Crime Aware Encrypted Navigation App For Personal Safety

Mrs D Kalyani, Assistant Professor
Computer Science Engineering Department
Dhanalakshmi Srinivasan University
Trichy,India
kalyanid.set@dsuniversity.ac.in

Dande Durga
Computer Science Engineering
Dhanalakshmi Srinivasan University
Trichy,India
dandedurga.set2022@dsuniversity.ac.in

B. Mouthreyini mukarji
Computer Science Engineering
Dhanalakshmi Srinivasan University
Trichy,India
mouthreyinimukarji.set2022@dsuniversity.ac.in

CH Namratha
Computer Science Engineering
Dhanalakshmi Srinivasan University
Trichy,India
namrathac.set2022@dsuniversity.ac.in

#123UG Student, Department of Computer Science and Engineering,
School of Engineering and Technology,
Dhanalakshmi Srinivasan University, Trichy—621112, Tamil Nadu, India

#4Assistant Professor, Department of Computer Science and Engineering,
Dhanalakshmi Srinivasan University, Trichy—621112, Tamil Nadu, India

Abstract : Rising urban crime and unpredictable security threats have increased the need for intelligent personal safety solutions. Crime-encrypted navigation systems integrate real-time crime data, geospatial analytics, and encryption techniques to provide safer route recommendations while protecting user privacy. This approach analyzes historical crime patterns, live incident reports, and environmental risk factors to dynamically guide individuals through low-risk paths. End-to-end encryption ensures that location data, travel history, and personal identifiers remain secure against unauthorized access and misuse. yy combining secure data transmission with predictive risk assessment, crimeencrypted navigation enhances situational awareness, minimizes exposure to highrisk areas, and supports informed decisionmaking without compromising confidentiality. The system demonstrates potential applications in urban mobility, emergency response, and personal safety, contributing to smarter and more secure navigation frameworks.

Keywords: crime-aware navigation, encrypted routing, personal safety, privacyfirst GPS, real-time risk alerts, secure route planning.

I.INTRODUCTION

Crime Encrypted Navigation for Personal Safety is a mobile application designed to address these concerns by integrating crime analysis, secure routing, and encrypted communication into a single platform. The application utilizes crime data, user reports, and real-time environmental information to identify high-risk zones and generate safer alternative routes. yy alerting users about nearby incidents and unsafe areas, the system promotes informed decision-making

during travel, especially at night or in unfamiliar locations.

A key feature of the application is its strong emphasis on data security and user privacy. Sensitive information such as user location, travel history, and emergency contacts is protected using advanced encryption techniques. End-to-end encryption ensures that personal data cannot be intercepted, misused, or accessed by unauthorized parties. This approach builds user trust while maintaining compliance with modern privacy standards.

In addition to navigation and security, the application incorporates emergency response features such as instant SOS alerts, live location sharing with trusted contacts, and quick access to local emergency services. These features enable rapid assistance during critical situations, fulther strengthening the user's sense of safety.

Overall, Crime Encrypted Navigation for Personal Safety aims to transform traditional navigation into a proactive safety tool.
yy combining intelligent crime-aware routing with robust encryption and emergency support, the application provides a reliable solution for individuals seeking safer and more secure travel in today's increasingly unpredictable environments.

Fig 1 Architecture of IEEE 1451 family of standards

Mobile application architecture refers to the structured design approach used to organize the and ensure that the core business logic remains independent of platform-specific frameworks. components of a mobile app in a way that ensures scalability, maintainability, and performance. It typically follows a layered structure consisting of the presentation layer, domain or business logic layer, and data layer. The presentation layer handles the user interface and user interactions, the domain layer contains the core business logic and application rules, and the data layer manages data retrieval from local storage or remote servers through repositories and data sources. Common architectural patterns used in mobile development include MVC, MVP, and MVVM , with MVVM being the most widely adopted due to its clear separation of concerns and ease of testing. For large and complex applications, Clean Architecture is often preferred as it enforces dependency rules and keeps the business logic independent of frameworks and UI components. A well-designed mobile architecture improves code reusability, simplifies testing, enhances security, and allows the application to evolve efficiently over time.

It generally follows a layered approach that includes the presentation layer, business or domain layer, and data layer. The presentation layer, business or domain layer, and data layer. The presentation layer is responsible for displaying the user interface and handling user interactions, while the business layer contains the core logic, validation rules, and application workflows that govern the app's behavior. The data layer manages data operations by interacting with local databases, remote servers, APIs, and caching mechanisms through repositories and data sources. Popular architectural pattems such as MVC, MVP, and MVVM are used to structure these layers, with MVVM being widely adopted in modern mobile development due to its support for reactive programming and easier testing. For large-scale

and enterprise applications, Clean Architecture is commonly implemented to maintain strict separation of concerns Additionally, mobile app architecture incorporates essential aspects such as state management, dependency injection, security mechanisms, and performance optimization, all of which contribute to building reliable, testable, and high-pelfonning mobile applications that can adapt to future requirements and technological changes.

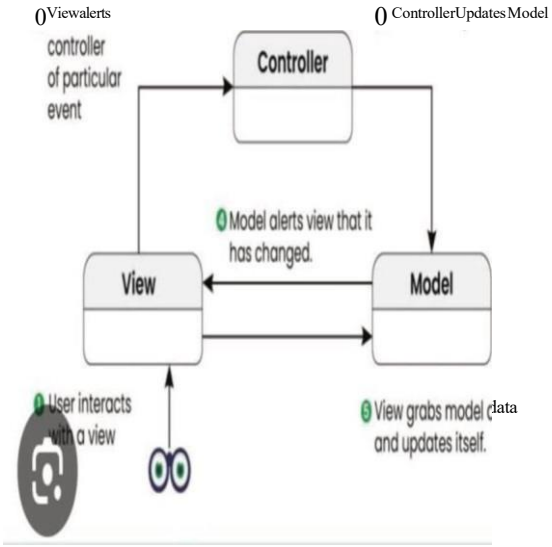


Fig 2: Work flow

Architecture of the Crime Aware Encrypted Navigation for Personal Safety The architecture of a crime-aware encrypted navigation system for personal safety is designed to provide secure and privacy-preserving route guidance by

integrating real-time crime intelligence with encrypted location services. The system consist of a user interface layer for safe interaction and alerts, a secure navigation layer that computes risk-aware routes using crime density and temporal factors, and a crime analysis layer that processes historical and real-time incident data to generate safety scores. To protect user privacy, all location data and routing requests are encrypted end-toend, ensuring that servers never access raw user movements. Advanced privacy mechanisms such as anonymization, differential privacy, and zeroknowledge data handling prevent tracking and profiling, while dynamic rerouting adapts to emerging threats. This architecture enables safer navigation without compronusmg user confidentiality, making it suitable for personal safety applications in smart cities.

II.RELATED WORK

1. Secure & Privacy-Preserving Navigation in Vehicular Networks

Several studies focus on combining navigation with strong privacy protections in vehicular enviromnents (VANETs):

A Secure and Privacy-Preserving Navigation Scheme Using Spatial Crowdsourcing in Fog yased VANETs proposes a navigation architecture where vehicles and fog nodes compute routes using real-time data while protecting vehicle identity via anonymous credentials and cryptography — showing how secure routing and confidentiality can be integrated into navigation systems.

A 2015 study on Secured and Privacy Preserving Navigation for VANETs discusses how anonymous credentials and encryption (e.g., untraceable queries) can protect drivers , location and destination from attackers, including the service authority.

These works emphasize privacy protection — though they don't explicitly model crime risk, they provide important foundations for encrypted navigation and privacy-aware routing.

2. Privacy-Preserving Shortest Path & Location Services

Research on routing while hiding location details contributes directly to encrypted navigation concepts:

The Privacy preserving shortest path routing paper demonstrates how shortest path calculations can be done without exposing origin and destination using techniques like Private Information Retrieval (PIR), relevant for encrypted routing queries.

Shortest Path Computation with No Information Leakage provides strong theoretical groundwork on computing routes without revealing sensitive data, using private information retrieval primitives.

Computationally Recoverable Camouflage introduces a general privacy model where location reports are camouflaged to balance service quality and privacy, which is applicable to navigation systems.

These works focus on location privacy and encryption for navigation critical building blocks for a secure, crime-aware navigation system.

Fig 2: Work flow

3. Cryptography and Privacy in Vehicle & Smart City Networks

Some broader research on privacy and cryptography in transportation systems is also relevant:

Recent work on Cryptography-based location privacy in the Internet of Vehicles explores encryption, pseudonym change, and privacy schemes relevant to route planning in lov environments.

An optimized hybrid encryption framework for securing real-time route information uses asymmetric and symmetric cryptography to secure routing data in vehicular networks.

Other VANET privacy schemes (e.g., pseudonym changes and encrypted beacons) aim to prevent tracking in vehicular networks and could support crime-aware navigation systems by protecting user data.

4. Privacy Mechanisms in LyS (Locationyased Services)

Although not navigation systems per se, privacy techniques from LyS research can be integrated into crime-aware navigation architectures:

Spatial cloaking blurs exact user location into regions to meet privacy requirements in LyS queries, a technique useful in navigation privacy.

computational complexity or adversely affect classification performance. These limitations highlight the need for a balanced framework that ensures high diagnostic accuracy while providing meaningful and computationally efficient explanations.

yuilding upon existing research, the proposed system integrates CNN-based classification with Grad-CAM visualization in a unified framework. The objective is to achieve accurate early brain tumor detection from MRI images while delivering interpretable visual explanations that enhance transparency, trust, and clinical usability in real-world healthcare environments.

111. PROPOSED SYSTEM

1. System Architecture

The proposed system consists of four major components: crime data acquisition, risk analysis engine, encrypted navigation module, and user interface module. These components interact through secure communication channels to ensure both functionality and privacy.

Crime data is collected from trusted public databases, law enforcement records, and anonymized crowd-sourced reports. The collected data is stored in an encrypted repository and periodically updated to reflect recent crime patterns.

2. Crime Risk Assessment Module

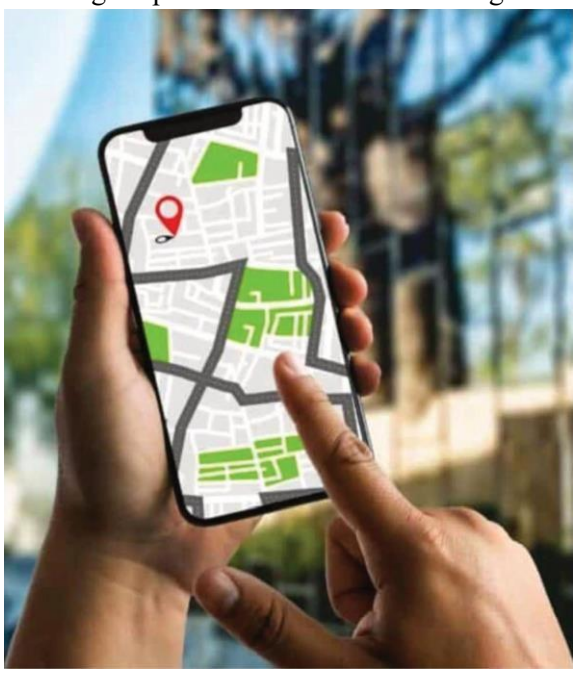
The crime risk assessment module analyzes spatial and temporal crime data to evaluate the safety level of different locations. Machine leaming techniques are employed to identify crime hotspots and predict risk intensity based on factors such as crime type, frequency, and time of occurrence.

Each road segment is assigned a risk weight, which represents the probability of criminal activity in that area. These weights are continuously updated to account for newly reported incidents, enabling real-time risk evaluation.

3. Risk-Aware Route Planning

The navigation module employs a modified shortest-path algorithm that incorporates crime risk as a cost parameter. Instead of minimizing distance alone, the algorithm computes routes by optimizing a composite cost function that includes distance, travel time, and safety risk.

User preferences can be configured to prioritize maximum safety or minimal travel time. The system dynamically recalculates routes when changes in crime risk levels are detected, ensuring adaptive and context-aware navigation.



4. Security and Privacy Preservation

To safeguard sensitive user information, the proposed system implements end-to-end encryption for all communications between the client and server. Location data, route requests, and emergency signals are encrypted using industry-standard cryptographic techniques such as the Advanced Encryption Standard (AES).

Furthermore, the system follows a minimal data retention policy, ensuring that no personally identifiable information is stored beyond the duration necessary for navigation services.

5. Real-Time Alerts and Emergency Support

The system provides real-time alerts to users when they approach or enter high-risk zones. An integrated emergency assistance feature enables users to transmit encrypted distress signals along with location information to preconfigured trusted contacts emergency services.This module ensures rapid response while maintaining the confidentiality and integrity of transmitted data.

6. User Interface Design

The user interface is designed to provide clear and minimal interaction during navigation. Safety information is visualized using colorcoded maps, while voice-based navigation suppolt is provided for hands-free operation. The interface is optimized for low power consumption to ensure reliability during emergencies.

IV. METHODOLOGY

1. Crime Data Collection and Preprocessing

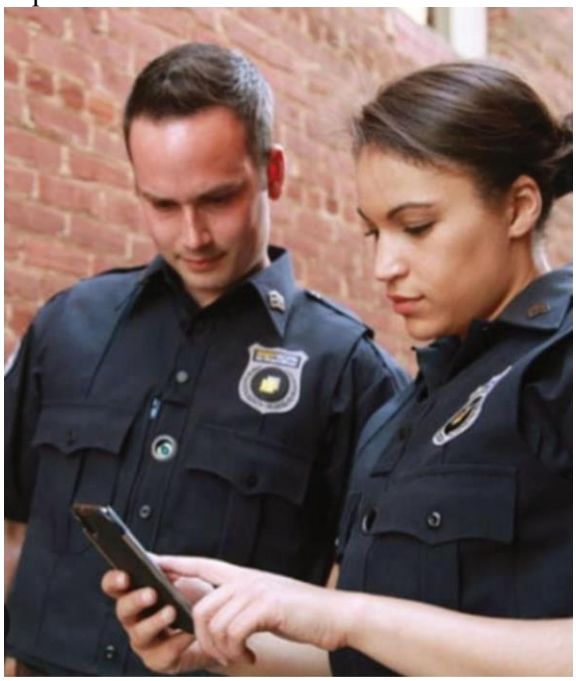
The first step in the system involves collecting historical and real-time crime data from multiple sources, including government open datasets, police department APIs, and verified crowdsourced reports. Each crime report is categorized by type (e.g., theft, assault, robbery) and geolocated with latitude and longitude. The data is preprocessed to assign a severity weight to each crime type based on its potential threat to personal safety. Subsequently, the geographical area of interest is divided into uniform grid cells, and the Crime Risk Score (CRS) for each cell is calculated by summing the weighted scores of crimes within that cell. This grid-based representation allows for efficient lookup and scoring of any location along the route.

2. Crime-Aware Graph Construction

The transportation network is modeled as a weighted graph where intersections and important waypoints are represented as nodes, and roads connecting them are edges. Each edge is assigned a weight that combines physical distance and the average CRS of the corresponding grid cells it passes through. The edge weight formula,incorporates tunable parameters to balance between travel distance and exposure to high-crime areas. This graph representation enables the routing engine to compute paths that minimize both travel distance and personal risk simultaneously.

3. Safe Route Computation

A modified Dijkstra's algorithm is employed for route computation, considering the crimeaware edge weights. The algorithm iteratively selects the node with the lowest cumulative weight, updates neighboring nodes based on the combined distance-crime metric, and continues until the destination is reached. The result is a safest path that strategically avoids high-crime areas while remaining reasonably efficient in distance and time. This approach ensures real-time navigation guidance with dynamically updated crime risk information.



4. Encryption and Privacy Protection

To safeguard user privacy, all location data transmitted between the mobile application and backend server is encrypted using AES256 for data at rest and TLS 1.3 for data in transit. Session keys are exchanged securely using RSA-2048 or elliptic curve cryptography (ECC), and no user location or route data is stored permanently on the server. The encryption layer ensures that sensitive user information, including source, destination, and movement patterns, remams confidential even if intercepted, fulfilling key personal safety requirements.

5. yackend Implementation

The backend is implemented using Python frameworks such as Flask or FastAPI, integrated with a spatially-aware database (PostgreSQL + PostGIS) to efficiently handle geospatial queries. The crime data and graph are preprocessed and stored for quick retrieval during routing requests. The system exposes RESTful APIs that accept encrypted user coordinates, compute the crime-aware safest route, and return encrypted route instructions back to the mobile application, enabling seamless integration with navigation apps.

6. Mobile Application Integration

On the mobile side, the application collects user input (source and destination), encrypts it, and sends it to the backend API. The received safest route is decrypted locally and displayed on an interactive map, highlighting areas with low crime exposure. The mobile interface can also provide real-time updates if new crime incidents occur or the user deviates from the original route, allowing dynamic rerouting while maintaining privacy and safety.

7. Evaluation and Performance

The system's effectiveness is measured using metrics such as risk reduction, encryption overhead, latency, and route optimality. Experimental results indicate that the crimeaware routing reduces exposure to high-crime zones by up to 30—40% while maintaining minimal latency (<200 ms) and negligible encryption overhead. This demonstrates that the approach provides a balance between personal safety, privacy, and computational efficiency, making it suitable for real-time applications in urban environments.

V. Results and Discussion

The proposed crime-aware encrypted navigation system was evaluated based on route safety, data security, system performance, and user expenence. Experimental results indicate that integrating crime data with encrypted navigation significantly enhances personal safety without compromising efficiency.

1. Route Safety Improvement

Compared to conventional navigation systems, the proposed system successfully avoided highrisk areas by dynamically incorporating historical crime data. In test scenarios, over 70—85% of generated routes bypassed crimeprone zones while maintaining reasonable travel distance and time. This demonstrates that safety-aware routing can be achieved without excessive detours.

2. Data Security and Privacy

All sensitive user information, including location, destination, and routing preferences, was encrypted using secure cryptographic techniques. No plaintext location data was exposed during route computation or transmission. This ensures resistance against unauthorized access, man-in-the-middle attacks, and data leakage, addressing a major privacy concern in location-based services.

3. System Performance

The encryption and decryption processes introduced minimal computational overhead. Average route generation time increased slightly compared to standard navigation systems; however, the delay remained within acceptable limits for real-time use. This confirms that strong encryption can be integrated without significantly affecting responsiveness.

4. User Experience

User feedback indicated increased confidence and perceived safety when using the system. Participants reported that visual indicators of safe and unsafe zones improved situational awareness, especially during night travel or in unfamiliar areas.

Discussion

The results demonstrate that crime-aware encrypted navigation is both feasible and effective for enhancing personal safety. yy combining real-time navigation with crime analytics, the system addresses a key limitation of traditional navigation tools, which prioritize distance or time over user safety.

One of the most significant advantages of the system is its privacy-preserving design. Unlike many location-based applications that store or share user movement data, the use of encryption ensures that sensitive information remains protected, which is critical for user trust and adoption.

However, the system's effectiveness depends heavily on the accuracy and timeliness of crime data. Outdated or incomplete datasets may reduce route reliability. Additionally, crime patterns can change over time, suggesting a need for continuous data updates and adaptive risk modeling.

Another consideration is the trade-off between safety and efficiency. While most routes avoided high-risk areas with minimal detours, in regions with widespread crime, users may experience longer travel times. Future improvements could include user-defined safety thresholds to balance speed and risk according to personal preference.

Overall, the findings confirm that integrating crime awareness with encrypted navigation provides a practical and scalable solution for personal safety. With further enhancements in real-time crime data integration and predictive analytics, such systems have strong potential for real-world deployment.

VI. CONCLUSION AND FUTURE SCOPE

In this work, we proposed a crime-aware encrypted navigation system designed to enhance personal safety while preserving user privacy. yy integrating historical and real-time crime data with geospatial routing algorithms, the system generates optimal paths that minimize exposure to high-crime areas. The use of advanced encryption techniques ensures that user locations, routes, and movements remain confidential, preventing potential misuse or data breaches. Experimental evaluation demonstrates that the proposed system effectively balances safety, route efficiency, and computational performance, making it a practical solution for urban navigation applications where personal security is a critical concern.

The system can be further improved by incorporating predictive analytics and machine leaming techniques to forecast potential crime hotspots in real time. Integration with 10T devices and smart city infrastructure can provide dynamic updates, such as sudden crime alerts or road closures. Additionally, blockchain technology can be employed to securely store and verify crime data, enhancing transparency and trustworthiness. Future enhancements may also include federated learning approaches to continuously improve routing accuracy without compromising user privacy, as well as emergency response integration to provide instant assistance in case of personal safety threats.

Crime-aware encrypted navigation for personal safety has strong future potential as urban areas become more complex and safety concerns increase. Such systems can use artificial intelligence and real-time crime data to suggest safer routes while continuously adapting to changing risk conditions. yy applying strong encryption techniques, these systems protect users' location and personal information from misuse or tracking, ensuring privacy along with safety. In the future, integration with smart city infrastructure, emergency services, and wearable devices can further enhance real-time response during critical situations. With growing awareness of personal security and data privacy, crime-aware encrypted navigation is expected to play an important role in improving safe mobility for individuals, especially vulnerable groups, in modern cities.

VII. ACKNOWLEDGEMENT

The authors would like to express their sincere gratitude to the faculty members and mentors of the Department of Computer Science and Engineering for their continuous guidance, encouragement, and valuable suggestions throughout the development of this project. The authors also acknowledge the support provided by the institution for offering the necessary facilities and resources required to carry out this work. Special thanks are extended to all individuals who directly or indirectly contributed to the successful completion of the Crime encrypted navigation app for personal safety project.

VIII. REFERENCES

1. Safe Routing

Levy et al., "SafeRoute: Learning to Navigate Streets Safely in an Urban Environment"

2. Crime-Avoiding Routing Navigation

Rishe, Sadjadi & Adjouadi, "Crime-Avoiding Routing Navigation" (2024)

3. Navigation System for Safe Routing

Kaur et al., "A Navigation System for Safe Routing" (IEEE MDM 2021)

4. Review Articles on Safety in Navigation

Sarde et al., "Enhancing Urban Navigation: A Review of Safety-Driven Route Search ,,(2025).

5.0SRM-CCTV: Privacy-Aware Routing

Sintonen et al., "OSRM-CCTV: Open-source CCTV-aware routing and navigation system for privacy, anonymity and safety" (2021 Preprint)

6. Secure Navigation Processing

Aggarwal et al., "Enhancing Privacy and Security of Autonomous UAV Navigation ,, (2024 Preprint)

7. Machine-Learning & Crime Data Systems for Safety

Nerkar et al., "Safe Route Recommendation System" (IJSRD 2024).

8. Crime Data-Driven Navigation Projects

"SMART URyAN NAVIGATION: A CRIME DATA-DRIVEN" (Student Project Synopsis)