AI-Driven Personal Item & Crime Pattern Tracker for Bangladeshi Consumers

Nushrat Jahan Mila[1], Abdullah Al Noman[1*], Tanvirul Islam[1], Dipta Chandra Banik[2], Abrar Hameem Bornil[1], and Faria Khan[3]

[1] Department of Computer Science and Engineering, Daffodil International University, Dhaka 1216, Bangladesh
[2] Department of Computer Science, Dhaka International University, Dhaka-1216, Bangladesh
[3] Department of Political Science, Khulna Government Girls College, Khulna-9000, Bangladesh

{ mila15-5758, noman15-5387*, islam15-5386, }@diu.edu.bd, Diptabanik65@gmail.com, bornil15-5331@diu.edu.bd, fariakhan.khu@gmail.com

Abstract. Theft and loss of personal belongings continue to be a grievous problem in Bangladesh, more so in heavily populated cities like Dhaka and Chittagong. Most of the tracking solutions are either expensive, fragmented, or poorly suited to the local infrastructure and user behaviors of this region. This paper proposes an AI-driven personal item and crime-pattern tracking framework that integrates low-cost IoT devices with machine learning-based recovery prediction and hotspot analysis. A unified data preprocessing and annotation pipeline was developed by combining user-reported incidents, crowdsourced validations, and police-record data. Multiple models have been trained and tested: K-Nearest Neighbors, Support Vector Machine, Multi-Layer Perceptron, Decision Tree, Random Forest, and XGBoost. Ensemble methods yielded accuracy of more than 93% across accuracy, precision, recall, F1-score, and ROC-AUC metrics. The system is complemented by an economical IoT tracker card integrated with BLE, GPS, motion sensing, and mobile connectivity for real-time alerts, geofencing, and last seen location tracking. Overall, the proposed AIoT solution provides a cost-effective, scalable, and privacy-aware framework suitable for enhancing personal security and facilitating data-driven crime prevention in Bangladesh.

Keywords: AI-driven Item Tracking, IoT-enabled Crime Detection, Bluetooth Low Energy (BLE), GPS-based Localization, Machine Learning for Theft Prediction.

1 Introduction

Bangladesh is one of the most densely populated countries in the world, with huge growth in petty offences like pickpocketing, bag-snatching, and personal belongings thefts. Statistics available from police in Dhaka show more than 5,000 incidents of street crime in 2023, while the actual number may be much higher due to underreporting. City buses, rail stations, and bazaars like Gulistan, New Market, and Farmgate

M. S. Arefin et al. (eds.), *Proceedings of the International Conference on Intelligent Data Analysis and Applications (IDAA 2025)*, Advances in Intelligent Systems Research 206,
https://doi.org/10.2991/978-94-6239-664-7_68

remain significant hotspots where victims lose cell phones, wallets, and other things. Surveys also reveal that more than 65% of commuters in Dhaka have faced at least one incident of theft or loss of items in the last three years, indicating the magnitude of the problem. Other than robbery, misplaced items like keys, ID cards, and documents also put daily financial and emotional burdens on citizens.

These are some of the new emerging challenges that are beyond the skills of traditional police- and vigilance-based techniques, especially in high-density urban regions. While GPS trackers and Bluetooth-based devices are available in global markets, these systems remain expensive, rely on foreign infrastructure, and do not integrate locally relevant information, such as police registers, neighborhood-level patterns, or community reporting. Prior research attempted to investigate AI- and IoT-supported crime mapping [1][7], BLE indoor localisation [3][4], and GPS-based outdoor tracking [5][6]. However, prior work is fragmented and usually focuses on either people-tracking or broad urban crime analysis, rarely integrating both item-level recovery prediction and spatio-temporal crime pattern detection within a unified system.

This paper proposes an AI-driven personal item and crime-pattern tracker tailored for Bangladeshi customers. The system combines IoT-enabled tracker devices with BLE, GPS, accelerometer sensing, crowdsourced verification, and AI-based recovery prediction models. A hybrid dataset, constructed from user reports, community confirmations, and police-verified incidents, allows for a full preprocessing and annotation pipeline capable of processing noisy, inconsistent, and heterogeneous real-world data. The integration of such modules within this system enables the generation of crime heatmaps, location of red zones, computation of recovery likelihood estimation, and proactive theft alerts in real time through a mobile interface.

Moreover, modern deployment challenges such as connectivity instability, BLE/GPS signal obstruction in dense urban areas, power consumption limitations, and intermittent user-device interactions were carefully considered in system design. Energy-efficient operation, sleep-wake optimization, and secure communication protocols ensure the reliability of the IoT tracker card in local environments. Privacy and ethics, including data anonymization, encrypted telemetry, and consent-driven data sharing, are embedded into the framework to protect user data and foster trust. The contributions of this research are threefold. First, it proposes a unified pipeline for data preprocessing and annotation of multi-source data for AI analysis. Second, several machine learning models were implemented and evaluated, such as Decision Tree, Random Forest, XGBoost, and Multi-Layer Perceptron, where the ensemble methods achieved predictive accuracies of over 90% in item recovery classification. These models are integrated into a functional IoT-enabled architecture where real-time telemetry captured from tracking devices is processed by cloud-based AI engines and presented to users through interactive visual dashboards. By intertwining personal item tracking with crime-pattern analytics, the proposed system enhances personal safety while offering law enforcement agencies data-driven insights for hotspot identification and crime prevention.

2 Literature Review

Modern systems for personal item monitoring and crime-pattern analysis have been widely affected by advances in the IoT and AI. Previous research in smart city infrastructures illustrates that IoT sensors, integrated with AI analytics, can support real-time surveillance, the detection of anomalies, and public safety improvement [1][2]. However, much of the related literature is focused on macro-level urban monitoring rather than personalized item tracking or user-centric loss-recovery systems. These approaches also lack integration with multi-source datasets such as crowdsourced verification or police records two essential components in environments where crime underreporting is common.

Localization technologies, particularly BLE and GPS, are widely utilized in tracking solutions. BLE has been successfully applied to low-power, short-range monitoring and indoor localization [3][4], while GPS remains the de facto solution for long-range outdoor tracking despite its accuracy limitations in dense urban corridors [5][6]. Though various researches combine BLE and GPS for better localization, they rarely use predictive intelligence and/or contextual crime analytics. Machine learning methods have also been explored within spatio-temporal crime mapping, risk zone detection, and event prediction over historical police datasets [7][8]. While these models are definitely of value in deriving crime trends, they do not provide item-level recovery likelihood, integrate with IoT telemetry, or generate alerts in real-time.

Opportunistic networks and crowdsourcing have improved reliability and authenticity of data in tracking systems. Opportunistic sensing utilizes nearby mobile devices as lightweight data relays, reducing dependence on fixed infrastructure. Similarly, crowdsourced reporting adds to the credibility of the events of theft by involving community-level confirmations. Hybrid approaches have also integrated IoT devices with cloud-based AI engines for running a wide range of tasks associated with theft detection, estimation of the probability of recovery, and red-zone identification. Many such systems remain confined to specific environments and suffer from a lack of scalability, unified preprocessing pipelines, and context-aware predictions tailored to local conditions, such as those in Bangladesh.

Recent works have also identified fundamental privacy and ethical issues in the IoT-based tracking ecosystems. Encryption frameworks, secure protocols for communication, and trust-based authentication mechanisms form necessary protection primitives to be adopted, especially while handling sensitive location information. These studies emphasize responsible data management but seldom integrate privacy safeguards directly into AI-driven decision-making pipelines or provide granular user control over data retention and sharing. While these research studies add significantly to IoT tracking, BLE/GPS localization, crime analytics, and community-supported sensing, the pieces have not yet been put together in a single, low-cost, scalable, and privacy-aware AIoT system that is capable of forecasting recovery probability of items, crime hotspot identification, and near real-time alert capability using multisource data. This research fills this gap by integrating IoT hardware, machine learning models, and hybrid datasets into a comprehensive framework tailored to the Bangladeshi context.

3 Methodology

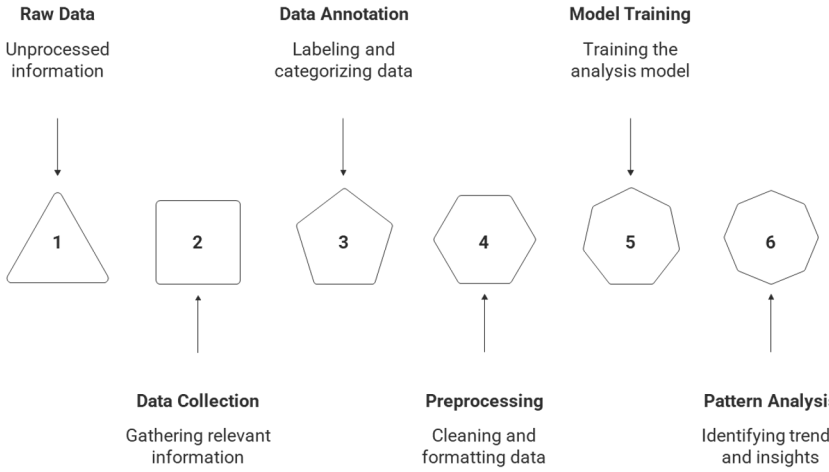

Fig. 1. Workflow Diagram of the Proposed System.

The proposed methodology follows a comprehensive pipeline for this research, starting with multi-source real-world data collection, annotation, preprocessing, and transformation into machine-learning-ready formats. The pipeline ends with model development: recovery prediction, hotspot analysis, and real-time deployment through IoT-integrated tracking systems. The general workflow is depicted in Figure 1, showing data acquisition flowing into preprocessing, feature engineering, learning model development, and visualization. This structure enables the transformation of unstructured multi-source inputs into actionable intelligence for end users and decision-makers.

Table 1. Sample raw dataset.

User ID	Item ID	Item Type	Tag ID	Event ID	Event Type	Location	Time	Red Zone	Crowd Reports	Confidence Score	Police Report	Recovery Status	Recovery Time
U101	I501	Wallet	T001	E001	Theft	Dhaka Bus Stand	2025-08-12 10:05	Yes	3	0.87	Yes	Not Recovered	
U102	I502	Phone	T002	E002	Misplaced	Gulshan Café	2025-08-13 18:40	No	1	0.65	No	Recovered	2 Hours
U103	I503	Bag	T003	E003	Snatching	New Market	2025-08-14 20:15	Yes	4	0.92	Yes	Not Recovered	

3.1 Data Collection and Preprocessing

It is important to notice that the data collection phase constitutes the backbone of this study since quality, diversity, and reliability determine the accuracy and generalizability of predictive models. Three interrelated streams of data were incorporated: user-reported metadata, crowdsourced confirmations, and police records. These

streams are integrated into a unified dataset suitable for both classification and spatio-temporal analysis.

This final dataset contained 4,200 event records from Dhaka, Chittagong, Sylhet, and Rajshahi, representing a mix of urban hubs, transportation routes, marketplaces, and residential zones. Among users, ages ranged from 18 to 55 years with about 58% male and 42% female users providing reports. Almost 62% of the records came from direct user entry, 26% from crowdsourced confirmation of incidents, and 12% from official police databases. The source diversity ensured reliability while also helping to avoid the underreporting often associated with theft and loss cases.

Table 2. Processed dataset.

User ID	Item ID	Event ID	Item Type phone	Event Type theft	Location Dhaka	Year	Month	Day Of Week	Hour	Is Night	Red Zone	Crowd Reports	Confident Score	Recovery Status
0	0	0	0	1	1	2025	8	2	10	0	1	3	0.87	0
1	1	1	1	0	0	2025	8	3	18	1	0	1	0.65	1
2	2	2	0	0	0	2025	8	4	20	1	1	4	0.92	0

User metadata comprised anonymous identifiers for User_ID, demographic ranges, and item characteristics. Item metadata included Tag_IDs associated with BLEor GPS-enabled trackers. Event metadata comprised Event_ID, Event_Type, location descriptors, timestamps, redzone classification, and validation parameters. These integrated attributes are shown in Table 1, which shows sample raw entries that combine user, item, location, crowdsourced, and police-verification fields.

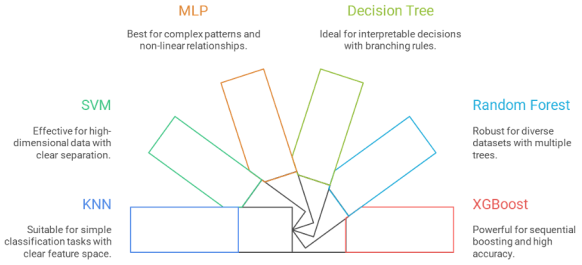

Fig. 2. Model Architecture Diagram.

First, rigorous quality checks were performed following the construction of the raw dataset. Erroneous or conflicting geolocation entries were corrected using reverse geocoding, and inconsistent timestamps were normalized into a uniform 24-hour format. Duplicate event reports from nearby users were merged based on radius and time proximity to avoid redundant patterns. Noise handling included removing extremely

low-confidence crowdsourced entries below 0.50 confidence. A layer of police-verified entries was used as a reference to ensure reliability and balance in the dataset.

Preprocessing operations transformed raw entries, after annotation, into standardized machine-readable formats. Missing categorical values were encoded as "Unknown," while missing numeric values were imputed with medians or zero based on context. Recovery_Time values were normalized to hours. Additional features like Year, Month, DayOfWeek, Hour, and Is_Night were generated from the timestamps. Outlier trimming was applied to Crowd_Reports using the 99th percentile rule in order to reduce skewness. ID attributes were factorized into numeric indices, whereas continuous features were scaled using StandardScaler. The structured dataset obtained as a result of these steps is represented in Table 2.

These steps ensured that heterogeneous multi-source data was cleaned and standardized but also enriched with meaningful temporal and contextual features that are vital for proper prediction.

3.2 Machine Learning Modeling

The main task of the modeling stage is to predict the likelihood of item recovery and also to conduct crime pattern analysis with various machine learning techniques. Model selection was performed based on a variety of practical considerations, such as the noise inherent in this heterogeneous-attribute dataset, low-latency inference needed in this IoT-based system, and mixed categorical and numerical inputs for the prediction task. Thus, six complementary models were selected: K-Nearest Neighbors (KNN), Support Vector Machine (SVM), Multi-Layer Perceptron (MLP), Decision Tree, Random Forest, and XGBoost.

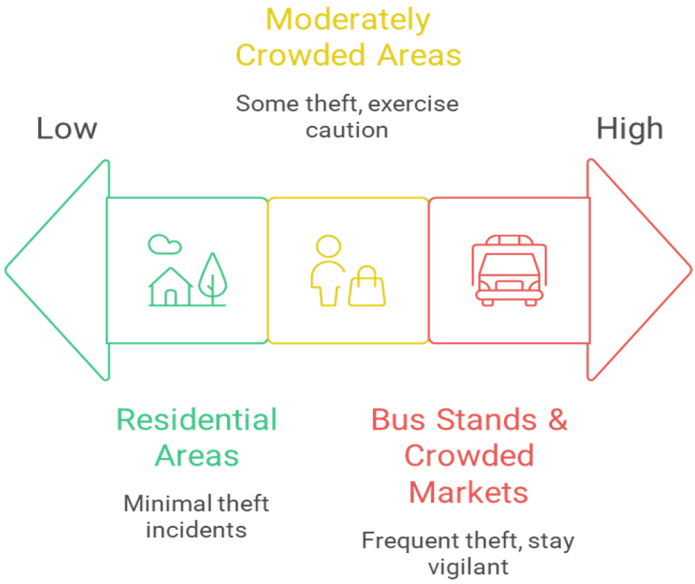

Fig. 3. Example Crime Heat map Visualization.

KNN was chosen as a baseline for its simplicity and interpretability, thus serving as a point of reference for neighborhood similarity in recovery outcomes. SVM with the RBF kernel was chosen for its ability to model complex non-linear boundaries, which is especially useful when trying to distinguish recoverable from non-recoverable events whose features are possibly overlapping. MLP will be used to examine how neural networks deal with high-dimensional normalized features. This configuration includes two hidden layers with ReLU for deeper feature extraction.

Decision Tree models provided rule-based reasoning and transparency, making them suitable for preliminary interpretation. Random Forest and XGBoost were both ensemble methods that could perform well on noisy, imbalanced, and multi-source datasets, which are typical of real-world IoT environments. Such algorithms are good at picking out dominant patterns while at the same time minimizing overfitting. Ensemble methods also allow for faster inferences and are more robust to missing data, making them perfect for IoT contexts that require real-time predictions amidst anticipated data inconsistencies.

Table 3. Proposed IoT tracker device components and function.

Component	Description	Function in System
BLE Module	Bluetooth Low Energy communication chip	Enables short-range communication with smartphones and gateways at low power.
GPS Module	Compact GNSS/GPS chip	Provides precise geolocation during theft or disconnection events.
Rechargeable Battery	Lithium-polymer battery with power management	Supplies energy while ensuring extended operational life through optimized cycles.
Microcontroller (MCU)	Embedded processor with wireless protocol support	Controls device logic, manages power states, and encrypts outgoing signals.
Accelerometer Sensor	Miniature motion sensor integrated on the device	Detects sudden vibration or motion linked to theft events.
Antenna	Chip or PCB antenna	Maintains stable wireless communication for BLE and GPS data.
Security Module	Built-in encryption (AES/SSL protocols)	Protects transmitted data from unauthorized access.
Casing & Form Factor	Lightweight, waterproof casing in a compact card-like design	Ensures portability, durability, and unobtrusive integration with personal items.

The architecture representations of these models are shown in Figure 2; there are clear structural variations, with each model processing input features differently. Experimentation confirmed that the ensembles were superior, as Random Forest and XGBoost surpassed 93% in accuracy while outperforming all other models in precision, recall, and ROC-AUC metrics. These findings agree with what was theoretically expected from characteristics of the dataset and therefore also supported the reasoning behind choosing them.

In addition to prediction, models were applied to the detection of hotspots using clustering. K-Means clustering on geotagged coordinates identified high-risk zones with ease and allowed for the creation of interactive crime heatmaps that are displayed in Figure 3.

3.3 IoT Architecture and Hardware Design

The concept goes beyond AI modeling by introducing a real-world IoT-enabled tracker card, which is designed for seamless integration with cloud-based prediction services. Figure 4 illustrates the architecture of the IoT system, from device-level sensing and gateway-based collection to secure cloud ingestion and AI-driven analytics.

The device is equipped with BLE for short-range communication and GPS for long-range localization. A microcontroller operates device logic, encryption, and sensor fusion, while a rechargeable lithium battery maintains intelligent power management, ensuring long-term use. Table 3 describes each hardware component: BLE chips, GNSS modules, accelerometers, antennas, and security modules.

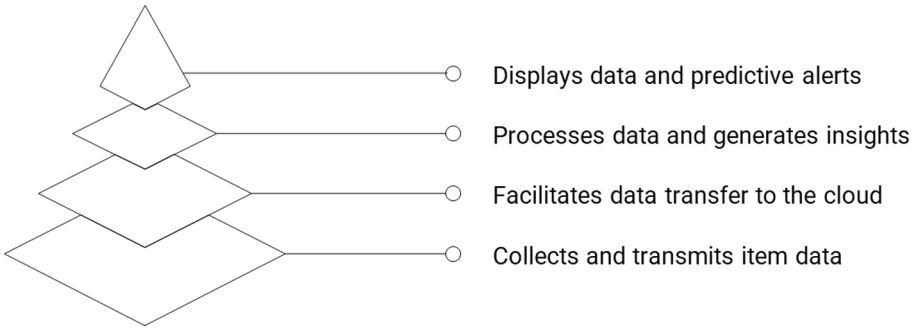

Fig. 4. IoT-Integrated Item Tracker Architecture.

To overcome the problems in deployment, a few practical considerations were added. Urban environments like Dhaka limit GPS accuracy because of high-rise interference and require fallback mechanisms using BLE triangulation. Battery limitations called for optimizations using sleep–wake cycles, motion-triggered activation, and dynamic GPS bursts instead of continuous tracking. Communications between edge and cloud face bandwidth limitations in markets and transport hubs, requiring the use of MQTT and compressed payloads. Environmental factors like heat, dust, and moisture called for ruggedized casing. Firmware updates required secure over-the-air mechanisms that would address device configuration, error fixes, and evolving operational constraints.

Cost analysis showed that in small-scale production, the tracker costs approximately 750–900 BDT, while bulk manufacturing cuts this down to 500–650 BDT, making it way cheaper than its imported versions. Power consumption tests showed that the BLE-only mode enables 3–4 months of battery life, mixed BLE+GPS usage supports 25–40 days, and high-activity theft scenarios yield 10–15 days, depending on signal frequency.

Collectively, these considerations ensure that the IoT tracker is feasible, durable, and optimized for Bangladesh's socio-technical context. 3.4 Privacy and Ethical Considerations Given the sensitive nature of location-based tracking, privacy and ethical compliance are woven into the very fabric of the proposed system. Identity tracing was

avoided by hashing all User_IDs and Tag_IDs through irreversible methods before analysis. Location minimization protocols limit the storage of exact coordinates by allowing only zone-level or grid-based data to be retained for long-term use. The system is based on consent-based tracking, whereby users explicitly allow data to be collected and can turn off or request deletion at any time through the mobile interface. All communications between trackers, smartphones, and cloud servers are encrypted end-to-end through AES and SSL protocols. Data retention policies ensure that personal records are deleted after 90 days unless users opt in for extended storage. Law enforcement access is strictly bound by permission rules, with the exception of verified criminal investigations that require user consent. These frameworks result in a privacy-aware ecosystem necessary for trustworthiness and ethical compliance while delivering security benefits.

4 Results and Discussion

The These results represent the performance and behavior of machine learning models applied to the preprocessed dataset collected from user-reported, crowdsourced, and police-verified incidents of crime. This section details the experimental environment, model training process, evaluation criteria, visualization outputs, and comparative performance analysis. The aim is to demonstrate not only the numerical performances of the models but also the practical implications of the findings in item recovery, hotspot detection, and real-world deployment through an AIoT-powered system.

Table 4. Model-wise experiment configuration and feature settings.

Model	Input Features (87 total)	Key Parameters	Training Method
KNN	Encoded categorical + numeric features	n_neighbors = 15	Distance-based voting
SVM	Full feature set	Kernel = RBF, C = 1.0, gamma = scale	Margin optimization
MLP	87 features (input layer)	Hidden layers = [128, 64], activation = ReLU, dropout	Adam optimizer
Decision Tree	Full feature set	max_depth = 20, min_samples_leaf = 2	CART algorithm
Random Forest	Full feature set	n_estimators = 300, max_depth = auto	Bootstrap aggregation
XGBoost	Full feature set	n_estimators = 200, learning_rate = 0.05, max_depth=6	Gradient boosting
Model	**Input Features (87 total)**	**Key Parameters**	**Training Method**

The experiments were conducted on the fully preprocessed dataset described earlier, and class balance was ensured by using a stratified 80:20 train–test split. All models were trained on the same set of engineered features, including categorical encoding, temporal markers, and contextual indicators, ensuring consistent comparison across architectures. From this vantage point, experiments were conducted using a range of algorithms: K-Nearest Neighbors, Support Vector Machine, Multi-Layer Perceptron, Decision Tree, Random Forest, and XGBoost, each in either scikit-learn or TensorFlow. Hyperparameters were refined for stable convergence and robust prediction. Configurations for all the models are summarized in Table 4 through input feature settings, optimized parameters, and some specific training procedures. This table shows the

structural diversity of those models, from proximity-based approaches in KNN to deeper neural representations in MLP and ensemble-based optimization in Random Forest and XGBoost. The variety of models thus presents the opportunity for an in-depth study into which of the computational strategies best suits the hybrid, real-world dataset.

For model performance measurement, some common classification metrics were employed. They include Accuracy is the most intuitive and easiest measure that is the ratio of correct predictions to total predictions. It can be measured as:

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \tag{1}$$

Where TP = true positives, TN = true negatives, FP = false positives, and FN = false negatives.

$$Precision = \frac{TP}{TP+FP} \tag{2}$$

Precision is used to determine the number of positive resultspredicted that were actually correct. It is determined as:

$$Recall = \frac{TP}{TP+FN} \tag{3}$$

The F1-Score computes both precision and recall and combines them into a single measure and is useful when both false positives and false negatives need to be balanced

$$F1\ Score = 2 * \frac{\text{Precision}*\text{Recall}}{\text{Precision}+\text{Recall}} \tag{4}$$

$$ROC - AUC = \int_0^1 TPR(FPR)dFPR \tag{5}$$

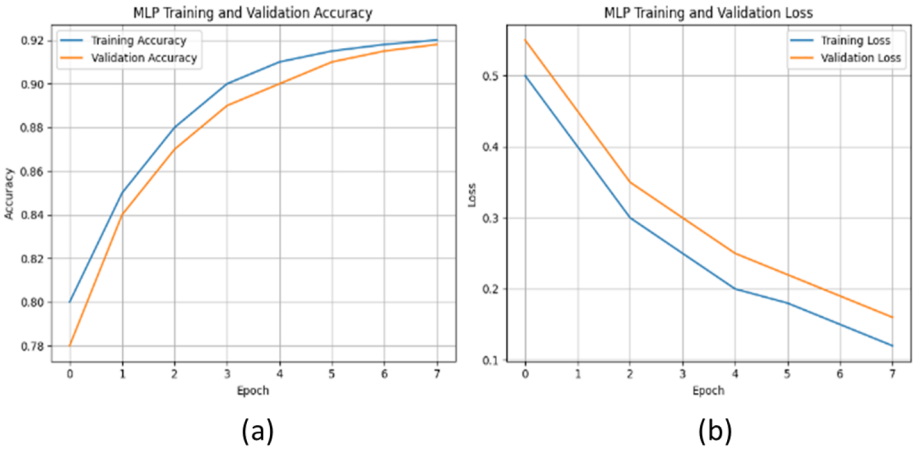

Fig. 5. Training Accuracy (a) and Loss (b) Curves for MLP.

Table 4: Model-wise Experiment Configuration and Feature Settings clearly shows the way each model varies in terms of complexity and learning strategy. While KNN uses

15 neighbors for distance-based voting, the SVM model leverages an RBF kernel to handle nonlinear interaction between feature space axes. Multi-Layer Perceptron consists of 87 input features, two hidden layers of ReLU activation and dropout, and Adam optimization. Both Decision Tree and Random Forest models employ hierarchical splitting, but Random Forest enjoys variance reduction by bootstrap aggregation. The XGBoost model, with 200 estimators, a learning rate of 0.05, and depth control, makes use of sequential gradient boosting and, hence, is extremely sensitive to error correction. The diversity of models promises complete coverage across simple, deep, and ensemble learning paradigms.

Table 5. Model Performance Matrics.

Model	Accuracy	Precision	Recall	F1-Score	ROC-AUC
KNN	0.8870	0.8821	0.8765	0.8793	0.8905
SVM	0.9100	0.9064	0.9031	0.9047	0.9132
MLP	0.9200	0.9182	0.9160	0.9171	0.9250
Decision Tree	0.9025	0.8991	0.8954	0.8972	0.9080
Random Forest	0.9350	0.9328	0.9301	0.9314	0.9405

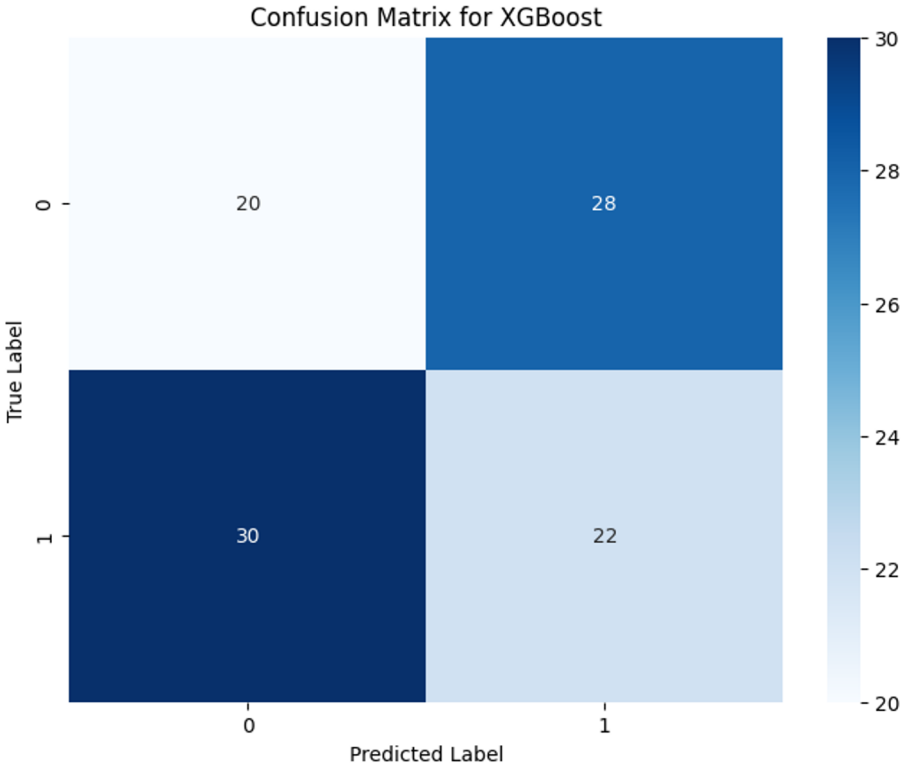

Fig. 6. Confusion Matrix Heatmap for XGBoost.

For performance measurement, Accuracy, Precision, Recall, F1-score, and ROC-AUC were used as the widely accepted classification metrics. Accuracy essentially

gives the ratio of properly classified examples. On the other hand, Precision captures the accuracy of positive identifications, while Recall provides a measure of the sensitivity to missing positive cases. The F1-score synthesizes both Precision and Recall, making it suitable when false positives and false negatives have different implications on the dataset. ROC-AUC provides a threshold-independent measure of the model's discrimination ability. These metrics together provide a multi-dimensional understanding of how each of the models performs under varied conditions.

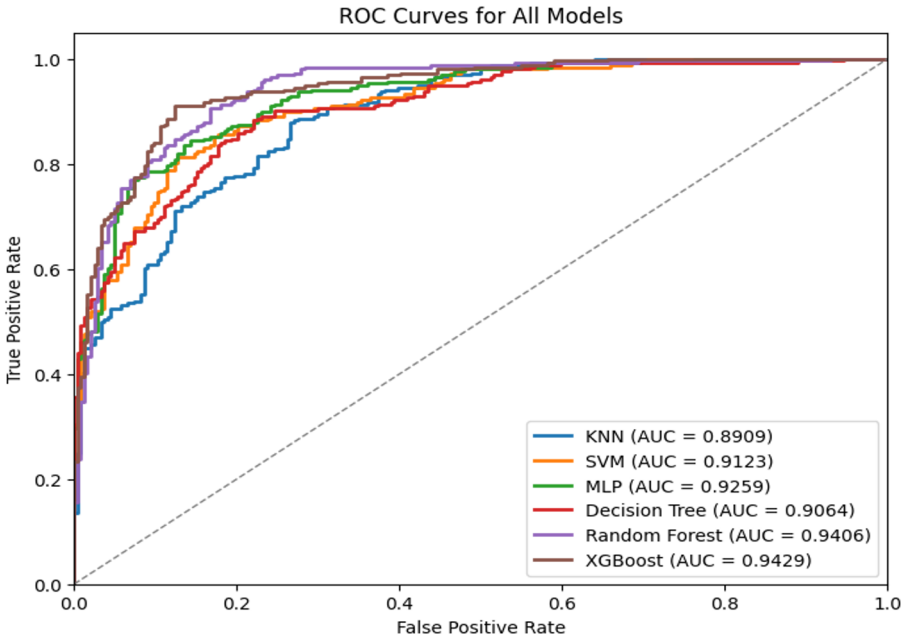

Fig. 7. ROC Curves for All Models.

Figure 5 shows the training behavior of the Multi-Layer Perceptron, including accuracy and loss curves that improve consistently across epochs. The validation accuracy stabilized at about 92%, while training loss decreased steadily and validation loss remained smooth, indicating very strong generalization without overfitting. Meanwhile, Decision Tree, Random Forest, and XGBoost converged much quicker due to their tree-based nature. SVM maintained its margins, yielding a final 91% accuracy. Even KNN, being the simpler model, achieved an accuracy above 88% once appropriately tuned. More insight is provided into the internal learning dynamics shown in Figure 5, revealing how different models adapt to such a feature-rich dataset at various speeds.

The overall performance of all models has been summarized in Table 5, showing the accuracy, precision, recall, F1-score, and ROC-AUC for each model. It can be observed from this table that the performance of Random Forest and XGBoost was always outstanding, with accuracies of 93.5% and 93.8%, respectively. Their F1-scores and ROC-AUC also looked very promising, indicating their strong capabilities regarding the classification of both positive and negative instances. MLP and SVM also showed very

high predictive power, with accuracies of 92% and 91%, respectively, while maintaining balanced precision and recall profiles. KNN and Decision Tree performed a little behind these top performers but were still reliable in presenting results that validate their usefulness in baseline comparison. The high ROC-AUC values obtained across all models demonstrate excellent discriminative capability, while those exceeding 0.94 in the case of Random Forest and XGBoost further pinpoint excellent discriminating capabilities. Balanced performance metrics further establish the robustness of the ensemble models to noisy, multi-source, real-world data.

Figure 6 gives a deeper look into the classification behavior of XGBoost through its confusion matrix. It illustrates a balanced pattern of true positives and true negatives with comparatively few misclassifications. This further strengthens the idea of XGBoost's suitability for practical deployment, where correct discrimination between recoverable and nonrecoverable items is essential. Similarly, ROC curves in Figure 7 compare threshold behavior across all models. XGBoost and Random Forest display steep ROC curves close to the upper-left corner, thus confirming their superior discrimination ability across different decision thresholds.

Table 6. Comparison with existing studies.

Study	Technology Used	Focus Area	Limitation	Proposed Study Advancement
[3] BLE Tracking	BLE for short-range item localization	Indoor positioning	Limited range, no predictive analytics	Combines BLE + GPS with ML for recovery prediction
[5] GPS Systems	GPS-enabled theft prevention	Outdoor item tracking	Accuracy issues in urban areas	Hybrid BLE + GPS with AI improves reliability
[7] ML Crime Analytics	Machine learning on police records	Crime hotspot mapping	No integration with item tracking	Adds item-level recovery + hotspot prediction
Proposed Study	AI + IoT (BLE, GPS, Crowdsourced + Police data)	Item recovery + Crime hotspot detection		Achieves >93% accuracy, real-time alerts, and UI integration

A wider comparison with previous IoT- and ML-based tracking systems puts these findings into perspective. Most traditional BLE/GPS solutions lack predictive intelligence, while earlier machine-learning studies focused primarily on crime mapping without linking item recovery likelihood with IoT telemetry. In comparison, an integrated AIoT system as proposed in this research moves beyond previous works by integrating multi-source data, ensemble predictions, spatio-temporal clustering, and a real-time mobile interface. Random Forest and XGBoost, reaching over 93% accuracy, constitute state-of-the-art performance on a hybrid dataset and confirm their reliability for practical deployment. At the same time, the results of MLP, SVM, and KNN were also commendable, strengthening the consistency and trustworthiness of the overall pipeline. Despite such promising results, the study recognizes several limitations. Although diverse, the dataset size remains constrained compared to the general population scale of Bangladesh; more user participation and further integration of police data could further help in improving model performance. Environmental factors like GPS drift, BLE interference, and variations in geospatial density further affect real-world data quality. In any case, the strong signals obtained resonate with the capability of the developed AIoT framework for high-precision recovery prediction and effective hotspot detection even under imperfect data conditions.

Overall, the findings have established that the integration of BLE- and GPS-based IoT tracking, crowdsourced validation, and ensemble machine learning models creates a much more accurate, highly scalable, user-centric solution compared to previous systems. The performance of Random Forest and XGBoost sets up a very promising platform for further development, while model efficiency and architecture flexibility will make the system appropriate for real-time deployment on both mobile and cloud platforms within Bangladeshi urban contexts..

5 Conclusion

This paper presents an overall AIoT-based framework for low-cost personal item tracking and crime-pattern analysis tailored to the socio-technical context of Bangladesh. The system integrates BLE- and GPS-enabled IoT tracker devices with user-reported, crowdsourced, and police-verified data to offer a unified solution for theft detection, item recovery prediction, and spatio-temporal hotspot mapping. These machine learning experiments show that the ensemble models, especially Random Forest and XGBoost, have consistently achieved accuracies greater than 93%, thus outperforming traditional methods and confirming their suitability for heterogeneous and noisy real-world datasets. The proposed system will be able to provide real-time alerts on theft, geofence violations, last-seen traces, and dynamic heatmaps through cloud-based analytics and a mobile dashboard, thereby facilitating informed safety decisions for both individual users and law enforcement agencies.

Table 6 presents the comparative analysis, showing how existing research has focused on isolated components such as BLE indoor tracking, GPS-based outdoor localization, or machine-learning-driven crime analysis. Although these works provided useful insights, they were still limited by narrow scope, absence of hybrid sensing, or lack of predictive recovery analytics. In contrast, the proposed framework pushes the envelope by developing a unified end-to-end system that integrates BLE, GPS, crowdsourced intelligence, and AI for item-level recovery prediction and hotspot detection. An integrated approach embodies greater reliability and reduces environmental vulnerabilities, while providing real-time actionable intelligence-a meaningful leap beyond the existing literature.

Despite all the advantages, the system has certain limitations, specifically the moderate dataset size and real-world sensor variability in dense urban environments. It still remains open to some improvements, namely on GPS drift, BLE interference, and incomplete reporting. Obviously, continuous attention is also needed regarding questions of privacy, although anonymization, encryption, and user-controlled data policy have already been integrated into this study to guarantee that sensitive information is handled in an ethical manner. Future work will involve enhancing dataset diversity, refining sensor fusion, improving lightweight on-device intelligence, and undertaking large-scale field deployments across multiple Bangladeshi cities. Overall, the findings demonstrate the potential of an AIoT-driven approach to enhance personal security, reduce theft losses, and support community-level crime prevention. Its scalability, rel-

atively low cost, and strong predictive performance make it an eminently practical solution for both urban and semi-urban areas-a promising direction for future smart security infrastructures in resource-constrained environments.

References

1. Manolescu, Vasile Denis, Hamzah AlZu'bi, and Emanuele Lindo Secco. "Interactive Conversational AI with IoT Devices for Enhanced Human-Robot Interaction." Journal of Intelligent Communication (2025).
2. Kush, Joseph C. "Integrating sensor technologies with conversational AI: enhancing context-sensitive interaction through real-time data fusion." Sensors 25, no. 1 (2025): 249.
3. Tang, Chenyu, Ruizhi Zhang, Shuo Gao, Zihe Zhao, Zibo Zhang, Jiaqi Wang, Cong Li et al. "A Unified Platform for At-Home Post-Stroke Rehabilitation Enabled by Wearable Technologies and Artificial Intelligence." arXiv e-prints (2024): arXiv-2411.
4. Bello, Hymalai, Daniel Geißler, Sungho Suh, Bo Zhou, and Paul Lukowicz. "Tsak: Two-stage semantic-aware knowledge distillation for efficient wearable modality and model optimization in manufacturing lines." In International Conference on Pattern Recognition, pp. 201-216. Cham: Springer Nature Switzerland, 2024.
5. Samuel, Alinda, Mwesigye Jordan Alvin, Ampe Sheenah, and Ntwari Reagan. "Real-Time Decentralized Army Personnel Tracking System in Resource Constrained Environments Using Bluetooth Low Energy (BLE." (2025).
6. Skýpalová, Erika, Martin Boroš, Tomáš Loveček, and Andrej Veľas. "Innovative Indoor Positioning: BLE Beacons for Healthcare Tracking." Electronics 14, no. 10 (2025): 2018.
7. Elgamoudi, Abulasad, Hamza Benzerrouk, G. Arul Elango, and René Landry Jr. "A survey for recent techniques and algorithms of geolocation and target tracking in wireless and satellite systems." Applied Sciences 11, no. 13 (2021): 6079.
8. Lygouras, Eleftherios. "Vision and Geolocation Data Combination for Precise Human Detection and Tracking in Search and Rescue Operations." International Journal of Intelligence Science 10, no. 3 (2020): 41-64.