International Journal of Enhanced Research in Science, Technology & Engineering
ISSN: 2319-7463, Vol. 14 Issue 2, February-2025

AI-Enhanced and Privacy-Focused Smart Lockbox Delivery Solutions for E-Commerce and Rapid Commerce Operations Using Agentic Systems

Raghavendar Rao Tadpatri

Independent Researcher, USA.

ABSTRACT

The paper introduces the Privacy Preserving Smart Lockbox Delivery (PPSLD) system that is aimed at improving privacy and security in the last-mile delivery process by reducing exposure of customer information. PPSLD is used to provide secure parcel recovery, as well as retain operational efficiency through the incorporation of two-stage credentialing, AI-based optimization, and agentic operations. Using secure tokenization and data storage with limited data means, the system manages the problem of privacy, including address disclosure and unauthorized access. There are still such issues as locker accessibility and metadata leakage. The paper highlights wider governance in the data retention and consent that is required to attain maximum privacy in the systems of delivering.

Keywords: Privacy Preserving, Smart Lockbox, Last-Mile Delivery, AI Optimization, Credentialing, Data Minimization, Security, Operational Efficiency.

INTRODUCTION

The discovery of fast commerce and e-commerce within the last few years has completely transformed the landscape of the delivery experience through the provision of fast and comfortable doorstep delivery. The systems are extremely privacy invasive because recurrent deliveries can easily identify delicate client data, including the location, preferences, and routines. The study presents a Privacy-Preserving Smart Lockbox Delivery (PPSLD) model that aims at reducing these risks by adding two-stage dynamic credentials to the lockbox deliveries made by vendors [1]. The system also incorporates AI-based locker management optimization and anomaly detection, as well as a layer of agentic operations that maintains privacy throughout the delivery process.

A. Problem Statement

The emergence of fast commerce and e-commerce makes the likelihood of privacy breaches during the last-mile delivery more common. The identities, locations, and preferences of the customers can be exposed due to the regular movements of the doorstep deliveries [2].

Objectives:

- To minimize customer data exposure through two-stage credentialing and AI-based privacy mechanisms.
- To improve delivery operations using AI for locker and improve the operational efficiency of the PPSLD system.
- To address privacy and security challenges, including metadata leakage and unauthorized access, while ensuring data protection.

B. Contributions

The study proposed the Privacy-Preserving Smart Lockbox Delivery (PPSLD) model that reduces privacy exposure through two-stage rotating credentials.

II. Background and Related Work

A. Self-Collection and Parcel Lockers

Parcel lockers and pickup points are a simplified method of delivering to the end consumer through the consolidation of multiple deliveries into one drop-off address [3]. These systems give the opportunity to make deposits and collect them later without the company needing a person to be present during the delivery [4].

B. Secure Delivery Confirmation

Logistics is a crucial field involving the proper receipt of deliveries to avoid miss deliveries and disputes. Most of the systems currently in place are using one-time passcodes (OTPs) to confirm the successful delivery of parcels that helps to minimize errors by means of authenticating the recipient [5]. The PPSLD model goes a bit further where time-bound credentials are assumed on the specific case of lockbox pickups in privacy mode.

C. Predictive Logistics and Operational Intelligence

Logistics predictive models find extensive application in demand prediction, route optimization and fraud detection. These models allow companies to optimise operations, lower costs and even improve customer experience by predicting the need to make deliveries and the possible challenges [6]. PPSLD combines these predictive technologies but with an important difference, which is privacy limitations.

III. Proposed System: Privacy Preserving Smart Lockbox Delivery (PPSLD)

A. Design Goals

Privacy: The first is privacy, which will minimize the disclosure of the identity of the customers and their addresses in the process of the last-mile delivery. PPSLD makes sure that multiple deliveries are not linked to identities and addresses by ensuring that there are secure lockboxes/rotating credentials [7].

Minimal Disclosure: PPSLD insists on only the disclosure of the information that is required to be delivered. Details of customers' identity and address information are maintained out of the delivery process except when needed to carry out the operations [8].

Security: In order to prevent unauthorized access to deliveries, the system is programmed so that the credentials to access lockers have a time constraint and are single-use.

Compatibility: PPSLD will integrate well with current delivery processes, allowing companies to implement this privacy-enhancing system without major modifications to their existing processes.

Usability: The usability of the system is user-friendly is the important design objective. Picking parcels should be an easy and swift process for the customers, not entangled by complexity [9].

B. System Components

Lockbox Node (LBN)

The Lockbox Node (LBN) refers to a physical part of the PPSLD system that contains customer parcels in a safe manner [10]. It has several compartments with electronic locks, whose configuration is customizable for various goods, such as temperature-controlled compartments to store sensitive goods.

Privacy Delivery Orchestrator (PDO)

The Privacy Delivery Orchestrator (PDO) is a backend service that handles the entire PPSLD system [11]. It takes privacy-mode delivery requests and arranges the whole process, all the way through and also assigns lockers and compartments, issuing deposit and pickup credentials as well as making sure that rotation of such credentials takes place after every stage of the process.

Courier Integration

Couriers only get the necessary information that they need to accomplish their work. They are given a job token, locker location and compartment assignment, plus no customer identity or address information is given [12]. A design that is used will keep couriers out of reach of personal customer information, and comply with the privacy ideals of the system.

Customer Pickup Interface

The customer pick up interface enables one to access their packages through the lockbox node. Once the delivery is successful, the customer is notified of their locker number, pickup timeframe and a pickup message, in the form of an OTP, a QR token, or even an app-based token [13].

C. Data Minimization Boundaries

LBN Storage

The Lockbox Node (LBN) will only record the important logs of the event and job name of unfamiliar jobs. It also does not store data of its customers and as such, there is no personal information kept at the delivery location [14].

Courier Data Access

Minimum data access is offered to couriers. These are also provided only with the locker specifications and the deposit check in the allotted compartment, so that they do not get any customer-specific information. The courier does not have to engage in handling customer-specific data but only the physical work of depositing.

Customer Data Storage

The Lockbox Node (LBN) will store no customer identity and/or order data. The information is stored in the e-commerce and coordinated by the Privacy Delivery Orchestrator (PDO) only when it needs to be coordinated [15].

D. Two-Stage Credential Workflow

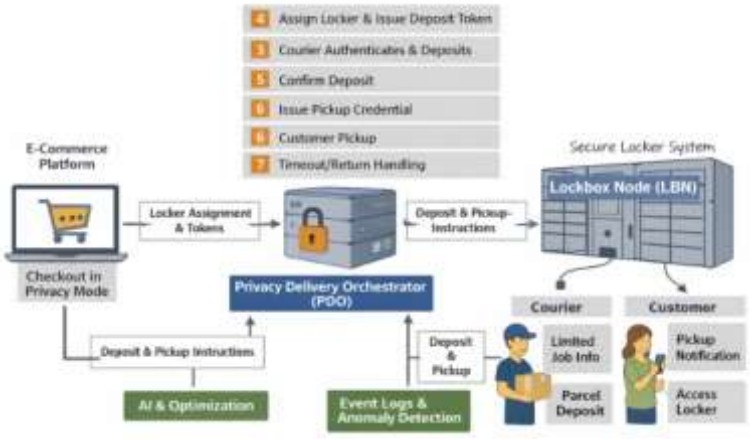

Fig 1. PPSLD baseline architecture: Platform to PDO to LBN and courier to customer Pickup

The Two-Stage Credential Workflow commences when the customer chooses the privacy mode during checkout, where he or she chooses a locker radius and pickup choice to avoid the revealing of any sensitive customer information. Privacy Delivery Orchestrator (PDO) provides an appropriate locker and a deposit token to the courier with a time limit. When he or she arrives, the courier verifies the token, places the parcel and the compartment is closed. The deposit token is then invalidated by the PDO and a new pickup credential is created for the customer.

E. Credential Rotation Logic (Algorithm Overview)

Inputs:
job_id: Unique identifier for the delivery job.
locker_id: Identifier for the assigned locker.
compartment_id: Identifier for the assigned compartment within the locker.
deposit_window: Time window during which the courier can deposit the parcel.
pickup_window: Time window during which the customer can pick up the parcel.

Steps: Issue Deposit Token
issue deposit_token(job_id, locker_id, compartment_id, expires=deposit_window_end)

Step 1: Courier confirms deposit
on deposit_confirmed(job_id):
invalidate deposit_token
issue pickup_token(job_id, locker_id, compartment_id, expires=pickup_window_end, single_use=true)

Step 2: Customer picks up the parcel
on pickup_success(job_id):
invalidate pickup_token
close job and retain minimal event log per retention policy

Step 3: Timeout handling
on pickup_timeout(job_id):
invalidate pickup_token
initiate return workflow
notify customer and vendor

IV. AI and Agentic Enhancements for PPSLD

A. AI Module 1: Locker Capacity Forecasting and Compartment Reservation

```python
import numpy as np
import matplotlib.pyplot as plt
from datetime import datetime, timedelta

def forecast_locker_capacity(time_of_day, historical_data):
    predicted_capacity = np.random.choice(historical_data, len(time_of_day))
    return predicted_capacity

def reserve_compartment(locker_id, predicted_capacity, reservation_time_window):
    available_capacity = predicted_capacity[-1]
    if available_capacity > 50:
        print(f"Locker {locker_id} reserved for {reservation_time_window} minutes.")
    else:
        print(f"Locker {locker_id} not available.")

time_of_day = ["Morning", "Afternoon", "Evening", "Night"]
historical_data = [80, 70, 60, 50]
predicted_capacity = forecast_locker_capacity(time_of_day, historical_data)
plt.figure(figsize=(8, 6))
plt.plot(time_of_day, predicted_capacity, marker='o', color='b')
plt.title('Predicted Locker Capacity Throughout the Day')
plt.xlabel('Time of Day')
plt.ylabel('Locker Availability (%)')
plt.grid(True)
plt.show()
reserve_compartment("Locker 1", predicted_capacity, 30)
```

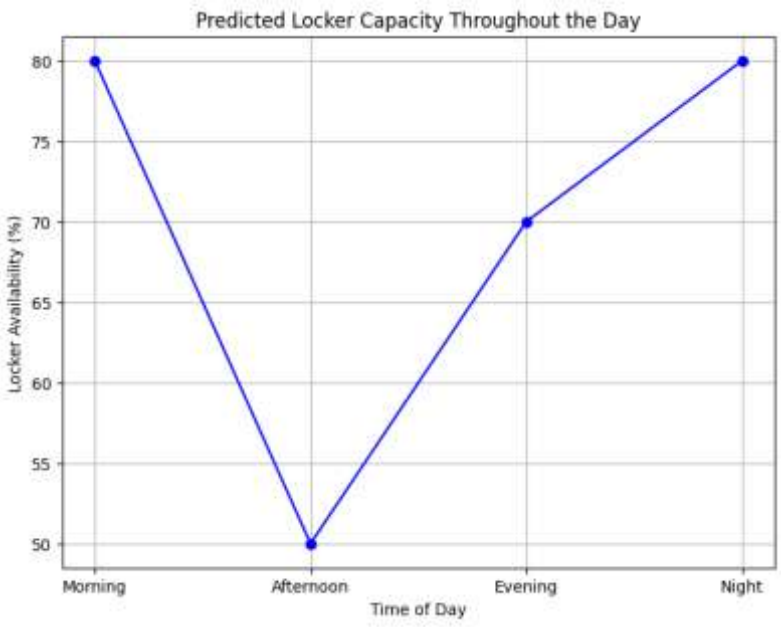

Fig 2. Predict Locker Capacity throughout the day

The module predicts the availability of locker compartments using past historical data on events and time-of-day trends. The plot indicates the daytime locker availability with a high availability in the morning, low availability in the afternoon, and high availability in the evening, with night depicting a moderate availability of the lockers.

B. AI Module 2: Multi-Criteria Locker Assignment Optimization

```
def calculate_locker_score(distance, congestion, compartment_type, risk_score, privacy_level):
    score = (distance * 0.3) + (congestion * 0.2) + (compartment_type * 0.1) + (risk_score * 0.1) + (privacy_level * 0.2)
    return score
def assign_locker(lockers, distances, congestion, compartment_types, risk_scores, privacy_levels):
    locker_scores = []
    for i in range(len(lockers)):
        score = calculate_locker_score(distances[i], congestion[i], compartment_types[i], risk_scores[i], privacy_levels[i])
        locker_scores.append((lockers[i], score))
    locker_scores.sort(key=lambda x: x[1], reverse=True)
    return locker_scores[0]
lockers = ["Locker A", "Locker B", "Locker C", "Locker D"]
distances = [18, 15, 20, 25]
congestion = [0.3, 0.6, 0.2, 0.5]
compartment_types = [1, 2, 3, 1]
risk_scores = [0.1, 0.3, 0.2, 0.4]
privacy_levels = [0.5, 0.8, 0.7, 0.6]
best_locker = assign_locker(lockers, distances, congestion, compartment_types, risk_scores, privacy_levels)
print(f"Best locker for assignment: {best_locker[0]} with score {best_locker[1]}")
```

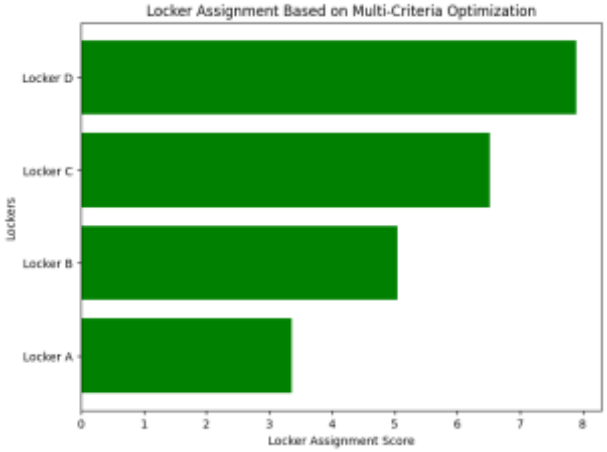

Fig 3. Locker assignment based on multiple optimization

The code assigns lockers according to various factors such as distance, congestion, type of compartment, risk score and level of privacy. The calculate locker score is used to calculate a score on each locker, and the assign locker is used to pick the best locker with the highest score. Locker D is assigned the highest score, which shows that it is the best in terms of being assigned to, and Locker A gets the lowest score.

C. AI Module 3: Pickup Compliance Prediction and Smart Windowing

```
from datetime import datetime
def predict_pickup_probability(time_of_day, distance, historical_latency):
    base_probability = 0.8
    time_factor = 1 - (time_of_day / 24)
    distance_factor = max(0, 1 - (distance / 20))
    pickup_probability = base_probability * time_factor * distance_factor * (1 - historical_latency)
    return pickup_probability

def adjust_pickup_window(probability, default_window=60):
    if probability > 0.8:
        return default_window
    elif probability > 0.5:
        return default_window + 30
    else:
        return default_window + 60
time_of_day = 15
distance = 10
historical_latency = 0.2
pickup_probability = predict_pickup_probability(time_of_day, distance, historical_latency)
adjusted_window = adjust_pickup_window(pickup_probability)
print(f"Pickup probability: {pickup_probability:.2f}, Adjusted Pickup Window: {adjusted_window} minutes")
```

```
Pickup probability: 0.12, Adjusted Pickup Window: 120 minutes
```

Fig 4. Pickup Compliance Prediction

The code forecasts the potential of a customer to collect his/her parcel within a window of time. The predict_pickup_probability is used to determine the probability on the basis of time of day, distance, and historical latency. The adjusted pickup window is used to reassess the size of the pickup window according to the estimated probability. The output shows the available pick-up probability and adjusted pick-up window in minutes, depending on the estimated probability outcome.

D. AI Module 4: Anomaly Detection for Unauthorized Access and Abuse

```
import numpy as np
from sklearn.ensemble import IsolationForest
def detect_anomalies(event_data):
    model = IsolationForest(contamination=0.1)
    predictions = model.fit_predict(event_data)
    return predictions
event_data = np.array([[3, 0, 0.1], [1, 1, 0.2], [0, 0, 0.05], [5, 0, 0.3], [2, 1, 0.4]])
predictions = detect_anomalies(event_data)
for i, pred in enumerate(predictions):
    print(f"Event {i+1}: {'Anomaly detected' if pred == -1 else 'Normal'}")
```

```
Event 1: Normal
Event 2: Normal
Event 3: Normal
Event 4: Normal
Event 5: Anomaly detected
```

Fig 5. Anomaly Detection

The Isolation Forest model is used as the model to detect anomalies in this code. It is capable of predicting normal and anomalous events using characteristics such as unsuccessful attempts to activate a token, reuse of a device, and times. An anomaly that is detected is flagged in the system as an event called Anomaly detected and helps in increasing security by detecting a suspicious event.

E. Agentic Operations Layer

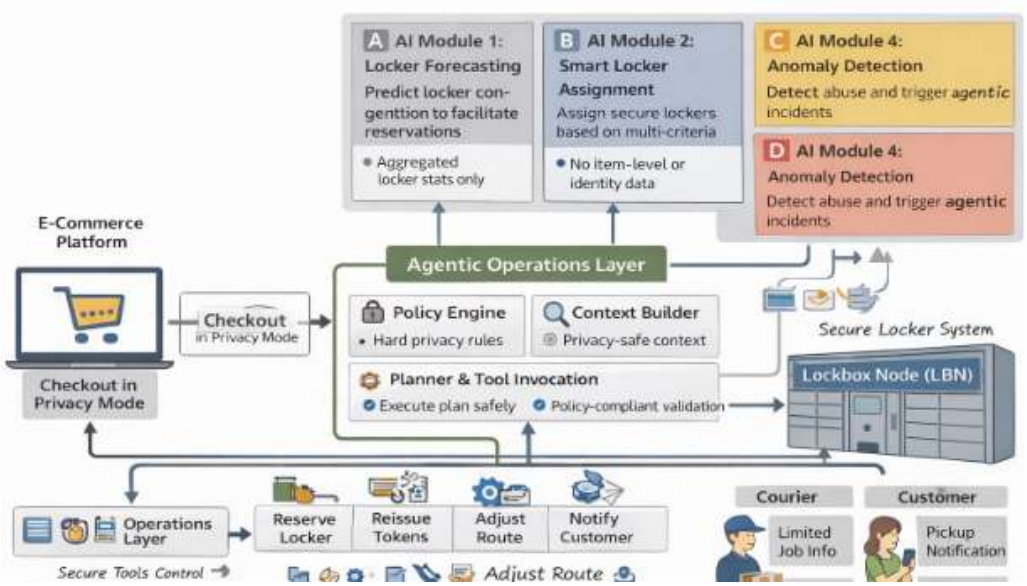

Fig 6. AI and Agentic Enhanced Architecture

The Agentic Operations Layer is an automated action that works off AI insights [16]. The actions of the agentic operations function include the reservation of lockers, redirection of deliveries, or customer notification. A policy engine controls it to ensure it is compliant with privacy and security requirements. The architecture incorporates AI Modules and an Agentic Operations Layer to the e-commerce platform and secure locker system. The Policy Engine makes policy decisions that uphold privacy, and the Context Builder takes into consideration minimal data manipulation.

F. AI Modules Summary Table

TABLE I. AI MODULES AND PRIVACY CONTROLS

AI Module	Privacy Constraints
A. Locker Forecasting	Uses aggregated locker stats only, no user/item-level data included.
B. Smart Locker Assignment	No item-level or identity data included in the locker assignment.
C. Pickup Compliance Prediction	Uses identifiers and coarse signals; avoids storing item details.
D. Anomaly Detection	Anomalies are detected based on event logs. No direct user data revealed.
E. Agentic Operations	Actions are performed based on a minimal privacy-safe context.

V. Privacy and Security Analysis

A. Threat Model

The threat model finds that there are a number of privacy and security predicaments to the delivery process. Unauthorized access may be made to the compartments using token theft, guessing, or shoulder surfing where sensitive customer information is revealed, and allows parcel theft [17]. The malicious actors can also utilize social engineering and deceive customers into disclosing their credentials, after which unauthorized access and data breach can occur.

B. Mitigations

The mitigations are aimed at implementing increased security and privacy during the delivery process. To make sure that deposit and pickup tokens are not used at the same time, two-stage credentialing is employed, so that deposit and pickup tokens do not coincide. The TTL is short and single-use tokens minimize the time interval during which the exploitation can take place and the tokens are canceled once they are used, which minimizes the possibility of unauthorized access. Brute-force attacks can be reduced through rate limiting and a lockout mechanism that controls the number of failed attempts [18].

TABLE II. THREATS AND MITIGATIONS

Threat	Impact	Mitigation
Token Interception	Unauthorized pickup	Short TTL, single-use, device binding option
Repeated Guessing	Unauthorized access	Rate limits, lockout, anomaly detection
Courier Profiling	Privacy loss	Pseudonymous job tokens, no identity on the courier app
Metadata Leakage	Preference inference	Coarse categories only, minimal logs, retention control
Insider Access	Privacy breach	Access control, audit logging, encryption, and least privilege

VI. Operational and Business Considerations

A. Deployment Models

Vendor-Owned Lockers: The firm owns its own lockers accessing complete security, privacy, and user experience. This will ensure uniformity in the quality of the services, but the infrastructure will be very expensive [19]. The lockers are owned by the vendors, are normally found close to stores or in the busiest places.

Neutral operator shared network: A neutral takes care of a common scheme of lockers that can be used by many vendors. It is a cost-effective way of infrastructure utilization as this model involves the sharing of infrastructure in various types of businesses, hence giving customers a range of brands under a single roof.

Partner Locations: The partner locations, such as apartment complexes, retail outlets, transit hubs, or campuses, contain lockers. In this model, the existing high-traffic locations are leveraged, and the customers can easily access them.

B. Customer Experience

Privacy mode should focus on simplicity to provide customers with an easy experience. The customers are given the privacy delivery option at the point of checkout, where none of the sensitive data would be exchanged. They are provided with a pickup token and information about lockers, when the customers choose the option [20]. This simplified process assures the customer little effort through it, and the privacy and security levels remain high.

C. Food Safety

Food deliveries need other considerations in order to be safe and quality. The pickup points need to be short so as to reduce spoilage and food needs to be collected quickly. There are temperature-regulated compartments to keep food at safe temperatures, especially the perishable foods [21]. The lockers should have a strong cleaning and hygienic policy that entails cleaning of the compartments regularly to prevent contamination.

VII. Evaluation Plan

A. Privacy Metrics

Address Disclosure Reduction: This index is used to measure the percentage of privacy-mode orders not delivered to the house door. The lesser the exposure to the address disclosure, the lower the chances of the address being revealed to customers during the delivery process, leading to more privacy guaranteed.

Contact Reduction: This measure is a percentage of the orders that are zero in-person delivered; the instructions are executed successfully, but delivery is arranged at the lockers, not to the customer.

Anonymity Set Proxy: The number of deliveries made by each locker per window will serve as a proxy of anonymity. The more deliveries produced, the more is the less recognizable a specific customer, and therefore greater protection of privacy.

B. Security Metrics

Unauthorized Attempts to Access: This data is an indicator of the number of unauthorized attempts to access per 10,000 shipments. A small figure means that the level of security is high, and unauthorized attempts at unlocking locked compartments are prevented [22].

Successful Fraud Rate: The successful rate of fraud is concerned with the successful rate of fraudulent activities. The optimum rate should be close to zero, meaning that the system is very effective in fraud prevention.
Mean Time to Detect and Contain Suspicious Activity: This is used to determine the average time of the system to detect and contain suspicious activities. Reduced response time represents a more responsive system and increased effectiveness of security.

C. Logistics Metrics

Courier Dwell Time: This is a metric that measures the time a courier spends when it is being dropped. Reduced dwell times indicate that the company has efficient delivery processes, whereas increased dwelling times can be taken to mean that there is a lack of efficiency in operations.

Failed Deposit Rate: This is used to determine the rate of couriers not making deposits in lockers. Reduced rate means higher efficiency of operation and fewer problems when making deposits.

Return Rate, Because of Not Picking Up: This indicator is a percentage that is used to track the percentage of parcels returned because the customer did not pick up the package within the specified pick-up timeline [23]. The lower rate of returns implies more productive pickups and communication with the customers.

Cost Per Successful Delivery: This is the cost of every successful delivery. Optimizing this measure makes such delivery processes cost-effective and does not undermine privacy and security.

D. AI and Agentic Metrics

Forecast Accuracy of Congestion Prediction: This is used to determine the quality of the AI models at predicting the locker congestion so that, at the point of necessity, the specific compartment is available.

Pickup Probability Model Calibration Error: This is a track that follows the error of the pickup probability model and evaluates well the model that is doing in predicting the pickup behaviour of customers [24].

Smart Windowing Reduction in the Missed Pickup Rate: Three is the measure that determines how effectively smart windowing reduces missed pickups and thereby enhances operational efficiency.

Success of Agentic Workflows on Exception Workflows: The measure is used to determine the success of agentic operations in exceptional workflows without involving humans to enhance system performance.

Policy Violation Rate: This measures policy violations by the verifier, and the goal of the policy violation rate is zero violations in order to achieve the privacy and security standard [25].

TABLE III. METRICS AND MEASUREMENT PLAN

Category	Metric	Measurement Plan
Privacy	Address disclosure reduction Contact reduction	Check delivery mode logs Courier handoff event absence
Security	Unauthorized access attempts	Event logs and anomaly alerts
Operations	Failed deposit rate Dwell time	Deposit confirmation failures Time at the locker per job
AI	Forecast accuracy	Backtest vs observed utilization
Agentic	Auto resolution rate	Workflow completion without human intervention

VIII. Discussion and Limitations

DISCUSSION

Privacy Preserving Smart Lockbox Delivery (PPSLD) system is very effective at minimizing the exposure of the last-mile through limiting the disclosure of addresses and identities. Nonetheless, complete privacy should be governed with a wider scope, such as the maintenance of the app's data retention, user agreement, and internal access restrictions [26]. Although it enhances security and convenience, the dependency of the system on the ways of locating lockers and optimizing AI should be controlled in order to address the fair availability and compliance with privacy.

LIMITATIONS

Users have restricted access because of locker placement, and metadata, including time and location, is still leaked [27]. Although mitigation is applied, such as the multiple locker options and the retention limits, these can be the privacy threats.

CONCLUSION

The Privacy Preserving Smart Lockbox Delivery (PPSLD) customer solution is a strong way to overcome the last-mile delivery issues due to its increased privacy and security. It guarantees that minimum exposure to customer data is created with the help of two-stage credentialing, AI-driven optimization, and agentic operations and makes operations more efficient. Though it covers some of the major issues concerned with privacy, total privacy needs to be contained within more extensive governance in data storage and authorization. Although PPSLD can increase customer experience through offering the secure and convenient pick-up of your parcels, issues related to locker accessibility and metadata leakage are still present. These limitations should be overcome with more work to achieve complete compliance with privacy.

REFERENCES

[1]. Breiman, L., 2001. Random forests. *Machine learning*, *45*(1), pp.5-32.
[2]. Friedman, J.H., 2001. Greedy function approximation: a gradient boosting machine. *Annals of statistics*, pp.1189-1232.
[3]. Hastie, T., Tibshirani, R. and Friedman, J., 2009. The elements of statistical learning.
[4]. Sculley, D., Holt, G., Golovin, D., Davydov, E., Phillips, T., Ebner, D., Chaudhary, V., Young, M., Crespo, J.F. and Dennison, D., 2015. Hidden technical debt in machine learning systems. *Advances in neural information*
[5]. Mitchell, M., Wu, S., Zaldivar, A., Barnes, P., Vasserman, L., Hutchinson, B., Spitzer, E., Raji, I.D. and Gebru, T., 2019, January. Model cards for model reporting. In *Proceedings of the conference on fairness, accountability, and transparency* (pp. 220-229).
[6]. Sharma, M.S., De Maio, M., Young, K. and Santopietro, J., 2022. Transformation of outpatient psychiatry. *Psychiatric Clinics*, *45*(1), pp.57-69.
[7]. Gama, J., Žliobaitė, I., Bifet, A., Pechenizkiy, M. and Bouchachia, A., 2014. A survey on concept drift adaptation. *ACM computing surveys (CSUR)*, *46*(4), pp.1-37.
[8]. ENTERPRISE, I.P.T., 2020. NIST privacy framework: a tool for improving privacy through enterprise risk management.
[9]. RISK, C., 2021. Risk management framework.
[10]. Tallyn, E., Revans, J., Morgan, E., Fisken, K. and Murray-Rust, D., 2021, May. Enacting the last mile: experiences of smart contracts in courier deliveries. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (pp. 1-14).
[11]. Zhang, Y. and Li, L., 2018. A new intelligent self-service express delivery system based on mobile cloud computing and WeChat. *International Journal of Autonomous and Adaptive Communications Systems*, *11*(1), pp.54-67.
[12]. Murray-Rust, D., Elsden, C., Nissen, B., Tallyn, E., Pschetz, L. and Speed, C., 2023. Blockchain and beyond: Understanding blockchains through prototypes and public engagement. *ACM Transactions on Computer-Human Interaction*, *29*(5), pp.1-73.
[13]. Ganesh, D., Suresh, K., Kumar, M.S., Balaji, K. and Burada, S., 2022, October. Improving security in edge computing by using cognitive trust management model. In *2022 International Conference on Edge Computing and Applications (ICECAA)* (pp. 524-531). IEEE.
[14]. Larsen, R.S. and Estes, D., 2019. Ieee smart village launches sunblazer iv and smart portable battery kits: Empowering remote communities. *IEEE Systems, Man, and Cybernetics Magazine*, *5*(3), pp.49-51.
[15]. Wu, C., Li, X., Luo, L. and Zeng, Q., 2022, June. G2Auth: secure mutual authentication for drone delivery without special user-side hardware. In *Proceedings of the 20th Annual International Conference on Mobile Systems, Applications and Services* (pp. 84-98).
[16]. Aveiro, D., Abreu, L., Pinto, D. and Freitas, V., 2023. DEMO models based automatic smart contract generation: A case in logistics using Hyperledger.
[17]. Sharp, J., Wu, C. and Zeng, Q., 2022, October. Authentication for drone delivery through a novel way of using face biometrics. In *Proceedings of the 28th Annual International Conference on Mobile Computing And Networking* (pp. 609-622).
[18]. Law, M.V., Naaman, M. and Dell, N., 2018, June. ShareBox: Designing A Physical System to Support Resource Exchange in Local Communities. In *Proceedings of the 2018 Designing Interactive Systems Conference* (pp. 1155-1167).
[19]. Roggeveen, A.L. and Sethuraman, R., 2020. Customer-interfacing retail technologies in 2020 & beyond: An integrative framework and research directions. *Journal of retailing*, *96*(3), pp.299-309.
[20]. Bello, J., Collins, S., Dreischmeier, R. and Libarikian, A., 2020. Innovating from necessity: The business-building imperative in the current crisis. *McKinsey Digital, April*, *16*.
[21]. Wilkinson, R., Hines, L., Holland, A., Mandal, S. and Phipps, E., 2020. Rapid evidence review of harm reduction interventions and messaging for people who inject drugs during pandemic events: implications for the ongoing COVID-19 response. *Harm reduction journal*, *17*(1), p.95.

[22]. Kielb, E.I., Mendoza, I.D., Morales-Juárez, A., Conzelmann, L., Velasquez, J.A. and Savaiano, D.A., 2023. Expanding Public and Private Partnerships to Improve Food Access for Families Enrolled in Supplemental Nutrition Programs. *Nutrition Today*, *58*(3), pp.119-123.

[23]. Dey, A., Nandi, S. and Sarkar, M., 2018, November. Security measures in IoT based 5G networks. In *2018 3rd International Conference on Inventive Computation Technologies (ICICT)* (pp. 561-566). IEEE.

[24]. Stickle, B., Hicks, M., Stickle, A. and Hutchinson, Z., 2022. Porch pirates: Examining unattended package theft through crime script analysis. In *Field Studies in Environmental Criminology* (pp. 106-122). Routledge.

[25]. Proper, S. and Nedar, V., 2022. Exploring Human-Centered AI: Designing The User Interface for an Autonomous Last Mile Delivery Robot.

[26]. Gormley, J.M., 2019. School nurse advocacy for student health, safety, and school attendance: Impact of an educational activity. *The Journal of School Nursing*, *35*(6), pp.401-411.

[27]. Lou, J.T., Bhat, S.A. and Huang, N.F., 2023. Blockchain-based privacy-preserving data-sharing framework using proxy re-encryption scheme and interplanetary file system. *Peer-to-Peer Networking and Applications*, *16*(5), pp.2415-2437.