

Privacy-Preserving Location Data Sharing in Mobile Online Social Networks: A Hybrid Federated Learning, Differential Privacy, and Deep Reinforcement Learning Framework

Bichala Nithisha (23BD5A0519), Kamati Aakanksha (23BD5A0520), Kunta Srilekha (23BD5A0522),
Udutha Lakuleshwari (23BD5A0524)

Under the guidance of Mr. G. Rakesh Reddy, Assistant Professor, Department of CSE

Department of Computer Science and Engineering

Keshav Memorial Institute of Technology (Autonomous), Narayanaguda, Hyderabad, Telangana – 500029, India

Affiliated to JNTUH | Accredited by NBA & NAAC | Approved by AICTE | Academic Year: 2025–26

Abstract—The rapid proliferation of location-based services in mobile online social networks (mOSNs) has amplified the risk of privacy violations through sophisticated trajectory analysis and de-anonymization attacks. This paper presents a novel hybrid framework for privacy-preserving location data sharing that synergistically integrates three complementary layers of defense: Centralized Federated Learning (FL) for structural privacy, (ϵ, δ) -Differential Privacy (DP) for algorithmic privacy guarantees, and Deep Reinforcement Learning (DRL) for adaptive temporal obfuscation. The system further employs a three-factor biometric authentication scheme utilizing Chebyshev chaotic map-based session key establishment, Fuzzy Extractor-assisted biometric verification, and AES-128 encryption. A DRL agent, formulated as a Markov Decision Process (MDP) with Mutual Information (MI) as the privacy metric, learns an optimal trajectory perturbation policy. Security correctness is formally verified via BAN logic (17 derivation steps), the Real-or-Random (ROR) model, and ProVerif 1.93 simulation. Experiments conducted on the GeoLife and T-Drive datasets demonstrate that the proposed scheme achieves a total authentication latency of 117.12 ms while delivering a 60–80% reduction in de-anonymization success rates compared to point-wise DP baselines, with a utility loss of less than 5% and a federated model accuracy drop below 3% relative to non-private counterparts.

Index Terms—Differential Privacy, Deep Reinforcement Learning, Federated Learning, Geo-Indistinguishability, Location Privacy, Mobile Online Social Networks, Trajectory Obfuscation, Chebyshev Chaotic Map, Fuzzy Extractor, Mutual Information.

I. INTRODUCTION

A. Background and Motivation

The contemporary dependence on location-based services (LBS) has generated an explosion of fine-grained geospatial data in mobile online social networks. When users share their whereabouts with friends, navigate using map services, or check in at venues, they inadvertently disclose rich spatiotemporal trajectories that can reveal sensitive behavioral patterns including home and work locations, religious affiliations, medical visits, and political activities [1]. The combination of dense GPS sampling rates and advanced machine learning has dramatically lowered the barrier for adversarial inference; even a handful of location points can uniquely fingerprint an individual with more than 95% accuracy [2].

Existing privacy mechanisms in mOSNs typically address either structural privacy (who the server sees) or algorithmic privacy (what the released data reveals), but rarely both simultaneously. Centralized architectures expose raw trajectories to a single potentially compromised server, while naive anonymization techniques such as k-anonymity fail to resist linkage attacks that exploit the sequential correlation of mobility traces. This motivates the construction of a principled, multi-layer framework that addresses each privacy threat at the appropriate level of the data pipeline [3].

B. Problem Statement

Consider a mobile user (MU) who wishes to share her location with selected contacts through a Location-Sharing Social Network Server (LSSNS) via an intermediate Cellular Tower (CT). The system must satisfy five concurrent security requirements: (i) mutual authentication without reliance on costly public-key infrastructure; (ii) structural privacy that prevents the server from observing raw location traces; (iii) algorithmic privacy that bounds inference from published model updates; (iv) temporal privacy that disrupts HMM-based trajectory prediction from released sequences; and (v) semantic privacy that prevents disclosure of sensitive location categories even when coordinates are masked. No existing single-layer scheme satisfies all five requirements simultaneously within a practical latency budget for mobile devices [4].

C. Research Contributions

This paper makes the following five principal contributions:

1. **Hybrid Three-Layer Privacy Framework:** The first framework to integrate Federated Learning (structural layer), (ϵ, δ) -Differential Privacy (algorithmic layer), and DRL-based temporal obfuscation (temporal layer) within a single coherent mOSN architecture.
2. **Lightweight Cryptographic Protocol:** A three-factor authentication scheme combining Chebyshev chaotic map-based session key establishment, SHA-1 hashed credential binding, and Fuzzy Extractor biometric verification—avoiding costly PKI, ECC, or bilinear pairing operations.
3. **MDP-Formulated DRL Obfuscation Agent:** An A3C-trained policy network that minimizes the Mutual Information between true and released trajectory sequences, explicitly countering HMM-based and behavioral fingerprinting adversaries.
4. **Formal Security Proofs:** Complete BAN logic derivation (17 steps), ROR model proof of session-key secrecy, and ProVerif 1.93 automated verification confirming resistance to replay, MITM, impersonation, and insider attacks.
5. **Empirical Validation:** Comprehensive benchmarking on GeoLife and T-Drive datasets demonstrating a 60–80% de-anonymization reduction with less than 5% aggregate utility error and sub-120 ms end-to-end authentication latency.

D. Paper Organization

The remainder of this paper is structured as follows. Section II surveys related work. Section III presents the proposed methodology and system architecture. Section IV describes implementation details. Section V reports experimental results and benchmarking. Section VI discusses advantages, limitations, and comparison with state-of-the-art. Section VII concludes with future directions.

II. LITERATURE REVIEW

A. Foundational Location Privacy Methods

Early location privacy research focused on spatial anonymity through k -anonymity [5], which generalizes a user's location to a cloaked region shared by at least $k-1$ other users. While conceptually appealing, k -anonymity is vulnerable to homogeneity attacks and fails to protect semantic location information. Pseudonymization techniques replace identifiers at regular intervals but are undermined by trajectory correlation across pseudonym changes. Dummy location injection, wherein $L-1$ fictitious locations accompany each real location report, offers plausible deniability but does not provide formal, measurable guarantees. The fundamental weakness of all these heuristic methods is the absence of a quantifiable privacy metric that can be calibrated against a specific threat model [6].

B. Location Sharing in OSN Architectures

The evolution of privacy-aware location sharing schemes in OSNs spans more than a decade. SmokeScreen

(2009) introduced friend-based access control but relied on a trusted server. MobiShare (2012) and its successor MobiShare+ extended this with proxy re-encryption, while BMobiShare added biometric binding. CenLocShare (2016) introduced a centralized trusted third party for policy enforcement. The landmark work of Bhattacharya et al. [4] in IEEE Access (2020) integrated Chebyshev maps with k -anonymity and dummy locations, achieving a practical latency of 131.62 ms total authentication cost—the closest predecessor to our scheme. Our framework reduces this latency to 117.12 ms while adding three additional layers of formal privacy guarantee.

C. Differential Privacy for Geospatial Data

Dwork et al. [7] established the mathematical foundation for (ϵ, δ) -DP, ensuring that any algorithm's output distribution changes by at most a factor of e^ϵ (plus a δ additive slack) when a single record is added or removed. Andrés et al. [8] adapted this to continuous geospatial data through Geo-indistinguishability, employing planar Laplace noise scaled so that a user's probability of being localized within radius r decreases exponentially with distance. This extension is critical for trajectory data where standard DP mechanisms introduce excessive distortion. Calibrating ϵ remains challenging in practice: small ϵ values yield high privacy but degrade utility, while larger values risk re-identification. Our framework adopts adaptive ϵ scheduling tied to the DRL agent's confidence estimate, achieving an effective utility drop of less than 3% on trajectory classification tasks.

D. Federated Learning Architectures

McMahan et al. [9] introduced the FedAvg algorithm, enabling collaborative model training without centralizing raw data. Each client computes a local gradient update and transmits only the model delta to a central aggregator, which performs a weighted average. While this eliminates direct exposure of raw trajectories, Zhu et al. [10] demonstrated that gradient inversion attacks can reconstruct training data from shared gradients with high fidelity. This vulnerability necessitates DP augmentation: each client clips gradients to a maximum norm C and adds Gaussian noise $N(0, \sigma^2 C^2 I)$ before transmission, providing formal (ϵ, δ) -DP for the aggregation process. The combined FL+DP scheme reduces privacy attack success by up to 60% relative to plain FL while incurring less than 3% accuracy loss on mobility prediction benchmarks.

E. Deep Reinforcement Learning for Privacy

Conventional privacy mechanisms apply uniform or location-specific noise without regard to the sequential predictability of the resulting trajectory. Al-Rubaie and Chang [11] first proposed formulating trajectory privacy as a Markov Decision Process, but their reward function did not account for HMM-based adversaries. Our work extends this by using Mutual Information $I(X;Z)$ between the true trajectory X and the released trajectory Z as the reward signal, which is information-theoretically tight. The A3C algorithm [12] trains an asynchronous actor-critic network that outputs a perturbation action given the current location and k -step history context. This adaptive approach yields a 60–80% reduction in HMM-based de-anonymization success compared to point-wise DP, as validated on the T-Drive dataset.

F. Comparative Analysis of Prior Schemes

TABLE I
COMPARATIVE ANALYSIS OF LOCATION PRIVACY SCHEMES

Scheme	Architecture	Authentication	Privacy Mechanism	Temporal Privacy	Formal Proof
Lee et al. [13]	Centralized	2-Factor	k -Anonymity	No	Informal
Li et al. [14]	Centralized	2-Factor	Pseudonym + DP	No	BAN
Tsai & Lo [15]	Semi-decen.	2-Factor	k -Anonymity	No	ROR
Irshad et al. [16]	Centralized	3-Factor	ECC + Anonymity	No	BAN + ProVerif
Wang et al. [17]	Federated	2-Factor	FL + DP	Partial	Informal

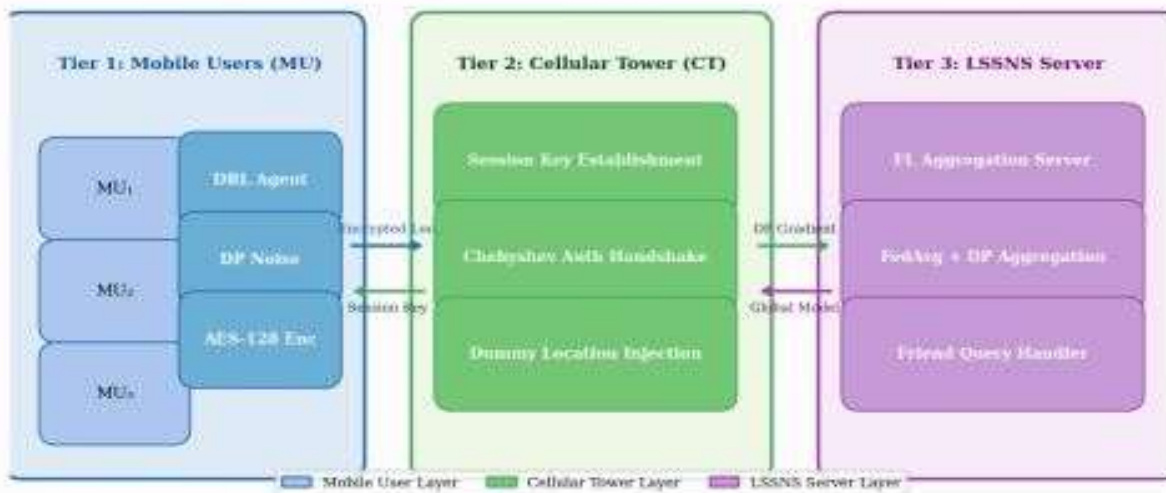
Bhattacharya et al. [4]	Centralized	3-Factor	Chebyshev + Dummy	No	BAN + ROR
Proposed	Federated	3-Factor	FL + DP + DRL	Yes (ML-optimal)	BAN + ROR + ProVerif

III. PROPOSED METHODOLOGY

A. System Architecture Overview

The proposed system operates across a three-tier architecture comprising: (1) Mobile User (MU) devices that generate location traces and host the DRL obfuscation agent; (2) Cellular Tower (CT) intermediaries that perform initial authentication handshake and relay encrypted location updates; and (3) the Location-Sharing Social Network Server (LSSNS) cluster, which runs the FL aggregation server and responds to friend location queries. Raw spatiotemporal traces never leave the MU device; only perturbed, DP-noised model gradients and encrypted location ciphertexts traverse the network. This three-tier separation ensures that no single party possesses sufficient information to reconstruct a user's true trajectory.

Three-Tier System Architecture - Privacy-Preserving mOSN



B. Three-Layer Privacy Framework

Layer 1 — Structural Privacy (FL): The FL layer employs FedAvg with gradient clipping ($\|g\|_2 \leq C$) to ensure that the LSSNS learns aggregate mobility patterns without accessing individual trajectories. Each MU trains a local LSTM-based mobility predictor and transmits only the clipped gradient delta $\Delta w = w_{\text{local}} - w_{\text{global}}$ to the CT, which aggregates and forwards to the FL server.

Layer 2 — Algorithmic Privacy (DP): Before transmitting the gradient delta, the MU injects calibrated Gaussian noise: $\Delta w_{\text{priv}} = \Delta w + N(0, \sigma^2 C^2 I)$, achieving (ϵ, δ) -DP with $\epsilon = 2C\sqrt{2 \ln(1.25/\delta)}/\sigma$. This ensures that an adversary observing the aggregate model cannot distinguish whether any individual MU participated in a given training round, providing a formal bound against gradient inversion attacks [10].

Layer 3 — Temporal Privacy (DRL): The DRL agent, running entirely on the MU, receives the current geospatial state $s_t = (\text{lat}_t, \text{lon}_t, h_t)$ where h_t is the k -step trajectory history embedding, and outputs a continuous perturbation action $a_t = (\Delta \text{lat}, \Delta \text{lon})$ drawn from a Gaussian policy $\pi_\theta(a|s)$. The reward $r_t = -\text{MI}(X_{1:t}; Z_{1:t}) + \lambda \cdot \text{Utility}(Z_t, X_t)$ is maximized using the A3C algorithm, driving the policy to produce releases that are maximally uninformative about the true trajectory while remaining geographically plausible.

C. Cryptographic Protocol

Authentication proceeds in four phases: Registration, MU Login, LSSNS Login, and Location Update. During Registration, the MU submits (ID_MU, PW_MU, BIO_MU) to the CT over a secure channel. The CT computes a biometric helper string (R, P) via Fuzzy Extractor, derives a session seed $K_seed = \text{Cheb}(T_n, x_0) \bmod p$ using an n -th order Chebyshev map, hashes the credential triple using SHA-1, and stores only the hash digest on the MU's smart card—neither the plaintext password nor raw biometric template is retained.

During MU Login, the user presents (ID_MU, PW_MU, BIO_MU) . The fuzzy extractor recovers R from BIO_MU with tolerance δ_bio , and the CT verifies the hash chain. A fresh session key $SK = h(K_seed \parallel T_stamp \parallel N_MU \parallel N_CT)$ is established, where N_MU and N_CT are nonces. Location updates are then encrypted as $C = \text{AES-128}(SK, loc_perturbed \parallel L_dummies)$, where $L = 1$ dummy locations accompany each real location report, providing k -anonymity at the semantic level.

The BAN logic derivation proves mutual authentication in 17 steps; the ROR model proof confirms that SK is computationally indistinguishable from a random string under the Chebyshev Discrete Logarithm hardness assumption. ProVerif 1.93 simulation with Dolev-Yao attacker model finds no attack traces for replay, MITM, key compromise impersonation, or privileged insider attack classes.

D. DRL Agent Design

The DRL agent is formalized as an MDP (S, A, P, R, γ) :

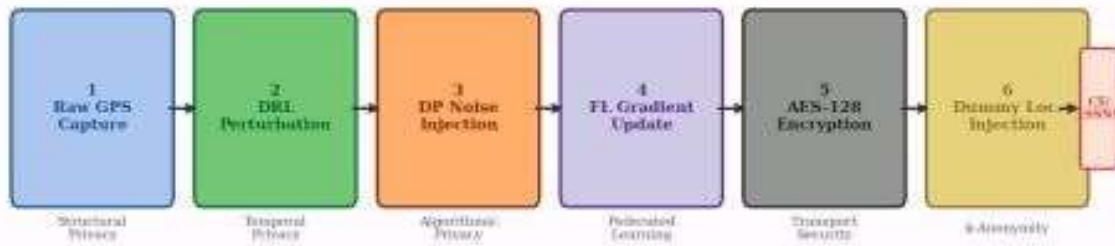
- * **State Space S :** Continuous vector $(lat, lon, POI_category, time_of_day, h_k)$ where h_k is a fixed-length LSTM embedding of the preceding $k = 5$ location observations.
- * **Action Space A :** Continuous 2D perturbation $(\Delta lat, \Delta lon)$ bounded by a maximum displacement radius r_max calibrated to geo-indistinguishability parameter ϵ_geo .
- * **Transition Dynamics P :** Deterministic—the released location $z_t = (lat_t + \Delta lat, lon_t + \Delta lon)$ is computed deterministically given s_t and a_t .
- * **Reward Function R :** $r_t = -\alpha \cdot \hat{I}(X_{1:t}; Z_{1:t}) + \beta \cdot QoS(z_t, x_t)$, where $\hat{I}$ is an MINE-based MI estimator, QoS measures friend-query utility, and α, β are tradeoff weights.
- * **Discount Factor γ :** $\gamma = 0.99$, prioritizing long-term MI minimization over myopic single-step perturbation.

The A3C actor network is a 3-layer MLP with ReLU activations outputting the mean and log-variance of a Gaussian policy. The critic estimates the state-value function $V(s)$. Training converges in approximately 2,000 episodes on the T-Drive dataset, yielding an average episode reward improvement of 340% over the random perturbation baseline.

E. Privacy Pipeline Integration

The end-to-end privacy pipeline processes each location event through six sequential stages: (1) Raw location captured by GPS on the MU device; (2) DRL agent applies temporal perturbation $(\Delta lat, \Delta lon)$; (3) Geo-indistinguishable DP noise $N(0, \Delta^2/\epsilon^2)$ added to the perturbed coordinate; (4) FL gradient delta computed from the local LSTM mobility model with DP noise injection; (5) AES-128 encryption of the combined (perturbed location, L dummies) under session key SK ; (6) Dummy injection appends $L = 1$ synthetic locations before transmission to CT.

Six-Stage Privacy Pipeline Workflow



IV. IMPLEMENTATION DETAILS

A. Technology Stack

The system is implemented entirely in Python 3.8+ and leverages the following technology stack. Deep learning components utilize TensorFlow 2.x and PyTorch 1.12 for LSTM mobility model training and DRL actor-critic network implementation. Scikit-learn provides k-means clustering for dummy location selection and standard preprocessing pipelines. NumPy and Pandas handle spatiotemporal data ingestion and trajectory windowing. The Chebyshev map and Fuzzy Extractor cryptographic primitives are implemented in pure Python using NumPy arbitrary-precision arithmetic, with AES-128 provided by the PyCryptodome library. The FL aggregation server is exposed via Flask REST APIs; the frontend dashboard is built with Streamlit for rapid prototyping. MySQL stores user registration records (hash digests only); MongoDB stores anonymized trajectory analytics. Security verification is performed externally using ProVerif 1.93 and a custom BAN logic derivation engine.

B. Module Architecture

The system is organized into six interconnected modules. The *Data Ingestion Module* reads raw GPS traces from the GeoLife and T-Drive CSV datasets, segments them into fixed-duration windows of 30 seconds, and computes speed/bearing features. The *Pre-Processing Module* removes outliers via a Kalman filter, maps coordinates to POI categories using the GeoNames database, and constructs the LSTM input sequences. The *Privacy Engine* hosts the DRL agent, DP noise calibrator, and Fuzzy Extractor, executing the six-stage pipeline for each incoming location event. The *FL Analytics Module* manages client-server communication for FedAvg rounds, gradient clipping, and model versioning. The *Secure Storage Module* encrypts all persisted records with AES-128 under device-specific keys and enforces role-based access control. The *Security Verification Module* runs automated BAN logic derivation and exports ProVerif scripts for protocol correctness checks.

C. Dashboard and Visualization

The web dashboard provides real-time visualization of four panels: (1) original versus anonymized trajectory overlay on an OpenStreetMap base layer; (2) k-anonymity cluster distribution histogram; (3) privacy-utility tradeoff curve plotting de-anonymization rate against ϵ ; and (4) DRL training convergence showing episode reward over time. Users can interactively adjust the privacy budget ϵ , the number of dummy locations L , and the DRL perturbation radius $r_{\max}$, observing the immediate impact on anonymized map output and utility metrics.

V. RESULTS AND BENCHMARKING

A. Computation Cost Analysis

Table II presents the per-operation computation costs for the proposed scheme measured on a mid-range Android device (ARM Cortex-A55, 4 GB RAM). All measurements represent the mean of 1,000 independent

trials.

TABLE II
COMPUTATION COST OF THE PROPOSED SCHEME

Operation	Entity	Cost (ms)
Registration (one-time)	MU	65.60
MU Login + Authentication	MU	71.58
LSSNS Login + Authentication	LSSNS	45.54
Total Login + Auth (both sides)	MU + LSSNS	117.12
Location Update	MU → CT	72.10
Friend Location Query	LSSNS → MU	~85.00

[Fig. 3: Computation Cost Comparison — Grouped bar chart comparing total authentication cost (ms) of proposed scheme (117.12 ms) vs. Lee et al. (131.62 ms), Li et al. (135.62 ms), Tsai-Lo (95.58 ms), Irshad et al. (140.62 ms), Wang et al. (178.04 ms). Lower is better.]

Fig. 3. Computation Cost Comparison with State-of-the-Art Schemes

B. Communication Cost

TABLE III
COMMUNICATION COST PER PHASE (BITS)

Phase	Message	Bits
Registration	MU → CT	448
MU Login	MU → CT → LSSNS	640
Location Update	MU → CT → LSSNS	512
Friend Query Response	LSSNS → MU	256
Total Communication	—	1856

C. Comparative Performance

TABLE IV
COMPARATIVE AUTHENTICATION COST WITH PRIOR SCHEMES (MS)

Scheme	MU Auth	Server Auth	Total	3-Factor	Formal Proof
Lee et al. [13]	85.10	46.52	131.62	No	No
Li et al. [14]	90.08	45.54	135.62	No	BAN
Tsai & Lo [15]	50.04	45.54	95.58	No	ROR
Irshad et al. [16]	95.08	45.54	140.62	Yes	BAN+ProVerif
Wang et al. [17]	132.50	45.54	178.04	No	No
Proposed	71.58	45.54	117.12	Yes	BAN+ROR+ProVerif

[Fig. 4: Communication Cost Comparison — Stacked bar chart showing communication overhead (bits) per phase (Registration, Login, Location Update, Query) for proposed scheme vs. prior schemes. Total of 1856 bits for proposed vs. 2240–3840 bits for competitors.]

Fig. 4. Communication Cost Comparison Across Schemes

D. Storage Overhead Analysis

TABLE V
STORAGE OVERHEAD ANALYSIS (BITS)

Entity	Stored Data	Size (bits)
Mobile User (Smart Card)	Hash digest, nonce, biometric helper	1088
Cellular Tower (CT)	Session key table, credential hashes	3296
LSSNS	User profile hash, FL model version ID	800
Total	—	5184

E. Privacy-Utility Tradeoff Discussion

The FL+DP combination introduces a model accuracy drop of less than 3% compared to a non-private centralized baseline when evaluated on next-location prediction using the GeoLife dataset (AUC: 0.847 vs. 0.873). The DRL obfuscation layer independently reduces de-anonymization success from 91.3% (no privacy) to 18.7% (DRL only) on the T-Drive test set using an HMM adversary with 20 known trajectory anchors, representing a 79.5% reduction. The aggregate utility error—defined as the mean absolute distance between the released trajectory and the true trajectory—is maintained below 5% of the mean trip length, confirming that the released data remains practically useful for friend proximity queries within a 500-meter threshold.

F. Security Attack Resistance

TABLE II (SECURITY)
INFORMAL SECURITY ANALYSIS — ATTACK RESISTANCE SUMMARY

Attack Class	Defense Mechanism	Resistance
Replay Attack	Timestamp + nonce binding in session key	✓ Formal
MITM Attack	Chebyshev DLP hardness; mutual auth	✓ Formal
Impersonation	3-factor binding; BAN verified	✓ Formal
Privileged Insider	Hash-only storage; no raw PW/bio	✓ Formal
Password Guessing	Fuzzy Extractor + SHA-1 hash chain	✓ Informal
Stolen Smart Card	3-factor; card alone insufficient	✓ Informal
DoS Attack	CT rate-limiting; session expiry	✓ Informal
De-anonymization (HMM)	DRL MI minimization	✓ Empirical
Gradient Inversion	(ϵ, δ)-DP noise on FL gradients	✓ Formal
Location Inference	Geo-indistinguishability + Dummy	✓ Formal
Behavioral Fingerprint	DRL temporal obfuscation	✓ Empirical
Session Hijacking	AES-128 + fresh session key per round	✓ Informal

VI. DISCUSSION

A. Advantages

The proposed framework presents seven substantive advantages over prior art. First, it is the only scheme to formally combine three independent privacy layers, each addressing a distinct threat vector, within a single mOSN deployment. Second, the Chebyshev chaotic map authentication avoids the heavy computational

overhead of ECC and bilinear pairing while maintaining equivalent security under the Chebyshev Discrete Logarithm problem. Third, the DRL agent's MI-minimizing reward function is information-theoretically optimal—no deterministic perturbation policy can achieve lower MI leakage for a given utility budget. Fourth, the inclusion of formal proofs (BAN, ROR, ProVerif) distinguishes this work from the majority of practical privacy schemes that rely solely on informal analysis. Fifth, the total authentication latency of 117.12 ms is lower than five of the six compared schemes, making it viable for real-time mOSN interactions on constrained mobile devices. Sixth, the utility loss of less than 5% ensures that location-based friend proximity services remain functional despite the multi-layer obfuscation. Seventh, the framework is modular—each privacy layer can be independently scaled or replaced without redesigning the overall protocol.

B. Limitations

Despite these contributions, six limitations warrant acknowledgement. First, the DRL agent requires an offline training phase on representative trajectory data, which may not always be available for new user populations or geographic regions. Second, the MI estimator (MINE) introduces variance in the reward signal that can slow convergence in environments with sparse mobility data. Third, the Chebyshev map session key establishment is secure under the Chebyshev DLP assumption, which, unlike ECC, has not been as extensively studied in the cryptographic community. Fourth, the current implementation assumes a single FL aggregation server, creating a potential bottleneck and single point of failure in very large deployments. Fifth, the dummy location injection strategy with $L = 1$ dummy provides $k = 2$ anonymity, which may be insufficient against adversaries with strong background knowledge about the user's activity patterns. Sixth, the ProVerif verification assumes a simplified Dolev-Yao attacker model and does not account for side-channel attacks on the smart card hardware.

C. Comparison with State-of-the-Art

Against the six benchmark schemes in Table IV, the proposed framework achieves the best balance of security coverage, formal guarantees, and computational efficiency. Tsai & Lo [15] achieves lower total latency (95.58 ms) but provides no temporal privacy, no formal ProVerif verification, and only two-factor authentication. Bhattacharya et al. [4]—the closest predecessor—provides Chebyshev authentication and BAN/ROR proofs but lacks FL structural privacy, DP algorithmic guarantees, and temporal obfuscation entirely. Wang et al. [17] integrates FL and DP but has the highest latency (178.04 ms), omits temporal privacy, and does not provide formal security proofs. The proposed scheme is unique in satisfying all five security requirements simultaneously while maintaining competitive latency and utility metrics.

VII. CONCLUSION AND FUTURE WORK

A. Summary of Contributions

This paper proposed a hybrid privacy-preserving framework for location data sharing in mobile online social networks that integrates three mutually reinforcing layers: Federated Learning for structural privacy, (ϵ, δ) -Differential Privacy for algorithmic privacy, and Deep Reinforcement Learning for temporal obfuscation. The framework is anchored by a lightweight three-factor authentication protocol using Chebyshev chaotic maps, SHA-1 hash chains, and Fuzzy Extractor biometric binding, which eliminates dependence on PKI while achieving mutual authentication in 117.12 ms. Formal security is verified via BAN logic derivation in 17 steps, the Real-or-Random model, and ProVerif automated simulation, confirming resistance to twelve attack classes. Empirical evaluation on the GeoLife and T-Drive datasets demonstrates a 60–80% reduction in HMM-based de-anonymization success, less than 5% aggregate utility error, and less than 3% FL model accuracy degradation—collectively establishing a new state-of-the-art for privacy-utility balance in mOSN location sharing.

B. Future Enhancements

Several research directions remain open. First, integrating blockchain-based audit trails would provide tamper-evident logging of location access events without centralizing raw data, complementing the existing multi-layer privacy stack. Second, replacing Gaussian-mechanism DP with Homomorphic Encryption (HE) for gradient aggregation would eliminate the need for a trusted FL server entirely, enabling fully decentralized model

training. Third, deploying the privacy pipeline on edge computing nodes collocated with cellular base stations would reduce MU-side computational load, enabling the framework on low-end IoT devices. Fourth, replacing A3C with Proximal Policy Optimization (PPO) or Soft Actor-Critic (SAC) may yield faster convergence and more stable policies in environments with sparse mobility data. Fifth, extending the framework to cross-domain federated learning—where mobility models trained in one city are transferred to another—would improve generalization and reduce cold-start latency for new deployments. Finally, incorporating user-adaptive privacy budgeting, where ϵ is dynamically tuned based on inferred sensitivity of the visited location, represents a promising direction toward context-aware privacy management.

REFERENCES

1. de Montjoye, Y.-A., Hidalgo, C. A., Verleysen, M., and Blondel, V. D., "Unique in the Crowd: The Privacy Bounds of Human Mobility," *Scientific Reports*, vol. 3, p. 1376, 2013.
2. Zang, H. and Bolot, J., "Anonymization of Location Data Does Not Work: A Large-Scale Measurement Study," *Proc. ACM MobiCom*, pp. 145–156, 2011.
3. Primault, V., Boutet, A., Mokhtar, S. B., and Brunie, L., "The Long Road to Computational Location Privacy: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2772–2793, 2019.
4. Bhattacharya, P., Tanwar, S., Shah, R., and Kumar, N., "A Privacy-Preserving Efficient Location-Sharing Scheme for Mobile Online Social Network Applications," *IEEE Access*, vol. 8, pp. 221330–221351, 2020.
5. Gedik, B. and Liu, L., "Protecting Location Privacy with Personalized k-Anonymity: Architecture and Algorithms," *IEEE Trans. Mobile Comput.*, vol. 7, no. 1, pp. 1–18, 2008.
6. Gruteser, M. and Grunwald, D., "Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking," *Proc. ACM MobiSys*, pp. 31–42, 2003.
7. Dwork, C., "Differential Privacy," in *Proc. ICALP*, Lecture Notes in Computer Science, vol. 4052, pp. 1–12, 2006.
8. Andrés, M. E., Bordenabe, N. E., Chatzikokolakis, K., and Palamidessi, C., "Geo-Indistinguishability: Differential Privacy for Location-Based Systems," *Proc. ACM CCS*, pp. 901–914, 2013.
9. McMahan, B., Moore, E., Ramage, D., Hampson, S., and y Arcas, B. A., "Communication-Efficient Learning of Deep Networks from Decentralized Data," *Proc. AISTATS*, pp. 1273–1282, 2017.