Dr .B .R . AMBEDKAR UNIVERSITY, ETCHERLA

COLLEGE OF ENGINEERING

IOT CHAIN AND MONITORING - CHAIN USING MULTILEVEL BLOCK CHAIN FOR IOT SECURITY

A Major project report submitted in partial fulfilment of the requirement for the award of degree of

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING

2021 – 2025

Presented by

M.Pavani-2181951029

D .Koteswar Rao Naik -2181951013

CH . Anusha -2181951010

CH . Anusha – 2181951008

P . Joicy -2181951045

UNDER THE GUIDANCE OF

Smt. B. Vyasa Geetha M. Tech (Ph.D)

(*Assistant Professor)*

Introduction:

The Internet of Things (IoT) often relies on centralized servers, leading to vulnerabilities such as DDoS attacks, single-point failures, and data tampering. To address these issues, a multilevel blockchain architecture is proposed. It integrates a lightweight IoT-Chain, operating directly on IoT devices for sensor data storage, and a Monitoring-Chain, based on Hyperledger Fabric, for metadata management and access control. By using a VRF-based lightweight consensus algorithm and Schnorr signatures , the solution achieves 96–99% reduction in consensus delay and sustains high transaction throughput (1024–1701 TPS). This ensures enhanced security, scalability, and reliability for IoT data management while overcoming the computational and storage limitations of traditional blockchain systems.

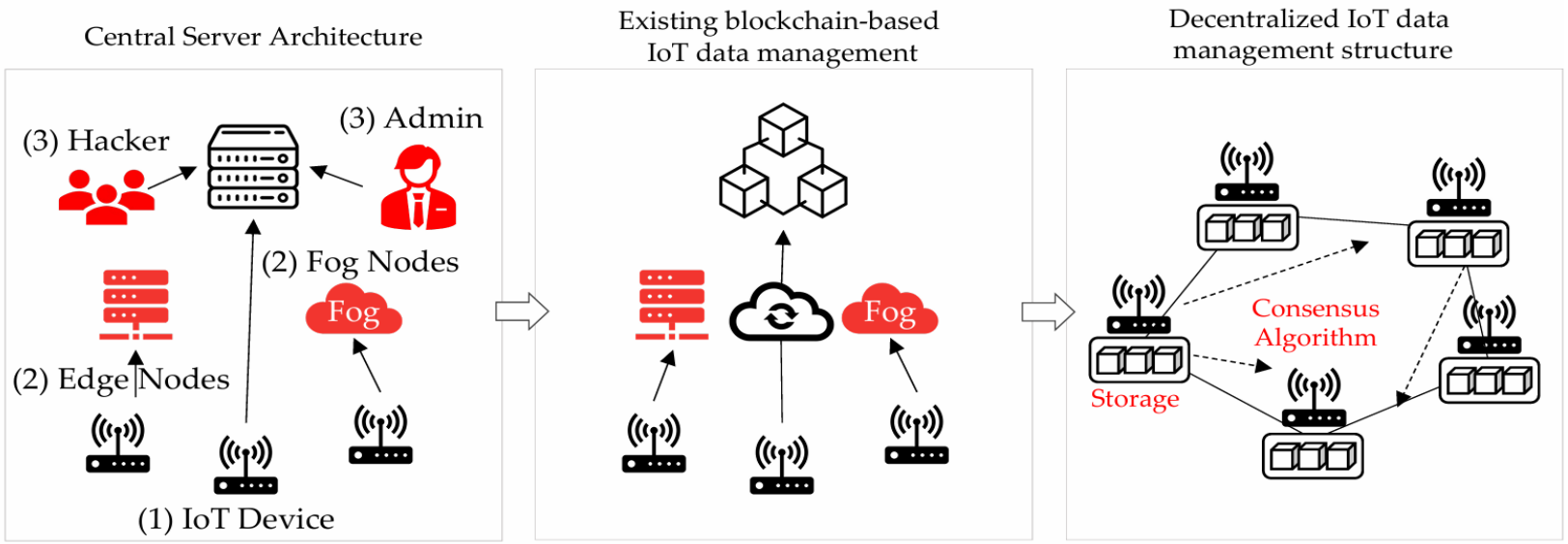
.

Challenges in IoT Security:

- Centralized structures are prone to single-point failures, DDoS attacks, and data tampering.
- IoT devices' limited computation and storage make traditional blockchain unsuitable.

Clear, bold statement:

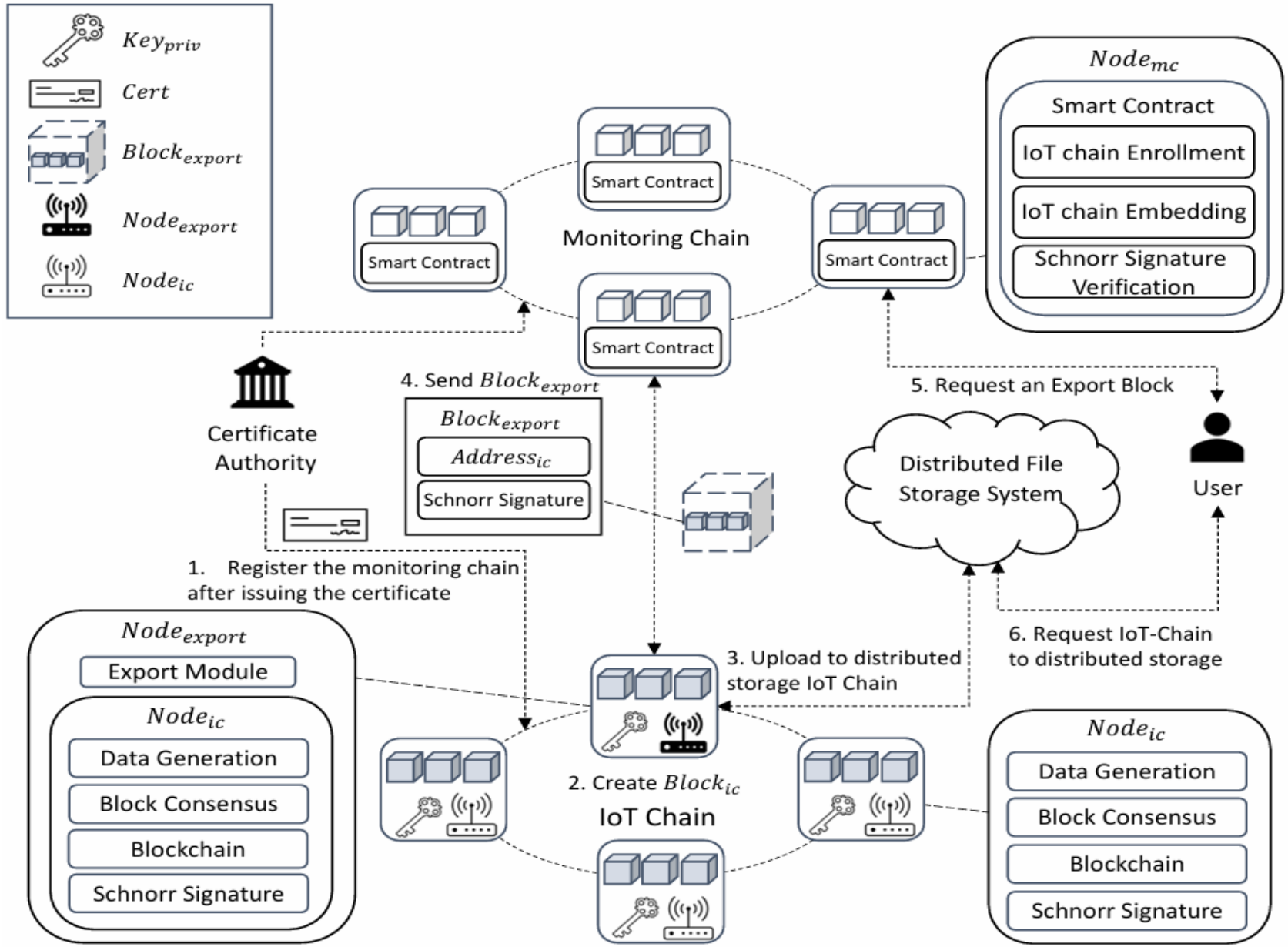
"How do we achieve secure and lightweight IoT data management using a decentralized system?“



Proposed Multilevel Blockchain Architecture:

Key Components:

- **IoT-Chain:**
  Lightweight blockchain on IoT devices for decentralized data management.
- **Monitoring-Chain:**
  Hyperledger Fabric-based metadata storage and access control.
- **Features:**
  Lightweight consensus with reduced computational and communication overhead . Enhanced security with Schnorr signatures and VRF-based leader Selection Include a simplified architecture diagram to visually represent the flow.


Key_{priv}
$Cert$
$Block_{export}$
$Node_{export}$
$Node_{ic}$
$Node_{mc}$
Smart Contract
IoT chain Enrollment
IoT chain Embedding
Schnorr Signature Verification
Smart Contract
Smart Contract
Monitoring Chain
Smart Contract
Smart Contract
Certificate Authority
4. Send $Block_{export}$
$Block_{export}$
$Address_{ic}$
Schnorr Signature
5. Request an Export Block
Distributed File Storage System
User
1. Register the monitoring chain after issuing the certificate
$Node_{export}$
Export Module
$Node_{ic}$
Data Generation
Block Consensus
Blockchain
Schnorr Signature
3. Upload to distributed storage IoT Chain
6. Request IoT-Chain to distributed storage
2. Create $Block_{ic}$
IoT Chain
$Node_{ic}$
Data Generation
Block Consensus
Blockchain
Schnorr Signature

Consensus Algorithm: The Core of Our Approach

- **Overview of Consensus in IoT-Chain:**

  Transactions are generated from IoT devices (data set-driven).

  - Leader node selected using Verifiable Random Function (VRF) for fairness and unpredictability.

  - Schnorr signature ensures efficient, lightweight signature compression.

Key Advantages of Our Consensus Mechanism:

- Low Latency:

Block creation delay reduced by 96% compared to PBFT and 99% compared to PoW (average 0.0044 seconds).

- Energy Efficiency:

Minimal CPU usage compared to PoW, enabling IoT-device compatibility.

- Scalability:

Handles high transaction throughput (1000+ TPS across varying data sizes).

Process Flow:

1. IoT devices execute VRF to generate transaction hash.
2. VRF selects the leader node for block creation.
3. Schnorr signatures ensure consensus verification with O(1) overhead.
4. Block propagated to all IoT devices and integrated into the IoT-Chain.

Data Integration and Consensus Workflow:

- Take a pre-processed dataset (sensor readings, system logs, etc.).
- Apply the consensus algorithm for:
    1. Transaction validation.
    2. Leader election via VRF.
    3. Secure block generation with Schnorr signatures.
- Export IoT-Chain to Monitoring-Chain using distributed file storage (DFS).

Experimental Results:

- **Blockchain Size Management:**
  - **Graph:** Capped size vs. uncapped size (IC with and without export).
  - **Consensus Efficiency:**
    - Latency comparison across algorithms (Proposed: 0.0044s, PBFT: 0.1266s, PoW: 5.528s).
  - **Transaction Throughput (TPS):**
    - Sustained 1000+ TPS across varying data sizes (e.g., 8B, 128B, 1KB, 10KB).
    - Use labeled graphs to showcase these findings.

Impact and Real-World Applications

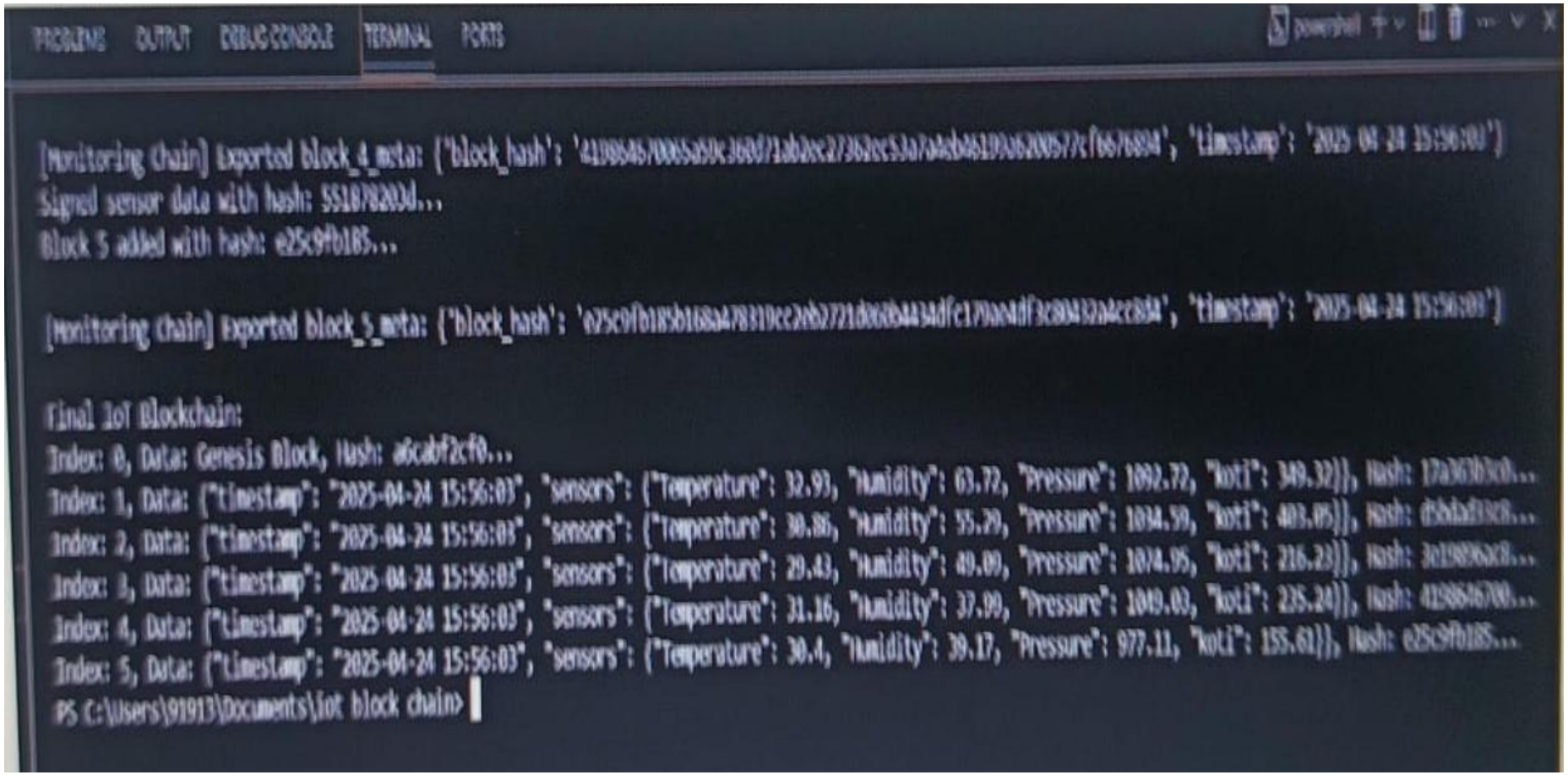
- **Impact:**

  Secure, lightweight, and scalable blockchain solution for IoT devices.

- **Applications:**

  - **Smart Cities:** Real-time traffic monitoring and control systems.
  - **Healthcare IoT:** Secure patient data collection and sharing.
  - **Industrial IoT:** Real-time sensor integration and tamper-proof logs.

Output:


PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
powershell
[Monitoring Chain] Exported block_4_meta: {'block_hash': '
', 'timestamp': '
Signed sensor data with hash: 55187
Block 5 added with hash: e25c9fb185...
[Monitoring Chain] Exported block_5_meta: {'block_hash': '
', 'timestamp': '
Final IoT Blockchain:
Index: 0, Data: Genesis Block, Hash: a6cabf2cf0...
Index: 1, Data: {"timestamp": "2025-04-24 15:56:03", "sensors": {"Temperature": 32.93, "Humidity": 63.72, "Pressure": 1092.72, "Koti": 349.32}}, Hash:
Index: 2, Data: {"timestamp": "2025-04-24 15:56:03", "sensors": {"Temperature": 30.86, "Humidity": 55.29, "Pressure": 1034.59, "Koti": 403.05}}, Hash:
Index: 3, Data: {"timestamp": "2025-04-24 15:56:03", "sensors": {"Temperature": 29.43, "Humidity": 49.00, "Pressure": 1074.95, "Koti": 216.23}}, Hash:
Index: 4, Data: {"timestamp": "2025-04-24 15:56:03", "sensors": {"Temperature": 31.16, "Humidity": 37.99, "Pressure": 1049.03, "Koti": 235.24}}, Hash:
Index: 5, Data: {"timestamp": "2025-04-24 15:56:03", "sensors": {"Temperature": 30.4, "Humidity": 39.17, "Pressure": 977.11, "Koti": 155.61}}, Hash: e25c9fb185...
PS C:\Users\91913\Documents\iot block chain>

Conclusion:

In conclusion, this study proposes a lightweight blockchain structure for IoT security, addressing key challenges. The system ensures data privacy and security, demonstrating efficient performance with over 1000 TPS. It is suitable for IoT devices with limited resources. Future research will focus on optimizing performance. The proposed approach shows promise for secure IoT applications. Overall, it provides a viable solution.

THANK YOU