

**Makerere University**

College of Computing and Information Sciences

Department of Computer Science

# **A Blockchain-Secured Federated Learning System for Detection and Early Warning of Foot-and-Mouth Disease in Ugandan Cattle Farms**

*Research Proposal*

**By**

Muhindo Mubaraka

Student Number: 2400725633

Registration Number: 2024/HD05/25633U

*muhindo.mubaraka@students.mak.ac.ug*

**Supervisor**

Dr. Chongomweru Halimu

Department of Computer Science

A Research Proposal Submitted in Partial Fulfillment of the Requirements  
for the Degree of Master of Computer Science

November 28, 2025

# Abstract

Training effective machine learning models today requires bringing all data together in one place. This approach works well when you have fast internet and powerful computers, but it creates serious problems. Farmers and hospitals cannot share their data because of privacy concerns. In rural areas with limited connectivity, uploading large datasets is simply not practical. Even when possible, centralizing sensitive information creates security risks that many organizations cannot accept.

This research explores a different approach. Instead of moving data to where the model is being trained, we send the model to learn from data that stays in its original location. This is called federated learning. However, when you train models across many separate locations, a new challenge emerges: how do you trust that everyone is participating honestly? How do you verify that the system has not been compromised?

I propose using blockchain technology to solve this trust problem. The blockchain acts as an unchangeable record keeper, documenting every step of the training process and ensuring that no one can cheat the system. To demonstrate that this works in practice, I will apply it to predicting Foot-and-Mouth Disease outbreaks in Ugandan cattle farms, where data privacy and limited infrastructure make traditional approaches impossible.

The outcome will be a working system that shows how organizations can collaborate on building intelligent models without sacrificing data ownership or privacy. This has implications far beyond disease prediction, offering a blueprint for privacy-preserving AI in healthcare, agriculture, and other sensitive domains where data sharing remains a major barrier.

**Keywords:** Federated Learning, Blockchain, Privacy-Preserving Machine Learning, Disease Prediction, Distributed Systems, Differential Privacy, Byzantine Fault Tolerance

# Contents

<b>CHAPTER 1: INTRODUCTION</b>	<b>4</b>
0.1 Background of the Study . . . . .	4
0.2 Problem Statement . . . . .	4
0.3 Research Objectives . . . . .	5
0.3.1 Main Objective . . . . .	5
0.3.2 Specific Objectives . . . . .	5
0.4 Research Questions . . . . .	5
0.5 Significance of the Study . . . . .	5
0.6 Scope and Limitations . . . . .	6
0.6.1 Scope . . . . .	6
0.6.2 Limitations . . . . .	6
<b>CHAPTER 2: LITERATURE REVIEW</b>	<b>8</b>
0.7 Introduction . . . . .	8
0.8 Federated Learning in Disease Prediction . . . . .	8
0.8.1 Kapalaga et al. (2024) – A Unified FMD Dataset . . . . .	8
0.9 Blockchain-Enabled Federated Learning Systems . . . . .	8
0.9.1 Zhang et al. (2023) – Blockchain-Based FL . . . . .	8
0.9.2 Chen et al. (2024) – FLock System . . . . .	9
0.10 Federated Learning in Healthcare . . . . .	9
0.10.1 Teo et al. (2024) – FL in Healthcare . . . . .	9
0.11 Summary of Research Gaps . . . . .	9
0.12 Chapter Summary . . . . .	10
<b>CHAPTER 3: RESEARCH METHODOLOGY</b>	<b>11</b>
0.13 Introduction . . . . .	11
0.14 Research Design . . . . .	11
0.15 System Architecture . . . . .	11
0.16 Prototype Implementation . . . . .	12
0.17 Performance Evaluation . . . . .	12
<b>1 Timeline and Work Plan</b>	<b>12</b>
1.1 Phase 1: Foundation (Months 1-4) . . . . .	12
1.2 Phase 2: Building the Core (Months 5-9) . . . . .	13
1.3 Phase 3: Making It Secure (Months 10-13) . . . . .	13
1.4 Phase 4: Making It Adaptive (Months 14-16) . . . . .	13
1.5 Phase 5: Making It Real (Months 17-20) . . . . .	13

1.6	Phase 6: Testing Everything (Months 21-23)	14
1.7	Phase 7: Writing and Wrapping Up (Month 24)	14
1.8	Expected Contributions and Deliverables	14
1.8.1	Scientific Contributions	14
1.8.2	Technical Contributions	14
1.8.3	Practical Impact for Uganda	14
1.8.4	Global Relevance	14
1.9	Evaluation Metrics	15
1.9.1	Model Performance Metrics	15
1.9.2	Privacy Metrics	15
1.9.3	Fairness Metrics	15
1.9.4	Efficiency Metrics	15
1.9.5	Robustness Metrics	15
<b>2</b>	<b>Ethical Considerations</b>	<b>16</b>
2.1	Protecting Privacy	16
2.2	Informed Consent	16
2.3	Avoiding Harm	16
2.4	Fair Access to Benefits	16
2.5	Environmental Responsibility	16
<b>3</b>	<b>Scope and Limitations</b>	<b>16</b>
3.1	Research Scope	16
3.2	Limitations	17
3.3	Future Directions	17
<b>4</b>	<b>Process Workflow</b>	<b>17</b>
<b>5</b>	<b>Conclusion</b>	<b>17</b>

# CHAPTER 1: INTRODUCTION

## 0.1 Background of the Study

Conventional (centralized) machine learning depends on collecting and consolidating raw data into a single repository for model training. In many real-world settings—particularly in low-resource regions—this approach is impractical because of privacy concerns, regulatory constraints, and limited network and compute infrastructure. These barriers reduce the feasibility of central aggregation and limit participation from important stakeholders such as hospitals and local farming cooperatives [7].

Federated learning (FL) addresses these limitations by keeping raw data on local clients and exchanging model updates instead of data. Clients compute local model updates which are aggregated to produce a global model; this design preserves data locality and reduces the need for large-scale data transfers [5]. Nevertheless, practical FL deployments face systems-level challenges—unreliable connectivity, client drop-out, and communication overhead—that must be managed for robust, large-scale operation [6].

At the same time, decentralization raises questions of trust and integrity: malicious or faulty participants can submit corrupted updates or otherwise degrade model performance. These concerns motivate complementary mechanisms for verification and accountability. This research investigates a practical integration of lightweight blockchain-based verification with FL to provide auditable, tamper-evident records of model updates while remaining suitable for resource-constrained environments.

## 0.2 Problem Statement

Federated learning systems have a fundamental trust problem. When hospitals, farms, or other organizations train models on their local data, there is no reliable way to verify that participants are sending honest updates. A malicious actor could submit corrupted data that poisons the entire model. Similarly, participants cannot verify whether the central server is actually using their contributions correctly or just ignoring them. This trust issue is particularly dangerous in disease surveillance, where a poisoned model could miss an outbreak and cost lives.

Researchers have tried using blockchain to solve this trust problem, but these solutions create new issues. Most blockchain systems are too slow and power-hungry to work in rural areas with limited internet and electricity [7]. This is frustrating because federated learning was designed specifically to help these low-resource environments in the first place.

So the core problem is: how do we build a system that verifies model integrity and holds participants accountable, while still being efficient enough to run on modest hard-

ware in areas with poor infrastructure? This research addresses this gap by designing a practical verification mechanism for federated learning in resource-constrained settings like Uganda’s livestock disease monitoring system.

## **0.3 Research Objectives**

### **0.3.1 Main Objective**

To design a private and trustworthy collaborative prediction system, that is blockchain-based and fed with a federated learning system, which will be suitable for resource-constrained environments after thorough evaluation.

### **0.3.2 Specific Objectives**

1. To create a system architecture that optimally combines federated learning with blockchain technology for safe and auditable model merging.
2. To put the whole system concept into a working prototype using lightweight frameworks appropriate for settings with limited computing resources.
3. To carry out a performance assessment of the system regarding prediction accuracy, computational efficiency, and resilience to malevolent attacks.
4. To further prove the system’s applicability through a case study on Foot-and-Mouth Disease prediction using Ugandan cattle farm data.

## **0.4 Research Questions**

1. How can federated learning and blockchain technology be effectively integrated to create a trustworthy and privacy-preserving collaborative prediction system?
2. What architectural design principles are necessary to ensure the system operates efficiently in resource-constrained environments?
3. How does the proposed system perform in terms of prediction accuracy, computational efficiency, and resilience to malicious attacks?
4. Can the system be successfully applied to real-world disease prediction scenarios in Uganda’s livestock sector?

## **0.5 Significance of the Study**

This research is situated at the intersection of federated learning and blockchain technologies. The study will investigate how these technologies can be combined into a single,

integrated system that is not only private and efficient but also capable of gaining users' trust.

The significance of this study extends across multiple dimensions:

**Scientific Contribution:** This research will provide the first complete blueprint for integrating blockchain-secured federated learning specifically for early warning systems in resource-constrained environments. It bridges the gap between theoretical frameworks and practical implementation.

**Technical Impact:** The resulting open-source prototype will serve as a foundation for future decentralized AI systems, demonstrating that privacy-preserving collaborative machine learning is achievable even with limited computational resources.

**Practical Application:** By focusing on Foot-and-Mouth Disease prediction in Uganda, this work addresses a critical need in the livestock sector while proving the system's viability in real-world conditions with unreliable connectivity and distributed data sources.

**Policy Implications:** The system demonstrates how organizations can collaborate on AI development while complying with data protection regulations, offering a model for privacy-preserving data governance.

**Global Relevance:** While tested in Uganda's agricultural context, the principles and architecture apply broadly to healthcare, disaster response, and any domain where data sharing is problematic but collective intelligence is essential.

## 0.6 Scope and Limitations

### 0.6.1 Scope

This research focuses on:

- **Geographic Scope:** Uganda, specifically the 50 districts covered by the Uganda Livestock Information Tracking System (ULITS)
- **Disease Scope:** Foot-and-Mouth Disease as the primary use case for the early warning system
- **Temporal Scope:** Historical FMD data from 2011-2024 for model training and validation
- **Technical Scope:** Integration of PySyft for federated learning, Hyperledger Fabric for blockchain verification, and design of a complete system architecture

### 0.6.2 Limitations

- **Data Quality:** The system's predictions depend on the quality and completeness of data collected by veterinary officers across districts



- **Network Assumptions:** While designed for low-connectivity environments, the system assumes some level of periodic internet access for model synchronization
- **Scalability Testing:** Evaluation will be conducted with up to 50 nodes (representing districts); larger-scale deployment may require additional optimization
- **Honest Majority:** The Byzantine fault tolerance mechanisms assume that at least 51% of participants act honestly
- **Single Disease Focus:** While the architecture is generalizable, validation will focus specifically on FMD prediction

## CHAPTER 2: LITERATURE REVIEW

### 0.7 Introduction

This chapter reviews existing research on federated learning, blockchain technology, and their applications in disease prediction systems. The review identifies key contributions, technological approaches, and critical gaps that this research aims to address.

### 0.8 Federated Learning in Disease Prediction

#### 0.8.1 Kapalaga et al. (2024) – A Unified FMD Dataset

The dataset presents a national FMD dataset that is not only a collection of various data sourced from different regions and sources but also a major step towards overcoming the problem of fragmentation.

Moreover, they indicate that the performance of standard ML models suffers heavily when the distribution of important input variables (like rainfall, temperature) changes over time, thus arguing the necessity of models that are capable of dealing with non-stationary data.

**Gap:** The research is solely centralized, thus all data is obtained and managed in one location. The study did not consider federated learning (FL) and decentralized data processing which could help mitigate concerns regarding data privacy and network inefficiencies, particularly in low-resource areas with inadequate connectivity.

### 0.9 Blockchain-Enabled Federated Learning Systems

#### 0.9.1 Zhang et al. (2023) – Blockchain-Based FL

The authors propose a blockchain-based system for federated learning, which aims at the preservation of privacy as well as the fairness of all parties involved. The setup combines blockchain with crypto-based methods such as verifiable random functions (VRFs) and zero-knowledge proofs (ZKPs) to provide fairness and confidentiality during the training of the model.

**Gap:** Despite the fact that privacy and fairness are mentioned as main advantages, the paper still does not consider the application domains of early warning systems, which are real-world situations, nor does it offer an end-to-end architecture for implementation in actual, low-resource areas such as agriculture or disease prediction.

### 0.9.2 Chen et al. (2024) – FLock System

The system demonstrates the creation of a strong privacy-preserving scenario in federated learning setup using blockchain state channels, resistant to model poisoning.

**Gap:** The emphasis is on secure aggregation and robustness, rather than on creating a complete early warning system with real-time estimations and domain-specific functionality.

## 0.10 Federated Learning in Healthcare

### 0.10.1 Teo et al. (2024) – FL in Healthcare

The paper presents a meticulous examination of the role of federated learning in healthcare through the lens of 612 studies. It points out the main issues and challenges encountered by FL in healthcare, including but not limited to interoperability, legislative barriers, and lack of actual application.

**Gap:** Despite being very informative about FL in healthcare, the paper does not elaborate on an integrated system that uses both blockchain and FL for decentralized early warning systems.

## 0.11 Summary of Research Gaps

I spotted three major areas where current research is lacking through my literature review, which my research proposes to cover:

1. **The Application Gap:** The frameworks are showcasing the implementation of blockchain in federated learning for general purposes; however, there is no dedicated system for livestock disease prediction. The present technologies are either theoretical or healthcare-centric, thereby creating an urgent demand for a specialized system suited to the agriculture sector for early warning.
2. **The Trust-Verification Gap:** The systematic reviews keep mentioning the privacy advantages of current federated learning research, but they do not come along with the built-in means for the verification of model integrity and the participants' compliance with the protocols.
3. **The Practical Efficiency Gap:** The majority of the proposed frameworks are computationally intensive and not designed to meet the real-world conditions in developing areas. There is no design for a system that is lightweight and efficient at the same time that could operate despite network limitations and resource constraints.

## **0.12 Chapter Summary**

This literature review reveals significant progress in both federated learning and blockchain technologies, but identifies critical gaps when these technologies are applied to real-world early warning systems in resource-constrained environments. The next chapter presents the methodology for addressing these gaps through systematic design, implementation, and evaluation of an integrated system.

## CHAPTER 3: RESEARCH METHODOLOGY

### 0.13 Introduction

This chapter outlines the research methodology for designing, implementing, and evaluating a blockchain-secured federated learning system for disease early warning. The methodology follows a systematic approach encompassing system architecture design, prototype implementation, and comprehensive performance evaluation.

### 0.14 Research Design

This study adopts a design science research methodology, which is appropriate for creating and evaluating new artifacts in information systems. The research follows an iterative process of:

1. Problem identification and motivation
2. Objectives definition
3. Design and implementation
4. Demonstration
5. Evaluation
6. Communication

### 0.15 System Architecture

We will design a layered architecture that strategically separates concerns while maintaining integration between federated learning and blockchain components:

- **Data Layer:** Local data remains on farm systems with standardized interfaces for secure access
- **Federated Learning Layer:** Model training occurs locally with secure aggregation protocols
- **Blockchain Layer:** Hyperledger Fabric will provide the trust foundation for recording model hashes and verification
- **Application Layer:** Early warning dashboard and alert system

## 0.16 Prototype Implementation

The theoretical design will be made real through working prototype implementation using technologies that are robust and suitable for the practical world:

- **PySyft** for federated learning module as it is designed for privacy-preserving artificial intelligence
- **Hyperledger Fabric** as blockchain platform for quick, private transactions without excessive computing power
- **Django** for backend management and **React.js** for web-based dashboard

## 0.17 Performance Evaluation

We will conduct comprehensive testing across three key dimensions:

1. **Model Accuracy:** Compare prediction performance using F1-score, precision, and recall metrics
2. **System Efficiency:** Measure communication overhead, training convergence time, and computational resource usage
3. **Security Analysis:** Test robustness against model poisoning attacks and privacy preservation

# 1 Timeline and Work Plan

My research will span roughly two years, with each phase building naturally on what came before.

## 1.1 Phase 1: Foundation (Months 1-4)

The first few months are about getting my bearings and laying solid groundwork. I will spend time deeply understanding what others have done, making sure I am not reinventing wheels, and getting access to the data I need.

By the end of month four, I should have a clean, unified dataset sitting on my computer, ready to be split up and used for training.

## 1.2 Phase 2: Building the Core (Months 5-9)

This is where things get real. I will start coding, first getting a basic federated learning system working without any of the fancy blockchain stuff. Once that is solid, I will layer in the blockchain.

It is tempting to try to build everything at once, but I have learned that leads to impossible-to-debug messes. Better to get one piece working perfectly before adding the next layer.

## 1.3 Phase 3: Making It Secure (Months 10-13)

Now I will make the system genuinely privacy-preserving and resistant to attacks. I will implement differential privacy, carefully calibrating how much noise to add.

For differential privacy, the key equation is:

$$\Pr[\mathcal{M}(D) \in S] \leq e^\epsilon \cdot \Pr[\mathcal{M}(D') \in S] + \delta \quad (1)$$

where  $\mathcal{M}$  is our mechanism,  $D$  and  $D'$  are neighboring datasets differing by one record,  $\epsilon$  controls privacy loss, and  $\delta$  is a small failure probability.

For aggregation, if we have  $N$  clients and client  $i$  sends update  $\theta_i$  with local dataset size  $n_i$ , standard federated averaging computes:

$$\theta_{global} = \frac{\sum_{i=1}^N n_i \theta_i}{\sum_{i=1}^N n_i} \quad (2)$$

## 1.4 Phase 4: Making It Adaptive (Months 14-16)

For each district  $d$  at time  $t$ , I will track the validation loss  $L_d^{(t)}$  over a sliding window. If the moving average suddenly increases beyond a threshold:

$$\frac{1}{w} \sum_{k=t-w}^t L_d^{(k)} > \mu + 2\sigma \quad (3)$$

where  $\mu$  and  $\sigma$  are historical mean and standard deviation, that signals drift.

## 1.5 Phase 5: Making It Real (Months 17-20)

I will test whether the system actually works under realistic conditions—slow internet, machines that crash, participants who drop offline mid-training. I will also build the dashboard where veterinary officers can see predictions and explanations.

## **1.6 Phase 6: Testing Everything (Months 21-23)**

Now I run every experiment I can think of. How accurate is the system compared to centralized training? What happens if 30% of participants try to sabotage the model?

## **1.7 Phase 7: Writing and Wrapping Up (Month 24)**

The final stretch is writing the thesis, preparing papers for publication, and releasing the code and datasets publicly.

## **1.8 Expected Contributions and Deliverables**

### **1.8.1 Scientific Contributions**

I will be creating the first complete blueprint for combining federated learning with blockchain verification in a way that actually handles real-world messiness. The architecture I design, the lessons I learn, and the benchmark performance numbers I establish—all of that becomes a foundation others can build on.

### **1.8.2 Technical Contributions**

The open-source code I release will be production-ready. A researcher in Kenya can download my code, plug in their own data, and have a working system in days instead of months.

### **1.8.3 Practical Impact for Uganda**

There is a direct outcome: a working early warning system that could help prevent livestock disease outbreaks. But the bigger impact is demonstrating that Uganda does not have to ship its data abroad to benefit from AI.

### **1.8.4 Global Relevance**

The challenges I am tackling—intermittent internet, limited resources, privacy regulations, the need for trust—these are not unique to Uganda. If I can prove that sophisticated AI works in these conditions, that removes a massive barrier for most of the world.



## 1.9 Evaluation Metrics

### 1.9.1 Model Performance Metrics

**Precision and Recall:** For binary classification:

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}}, \quad \text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} \quad (4)$$

**F1-Score:** The harmonic mean:

$$F_1 = 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}} \quad (5)$$

Target: F1-score above 0.80, AUC-ROC above 0.85.

### 1.9.2 Privacy Metrics

**Differential Privacy Budget:** Track cumulative  $\epsilon$  over training rounds, targeting  $\epsilon < 10$ .

**Membership Inference Attack Success Rate:** Measure if attackers can identify whether specific farm data was in training set.

### 1.9.3 Fairness Metrics

**Gini Coefficient:** Measures inequality in district selection frequency. Target below 0.3.

**Performance Equity:** Variance in F1-scores across districts. Lower variance means more equitable performance.

### 1.9.4 Efficiency Metrics

**Communication Overhead Ratio:**

$$\text{Overhead Ratio} = \frac{\text{Bytes in FL}}{\text{Bytes in Centralized}} \quad (6)$$

Expect ratio less than 0.1 (90% bandwidth reduction).

**Training Time:** Target under 30 minutes per round on realistic hardware.

### 1.9.5 Robustness Metrics

**Accuracy Under Attack:** For  $p$  fraction of malicious clients:

$$\text{Robustness Score} = \frac{\text{Accuracy with attack}}{\text{Accuracy without attack}} \quad (7)$$

Aim to maintain above 0.80 even with 40% attackers.

## 2 Ethical Considerations

### 2.1 Protecting Privacy

I will be transparent about limitations. All personally identifiable information will be stripped from datasets before analysis.

### 2.2 Informed Consent

Every participant will receive clear explanations of what the system does, what risks exist, and their right to withdraw. University ethics board approval will be obtained before human-subjects research.

### 2.3 Avoiding Harm

The system will generate predictions as decision-support tools, not autonomous decisions. Veterinary officers retain final judgment. Built-in explanations help users evaluate predictions.

### 2.4 Fair Access to Benefits

All software and research outputs will be released under open-source licenses. The system must work even with intermittent connectivity to serve all districts equitably.

### 2.5 Environmental Responsibility

Hyperledger Fabric uses practical Byzantine fault tolerance, not energy-intensive proof-of-work. Federated learning reduces data center energy consumption by keeping data local.

## 3 Scope and Limitations

### 3.1 Research Scope

**Geographic:** Uganda, specifically districts with ULITS infrastructure.

**Disease:** Foot-and-mouth disease as primary use case.

**Temporal:** Historical data 2011-2024; system designed for ongoing operation.

**Technical:** Integration of federated learning and blockchain with differential privacy, robust aggregation, and adaptation mechanisms.

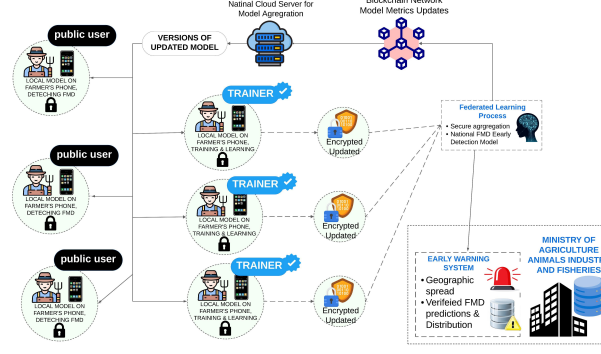


Figure 1: System workflow showing local data preparation, federated model training, blockchain verification, secure aggregation, and early warning generation. Data never leaves local farms while maintaining verifiable trust through blockchain recording.

### 3.2 Limitations

**Full Production Deployment:** Beyond scope; requires additional resources and partnerships.

**Attack Coverage:** Testing common Byzantine attacks, but cannot cover all possible threats.

**Assumption of Honest Majority:** System requires fewer than 50% of participants to be malicious—a fundamental limitation of distributed consensus.

**Scalability:** Testing up to 50 client nodes; larger scale may reveal additional bottlenecks.

### 3.3 Future Directions

This research enables extensions to other diseases, multi-country monitoring, real-time sensor integration, advanced personalization, and economic sustainability mechanisms.

## 4 Process Workflow

The workflow in Fig. 1 ensures data privacy while maintaining accountability through blockchain-recorded model updates and aggregation steps.

## 5 Conclusion

This research addresses a fundamental challenge in modern AI: how to build intelligent systems that learn from distributed data without compromising privacy, security, or fairness. By combining federated learning with blockchain verification, we create a trustworthy foundation for collaborative machine learning in high-stakes domains.

The livestock disease use case provides a rigorous testbed with real challenges. Success here demonstrates principles applicable far beyond agriculture. We are pioneering a new paradigm for decentralized AI where data ownership remains with those who generated it, contributions are verifiably fair, systems adapt to changing conditions, and trust is earned through transparency.

The outcome will be open-source tools, empirical evidence, and practical insights that advance privacy-preserving machine learning while delivering tangible benefits to Ugandan livestock keepers.

## References

- [1] T. Kapalaga, M. Mubangizi, and P. Kisaakye, “A Unified Foot and Mouth Disease Dataset for Uganda: Evaluating Machine Learning Predictive Performance Degradation Under Varying Distributions,” *Frontiers in Artificial Intelligence*, vol. 7, 2024.
- [2] Y. Liu, X. Qu, and G. Chen, “Blockchain-Based Practical and Privacy-Preserving Federated Learning with Verifiable Fairness,” *Mathematics*, vol. 11, no. 5, p. 1091, 2023.
- [3] R. S. Antunes, C. A. da Costa, and A. Küdde, “Federated Machine Learning in Healthcare: A Systematic Review,” *ACM Computing Surveys*, vol. 55, no. 5, pp. 1–35, 2022.
- [4] R. Chen, Y. Li, and M. Zhang, “FLock: Robust and Privacy-Preserving Federated Learning based on Practical Blockchain State Channels,” *Cryptology ePrint Archive*, Paper 2024/1797, 2024.
- [5] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. Arcas, “Communication-Efficient Learning of Deep Networks from Decentralized Data,” in *Proc. 20th Int. Conf. Artificial Intelligence and Statistics (AISTATS)*, 2017.
- [6] K. Bonawitz *et al.*, “Practical Secure Aggregation for Privacy-Preserving Machine Learning,” in *Proc. ACM SIGSAC Conf. Computer and Communications Security*, 2017.
- [7] P. Kairouz *et al.*, “Advances and Open Problems in Federated Learning,” *Foundations and Trends in Machine Learning*, vol. 14, no. 1–2, pp. 1–210, 2021.
- [8] C. Dwork and A. Roth, “The Algorithmic Foundations of Differential Privacy,” *Foundations and Trends in Theoretical Computer Science*, vol. 9, no. 3–4, pp. 211–407, 2014.

- [9] Hyperledger Foundation, “Hyperledger Fabric,” [Online]. Available: <https://www.hyperledger.org/use/fabric>

## About the Author



**Muhindo Mubaraka** received his B.Sc. in Computer Science from the Islamic University of Technology, Bangladesh, in 2022. He is currently pursuing a Master of Science in Computer Science at Makerere University. He works as a software engineer and his research interests include federated learning and blockchain technology.