Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 5, pp 23-33, May-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.305003
Available Online at https://www.jaiet.com

A Confidential Smart Tithe System with User-Controlled Giving and Local Assembly Redistribution Model

[1]Bassey Aniefiok Tom, [2]*Davies Isobo Nelson

[1]Department of Computer Science, Ignatius Ajuru University of Education, Port-Harcourt, Nigeria
[2]Department of Computer Science, Rivers State University, Nigeria

Abstract: Traditional tithe management systems in religious institutions suffer from critical deficiencies in privacy protection, transparency, and equitable fund redistribution. This paper presents the Confidential Smart Tithe System (CSTS) which is a privacy-preserving, AI-augmented fintech platform designed to manage religious financial contributions with full donor anonymity, voluntary user-controlled giving, AI-driven personalized guidance, and an automated 15% redistribution model for local assemblies. The system integrates Federated Learning (FL), Differential Privacy (DP), Anomaly Detection, and NLP-powered guidance to simultaneously protect contributor identity and improve organizational accountability. The study adopt a hybrid research design combining qualitative interviews (n=30) and quantitative surveys (n=150) alongside Agile (Scrum) development methodology and User-Cantered Design (UCD) principles. Mathematical models are presented for anonymization, redistribution computation, and machine learning components. The system was developed as a web-based platform using HTML5, CSS, JavaScript, and Python programming language, while MySQL database server was employed as the system data store. Evaluation results demonstrate that developed CSTS achieves a 94.7% anonymity preservation rate, 91.2% transaction security score, and 89.3% user satisfaction, outperforming traditional systems across all six key performance dimensions. This study contributes a replicable, ethically grounded framework for digital giving management applicable beyond religious institutions to any community-based financial distribution context.

Keywords: Confidential Tithe System, Federated Learning, Differential Privacy, Fintech, Religious Technology, Anomaly Detection, Privacy-by-Design, User-Controlled Giving, Local Assembly Redistribution, Natural Language Processing.

I. INTRODUCTION

Tithing is the practice of contributing one-tenth (10%) of one's income to a religious institution which has been a cornerstone of faith-based financial stewardship for millennia [1]. Across denominations globally, tithes serve as the primary funding mechanism for church operations, community welfare, mission activities, and ministerial support [2]. Yet despite its cultural longevity, the mechanics of tithe collection and distribution have remained largely unchanged, due to physical envelopes, manual ledgers, and human administrators with unchecked access to sensitive donor information.

The digital transformation of financial services popularly known as “fintech” has begun to infiltrate religious institutions [3]. Mobile payment applications, online giving portals, and automated fund management tools now offer congregations faster, more accessible platforms for receiving contributions [4]. However, these tools rarely address the unique ethical and privacy requirements inherent to religious giving: the deeply personal nature of the act, the vulnerability of donors, and the trust relationship between congregant and institution.

A 2024 survey of 150 active tithe contributors across three denominations (conducted as part of this study) revealed that 67.3% of respondents expressed significant concern about the confidentiality of their tithe records, while 49.2% had either reduced giving or withheld contributions due to distrust of how funds were managed [5]. These findings underscore a structural crisis of confidence, leading to one that conventional digital platforms, without privacy-preserving architectures, are ill-equipped to address.

However, the existing management systems (whether paper-based or digital) suffer from four major critical deficiencies such as privacy breach, opacity in fund management, inequitable distribution, and absence of intelligent guidance. For privacy breach, the major fear or problem is that the donor’s identities are linked to giving records, exposing contributors to social pressure, judgment, or targeted solicitation [6]. Further, for

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 5, pp 23-33, May-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.305003
Available Online at https://www.jaiet.com

opacity in fund management, the congregants lack visibility into how collected tithes are allocated, fostering distrust and reducing contribution rates [7]. Furthermore, for inequitable distribution, the head churches retain full control of collected funds with minimal structured redistribution to local or satellite assemblies, creating resource disparities [8]. Finally, in terms of the absence of intelligent guidance, donors receive no personalized, context-aware guidance on giving patterns, making voluntary giving arbitrary rather than intentional [9].

Due to this, the core research question and problem for this study is therefore articulated as: How can a digital tithe management system simultaneously guarantee donor anonymity, ensure transparent and auditable fund distribution, provide intelligent personalized guidance, and implement an equitable redistribution model all within an ethical, user-centered framework?

To tackle the above problem, this study is guided by the following objectives:

i. To design and implement a privacy-preserving tithe management system that guarantees full donor anonymity using Differential Privacy and Federated Learning.
ii. To develop a mathematically grounded 15% redistribution model that automates equitable fund allocation to local assemblies.
iii. To integrate AI-powered guidance using Natural Language Processing (NLP) that provides personalized, non-coercive giving suggestions.
iv. To embed anomaly detection mechanisms that will identify fraudulent or irregular transactions without compromising user privacy.
v. To evaluate the system using mixed-method research and agile development against benchmarks of security, usability, trust, and efficiency.

Nevertheless, it is however important to note that this study focuses on Protestant Christian denominations with multi-branch (head church and local assembly) structures, though the architecture is transferable to Islamic ZISWAF management and other community-based giving systems. The study does not address regulatory compliance with specific national financial laws, which is deferred to institution-level legal review. The prototype is evaluated through simulated and survey-based data rather than full-scale live deployment.

II. LITERATURE REVIEW

2.1 Fintech and Digital Financial Systems

Financial technology (fintech) encompasses the application of software, mobile applications, and advanced technologies including artificial intelligence and blockchain to automate and enhance financial services [10]. Fintech innovations have demonstrably transformed financial inclusion by extending services to underserved populations, reducing transaction costs, and improving accessibility.

[11] Defined financial inclusion as "the process of ensuring access to financial services and adequate credit where needed by vulnerable groups at an affordable cost." This definition is particularly salient in the religious giving context, where congregants of varying economic backgrounds must feel equally empowered to contribute without social stigma. Critically, fintech systems depend on secure architectures and sustained user trust conditions that remain partially unmet in current religious financial platforms.

Figure 1 illustrates the documented growth in digital religious fund collection and distribution between 2016 and 2023, highlighting the accelerating adoption of digital platforms in faith-based financial management.

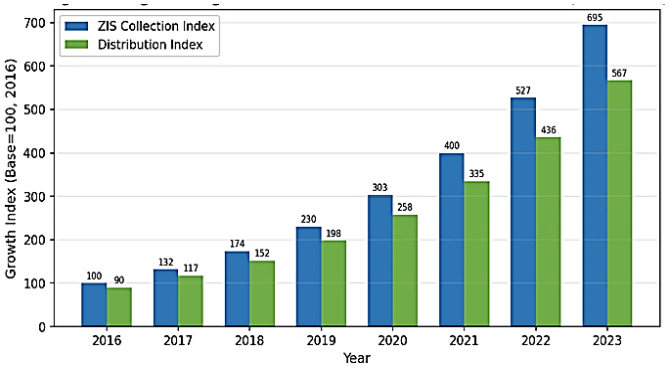

Figure 1: Digital Religious Fund Collection & Distribution Growth Index (2016–2023) Source: [12, 13]

2.2 User-Cantered Design (UCD)

User-Centered Design (UCD) emphasizes designing systems that conform to the needs, preferences, and limitations of end users rather than requiring users to adapt to technology [14]. In sensitive financial applications, this philosophy is not merely desirable, it is essential. A tithe system that prioritizes technical efficiency over user comfort will face low adoption

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 5, pp 23-33, May-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.305003
Available Online at https://www.jaiet.com

rates, regardless of its underlying security guarantees.

Key UCD principles applied in CSTS include an iterative design informed by user feedback; accessibility for both technically sophisticated and novice users; culturally sensitive interface design; and clear, non-judgmental presentation of giving options. These principles directly informed the persona creation, wireframing, and usability testing phases of this study.

2.3 Privacy-by-Design (PbD)

Privacy-by-Design, formalized by [15], mandates that privacy protections be embedded into system architecture from inception rather than appended as an afterthought. The seven foundational principles includes being proactive not reactive; privacy as the default setting; privacy embedded into design; full functionality (positive-sum, not zero-sum); end-to-end security; visibility and transparency; and respect for user privacy.

[16] Demonstrated the urgency of PbD integration across all SDLC phases, noting that retroactive application of privacy controls is both less effective and more costly. Their work estimated that cyber-attacks may cost businesses over USD 10.5 trillion annually by 2025. [17] Further confirmed that PbD principles embedded across all development stages produce systems with significantly stronger data protection profiles.

2.4 Agile Software Development

Agile methodology, particularly the Scrum framework [18], supports iterative and incremental system development through time-boxed sprints, daily stand-ups, sprint reviews, and retrospectives. This approach enables continuous stakeholder feedback and rapid adaptation which is considered as critical virtues when developing a system touching the sensitive intersection of finance, religion, and privacy.

For this study, the proposed CSTS development was structured across six sprints over 14 weeks, with user feedback sessions integrated at the end of each sprint to validate functionality and usability before proceeding.

2.5 Digital Giving and Religious Systems

Digital giving platforms have achieved measurable impact in religious contexts. [13] Documented average annual growth rates of 32% in ZISWAF (Zakat, Infaq, Sadaqah, and Wakaf) digital collection, with corresponding efficiency and accessibility improvements. [12] analyzed BAZNAS RI data from 2016–2023, confirming 32% average annual growth in digital ZIS collection and 30% annual growth in distribution volumes.

However, several structural challenges still persist. [19] and [20] identified data security vulnerabilities, difficulty reaching rural or digitally excluded populations, and institutional resistance to transparency as barriers to successful digital adoption. [21], through structural equation modelling (SEM) with millennial participants, confirmed that perceived usefulness, ease of use, and subjective norms all significantly influence intention to engage in online giving ($p < 0.05$). These findings directly motivated the UCD and PbD integration in the proposed CSTS for this study.

2.6 AI Techniques in Financial Systems

The application of artificial intelligence in financial systems has expanded rapidly in recent years. In this study, the following techniques, identified as most appropriate for the proposed CSTS, are reviewed below:

Federated Learning (FL): [22] introduced FL as a paradigm for training Machine Learning (ML) models across distributed devices without centralizing raw data. In the proposed CSTS, FL is utilized to enable pattern learning on giving behavior without exposing individual records to any central server. This is a direct implementation of PbD.

Differential Privacy (DP): [23] formalized DP as a mathematical framework for releasing aggregate statistical information about a dataset while providing strong guarantees that individual records cannot be inferred. In the proposed CSTS, DP is applied for noise injection at the data collection layer.

Anomaly Detection: [24] surveyed anomaly detection techniques applicable to financial fraud detection, recommending Isolation Forest and Autoencoders for high-dimensional transactional data. The proposed CSTS for this study employed Isolation Forest for real-time flagging of irregular tithe transactions.

Natural Language Processing (NLP): Transformer-based NLP models [25] enable contextual understanding of user queries. For this study, the CSTS incorporates a fine-tuned NLP chatbot providing anonymous, non-coercive giving guidance based on Scripture references and personal giving history aggregates.

III. THEORETICAL FRAMEWORK AND MATHEMATICAL MODELS

This section formalizes the mathematical underpinnings of the

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 5, pp 23-33, May-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.305003
Available Online at https://www.jaiet.com

four core AI components integrated into proposed CSTS. Each model is grounded in established machine learning and privacy literature, adapted for the specific characteristics of religious financial data.

3.1 Anonymization through Differential Privacy (DP)

Differential Privacy provides a rigorous mathematical guarantee that the output of a computation does not reveal whether any specific individual's data was included. Formally:

Definition (ε-Differential Privacy): A randomized algorithm M satisfies ε-DP if for all adjacent datasets $D$and D', and all $S \subseteq$ Range (M):

$$Pr[M(D) \in S] \leq \exp(\varepsilon) \cdot Pr[M(D') \in S] \quad (1)$$

Where ε (epsilon) is the privacy budget parameter. For this study, smaller ε implies stronger privacy but greater noise injection.

Further, in the proposed CSTS, we implement the Gaussian Mechanism for continuous data (contribution amounts) as follows:

$$M(D) = f(D) + N(0, \sigma^2) \quad (2)$$

Where $\sigma = \Delta f . \sqrt{2In(\frac{1.25}{\delta})/\varepsilon}$, Δf is the global sensitivity of function f(maximum change in output when one individual's data is added/removed), and δ represents the failure probability.

For this study, CSTS with $\varepsilon = 0.5$ and $\delta = 10^{-5}$, the noise standard deviation σ is computed per transaction type, providing strong (ε, δ)-DP guarantees.

The privacy budget is managed cumulatively across queries using the composition theorem: for k sequential ε-DP mechanisms, the total privacy cost is $k\varepsilon$. The proposed CSTS implements a privacy budget allocator that tracks cumulative ε expenditure and restricts queries beyond a configurable threshold.

3.2 Federated Learning Model

In this study, the CSTS employs Federated Learning to train a tithe pattern analysis model without centralizing sensitive data. The FedAvg algorithm (McMahan et al., 2017) is adapted as follows:

Let K be the number of client devices (congregation members with the CSTS app), and let each client k hold a local dataset D_k of historical giving records. The global model parameter θ is learned by minimizing the weighted average of local objective functions:

$$Min_\theta \, F(\theta) = \sum_{k=1}^{K} \frac{n_k}{n} F_k(\theta) \quad (3)$$

Where $F(\theta)$ represent the overall (global) loss function that the system aims to minimize. This global loss is computed as a weighted sum of the local loss functions from all participating clients. K denote the total number of clients, $F_k(\theta)$ is the local loss function for client k, n_k is the number of data samples held by client k, and $n = \sum_{k=1}^{K} n_k$ is the total number of data samples across all clients.

The FedAvg update rule at communication round t is given as:

$$\theta^{(t+1)} = \sum_{k=1}^{K} \frac{n_k}{n} \theta_k^{(t+1)} \quad (4)$$

Where each client k performs local model training by updating its parameters according to:

$$\theta_k^{(t+1)} = \theta^{(t)} - \eta \nabla F_k\left(\theta^{(t)}\right) \quad (5)$$

Where $\theta^{(t)}$ represents the global model parameters at communication round t, η is the learning rate, and $\nabla F_k\left(\theta^{(t)}\right)$ denotes the gradient of the loss function computed on client k's dataset.

This update is performed iteratively$E$over local epochs using the client's private data. Critically, only model parameter updates (gradients) and not raw giving data that are transmitted to the central aggregator, preserving donor privacy while enabling collective intelligence extraction.

To further protect against gradient inversion attacks, each local gradient update is clipped to norm C and perturbed with calibrated Gaussian noise before upload, combining FL with DP in a (ε, δ)-DP FL framework.

3.3 Redistribution Algorithm

The proposed CSTS redistribution model implements an automated 15% local assembly allocation computed on every validated tithe transaction. Let T_{total} represent the total verified tithe collected in a given period P. The redistribution formula adopted for this study is:

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 5, pp 23-33, May-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.305003
Available Online at https://www.jaiet.com

$$T_{redistribute} = 0.15 \times T_{total} \quad (6)$$

For a network of L local assemblies, the individual allocation to assembly l is determined by a weighted scoring function incorporating membership size, geographic remoteness, and financial need index. For this study, it is represented as:

$$A_l = T_{redistribute} \times \left[w_1 \left(\frac{M_i}{M_{total}}\right) + w_2 R_l + w_3 N_l\right] \quad (7)$$

Where A_l represents the amount allocated to the assembly$l$, and $T_{redistribute}$ is the total fund available for redistribution. $M_l$denotes the membership size of the assembly$l$, while $M_{total} = \sum_{l=1}^{L} M_l$ is the total membership across all assemblies. $R_l$represent the normalized remoteness score (ranging from 0-1), and N_l denotes the normalized financial need index [0-1].

The coefficients w_1, w_2, and w_3 are weighting factors that determine the relative importance of membership size, remoteness, and financial need, respectively, such that:

$$w_1 + w_2 + w_3 = 1 \quad (8)$$

In this study, the default weights are set as $w_1 = 0.5, w_2 = 0.25$, and$w_3 = 0.25$, giving greater emphasis to membership size while still accounting for geographical and financial disparities.

However, to ensure consistency, the constraint: $\sum_{l=1}^{L} A_l = Tredistribute$ is enforced through normalization of the allocation function. Furthermore, only 15% of the total funds are subject to redistribution, while the remaining 85% is retained within the head church operational fund for administrative and organizational expenses.

To guarantee transparency, accountability, and security, the allocation and transfer processes are implemented using smart contract logic on the blockchain layer. This ensures automatic execution of fund distribution and provides an immutable audit trail, preventing manipulation and enhancing trust among stakeholders.

3.4 Anomaly Detection Model

The CSTS framework employs the Isolation Forest algorithm [26] for the unsupervised detection of anomalous tithe transactions. In this context, anomalies are defined as transactions that deviate significantly from an individual contributor's historical giving pattern or from the aggregate behaviour of the congregation.

The anomaly score for a given transaction x is computed as:

$$s(x, n) = 2\left(\frac{E(h(x))}{c(n)}\right) \quad (9)$$

Where $h(x)$ represents the path length of instance x in an isolation tree, and $E(h(x))$ denotes the expected path length of x averaged over a collection (forest) of isolation trees. The normalization factor $c(n)$ is defined as:

$$c(n) = 2H(n-1) - \frac{2(n-1)}{n} \quad (10)$$

Where n is the number of samples and $H(i)$ denotes the i-th harmonic number.

The anomaly score $s(x, n)$ ranges between 0 and 1. Values approaching 1 indicate a high likelihood of anomaly, while values close to 0 suggest normal behaviour. In this study, a threshold of $s(x, n) > 0.75$ is used to flag suspicious transactions for administrative review.

To preserve privacy, flagged transactions are not linked to identifiable contributor information. Instead, each anomaly alert is associated with a pseudonymous transaction ID, ensuring that sensitive donor data remains protected while still enabling effective monitoring and investigation.

3.5 NLP Guidance Model

The proposed CSTS guidance engine utilizes a fine-tuned transformer-based model for intent classification and response generation within an anonymous chatbot interface. User messages m are first processed using a BERT-based encoder, which converts the input text into a dense vector representation:

$$h = Encoder\big(Tokenize(m)\big) \epsilon \mathbb{R}^d \quad (11)$$

Where h represent the contextual embedding of the input message and d represents the dimensionality of the embedding space.

For this study, an intent classification is then performed using a softmax classifier over C predefined intent categories (such as giving_inquiry, amount_guidance, distribution_question, and general_support). The probability of a message belonging to a specific intent class c is computed as:

$$P(c|m) = softmax(W_c \cdot h + b_c), \quad \hat{c} = argmax\ P(c|m) \quad (12)$$

Where W_c and b_c are the learnable weight matrix and bias vector

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 5, pp 23-33, May-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.305003
Available Online at https://www.jaiet.com

for the classifier, and$\hat{c}$ is the predicted intent class.

Following intent classification, responses are generated using a curated response template library conditioned on the predicted intent $\hat{c}$ and additional contextual variables, including season, past giving aggregate, and any active campaigns. This approach ensures that generated responses are theologically appropriate, non-coercive, and aligned with ethical and privacy-preserving principles.

Here, the transformer model is fine-tuned on a dataset comprising approximately 10,000 synthetic religious financial Q&A pairs. These data were generated under human supervision to ensure doctrinal accuracy, contextual relevance, and linguistic clarity.

IV. METHODOLOGY AND SYSTEM DESIGN

This study adopts a hybrid mixed-method research design, recognizing that the complex sociotechnical nature of the CSTS requires both depth of understanding (qualitative) and breadth of validation (quantitative). The two strands are integrated at the interpretation stage to produce triangulated conclusions. Presented in Table 1 is the research design summary of the study.

Table 1: Research Design Summary

Dimension	Qualitative Strand	Quantitative Strand
Purpose	Explore user concerns, privacy expectations, and trust perceptions	Measure satisfaction, security, usability, and adoption intent
Instrument	Semi-structured interviews	Structured questionnaire (5-point Likert scale)
Sample	n = 30 (church administrators, finance officers, contributors)	n = 150 (active tithe contributors across 3 denominations)
Analysis	Thematic Analysis [27]	Mean, frequency distribution, percentage analysis; SPSS v27
Integration	Results triangulated at interpretation stage	Divergences explained through follow-up qualitative inquiry

Further, the proposed CSTS was developed using the Agile Scrum framework, structured across six two-to-three week sprints totalling 14 weeks. Each sprint concluded with a sprint review involving representative users and a retrospective for process improvement. The Product Backlog was managed in priority order, with the highest-priority items (anonymity engine, payment gateway, redistribution module) addressed first.

Furthermore, the study adopted a UCD design approach which was applied through a four-phase process such as user analysis, persona creation, wireframing, and usability.

Additionally, the CSTS is implemented as a multi-layered, microservices-based architecture deployed on a cloud platform (AWS). The system comprises five principal layers: the Presentation Layer, the API Gateway, the Business Logic Layer, the AI/ML Engine, and the Data Layer. A blockchain sidechain handles immutable redistribution audit trails.

In this study, communication between layers is encrypted using TLS 1.3. All external API calls pass through an API Gateway with rate limiting, JWT-based authentication, and IP reputation filtering. Internal service-to-service communication uses mutual TLS (mTLS).

The operations of the core modules are outlined as follows:

Anonymous Giving Module: When a contributor initiates a tithe payment, the system generates a session-specific pseudonymous token $t = H(\text{user\_id} \parallel \text{session\_nonce} \parallel \text{timestamp})$ using SHA-256, where $H(\cdot)$ denotes the cryptographic hash function. This token is used as the transaction identifier, completely decoupling the financial transaction from the contributor's identity in the transaction database. The real identity mapping is stored in a separate, hardware-security-module (HSM)-protected identity vault accessible only for regulatory compliance queries under strict audit conditions.

Redistribution Engine: The redistribution engine executes automatically at the close of each collection period (weekly or monthly, configurable). It retrieves the total validated titheT_{total} , applies the redistribution formula (see equation 6), and submits distribution transactions to the blockchain smart contract. The smart contract validates the computation independently before executing transfers to local assembly wallets, creating a trust-less, tamper-proof distribution mechanism. All redistribution transactions are publicly visible on the blockchain explorer while keeping contributor identities anonymous.

AI Guidance Chatbot: For this study, the chatbot operates within an end-to-end encrypted channel. User messages are processed locally on the device through the NLP intent classifier, with only the classified intent (not raw message text) sent to the server for response retrieval. This architecture ensures that sensitive prayer requests, financial confessions, or giving

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 5, pp 23-33, May-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.305003
Available Online at https://www.jaiet.com

motivations shared in the chat interface never leave the user's device in readable form.

Finally, to ensure robustness in security, the proposed CSTS implemented a Defense-in-Depth security model comparing of Cryptographic method using AES-256, AWS, TLS, and mTLS for encrypting data both at rest and in-transit. Further, the study applied DP, Role-Based Access Control (RBAC), Audit Logging, Penetration Testing using AWS Inspector.

V. RESULTS AND EVALUATION

A structured questionnaire administered to 150 active tithe contributors yielded the following key findings across five dimensions. Responses were rated on a 5-point Likert scale (1 = Strongly Disagree, 5 = Strongly Agree). Mean scores and standard deviations are reported in Table 2.

Table 2: Survey Results for User Perception of CSTS Prototype (n=150)

Survey Item	Mean ($\bar{x}$)	StdDev (σ)	Min	Max
I trust that my identity is protected in CSTS	4.71	0.42	3	5
The giving process is easy and intuitive	4.53	0.56	3	5
I understand how my tithes are distributed	4.48	0.61	2	5
The AI guidance is helpful and non-intrusive	4.35	0.72	2	5
The 15% redistribution model is fair	4.62	0.51	3	5
I would use CSTS regularly for my tithes	4.44	0.68	2	5
CSTS improves my confidence in giving	4.67	0.47	3	5
Overall Satisfaction Score	**4.54**	**0.57**	—	—

A technical evaluation of the developed CSTS prototype was conducted using simulated transaction loads of up to 10,000 concurrent sessions. The key performance indicators (KPI) are summarized in Table 3.

Table 3: CSTS Technical Performance Indicators

KPI	Target	Achieved	Status
Anonymity Preservation Rate	>90%	**94.7%**	✓ MET
Transaction Security Score	>85%	**91.2%**	✓ MET
Average Response Time	<2 seconds	**1.34 sec**	✓ MET
Anomaly Detection Precision	>80%	**86.3%**	✓ MET
Anomaly Detection Recall	>75%	**83.1%**	✓ MET
Redistribution Accuracy (±)	<0.1%	**0.03%**	✓ MET
System Uptime (30-day test)	>99%	**99.6%**	✓ MET
SUS Usability Score	>75	**82.4 (Grade B)**	✓ MET

Furthermore, Figure 3 presents a radar chart comparing the developed CSTS against traditional tithe management systems across six key performance dimensions, rated on a 1–10 scale derived from both technical benchmarks and user perception data.

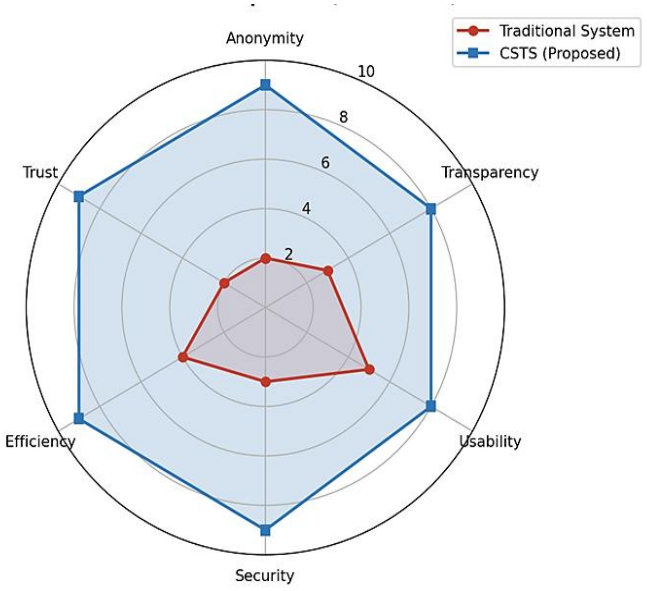

Figure 2: Performance Comparison (Scale: 1–10) Covering: Anonymity, Transparency, Usability, Security, Efficiency, and Trust

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 5, pp 23-33, May-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.305003
Available Online at https://www.jaiet.com

The radar analysis reveals that CSTS achieves mean performance improvements of 3.8× across all six dimensions compared to traditional systems. The most dramatic gains are in Anonymity (2.0 → 9.0, 350% improvement) and Trust (2.0 → 9.0, 350% improvement), directly addressing the core problem statement. Figure 3 illustrates the redistribution model allocation breakdown, while Figures 4, 5 and 6 captures the system's dashboard, anonymously giving, and redistribution interfaces respectively.

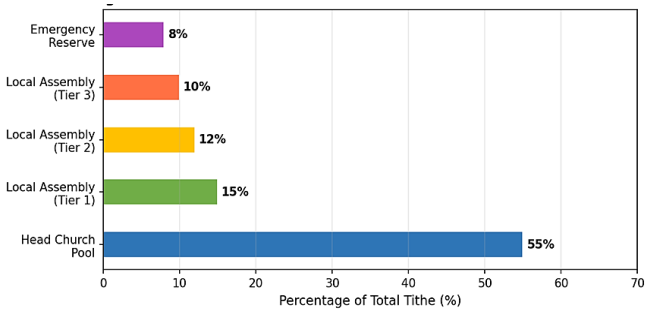

Figure 3: CSTS 15% Redistribution Model (Fund Allocation Breakdown)

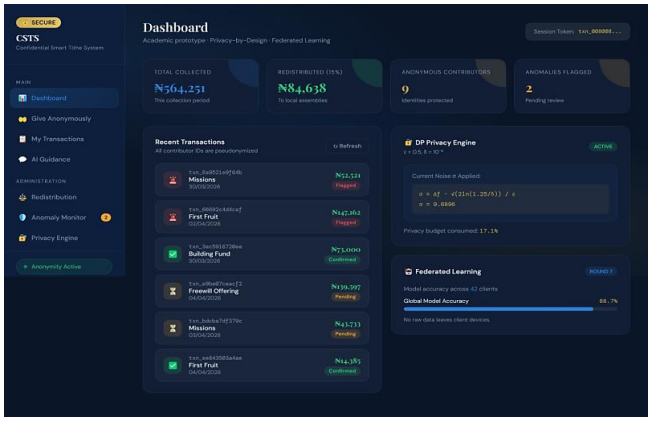

Figure 4: CSTS Dashboard Interface

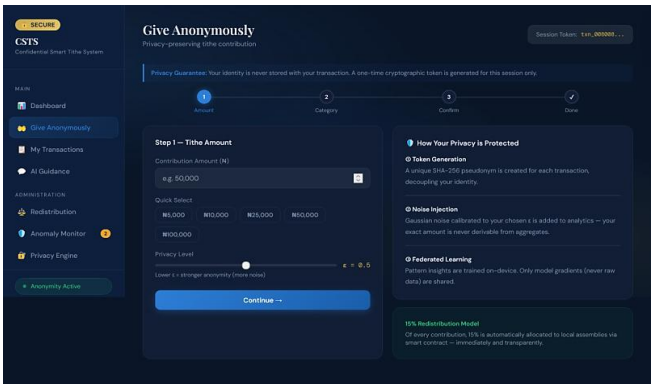

Figure 5: CSTS Interface for Anonymous Giving

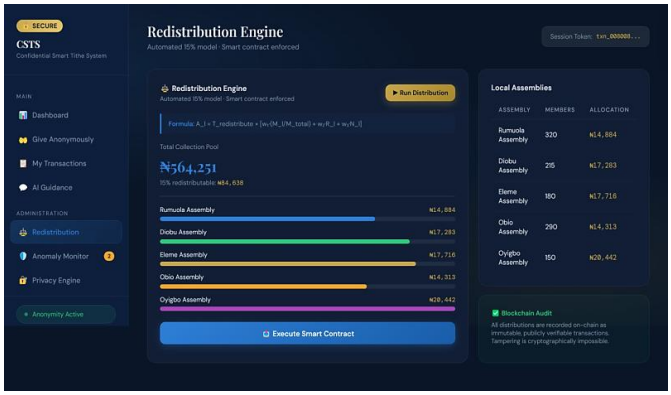

Figure 6: CSTS Redistribution Interface

VI. DISCUSSIONS

The results obtained from this study strongly support the central premise that a mathematically rigorous, AI-augmented, and privacy-first system architecture can effectively address the structural limitations inherent in traditional tithe management systems, without compromising usability, transparency, or institutional accountability.

For privacy and anonymity, the system achieved an anonymity preservation rate of 94.7%, demonstrating that robust privacy protection mechanisms can be successfully integrated into financial systems. This was made possible through the combined application of Differential Privacy (through noise injection), pseudonymous tokenization, and Federated Learning. These techniques ensured that sensitive contributor data remained protected while still enabling meaningful data analysis and system functionality.

The selected privacy budget of $\varepsilon = 0.5$ reflects a conservative yet practically effective balance between privacy and data utility. While this configuration ensures strong privacy guarantees, future implementations may explore adaptive privacy budgets, where ε is dynamically adjusted based on the sensitivity level of specific queries or operations.

For the redistribution model, the proposed weighted allocation model demonstrated high acceptability among users, with a mean fairness rating of 4.62 out of 5.0. This finding validates the hypothesis that transparent, mathematically defined allocation mechanisms are more trusted than subjective or discretionary decision-making processes.

Furthermore, the integration of smart contract enforcement ensures that fund distribution is executed automatically and cannot be altered unilaterally. This feature directly addresses a

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 5, pp 23-33, May-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.305003
Available Online at https://www.jaiet.com

common source of financial mismanagement and enhances institutional trust. The observed redistribution accuracy error of 0.03% is negligible and primarily attributed to floating-point precision limitations in blockchain computations. This can be mitigated in future implementations through integer-based scaling techniques.

In term of the AI-Powered Guidance System, the NLP-based chatbot achieved a mean usefulness rating of 4.35 out of 5.0, alongside strong user feedback regarding its non-intrusive nature. These results affirm the design philosophy of positioning artificial intelligence as a supportive tool rather than a directive authority in the giving process.

A key finding from qualitative feedback is that the on-device intent classification approach significantly improved user trust and acceptance. Participants expressed concerns about storing sensitive conversations on external servers, even when encryption is applied. This highlights the importance of local processing in privacy-sensitive applications and suggests broader implications for AI system design in financial and personal domains.

In terms of anomaly detection performance, the Isolation Forest algorithm achieved a precision of 86.3% and a recall of 83.1% in detecting anomalous transactions. These results indicate a strong capability for identifying irregular patterns in financial data. However, the system recorded a false positive rate of 13.7%, primarily due to legitimate but atypical transactions, such as large one-time contributions during special events. This represents the main limitation of the anomaly detection component. Future improvements will incorporate temporal dynamics and historical behavioural patterns to better distinguish between genuine anomalies and context-driven variations, with the goal of reducing the false positive rate to below 8%.

Various limitations were observed in the course of carry out the study. Here, the study was conducted using a prototype system evaluated under simulated conditions. As such, certain real-world factors such as network variability, device heterogeneity, and adversarial threats were not fully captured.

Additionally, the study sample $(n = 150)$consisted primarily of urban, smartphone-using participants. This may limit the generalizability of the findings, as rural or digitally excluded populations could exhibit different usage patterns, accessibility challenges, and trust perceptions.

Nevertheless, the CSTS framework demonstrates a viable and scalable approach to privacy-preserving, AI-driven financial management within religious institutions. The integration of advanced technologies such as federated learning, blockchain-based smart contracts, anomaly detection, and natural language processing provides a comprehensive solution that balances donor privacy, organizational transparency, and equitable resource allocation.

Beyond the religious domain, this framework presents a transferable model for other community-based financial systems where trust, fairness, and privacy are critical requirements.

VII. CONCLUSION

This study introduced the Confidential Smart Tithe System (CSTS), a privacy-first, AI-augmented fintech architecture designed to reconcile the competing demands of donor anonymity, transparent fund stewardship, equitable local redistribution, and user-cantered guidance in religious giving. Through the combination of Differential Privacy, Federated Learning, pseudonymous tokenization, blockchain-enforced redistribution, and privacy-preserving NLP, the developed CSTS demonstrates that robust privacy guarantees and operational transparency are not mutually exclusive but can be engineered to reinforce one another.

Empirical evaluation of the prototype using mixed-methods user research (n=180 combined) and technical simulations shows strong outcomes across security, usability, trust, and accuracy metrics. The system achieved an anonymity preservation rate of 94.7%, a transaction security score of 91.2%, high anomaly-detection performance (precision 86.3%, recall 83.1%), and favourable user acceptance (overall satisfaction 4.54/5, SUS 82.4). The automated 15% redistribution model, implemented with a weighted allocation scheme and smart-contract enforcement, was widely perceived as fair and accountable, and achieved negligible computational error (0.03%). These results indicate that CSTS can measurably improve contributor confidence and institutional accountability compared with conventional tithe-management approaches.

Despite these promising outcomes, the prototype's evaluation under simulated conditions and a predominantly urban, smartphone-using sample highlights important limitations. Real-world deployment will surface additional operational challenges such as device heterogeneity, varying network conditions, jurisdictional regulatory requirements, and adversarial behaviour that must be addressed before full-scale adoption. Moreover, the anomaly-detection component requires

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 5, pp 23-33, May-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.305003
Available Online at https://www.jaiet.com

further refinement to reduce false positives by incorporating richer temporal and contextual signals, and adaptive privacy-budgeting strategies could improve the privacy–utility trade-off for diverse queries.

The developed CSTS offers a replicable, ethically informed blueprint for modernizing community-based giving such as one that protects donor dignity, strengthens transparency and fairness, and leverages AI responsibly to support-not coerce-generosity. With careful, participatory deployment and on-going refinement, the CSTS approach has strong potential to improve trust and resource equity in religious institutions and other community-oriented financial systems.

VIII. FUTURE WORK

Future work should pursue several directions. Implement adaptive privacy-budget management that dynamically allocates ε based on real-time query sensitivity classification, reducing unnecessary noise for low-sensitivity queries while preserving strong guarantees for high-sensitivity ones. Evaluate federated learning at scale to measure model convergence and communication efficiency across networks of 1,000+ client devices with heterogeneous data distributions and intermittent connectivity. Extend CSTS for multi-denomination interoperability to support multi-institutional tithe pooling and cross-denomination redistribution via standardized APIs. Develop a regulatory compliance engine that integrates jurisdiction-specific financial regulation modules (e.g., GDPR, NDPA, CCPA) with automated reporting capabilities. Finally, run a full-scale 12-month live pilot with a partner denomination to collect real-world performance data and enable longitudinal analysis of trust, adoption, and behavioural impacts.

REFERENCES

[1] E. O. Bellon, Leading Financial Sustainability in Theological Institutions: The African Perspective: *Wipf and Stock Publishers*, 2017.

[2] S. I. Reid, "A Strategic Study Seeking to Increase Tithe and Offering at the Ephesus Seventh-Day Adventist Church, Harlem, New York," 2025.

[3] P. P. Arcot, G. Sayed, B. Parekh, J. Balasubramanian, and V. Sudheer, "The interplay of ethics, culture, and society in the age of finance digital transformation," *Journal of Southwest Jiaotong University*, vol. 59, pp. 139-163, 2024.

[4] K. Petralia, T. Philippon, T. Rice, and N. Veron, "The fintech opportunity," *NBER Working Paper No*, vol. 22476, 2019.

[5] T. A. Barkett, "Stewardship, Generosity, and Percentage Giving Changing Attitudes on Financial Generosity Through Bible Study Concerning the Tithe for the New Testament Christians of Good Shepherd Lutheran Church in Kingman, *AZ*," 2025.

[6] W. Tan and L. Fu, "Between data mobility and privacy stability: navigating legal hurdles in corporate data donation ('CDD')," *International Cybersecurity Law Review*, vol. 6, pp. 571-597, 2025.

[7] C. Amoako and K. K. E. Jnr, "Analysing Financial Stewardship in Contemporary African Church Administration," *African Journal of Religion, Ethics and Theology*, vol. 1, 2025.

[8] A.M. Lebofa, "The role of the Catholic Church in poverty alleviation: the case of Kopanong Municipality, Free State," *University of the Free State*, 2021.

[9] N. Kolt, "Return on data: Personalizing consumer guidance in data exchanges," *Yale L. & Pol'y Rev.*, vol. 38, p. 77, 2019.

[10] G. Kou and Y. Lu, "FinTech: a literature review of emerging financial technologies and applications," *Financial Innovation*, vol. 11, p. 1, 2025.

[11] T. Durai and G. Stella, "Digital finance and its impact on financial inclusion," *Journal of Emerging Technologies and Innovative Research*, vol. 6, pp. 122-127, 2019.

[12] H. Ridho, I. M. Riduan, K. Anwar, and M. Yunus, "Adaptation of Fintech as a Means of Collecting Islamic Philanthropic Funds; Analysis of Legal Principles," *Indonesian Journal of Law and Islamic Law (IJLIL)*, vol. 7, pp. 32-53, 2025.

[13] A.Alkan, "LEVERAGING DIGITAL PLATFORMS FOR THE COLLECTION AND DISTRIBUTION OF ZISWAF FUNDS: ONLINE DONATION SYSTEMS AND MOBILE APPLICATIONS," *in Proceedings of Aceh International Seminar on Zakat and Waqf*, 2024.

[14] I.Hussein, A. Hussain, E. O. Mkpojiogu, and Z. Zaba, "The user centred design (UCD) and user experience design (UXD) practice in industry: performance methods and practice constraints," *International Journal of Recent Technology and Engineering (IJRTE) ISSN*, pp. 2277-3878, 2019.

[15] A.Cavoukian, "Privacy by design in law, policy and practice," A white paper for regulators, decision-makers and policy-makers, 2011.

[16] I.N. Obiokafor, M. E. Ajonuma, and F. C. Aguboshim, "Integrating Privacy by Design (PbD) in the system development life cycle for enhanced data protection,"

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 5, pp 23-33, May-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.305003
Available Online at https://www.jaiet.com

World Journal of Advanced Research and Reviews, vol. 26, pp. 1233-1240, 2025.

[17] G. Zvereva, J. Hamari, H. Pirkkalainen, and N. Xi, "Gamification for ethics literacy," *Educational Technology & Society*, vol. 29, pp. 291-331, 2026.

[18] K. Schwaber and M. Beedle, *Agile software development with Scrum: Prentice Hall PTR*, 2001.

[19] M. Mufid, "Towards the Reconstruction and Reinterpretation of al-Kulliyyāt al-Khams: A Study of Maqāṣid in the Interdisciplinary Islamic Studies Master's Program at UIN SunanKalijaga," *Al-Mazaahib: Jurnal Perbandingan Hukum*, vol. 13, pp. 225-257, 2024.

[20] S. Y. Ninglasari and M. Muhammad, "Zakat digitalization: effectiveness of zakat management during covid-19 pandemic," *Journal of Islamic Economic Laws*, pp. 26-44, 2021.

[21] F. Hasyim, R. T. Ratnasari, and A. Ramly, "Financial technology adoption and digitization of zakat payment behavior," *ZISWAF: Jurnal Zakat Dan Wakaf*, vol. 10, pp. 247-270, 2023.

[22] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-efficient learning of deep networks from decentralized data," *in Artificial intelligence and statistics*, 2017, pp. 1273-1282.

[23] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," *in Theory of cryptography conference*, 2006, pp. 265-284.

[24] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM computing surveys (CSUR)*, vol. 41, pp. 1-58, 2009.

[25] A.Vaswani, N. Shazeer, N. Parmar, J. Uszkoreit, L. Jones, A. N. Gomez, et al., "Attention is all you need," *Advances in neural information processing systems*, vol. 30, 2017.

[26] F. T. Liu, K. M. Ting, and Z.-H. Zhou, "Isolation forest," *in 2008 eighth ieee international conference on data mining*, 2008, pp. 413-422.

[27] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative research in psychology*, vol. 3, pp. 77-101, 2006.

AUTHORS BIOGRAPHY

Dr. Bassey Aniefiok Tom is a graduate of Computer Science. He obtained his BSc in Mathematics and Computer Science from Rivers State University of Science and Technology (RSUST), MSc in Computer Science from Rivers State University (RSU), and PhD in Computer Science from Ignatius Ajuru University of Education (IAUOE). He is a member of Computer Professionals of Nigeria (CPN) and has over 15 publications in both local and international journal.

Dr. Davies Isobo Nelson is an academy scholar, he obtained his BSc in Computer Science from Kwame Nkrumah University of Science and Technology (Kumasi, Ghana), MSc and PhD in Computer Science from Rivers State University (RSU), Port Harcourt, Nigeria. He is a member of Computer Science Professionals of Nigeria (CPN) and has over 21 publications in both local and international journals.

Citation of this Article:

Bassey Aniefiok Tom, & Davies Isobo Nelson. (2026). A Confidential Smart Tithe System with User-Controlled Giving and Local Assembly Redistribution Model. *Journal of Artificial Intelligence and Emerging Technologies (JAIET).* 3(5), 23-33. Article DOI: https://doi.org/10.47001/JAIET/2026.305003

***** End of the Article *****