Security in Cloud Computing and IOT

Submitted by: Group 1

Privacy-Preserving Verifiable Federated Aggregation via Blockchain and Secret-Key Algebraic Signatures

Abstract:

The rapid growth of Internet of Things (IoT) systems has led to large-scale generation of sensitive data that is commonly outsourced to cloud servers for storage and processing, raising serious concerns regarding privacy, data integrity, and trust. Traditional centralized data aggregation approaches require full trust in the cloud server and intermediate entities, making them vulnerable to data forgery, tampering, and insider attacks. To address these challenges, this project proposes a privacy-preserving and verifiable federated data aggregation framework in which multiple independent IoT devices securely submit authenticated data files without relying on centralized trust. Each device generates a secret-key algebraic signature over its data, enabling efficient and verifiable authentication. A blockchain-based verifier validates the authenticity of submitted data and records verification outcomes in an immutable and auditable ledger, while the cloud server aggregates only verified data files without inspecting their sensitive contents. The proposed design ensures data integrity, privacy preservation, and transparency in outsourced data aggregation and demonstrates the feasibility of secure, auditable, and lightweight verification suitable for IoT-cloud environments.

Keywords:

- Federated Data Aggregation

- IoT Security
- Blockchain Verification
- Algebraic Signatures
- Privacy-Preserving Systems
- Secure Outsourced Computation

Concept Map:

- IoT Devices
  → generate data files
  → sign with secret-key algebraic signature
- Blockchain Verifier
  → verifies authenticity
  → logs verification immutably
- Cloud Server
  → aggregates verified files
  → no access to raw trust decisions

Problem Definition:

How can multiple independent IoT devices securely submit data to a cloud server such that:

- Data integrity is verifiable
- Privacy is preserved
- No single entity needs to be fully trusted
- Aggregation occurs only over verified data

Threat Model:

Adversaries Considered:

- Malicious IoT device submitting forged/tampered data
- Curious or dishonest cloud server
- Compromised verifier attempting to approve invalid data

Assumptions:

- Secret keys are securely provisioned
- Blockchain testnet behaves correctly
- Network attacker can observe but not break cryptography

Entities:

1. IoT Devices (Data Owners)
2. Blockchain-Based Verifier
3. Cloud Aggregation Server

Workflow:

1. IoT device generates a data file
2. Device computes secret-key algebraic signature
3. File + signature sent to verifier
4. Verifier validates and logs result on blockchain
5. Server aggregates only verified files

Proposed Method:

Replace trust-based data aggregation with cryptographically verifiable and blockchain-audited federated aggregation.

Novel Aspects:

- Federated aggregation of data files, not ML models
- Lightweight secret-key algebraic signatures (IoT-friendly)
- Blockchain used purely as verifier and audit layer, not storage

- Privacy preserved by verification without content inspection

Modules:

1. **IoT Client Module**
   a. Data generation
   b. Signature computation
2. **Signature Module**
   a. Algebraic signing
   b. Verification logic
3. **Blockchain Verifier Module**
   a. Verification logging
   b. Immutable ledger
4. **Aggregation Server Module**
   a. Accepts verified data
   b. Combines files

Tools:

- Python 3
- NumPy / Pandas
- Simulated blockchain (testnet model)
- GitHub for version control

Evaluation Plan:

Datasets / Testbed

- Synthetic IoT sensor files
- Simulated malicious inputs

Metrics

- Verification accuracy

- False acceptance/rejection rate
- Aggregation correctness
- Overhead (time, storage)

Baselines

- No verification aggregation
- Centralized trusted server model

Attack Scenarios

- Forged file injection
- Tampered signature
- Replay attack
- Verifier misbehavior attempt

Threats to Validity:

- Simulated blockchain ≠ full public network
- Simplified cryptographic primitives
- Limited scale of IoT nodes

Ethics & Safety:

- No real personal data used
- No financial blockchain transactions
- System designed for defensive security research

Two-Month Execution Plan (8 weeks):

Week	Task

1	Literature review + final architecture
2	Data & signature module
3	Verifier implementation
4	Aggregation server
5	Attack simulation
6	Evaluation & results
7	Deploying the complete project on GitHub with proper documentation
8	Conference Paper

Risk Register:

Risk	Impact	Mitigation
Crypto complexity	Medium	Use algebraic simulation
Blockchain issues	Low	Testnet/simulation
Scope creep	Medium	Fixed feature list
Time overrun	Medium	Weekly milestones

AI Log:

Purpose of AI Assistance

Concept clarification, architecture design, security reasoning, and academic structuring.

Prompts Used

- “Explain federated aggregation in simple words”
- “Align blockchain verification with IoT data aggregation”
- “Explain Verifiable Federated Learning”
- “What is meant by Algebraic Signature”

Summary of AI Suggestions Used

- Clarified **federated aggregation** as a decentralized approach where multiple IoT devices independently contribute data without a central data collection authority.
- Explained how **blockchain verification** can be integrated with IoT data aggregation by using the blockchain as a tamper-proof verifier and audit log rather than a data storage layer.
- Differentiated **verifiable federated learning** from simple federated aggregation, helping the group narrow the project scope to verifiable data aggregation instead of model training.
- Introduced **algebraic signatures** as lightweight cryptographic constructs that enable efficient data integrity verification suitable for resource-constrained IoT devices.
- Helped structure the system into clear entities: IoT devices, blockchain verifier, and cloud aggregation server.

Items Rejected and Reasons

- Full federated machine learning training-
  Rejected because the project focuses on file-based data aggregation rather than model updates.
- Storing IoT data directly on the blockchain-
  Rejected due to scalability, cost, and privacy limitations of blockchain storage.
- Public-key digital signatures for every IoT device-
  Rejected because they introduce higher computational overhead and complex key management for IoT environments.
- Assuming complete trust in the cloud server-
  Rejected to maintain a realistic threat model aligned with cloud security objectives.

Claim Tagging

Claim 1

Federated aggregation reduces reliance on a centralized trusted data collector.
Tag: Verified
(Confirmed through standard federated system principles.)

Claim 2

Blockchain can be used as a neutral and tamper-proof verifier for IoT data aggregation.
Tag: Verified
(Validated by existing blockchain audit and verification use cases.)

Claim 3

Algebraic signatures are lightweight and suitable for IoT devices.
Tag: To Verify
(Requires literature review or experimental validation in Week 1–2.)

Claim 4

The proposed system preserves data privacy by verifying authenticity without accessing raw data contents.
Tag: Assumed
(Reasonable but not formally proven in this implementation.)

Claim 5

The system scales effectively with an increasing number of IoT devices.
Tag: To Verify
(Requires scalability experiments.)

AI-Identified Issues

- Lack of formal cryptographic security proofs
- No real IoT hardware deployment
- Privacy guarantees are informal and assumption-based
- Key management for secret keys not fully detailed
- Limited adversarial attack coverage