Mishra, C. (2023). Pneumonia Detection Through X-Ray Images Using Convolution Neural Network. In Advancements in Bio-Medical Image Processing and Authentication in Telemedicine (pp. 201-218). IGI Global.
- [96] Gupta, S., & Garg, P. (2023). Code-based post-quantum cryptographic technique: digital signature. Quantum-Safe Cryptography Algorithms and Approaches: Impacts of Quantum Computing on Cybersecurity, 193.
- [97] Prakash, A., Avasthi, S., Kumari, P., Rawat, M., & Garg, P. (2023). Modern healthcare system: unveiling the possibility of quantum computing in medical and biomedical zones. Quantum-Safe Cryptography Algorithms and Approaches: Impacts of Quantum Computing on Cybersecurity, 249.
- [98] Gupta, S., & Garg, P. (2024). Mobile Edge Computing for Decentralized Systems. Decentralized Systems and Distributed Computing, 75-88.
- [99] Gupta, M., Garg, P., & Malik, C. (2024). Ensemble learning-based analysis of perinatal disorders in women. In Artificial Intelligence and Machine Learning for Women's Health Issues (pp. 91-105). Academic Press.
- [100] Malik, M., Garg, P., & Malik, C. (2024). Artificial intelligence-based prediction of health risks among women during menopause. Artificial Intelligence and Machine Learning for Women's Health Issues, 137-150.
- [101] Garg, P. (2024). Prediction of female pregnancy complication using artificial intelligence. In Artificial Intelligence and Machine Learning for Women's Health Issues (pp. 17-35). Academic Press.
- [102] Pokhrel, L., Arsalan, M., Rani, P., Garg, P., & Pinheiro, P. R. (2026). AI-Powered Healthcare Solutions: Bridging the Medical Gap in Underserved Communities Worldwide. In Applied AI and Computational Intelligence in Diagnostics and Decision-Making (pp. 57-86). IGI Global Scientific Publishing.
- [103] Kapoor, S., Parmar, R., Sharma, N., Garg, P., & Singh, N. J. (2026). AI and Computational Intelligence in Healthcare: An Introductory Guide. In Applied AI and Computational Intelligence in Diagnostics and Decision-Making (pp. 1-26). IGI Global Scientific Publishing.
- [104] Pokhrel, L., Kumar, A., Garg, P., Anand, N., & Singh, N. (2026). AI and IoT in Global Health: Ethical Lessons From Pandemic Response. In Development and Management of Eco-Conscious IoT Medical Devices (pp. 367-394). IGI Global Scientific Publishing.
- [105] Parmar, R., Singh, A., Garg, P., Sharma, T., & Pinheiro, P. R. (2026). Blockchain for Ethical Supply Chains: Transparency in Medical IoT Manufacturing. In Development and Management of Eco-Conscious IoT Medical Devices (pp. 337-366). IGI Global Scientific Publishing.
- [106] Gupta, S., Garg, P., Agarwal, J., Thakur, H. K., & Yadav, S. P. (2024). Federated learning based intelligent systems to handle issues and challenges in IoVs (Part 1). <https://doi.org/10.2174/97898153130311240301>
- [107] Gupta, S., Chaudhary, G., & Garg, P. (2013). Modified AODV Routing Protocol through Cache Memory for Finding New Routing Paths in MANETs. International Journal of Computer Science & Management Studies, 13(3).
- [108] Gupta, A., & Garg, P. (2021). Emerging Techniques for Handling Pandemic Challenges. Enabling Healthcare 4.0 for Pandemics: A Roadmap Using AI, Machine Learning, IoT and Cognitive Technologies, 189-209.
- [109] Chaudhary, A. P., Mishra, A., Kumar, D., & Garg, P. (2023, April). Human Emotion Recognition using Deep Learning. In 2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN) (pp. 191-197). IEEE.
- [110] Nagpal, S., Garg, P., Gaba, S., & Aggarwal, A. (2023). An improved genetic quantum cryptography model for network communication. Quantum-Safe Cryptography Algorithms and Approaches: Impacts of Quantum Computing on Cybersecurity, 177.
- [111] Yadav, M., Swami, V., Kumar, N., & Garg, P. (2025). Comparative study of Repairable Juice Plants using RPGT. Reliability: Theory & Applications, 20(2 (84)), 776-783.
- [112] Gupta, A., Garg, P., & Yadav, P. (2025). Role of Generative AI Towards Education and Learning: Present & Future. TPM-Testing, Psychometrics, Methodology in Applied Psychology, 32(S6 (2025): Posted 15 Sept), 1059-1076.
- [113] Dalal, P., Beniwal, G., Sharma, V., Garg, P., & Ahmed, K. (2025). Predicting Student Motivation and Engagement through Machine Learning Models. TPM-Testing, Psychometrics, Methodology in Applied Psychology, 32(S7 (2025): Posted 10 October), 393-411.
- [114] Gupta, A., Mund, A., Roy, S., Garg, P., & Yadav, D. K. (2025). Trust in AI Systems: A Social-psychological Investigation of Human-AI Collaboration. TPM-Testing, Psychometrics, Methodology in Applied Psychology, 32(S7 (2025): Posted 10 October), 428-446.
- [115] Bhardwaj, A., Das, A., Garg, P., & Yadav, S. (2025). Material-Driven Performance Analysis of a Vertical Nanowire Tunnel FET for Analog Applications. Journal of Electronic Materials, 1-12.
- [116] Dalal, P., Sharma, B., Sharma, T., Garg, P., & Ahmed, K. (2025). Explainable AI for Understanding Human Decision Making Patterns. TPM-Testing, Psychometrics, Methodology in Applied Psychology, 32(S7 (2025): Posted 10 October), 412-427.
- [117] Sharma, K. K., Verma, P. K., Garg, P., & Shrotriya, V. K. (2025, October). Predicting costs and benefits of IoT-based energy management for optimizing sustainable energy storage in rural areas. In AIP Conference Proceedings (Vol. 3343, No. 1, p. 040017). AIP Publishing LLC.
- [118] Ahmed, K., Baranwal, A., Sharma, N., Garg, P., & Singh, N. (2026). The Role of Federated Learning in AI-Powered Integrated Healthcare Solutions. In Enabling Collaborative Health Intelligence With Federated Learning (pp. 421-448). IGI Global Scientific Publishing.
- [119] Gupta, S., Garg, P., Agarwal, J., Thakur, H. K., & Yadav, S. P. (2025). Federated learning based intelligent systems to handle issues and challenges in IoVs (Part 2). Bentham Science Publishers. <https://doi.org/10.2174/97898153222241250301>

- [120] Garg, P., Pranav, S., & Prerna, A. (2021). Green internet of things (G-IoT): A solution for sustainable technological development. In *Green Internet of Things for Smart Cities* (pp. 23-46). CRC Press.
- [121] Malik, A., Nandal, D., Gupta, V., Garg, P., & Nandal, V. Intelligent Systems and Applications in Engineering.
- [122] Gupta, S., Garg, P., Agarwal, J., Thakur, H. K., & Yadav, S. P. (Eds.). (2025). Federated learning based intelligent systems to handle issues and challenges in IoVs (Part 2).
- [123] Garg, P., Bhatt, M., Parmar, R., & Arsalan, M. (2025). Generative AI: Evolution, Applications, Challenges And Future Prospects. Applications, Challenges And Future Prospects (May 17, 2025).
- [124] Kumar, A. K., Kumar, Y., Khurana, D., Kumar, S., & Garg, P. (2025, November). A Hybrid Ensemble Learning Framework for Interpretable Student Performance Prediction Using Academic and Extracurricular Factors. In *2025 International Conference on Innovations and Emerging Technologies In AI & Communication Systems (IETACS)* (pp. 666-672). IEEE.
- [125] Khurana, D., Kumar, Y., Kumar, N., Kumar, S., & Garg, P. (2025, November). Transformer-Based Movie Recommendation System with Autoencoder-Enhanced Feature Compression. In *2025 International Conference on Innovations and Emerging Technologies In AI & Communication Systems (IETACS)* (pp. 685-690). IEEE.
- [126] Garg, P. (2025, November). Comparative Analysis of Various Neural Networks for Galaxies Classification. In *2025 International Conference on Innovations and Emerging Technologies In AI & Communication Systems (IETACS)* (pp. 697-701). IEEE.
- [127] Saggu, A. K., Babbar, N., & Garg, P. (2025, November). Health-Guard AI: Integrated Health Report Management and Analysis. In *2025 International Conference on Innovations and Emerging Technologies In AI & Communication Systems (IETACS)* (pp. 614-623). IEEE.
- [128] Kumar, S., Kumar, Y., Kumar, N., Khurana, D., & Garg, P. (2025, November). Hybrid FCM-DNN Model for Uncertainty-Aware Air Quality Classification Using Multi-Pollutant Data. In *2025 International Conference on Innovations and Emerging Technologies In AI & Communication Systems (IETACS)* (pp. 679-684). IEEE.
- [129] Babbar, N., Singh, H. V., Bendale, S., & Garg, P. (2025, November). Stock Market Price Prediction Using Big Data Analysis: A Performance Evaluation Study. In *2025 3rd International Conference on Computational Intelligence and Network Systems (CINS)* (pp. 1-6). IEEE.
- [130] Singh, A. K., Kori, G., Garg, P., & Srivastava, G. (2025, November). Bank Churn Prediction Using Machine Learning. In *2025 IEEE 7th International Conference on Computing, Communication and Automation (ICCCA)* (pp. 1-6). IEEE.
- [131] Bhardwaj, A., Das, A., Garg, P., & Yadav, S. (2026). Material-Driven Performance Analysis of a Vertical Nanowire Tunnel FET for Analog Applications. *Journal of Electronic Materials*, 55(1), 1099-1110.
- [132] Srivastava, A. K., Shankdhar, D., Ror, R., & Garg, P. (2026). Harnessing YOLOv5 for real-time object detection: A cloud-based approach. In *Recent Advances in Computational Methods in Science and Technology* (pp. 441-450). CRC Press.
- [133] Srivastava, A. K., Shukla, A., Gupta, H., Saxena, K., & Garg, P. (2026). Towards intelligent attendance management system with face recognition using LBPH algorithm. In *Recent Advances in Computational Methods in Science and Technology* (pp. 8-15). CRC Press.
- [134] Srivastava, A. K., Garg, P., & Pandey, H. (2026). Vedcure: Towards intelligent ayurvedic drug recommendation and disease prediction. In *Recent Advances in Computational Methods in Science and Technology* (pp. 16-23). CRC Press.
- [135] Upadhyay, D., Garg, P., & Babbar, N. (2026). Blockchain and IoT based smart contract framework for efficient and secure product life management. *Discover Internet of Things*.
- [136] Singh, A., Parmar, R., Bhardwaj, P., Sharma, V., & Garg, P. (2026). Fusion of Aerial Networks with Advanced Computing Paradigms. *Edge Computing and Aerial Platforms*, 355-367.
- [137] Kumari, M., Baranwal, A., Sonal, & Garg, P. (2026). Application of Aerial Edge Computing in Disaster Management. *Edge Computing and Aerial Platforms*, 103-122.
- [138] Aditi, Saraswat, P., Sharma, V., & Garg, P. (2026). Advances in Aerial Platforms and Edge Computing. *Edge Computing and Aerial Platforms*, 123-143.
- [139] Garg, P., Arora, K., Bawane, R., Gupta, C., & Ahmed, K. (2025). Detection and Prevention of Cyber Attack and Threat using AI.
- [140] Ahmed, K., Ahmed, A., Khan, J., Garg, P., Seth, S., & Mallik, S. (2025). Principal Component Analysis Based Clustering of Insecticides and Molecular Docking of Pyrethroids Insecticides.
- [141] Kumar, B., Kumar, A., Nanwal, J., Garg, P., & Patnaik, P. (2025, November). Ensemble of YOLOv5 and Segment Anything Model for Brain Tumor Detection. In *2025 2nd International Conference on Advanced Computing and Emerging Technologies (ACET)* (pp. 1-5). IEEE.
- [142] Arsalan, M., Anas, M., & Garg, P. (2025). Transparent AI for Drug Discovery and Development. Available at SSRN 5844242.
- [143] Singh, A., Bhardwaj, P., Garg, P., & Singh, N. (2026). Introduction to explainable artificial intelligence in healthcare. In *Explainable AI in Clinical Practice* (pp. 23-44). Academic Press.
- [144] Kapoor, S., Singh, A., Garg, P., & Ramasamy, L. K. (2026). Explainable artificial intelligence in a diagnostic support system. In *Explainable AI in Clinical Practice* (pp. 131-145). Academic Press.
- [145] Ahmed, K., Anas, M., & Garg, P. (2026). Case studies on unlocking the potential of Industry 4.0 for sustainable manufacturing through generative AI-driven innovations. Available at SSRN 6356958.
- [146] Garg, P., & Oruganti, S. K. (2026, March). AI Assisted Routing Optimization in Opportunistic IoT Networks using Machine Learning: A Comprehensive review on Protocols & Simulators. In *Sustainable Global Societies Initiative* (Vol. 1, No. 4). Vibrasphere Technologies.
- [147] Arsalan, M., Pokhrel, L., & Garg, P. (2026). Architecture, Components, and tools in Integrated AI-Augmented Intelligence: A design perspective. Components, and tools in Integrated AI-Augmented Intelligence: A design perspective (March 19, 2026).
- [148] Singh, H., Ahmed, K., & Garg, P. (2026). Human Versus Machine Customer Behaviour and Functional Differences. Available at SSRN 6441098.
- [149] Saraswat, P., & Garg, P. (2026). Soft Computing In AI Agents.
- [150] Saraswat, P., & Garg, P. (2026). Water Quality Prediction Using IoT Sensors and Deep Networks.
- [151] Arsalan, M., Ahmed, K., & Garg, P. (2026). Machine learning for Anomaly detection in sensor networks. Available at SSRN 6441518.
- [152] Kumari, M., & Garg, P. (2026). Hybrid Cloud Infrastructure: Models, Benefits and Security and Challenges. Benefits and Security and Challenges (March 19, 2026).
- [153] Singh, H., & Garg, P. (2026). Demystifying Artificial Distributed Intelligence (ADI). Available at SSRN 6442698.
- [154] Saraswat, P., & Garg, P. (2026). Human AI Collaboration the future of clinical decision making.
- [155] Saraswat, P., & Garg, P. (2026). Breaking Data Boundaries: Federated Learning in Digital Healthcare.
- [156] Singh, A., Parmar, R., Bhardwaj, P., Sharma, V., & Garg, P. (2026). Fusion of Aerial Networks with Advanced Computing Paradigms. *Edge Computing and Aerial Platforms*, 355-367.

- [157] Kumari, M., Baranwal, A., Sonal, & Garg, P. (2026). Application of Aerial Edge Computing in Disaster Management. *Edge Computing and Aerial Platforms*, 103-122.
- [158] Aditi, Saraswat, P., Sharma, V., & Garg, P. (2026). Advances in Aerial Platforms and Edge Computing. *Edge Computing and Aerial Platforms*, 123-143.
- [159] Garg, P. (2026). Zero-Trust Security Enforcement through AI-Powered Anomaly Detection in Cloud Systems. *Journal of Artificial Intelligence in Governance and Public Policy (JAIGPP)*, 1(1), 1-8.
- [160] Singh, A. P., Sharma, A., & Garg, P. (2026, January). AI-Powered Adaptive Mock Interview Generation System. In *2026 International Conference on AI-Driven Smart Systems and Ubiquitous Computing (ICAUC)* (pp. 1421-1426). IEEE.
- [161] Raghav, A., Mishra, A., & Garg, P. (2026, January). Enhancing Healthcare Access: An AI-driven Chatbot for Doctor Appointment Management. In *2026 International Conference on AI-Driven Smart Systems and Ubiquitous Computing (ICAUC)* (pp. 910-914). IEEE.
- [162] Kumar, B., Chauhan, D., Singh, H., Verma, H., Sahu, K., & Garg, P. (2026, January). Decoding Linear A with Artificial Intelligence: A Comprehensive Machine Learning and NLP Framework. In *2026 International Conference on AI-Driven Smart Systems and Ubiquitous Computing (ICAUC)* (pp. 1-7). IEEE.
- [163] Gupta, V., Chakravarti, L., Akhtar, M. M., Maheshwari, P., Garg, P., & Tiwari, D. (2026, January). A Sentence-Level Risk Estimator for Identifying Hallucinations in Generative AI. In *2026 International Conference on AI-Driven Smart Systems and Ubiquitous Computing (ICAUC)* (pp. 1619-1626). IEEE.
- [164] Patnaik, P., & Garg, P. (2026). *Principles of Artificial Intelligence: Cognitive Architectures, Large Language Models, and Computational Limits*. Deep Science Publishing.
- [165] Singh, K., & Garg, P. (2026). *Trustworthy Deep Learning: Robustness, Uncertainty Quantification, and Adversarial Resilience*. Deep Science Publishing.
- [166] Garg, P. (2026). Survey of Load Balancing Strategies in Fog-Cloud Architectures for IoT Integration. *International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)*, 9(2), 595-604.
- [167] Tiwari, D., Bhati, B. S., Garg, P., & Babbar, N. (2026). A novel lexicon dictionary and CNN-LSTM employed hybrid approach for sentiment detection of COVID-19 vaccines. *Scientific Reports*.
- [168] Sethi, P., Kumar, B., Garg, P., & Yadav, P. (2026, February). Graph Neural Networks for Causal Inference in Climate Science: A Novel Approach to Modeling Complex Interactions. In *2026 International Conference on Intelligent Computing and Automation for Sustainable Solutions (ICASS)* (pp. 1-7). IEEE.
- [169] Kumar, B., Garg, P., Garg, A., Nanwal, J., & Yadav, P. (2026, February). An AI-Centric Multimodal Framework for Cognitive Productivity and Digital Wellbeing. In *2026 International Conference on Intelligent Computing and Automation for Sustainable Solutions (ICASS)* (pp. 1-7). IEEE.
- [170] Ahmed, K., Mathur, T., Chaudhary, Y., Anshika, A., Garg, P., & Tiwari, D. (2026, April). ParseRAG: Layout-Aware Open-Source Alternative. In *2026 Eighth International Conference on Computational Intelligence and Communication Technologies (CCICT)* (pp. 799-804). BM Institute of Engineering & Technology.
- [171] Yadav, P., Raj, M., Kaushik, S., Goel, P., Garg, P., & Tiwari, D. (2026, April). Employing Enhanced LSTM and Large Language Models for Stock Price Prediction Using Sentiment Analysis. In *2026 Eighth International Conference on Computational Intelligence and Communication Technologies (CCICT)* (pp. 617-622). BM Institute of Engineering & Technology.
- [172] Gupta, V., Sharma, H., Nagpal, N., Garg, P., & Tiwari, D. (2026). Feel Frames: An Emotion Based Video Summarization using Multimodal Deep Learning. *Procedia Computer Science*, 282, 715-724.
- [173] Singh, H., Ahmed, K., Kumar, U., & Garg, P. (2026, July). Comparative Analysis of Machine Learning and Large Language Model Architectures for Intelligent Medical Diagnosis and Clinical Decision Support Systems. In *Adroid Conference Series: Engineering and Technology* (Vol. 2, No. 1, pp. 125-138).
- [174] Singh, H., Ahmed, K., Prajapati, P., & Garg, P. (2026, July). Federated Learning with Differential Privacy: A Comprehensive Framework for Privacy-Preserving Distributed Machine Learning. In *Adroid Conference Series: Engineering and Technology* (Vol. 2, No. 1, pp. 139-155).
- [175] Singh, H., Ahmed, K., & Garg, P. (2026, July). Survey on Internet of Things (IoT) Forensics: Challenges, Approaches, Privacy-Aware Frameworks and Open Issues. In *Adroid Conference Series: Engineering and Technology* (Vol. 2, No. 1, pp. 156-170).
- [176] Singh, H., Ahmed, K., & Garg, P. (2026, July). Supply Network Disruption Prediction using Heterogeneous Graph Neural Networks and Temporal Embeddings. In *Adroid Conference Series: Engineering and Technology* (Vol. 2, No. 1, pp. 171-186).
- [177] Saraswat, P., Kumari, S., & Garg, P. (2026, July). Future Directions in Digital Social Linguistics. In *Adroid Conference Series: Engineering and Technology* (Vol. 2, No. 1, pp. 187-203).
- [178] Saraswat, P., Yadav, A., & Garg, P. (2026, July). Comparing Supervised and Unsupervised Learning Approaches for Specific Tasks. In *Adroid Conference Series: Engineering and Technology* (Vol. 2, No. 1, pp. 220-236).
- [179] Saraswat, P., Aishwarya, S., & Garg, P. (2026, July). Foundation of Self-Learning AI for Drones. In *Adroid Conference Series: Engineering and Technology* (Vol. 2, No. 1, pp. 237-254).
- [180] Ahmed, K., Singh, H., Anas, M., & Garg, P. (2026, July). The Future of Artificial Intelligence in Healthcare. In *Adroid Conference Series: Engineering and Technology* (Vol. 2, No. 1, pp. 255-270).
- [181] Ahmed, K., & Garg, P. (2026, July). AI-Driven Fault Detection and Diagnostics. In *Adroid Conference Series: Engineering and Technology* (Vol. 2, No. 1, pp. 271-292).
- [182] Kumari, M., Pandey, S., & Garg, P. (2026, July). Quantum AI for Drug Discovery and Material Science. In *Adroid Conference Series: Engineering and Technology* (Vol. 2, No. 1).
- [183] Kumari, M., Jha, S. K., & Garg, P. (2026, July). Opportunities and Challenges of AI in Education. In *Adroid Conference Series: Engineering and Technology* (Vol. 2, No. 1, pp. 328-341).
- [184] Pokhrel, L., Kumar, A., & Garg, P. (2026, July). Impact of AI on Employment and Workforce Transformation. In *Adroid Conference Series: Engineering and Technology* (Vol. 2, No. 1, pp. 342-356).
- [185] Singh, H., Ahmed, K., Kumar, A., & Garg, P. (2026, July). AI-Driven Optimization in Supply Chain Operations: A Machine Learning Framework for Demand Forecasting and Inventory Management. In *Adroid Conference Series: Engineering and Technology* (Vol. 2, No. 1, pp. 357-371).
- [186] Saraswat, P., Kumar, R., & Garg, P. (2026, July). Human Perception and Virtual Reality: What Is the Connection?. In *Adroid Conference Series: Engineering and Technology* (Vol. 2, No. 1, pp. 409-427).
- [187] Ahmed, K., Arsalan, M., Sharma, P. K., & Garg, P. (2026, July). Quantum Technology in Medical Diagnosis. In *Adroid Conference Series: Engineering and Technology* (Vol. 2, No. 1, pp. 428-448).
- [188] Saraswat, P., Sharma, P., & Garg, P. (2026, July). The Challenges of AI Implementation in Business. In *Adroid Conference Series: Engineering and Technology* (Vol. 2, No. 1, pp. 204-219).

- [189] Trivedi, S., Beri, T., Arora, A., & Garg, P. (2026, June). NoduleNet: Deep Learning-Based Computational Model for Thyroid Cancer Detection. In 2026 6th International Conference on Emerging VLSI and Semiconductor Technology for AI and Computing Applications (EVST) (pp. 1-7). IEEE.
- [190] Joshi, V., Tyagi, U., Jakhar, V., Gaur, M., & Garg, P. (2026, June). HealthQ: A Retrieval-Augmented Health Policy Query Chatbot. In 2026 6th International Conference on Emerging VLSI and Semiconductor Technology for AI and Computing Applications (EVST) (pp. 1-6). IEEE.
- [191] Saraswat, P., Sharma, V., & Garg, P. (2026, June). Energy Optimization In Smart IoT Enabled Smart Home System Through Machine Learning Techniques. In 2026 6th International Conference on Emerging VLSI and Semiconductor Technology for AI and Computing Applications (EVST) (pp. 1-6). IEEE.
- [192] Saraswat, P., Tiwari, B., & Garg, P. (2026, June). An Empirical Study on Salary Determinants Using Machine Learning. In 2026 6th International Conference on Emerging VLSI and Semiconductor Technology for AI and Computing Applications (EVST) (pp. 1-5). IEEE.
- [193] Pokhrel, L., Arsalan, M., Tiwari, B., & Garg, P. (2026, June). Food Delivery Time Prediction Using Machine Learning Algorithms: A Comparative Study with Hybrid XGBoost-LSTM Architecture. In 2026 6th International Conference on Emerging VLSI and Semiconductor Technology for AI and Computing Applications (EVST) (pp. 1-7). IEEE.
- [194] Garg, P., & Kumar, V. (2026, June). Millimeter-Wave 60 GHz On-Chip Dipole Antenna with Silicon Lens Integration in SiGe Technology. In 2026 6th International Conference on Emerging VLSI and Semiconductor Technology for AI and Computing Applications (EVST) (pp. 1-5). IEEE.
- [195] Arora, A., Trivedi, S., Tyagi, R., & Garg, P. (2026, June). LungVision: Classifying lung diseases using CNN ensembles. In 2026 6th International Conference on Emerging VLSI and Semiconductor Technology for AI and Computing Applications (EVST) (pp. 1-6). IEEE.
- [196] Arora, A., Trivedi, S., Sharma, R., Tiwari, R., Chaudhary, S., & Garg, P. (2026, June). Comparative Study of ResNet-152 and ViTPose-G for Human Pose Detection on the COCO Yoga Dataset. In 2026 6th International Conference on Emerging VLSI and Semiconductor Technology for AI and Computing Applications (EVST) (pp. 1-6). IEEE.
- [197] Kaur, M., Chhillar, V., Kumar, V., & Garg, P. (2026, June). Exploration and Recognition of Autism Spectrum Disorder through Machine Learning Approaches. In 2026 6th International Conference on Emerging VLSI and Semiconductor Technology for AI and Computing Applications (EVST) (pp. 1-6). IEEE.
- [198] Singh, R., Singh, G., Kumar, V., Kumari, M., Kumar, A., & Garg, P. (2026, June). Optimization of Battery Electric Vehicle Thermal Management System Using MATLAB Simscape for Enhanced Charging Efficiency. In 2026 6th International Conference on Emerging VLSI and Semiconductor Technology for AI and Computing Applications (EVST) (pp. 1-6). IEEE.
- [199] Chauhan, A., Singh, G., Kumar, V., Kumari, M., Kumar, A., & Garg, P. (2026, June). An Intelligent Thermal Control and Optimization Framework for Efficient and Safe Battery Charging in Electric Vehicles. In 2026 6th International Conference on Emerging VLSI and Semiconductor Technology for AI and Computing Applications (EVST) (pp. 1-6). IEEE.
- [200] Kumar, S., Kumar, Y., Khurana, D., Kumar, N., & Garg, P. (2026, June). AI-Driven Discovery of Cybercrime Insights from Diverse Web Data. In 2026 6th International Conference on Emerging VLSI and Semiconductor Technology for AI and Computing Applications (EVST) (pp. 1-6). IEEE.
- [201] Chaudhary, N., Tyagi, N., Sharma, N., Gupta, M., & Garg, P. (2026, June). BusOptima-Bus Scheduling & Route Management System. In 2026 6th International Conference on Emerging VLSI and Semiconductor Technology for AI and Computing Applications (EVST) (pp. 1-6). IEEE.
- [202] Srivastava, A. K., Singh, A., Umrao, A., & Garg, P. (2026, June). A Retrieval-Augmented Framework for Context-Aware Document Querying. In 2026 6th International Conference on Emerging VLSI and Semiconductor Technology for AI and Computing Applications (EVST) (pp. 1-7). IEEE.
- [203] Gupta, T., Bhargava, D., & Garg, P. (2026, June). A Comprehensive Survey on Malware Botnet Detection Using Deep Learning in IoT and Android Platforms with Edge AI. In 2026 6th International Conference on Emerging VLSI and Semiconductor Technology for AI and Computing Applications (EVST) (pp. 1-7). IEEE.
- [204] Trivedi, S., Shukla, B., Garg, Y., Satish, T., & Garg, P. (2026, June). Enhancing Social Media Security Through Explainable Ensemble Learning. In 2026 6th International Conference on Emerging VLSI and Semiconductor Technology for AI and Computing Applications (EVST) (pp. 1-6). IEEE.
- [205] Arora, P., Arora, R., Tiwari, D., & Garg, P. (2026, June). Automated Brain Tumor Classification from MRI Images Through InceptionNet Architecture. In 2026 6th International Conference on Emerging VLSI and Semiconductor Technology for AI and Computing Applications (EVST) (pp. 1-6). IEEE.
- [206] Srivastava, S., Singh, S., Goswami, S., Gupta, M., & Garg, P. (2026, June). SignSpeak: A Real-Time Deep Learning Framework for Bidirectional Sign Language Translation. In 2026 6th International Conference on Emerging VLSI and Semiconductor Technology for AI and Computing Applications (EVST) (pp. 1-7). IEEE.
- [207] Srivastava, A. K., Garg, P., & Singh, A. (2026, June). ExplainFusion: An Ensemble Explainable AI Framework with Evidence-Grounded LLM-Based Clinical Explanations. In 2026 6th International Conference on Emerging VLSI and Semiconductor Technology for AI and Computing Applications (EVST) (pp. 1-8). IEEE.