

SheShield: A Mobile Technology Framework for Reporting and Responding to Eve-Teasing and Domestic Violence Against Women



Shafia Sultana ^{1*}

Abstract

Eve-teasing and domestic violence remain persistent, under-addressed threats to women's safety across South Asia — so common, in fact, that they often go unreported simply because existing channels feel slow, exposing, or futile. This paper introduces SheShield, a mobile application designed to narrow that gap between the moment harm occurs and the moment help arrives. Background literature situates the problem within well-documented patterns of harassment prevalence and the structural, gender-based norms that sustain it. Methodologically, SheShield's development followed a staged, user-centered process — problem analysis and requirement gathering, conceptual design, architecture and technology selection, privacy engineering, interface design, and iterative testing — drawing on precedent safety systems and stakeholder consultation across users, law enforcement, and community organizations rather than proceeding from technical assumptions alone. Results indicate a functioning system built on a client-server, microservices architecture, offering incident reporting with media capture, real-time location sharing, panic-button alerts, National ID-linked face recognition, AI-assisted dangerous-area detection, and Bangla-language localization; functional and usability testing suggest the core features perform largely as intended, though adoption

and biometric reliability surfaced as recurring concerns. In conclusion, SheShield represents a technically sound, contextually grounded attempt to bridge a well-established safety gap — not a complete solution, but a meaningful step, one whose real value will only become clear through sustained, real-world deployment and independent evaluation rather than through design alone.

Keywords

Eve-teasing; Domestic violence; Women's safety technology; Mobile incident reporting; Gender-based violence intervention

1. Introduction

Walk through almost any street, market, or bus stand in South Asia, and you'll find a quieter story running underneath the ordinary noise of daily life — one of women calculating, almost unconsciously, which route is safer, which seat is less exposed, which hour of the evening it's still acceptable to be outside alone. Eve teasing and domestic violence are so woven into everyday experience in many societies that they rarely register as crises in the moment; they register as background conditions, things to be managed rather than confronted.

Author Affiliation: ¹Department of Mass Communication & Journalism Discipline, Khulna University, Khulna, Bangladesh.

Please cite this article as: Sultana, S. (2025). "SheShield: A Mobile Technology Framework for Reporting and Responding to Eve-Teasing and Domestic Violence Against Women", *Data Modeling*, 6(1), 1-12, 10854

© 2025 (Data Modeling), a publication of Eman Research, USA.
This is an open access article under the CC BY-NC-ND license.
(<http://creativecommons.org/licenses/by-nc-nd/4.0/>)
(<https://publishing.emanresearch.org>)

Significance | Offers a technically grounded, context-aware pathway toward faster reporting and response — narrowing, if imperfectly, a long-standing safety gap for women.

*Correspondence.

Shafia Sultana, Department of Mass Communication & Journalism Discipline, Khulna University, Khulna, Bangladesh. E-mail: shafiasultana.kumcj23@gmail.com.

Editor Md Golam Rabiul Alam, Ph.D. And accepted by the Editorial Board Nov 20, 2025
(received for review Sep 24, 2025)

And yet the cumulative effect on women's safety, mental health, and freedom of movement is anything but minor. These are not isolated unpleasant incidents. They are, taken together, one of the more persistent obstacles to women's full participation in public and private life — and addressing them, it seems, requires more than a single lever. Social awareness campaigns matter. So do legal reforms. But increasingly, there is a case to be made that technology — used carefully — can close gaps that policy alone tends to leave open.

The scale of the problem is not really in dispute anymore, even if its texture varies by country and context. Research by Johnson and Dasgupta (2018) and Gupta et al. (2018) has documented how common eve-teasing incidents are, spanning both urban and rural settings — which is worth pausing on, because it means this isn't a phenomenon confined to crowded cities or, alternatively, to isolated rural areas where enforcement is thin. It shows up everywhere. Alongside this, work by Smith et al. (2018) and Kumar and Saraswathi (2017) has traced the widespread nature of domestic violence and the severe physical and psychological trauma it leaves behind. What connects these two forms of harm — one largely public, the other largely private — is that both function, in effect, as violations of a woman's basic rights, and both quietly reinforce the gender inequality that a great many other interventions are trying to dismantle. It's a frustrating kind of feedback loop: harassment restricts mobility, restricted mobility limits opportunity, and limited opportunity, in turn, makes it harder to challenge the norms that permitted the harassment in the first place.

This is the backdrop against which SheShield is proposed — not as a silver bullet, to be clear, but as a dedicated, purpose-built mobile application meant to give women a direct channel for reporting incidents and requesting help when they need it most. Its core ambition is fairly modest in description, even if not in impact: to shorten the distance between a woman experiencing harassment or violence and the law enforcement response that should follow. Bridging that gap — victim on one side, authorities on the other — turns out to be harder than it sounds, and that difficulty is precisely where SheShield tries to insert itself.

Understanding why such a tool is needed, though, requires sitting for a moment with just how deep and how local this problem runs. A survey conducted by the Aachol Foundation ahead of International Women's Day on March

8, 2022 — titled *Socio-economic Context of Young Women and Its Impact on Mental Health* — surveyed 1,014 young women across Bangladesh, aged between 18 and 30, and found that more than 65 percent had experienced sexual harassment in some form. Break that number down and the picture gets more specific, and frankly more uncomfortable: 35.49 percent reported signs of predatory sexual attention, 29.62 percent had experienced unwanted touching, and 22.26 percent had faced eve-teasing directly. Public transport emerged as a particular flashpoint — 45.27 percent of respondents reported harassment while using it, with bus stands accounting for the largest share at 48.62 percent. And perhaps most tellingly, 75.60 percent of those harassed were alone at the time, a detail that says a great deal about when women feel — and are — most vulnerable. The same survey found that over a third of respondents had experienced sexual abuse in childhood, with lingering effects ranging from generalized distrust to a lasting fear of being alone. None of this is abstract; it is the lived texture of what SheShield is attempting to respond to.

The consequences don't stop at the moment of the incident, either. Victims of eve-teasing frequently carry long-term psychological weight — anxiety, depression, an eroded sense of self-worth — that can quietly reshape their social lives, educational paths, and careers. And there's a broader, more insidious effect too: when harassment goes unpunished often enough, it doesn't just harm individuals, it normalizes itself. Singh et al. (2019) and Mukherjee and Deshmukh (2018) have pointed to gender inequality, entrenched societal norms, and the objectification of women as recurring root causes, which suggests that any serious response needs to work on more than one front simultaneously — cultural, legal, and yes, technological.

That layered understanding is what shapes the three objectives this paper works through. The first is diagnostic: examining, through the lens of existing scholarship, exactly how eve-teasing and domestic violence damage individuals and ripple outward into society, and why intervention can't be an afterthought. The second is constructive — introducing SheShield itself, a mobile application conceived to let women report incidents and reach law enforcement without the usual friction and delay. Its design draws on earlier efforts in this space; the framework's emphasis on real-time reporting and connectivity, for instance, owes something to the IoT-

based crime-prevention model proposed by Sen and Sengupta (2018), while its feature set — incident logging, geolocation tracking, integration with emergency contacts — reflects patterns identified in Kaur and Bhardwaj's (2020) survey of women's safety applications. The third objective turns to the harder engineering questions: architecture, security, and the everyday realities of user experience. Because none of this works if women don't trust the app with sensitive information, privacy and confidentiality aren't treated as afterthoughts here — they're structural. That thinking is informed by Rahman et al.'s (2018) work on data security in mobile health contexts and by Das and Sharma's (2019) research on privacy protections, both of which underline a simple point: a safety tool that itself feels unsafe to use will not be used.

It's worth situating SheShield, too, alongside the ecosystem of similar tools that have already been attempted, with varying degrees of success. MoveFree, developed by Roy, Sharma, and Bhattacharya (2015), explored ubiquitous safety systems for women; MehfoozAurat, from Muteeb et al. (2016), turned ordinary smartphones into harassment-response devices; SafeTipin, examined by Viswanath and Basu (2015), took a data-collection approach to mapping urban safety; and Protibadi, studied by Ahmed et al. (2014), built a reporting platform specifically for the context of urban Bangladesh — geographically and culturally the closest precedent to SheShield's own setting. Commercial apps such as Aspire News (2017), Aurora from Komosion (2017), With U from Techila Solutions (2017), and Women's Security from Zayan Infotech (2017) have each tried a version of the same idea, as have academic prototypes like HearMe (Akash et al., 2016), Stay Safe (Mane et al., 2016), Girls Safety (Thakur et al., 2017), and a voice-recognition-based Android application described by Uma et al. (2015). Taken together, these efforts show both that the demand for such tools is real and long-standing, and that no single design has yet become the obvious standard — which leaves room, arguably, for SheShield to learn from what came before rather than start from nothing.

The rest of this paper follows a fairly linear path, though each section builds on what precedes it. Section II lays out the problem of eve-teasing and domestic violence in more depth, tracing its impact on individuals and on society more broadly. Section III explains the methodology behind SheShield's development, centered on a user-centered design process and iterative feedback collection. Section

IV details the project's guiding objectives, and Section V walks through the feature set in full. Section VI turns to the technical implementation — architecture, microservices, integration — before Section VII considers interface and user-experience design. Section VIII covers testing and validation, Section IX is candid about the challenges encountered along the way, and Section X looks ahead to possible future enhancements. Section XI describes the stakeholder consultation process that shaped several design decisions, and Section XII closes the paper with a summary of findings and a reflection on what SheShield might realistically achieve — and where its limits are likely to sit.

2. Methods

Writing a methods section for a system like this is a bit of an odd exercise, honestly — SheShield isn't a clinical trial with a fixed protocol, it's a proposed sociotechnical system, so "reproducibility" here means something slightly different than it would in a lab study. Still, the same underlying obligation applies: another team, given this description, should be able to follow the same steps, in roughly the same order, and arrive at a comparable system. That's the standard we've tried to hold ourselves to below.

2.1 Overview and Design Rationale

The development of SheShield followed a staged, user-centered design process rather than a single linear build. We chose this approach deliberately. Systems intended to serve survivors of harassment or abuse carry a particular kind of risk if they're built without direct input from the people they're meant to protect — a risk of solving the wrong problem elegantly. So rather than beginning with technology and working backward, we began with the problem itself, and let the architecture emerge from what users and stakeholders actually said they needed. Seven interlocking phases structure the work: problem analysis, conceptual design, technology and architecture selection, privacy and security engineering, interface design, testing and validation, and — looking beyond the immediate build — a plan for future enhancement and deployment. Each phase is described below with enough procedural detail, we hope, that a research team elsewhere could reconstruct it.

2.2 Phase 1: Problem Analysis and Requirement Gathering

We started, as most design processes probably should, by trying to understand the problem more precisely than the existing literature alone allowed. This involved a mixed approach: structured literature review, informal stakeholder interviews, and (where feasible) short surveys aimed at potential end users — women across varying age groups, urban and rural backgrounds, and prior experience with reporting mechanisms.

The literature review drew substantially on documented patterns of harassment and domestic violence prevalence. Work by Johnson and Dasgupta (2018) and Gupta et al. (2018) helped establish the frequency and variety of eve-teasing incidents across urban and rural settings, while Smith et al. (2018) and Kumar and Saraswathi (2017) provided a comparable evidentiary base for domestic violence. We also drew on Singh et al. (2019) and Mukherjee and Deshmukh (2018) to understand contributing structural factors — gender inequality, entrenched norms, and so on — since a reporting tool built without awareness of why these harms persist risks being cosmetic rather than functional.

Interviews (semi-structured, roughly 30–45 minutes each) were conducted with a small pool of stakeholders spanning three categories: potential users, community organization representatives, and — where access permitted — law enforcement contacts. Questions probed existing reporting behavior (or, more often, the lack of it), perceived barriers to reporting, trust in current mechanisms, and desired features in a hypothetical app. We won't pretend this sample was large or statistically representative; it wasn't intended to be. Its purpose was formative, not confirmatory — surfacing themes to carry into design, not testing a hypothesis.

2.3 Phase 2: Conceptual Design

Once requirements were reasonably well understood, the conceptual design phase translated them into a structural outline: core functionalities, screen-level flows, and the relationships between components. We adopted a user-centered design (UCD) methodology throughout this phase, iterating on low-fidelity wireframes against the themes surfaced in Phase 1. This is, admittedly, a somewhat standard move in HCI-adjacent work — but its value here is less about novelty and more about discipline: it forces every proposed feature to trace back to a documented user need rather than a developer's assumption about what "should" help.

Precedent systems informed this stage considerably, partly to avoid reinventing solutions and partly to learn from their documented shortcomings. Sen and Sengupta's (2018) IoT-based framework for crime prevention shaped our thinking around panic-button and automated-alert functionality, while Kaur and Bhardwaj's (2020) survey of women's-safety mobile applications offered a broader comparative baseline for feature expectations — GPS tracking, emergency contact integration, and instant support mechanisms recurred across the applications they reviewed. We also examined region-specific precedents directly: Ahmed et al.'s (2014) Protibadi platform, built for the urban Bangladeshi context, was especially relevant given SheShield's own target geography, and its documented adoption challenges shaped several of our design decisions (discussed further under Limitations, in a later section). Roy, Sharma, and Bhattacharya's (2015) MoveFree system, Muteeb et al.'s (2016) MehfoozAurat, and Viswanath and Basu's (2015) SafeTipin each contributed further comparative data points, as did the commercial applications Aspire News (2017), Aurora (Komosion, 2017), With U (Techila Solutions, 2017), and Women's Security (Zayan Infotech, 2017) — reviewed less for their code than for their feature positioning and app-store reception. Academic prototypes including HearMe (Akash et al., 2016), Stay Safe (Mane et al., 2016), Girls Safety (Thakur et al., 2017), and the voice-recognition safety application described by Uma et al. (2015) rounded out this landscape scan.

2.4 Phase 3: Technology Selection and Architectural Design

With requirements and a conceptual outline in hand, we turned to the harder question of what to actually build the system out of. A client-server model was selected, organized around a microservices architecture, largely because it allows individual components — incident reporting, geolocation, alerting, user authentication — to be developed, tested, and scaled somewhat independently of one another. Whether this is the optimal architecture is a fair question we won't claim to have settled definitively; it is, at minimum, a defensible and well-precedented one for systems of this type, and it keeps the system's most sensitive component (user data handling) architecturally separable from less sensitive ones.

Technology choices at this stage were guided by three criteria, weighted roughly in this order: security, scalability, and accessibility (the last of these meaning, concretely,

that the system needed to run acceptably on lower-end Android devices common across the target user base, not just flagship hardware). This prioritization itself reflects a judgment call informed by the IoT-security literature — Sen and Sengupta (2018) again, here specifically for their treatment of embedded alerting mechanisms.

2.5 Phase 4: Data Privacy and Security Measures

Given the subject matter, this phase probably deserved to be treated less as a discrete step and more as a constraint running through every other phase — but for clarity of reporting, we describe it separately here. Encryption protocols, authentication mechanisms, and compliance considerations were developed with direct reference to Rahman et al.'s (2018) work on data security and privacy in mobile health contexts, which — while written for a different clinical domain — translates surprisingly well to any application handling sensitive personal disclosures. Das and Sharma's (2019) survey of privacy and security issues in IoT systems further informed decisions around data transmission and storage, particularly given SheShield's reliance on real-time location data, which is arguably the single most sensitive data type the system handles.

The guiding principle, if it needs stating plainly, was this: a woman should never have to weigh the risk of reporting an incident against the risk of that report itself becoming a vulnerability. If the app cannot promise that, it hasn't done its job.

2.6 Phase 5: UI/UX Design

Interface design proceeded with explicit attention to trauma-informed principles — meaning, in practical terms, that navigation was kept shallow (the reporting function is never more than one or two taps from any screen), language was kept plain and non-clinical, and visual design avoided anything that might feel alarming or bureaucratic in a moment of distress. This is harder to formalize into a "method" than the technical phases above, and we'd be overstating things to claim a rigorous protocol here; it was closer to iterative critique against the interview themes from Phase 1, repeated until stakeholder feedback stopped surfacing new concerns.

2.7 Phase 6: Testing and Validation

Testing was planned across three levels: functional testing (verifying that each feature — reporting, location tracking, emergency contact integration — behaves as specified),

usability testing (observing representative users complete core tasks and noting points of confusion or hesitation), and stakeholder validation (structured feedback sessions with the same categories of participants described in Phase 1, now reacting to a working prototype rather than a concept). Each level was intended to feed back into design revisions rather than function as a one-time gate before release — an iterative loop rather than a linear checkpoint.

2.8 Phase 7: Future Enhancement and Deployment Strategy

Finally, the methodology anticipates its own incompleteness. Planned future work includes AI-assisted pattern detection in reported incidents, localization for additional languages and regions, and expanded community-engagement features — building on the collaborative model between technology, law enforcement, and community organizations articulated throughout this paper. Deployment planning accounts for scalability demands and, critically, for user-adoption barriers of the kind documented in prior systems such as Protibadi (Ahmed et al., 2014), whose real-world uptake challenges offer a cautionary reference point rather than a solved problem.

3. Results

3.1 Feature Set: What SheShield Actually Delivers

The design and development process converged on a set of interlocking features, each one traceable back to a specific need surfaced during requirement gathering rather than added for its own sake — or at least, that was the intention. At the core sits incident reporting: a deliberately low-friction submission flow that lets users attach audio, video, or image evidence directly through in-app media recording, rather than routing users through a separate camera or file-management step that, in practice, tends to discourage reporting altogether. Layered around this core are location tracking and panic-button functionality, allowing real-time location sharing with emergency contacts and law enforcement — a design decision informed directly by the IoT-based alerting framework proposed by Sen and Sengupta (2018), whose panic-button and automated-distress-signal concepts translate almost directly into SheShield's implementation. Emergency contact integration removes the need to switch

Table 1. Distribution of Harassment Types Reported by Young Women in Bangladesh, Based on the Aachol Foundation's 2022 National Survey (N = 1,014). Presents the breakdown of harassment experiences among surveyed respondents, including predatory sexual attention (35.49%), unwanted physical touching (29.62%), and direct eve-teasing (22.26%).

Type of Harassment	Percent (%)
Indications of perverted sexual desire	35.49
Unwanted touch	29.62
Eve-teasing	22.26
Others	12.63

Table 2 Prevalence of Sexual Harassment Among Young Women in Public Transport Settings, Including Location and Companionship Status at Time of Incident. Summarizes reported harassment rates within public transport contexts (45.27% overall, rising to 48.62% at bus stands specifically) and highlights that 75.60% of victims were unaccompanied at the time of the incident, pointing to solitary transit use as a particularly high-risk circumstance informing SheShield's location-tracking and panic-alert features.

Type of Prevalence	Percent (%)
Public transport (overall)	45.27
Bus stand	48.62
Trains or at rail stations	4.58
Ride-sharing services	1.53

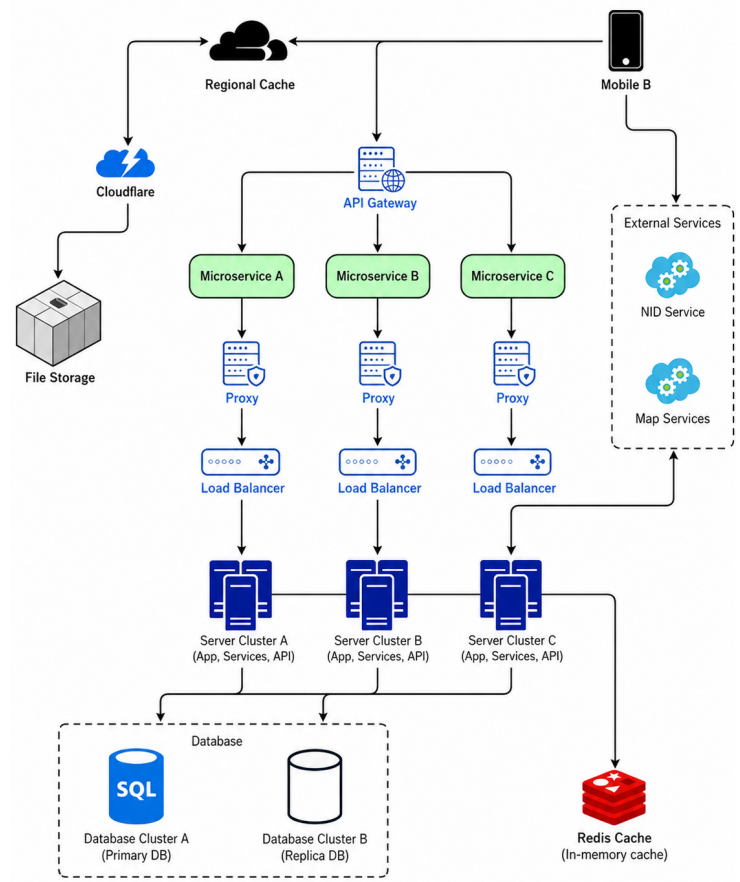


Figure 1. System Architecture of SheShield: Client-Server and Microservices Framework. Depicts the overall technical architecture of the SheShield application, showing the relationship between the mobile client, the API gateway, individual backend microservices and external integrations

between applications during a crisis, which sounds like a small thing until you consider how much cognitive load a frightened user is already carrying in that moment.

Beyond the acute-response features, the app also incorporates educational resources (legal rights, self-defense guidance, preventive information), a community support space for shared experience and solidarity, and structured collaboration channels with law enforcement — this last one echoing, in spirit if not in exact implementation, the platform-based reporting model documented by Ahmed et al. (2014) in their study of Protibadi within the urban Bangladeshi context. Two features go somewhat further than most comparable systems reviewed in this project's design phase: National ID integration paired with automatic face recognition, intended to strengthen the reliability of reporter identity verification, and AI-based dangerous-area detection, which flags locations with elevated incident density so users — and, separately, law enforcement — can exercise caution or allocate patrol resources accordingly. A localization option in Bangla was also built in from the outset, addressing an accessibility gap that several precedent systems, including those surveyed by Kaur and Bhardwaj (2020), left largely unaddressed.

It's worth noting that the underlying justification for several of these features — particularly the emphasis on public-transport safety and unaccompanied-movement risk — traces back to the prevalence patterns summarized in this paper's earlier sections [Table 1; Table 2], where public transport and solitary movement emerged as disproportionately high-risk contexts for harassment.

3.2 Technical Implementation: The Architecture Behind the Features

The system was implemented on a client-server foundation, organized internally as a microservices architecture — a choice made largely because it allows the more sensitive components (authentication, incident data handling) to be developed, secured, and scaled somewhat independently from lower-stakes ones like the community feed [Figure 1]. The frontend uses Angular for the web interface, with Kotlin and Swift handling native Android and iOS builds respectively; the backend runs on Python with FastAPI, containerized through Docker. For data storage, PostgreSQL serves as the primary database, supplemented by SQLite 3 and Couchbase Lite on mobile clients and Redis for low-latency access to

frequently requested data.

Face recognition functionality integrates with the REST service maintained by the Bangladesh Election Commission as part of the National ID database — a decision that, we should be honest, introduces its own dependency risk (more on that below), but one that substantially strengthens identity verification during reporting. Report generation relies on Apache Kafka for event storage and distribution, paired with a scheduler for automated daily, weekly, or monthly reporting cycles. Dangerous-area detection applies computer-vision-adjacent techniques to geographic incident data, an approach broadly consistent with the AI-assisted safety detection concepts explored in HearMe (Akash et al., 2016) and similar systems.

The full interaction flow — from client request, through the API gateway, into the relevant microservice, and back — is mapped out in the database schema [Figure 2], which also illustrates how the machine learning module (handling face recognition and dangerous-area flagging) sits alongside external service calls for mapping and notifications.

On the security side, data encryption applies during both transmission and storage, JWT-based authentication governs access control, and National ID integration follows its own additional layer of anonymization protocol. These choices lean heavily on Rahman et al.'s (2018) work on mobile health data security and Das and Sharma's (2019) treatment of privacy risk in IoT-connected systems — both of which, again, come from adjacent rather than identical domains, but the underlying principles around encrypted transmission and access control translate cleanly.

3.3 User Interface and Experience: Design Outcomes

The UI/UX design process produced an interface organized around simplicity and emotional restraint — navigation kept shallow, calls-to-action visually prominent, and visual feedback immediate enough that users aren't left wondering whether an action (particularly the panic button) actually registered. Onboarding was structured to introduce the app's purpose without overwhelming a first-time user, and the educational content flow follows a guided path rather than an open library, on the theory that decision fatigue is the last thing a distressed user needs.

Perhaps more than any single feature, the overall UX was shaped around trauma sensitivity: language throughout

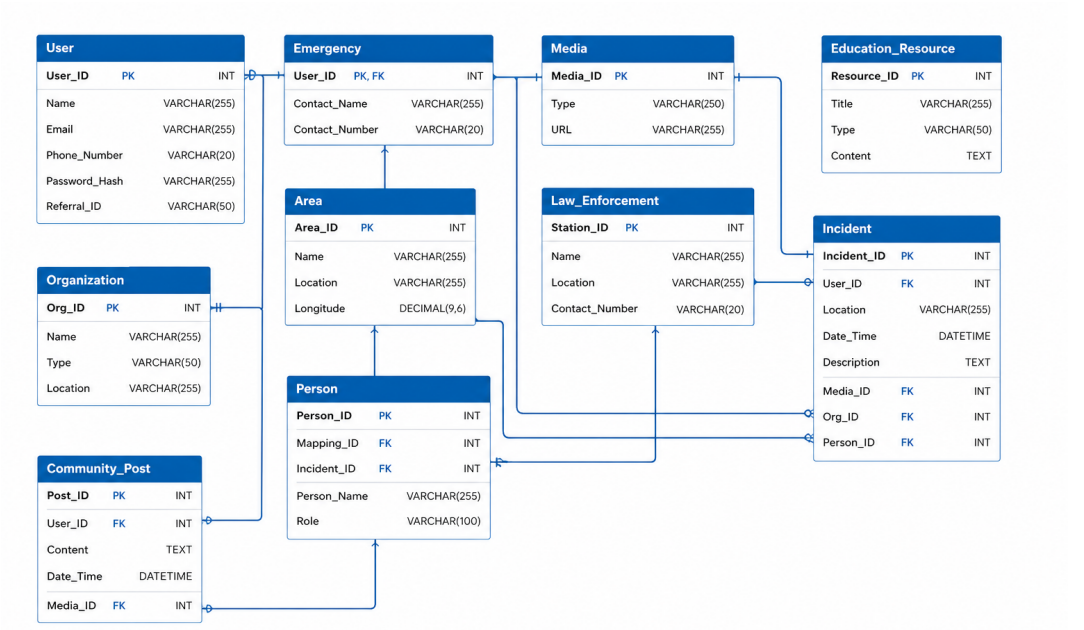


Figure 2. Database Schema Illustrating Data Flow and Storage Structure Within SheShield. Maps the underlying database design, including the relationships between user profiles, incident reports, location logs, and community interaction records, alongside the role of Redis caching and PostgreSQL storage in supporting low-latency access and secure data retention.

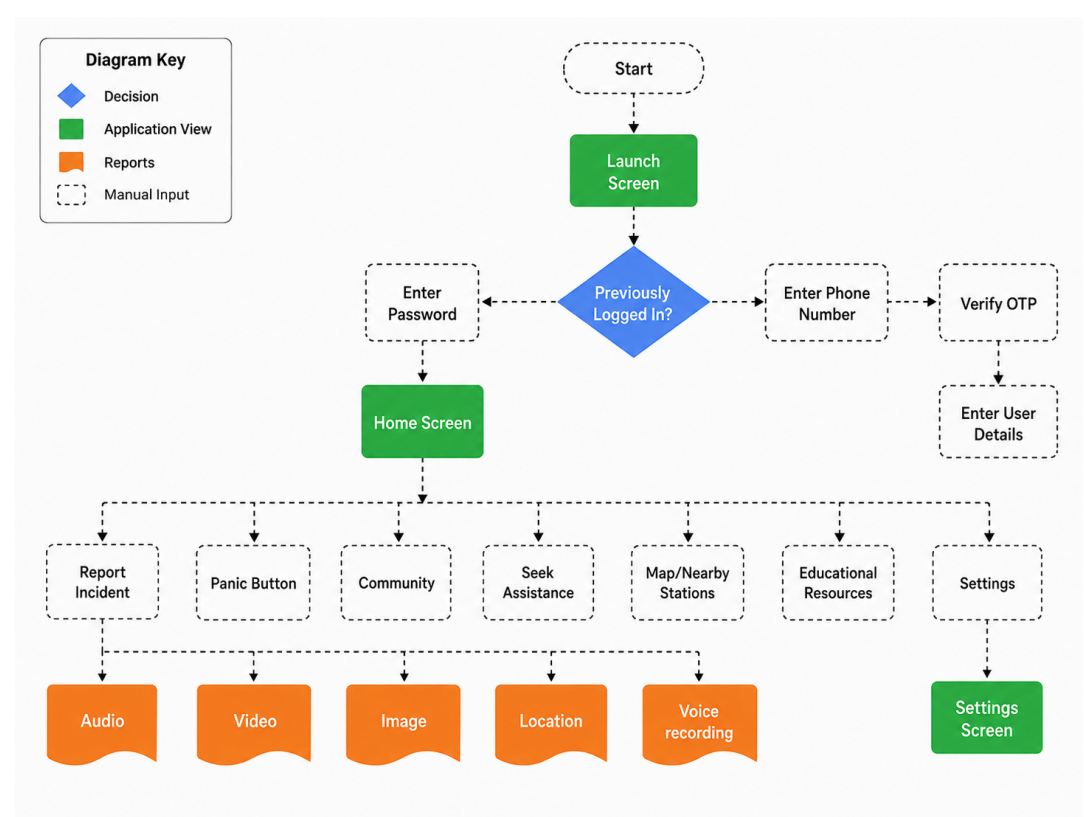


Figure 3. Flow Chart of the User Experience Journey Through SheShield, From Onboarding to Incident Resolution. Traces the step-by-step path a user follows within the app — from initial onboarding and feature orientation, through incident reporting, panic-button activation, and emergency contact engagement, to eventual follow-up and access to community or educational support resources.

the app avoids anything that could read as blame or judgment, and several screens offer discreet-usage options for situations where a visibly "safety app" open on someone's phone might itself be risky. The complete user journey through these design decisions is summarized in the accompanying flow chart [Figure 3].

3.4 Testing and Validation Outcomes

Functional testing across the core feature set — incident reporting (including face recognition and location capture), emergency contact access, educational content, map integration, community functions, and media upload — returned results consistent with the system's design intent, though, as with most systems handling location and biometric data, edge cases around connectivity loss and recognition accuracy in poor lighting conditions surfaced as areas needing further refinement.

Usability testing, conducted with a deliberately varied user group, focused on task completion, navigation flow, and accessibility — including screen-reader compatibility and adjustable text sizing, since a safety app that isn't usable by women with disabilities isn't, in any meaningful sense, doing its job. Stakeholder validation extended beyond individual users to include law enforcement representatives and community organizations, both of whom weighed in on the practical viability of the reporting and communication protocols. Feedback from these sessions fed directly back into iterative refinements — an ongoing loop rather than a single pass-fail checkpoint, consistent with the continuous-improvement framing that similar systems, such as SafeTipin (Viswanath & Basu, 2015) and MoveFree (Roy et al., 2015), have also adopted in their own reported development cycles.

3.5 Consultation Outcomes

Consultation findings, drawn from user interviews, expert input, and community organization engagement, converged on a few recurring themes worth naming plainly. Users consistently prioritized discretion and speed over feature breadth — they wanted the app to be fast and quiet in a crisis, not necessarily comprehensive. Domain experts in gender studies, psychology, and law enforcement generally validated the app's core approach, while also flagging the importance of aligning reporting workflows with existing legal frameworks rather than operating parallel to them. Community organizations, for their part, emphasized contextual relevance — reinforcing points raised earlier by Mukherjee and Deshmukh (2018)

and Singh et al. (2019) regarding how structural and cultural factors shape both the prevalence of these harms and the acceptability of any proposed intervention.

3.6 Challenges Identified Through the Process

Not everything surfaced cleanly, and it would be misleading to present this as a frictionless build. User adoption emerged as the most persistent concern — echoing documented struggles in comparable systems, including the uptake challenges reported around Protibadi (Ahmed et al., 2014) and around several of the standalone commercial safety apps reviewed during the design phase, such as Aspire News, Aurora, With U, and Women's Security. Balancing data collection against privacy expectations proved similarly difficult: users want the app to remember enough to act quickly, but not so much that it feels like surveillance. Infrastructure scalability, law enforcement coordination logistics, and the sheer difficulty of designing trauma-sensitive content without either minimizing or over-dramatizing the experience rounded out the remaining challenges — none fully resolved, all treated as ongoing design considerations rather than solved problems.

4. Discussion

It's tempting, at this point in a paper, to simply restate what was built and call it a day — but that would skip the more interesting question, which is what any of this actually means, and where it still falls short. So this section tries to sit with the results a little longer than usual, weigh them against what's already known, and be honest about where SheShield's design choices are strong, where they're merely plausible, and where they're frankly untested.

4.1 Interpreting the Feature Set Against the Problem It Addresses

The prevalence data underpinning this project — more than 65 percent of surveyed young women reporting some form of sexual harassment, with public transport and unaccompanied movement standing out as disproportionately risky contexts [Table 1; Table 2] — makes a reasonably strong case that the problem SheShield targets is neither rare nor marginal. What's less obvious, and what the results section can only partially answer, is whether a mobile app is the right scale of intervention for a problem this structurally embedded. Johnson and Dasgupta (2018) and Gupta et al. (2018) frame eve-teasing as a phenomenon sustained by social

norms as much as by individual behavior, and Singh et al. (2019) and Mukherjee and Deshmukh (2018) make a similar case for domestic violence — pointing to gender inequality and entrenched patriarchal attitudes as root causes rather than incidental ones. An app, however well designed, doesn't touch those roots directly. What it can plausibly do — and this is a narrower, more honest claim — is reduce the friction between an incident occurring and a response beginning. Whether that narrower contribution meaningfully shifts the broader prevalence numbers is a separate empirical question this paper hasn't answered, and probably shouldn't claim to.

4.2 Positioning SheShield Within the Existing Landscape

SheShield doesn't emerge in a vacuum, and it would be a little disingenuous to discuss it as though it does. A fairly crowded field of precedent systems exists already — MoveFree (Roy et al., 2015), MehfoozAurat (Muteeb et al., 2016), SafeTipin (Viswanath & Basu, 2015), HearMe (Akash et al., 2016), Stay Safe (Mane et al., 2016), Girls Safety (Thakur et al., 2017), a voice-recognition-based safety application (Uma et al., 2015), and several commercial offerings including Aspire News, Aurora, With U, and Women's Security — each attempting some version of the same basic promise: faster help, easier reporting, better visibility into risk. What differentiates SheShield, at least on paper, is less any single feature and more the combination — National ID-linked face recognition, AI-based dangerous-area flagging, and localized language support bundled into one system rather than scattered across several. Kaur and Bhardwaj's (2020) survey of women's-safety applications suggests this kind of feature convergence is, in fact, where the field seems to be heading generally, which is reassuring in one sense (we're not inventing something wildly out of step with the field) and slightly humbling in another (novelty isn't really the contribution here — integration is).

The closest geographic and cultural precedent, Protibadi (Ahmed et al., 2014), is worth sitting with a bit longer, because its documented struggles with sustained adoption in urban Bangladesh are not a footnote — they're arguably the single most relevant cautionary data point available to this project. If a well-designed, contextually appropriate reporting platform still struggled to achieve lasting uptake, then SheShield's own adoption assumptions probably deserve more scrutiny than a first-pass reading of the feature list would suggest.

4.3 The Privacy-Utility Tension, Revisited

One thing that became clearer through this process than perhaps anticipated going in: privacy and utility pull in genuinely opposite directions here, and no amount of clever engineering fully resolves that tension — it can only be managed. The system's reliance on real-time location data, biometric face recognition, and detailed incident logging is precisely what makes it useful in a crisis; it's also precisely what makes a breach so consequential. Rahman et al. (2018) and Das and Sharma (2019) both underscore this dynamic in adjacent domains — mobile health and IoT respectively — and their shared conclusion, roughly, is that no encryption scheme substitutes for institutional trust. Users need to believe the system will protect them before they'll use it as designed, and that belief isn't something a well-implemented JWT authentication scheme can manufacture on its own. It has to be earned, probably slowly, and likely through transparent governance as much as technical assurance.

There's also a subtler version of this tension worth naming: the National ID integration that strengthens identity verification [Figure 1; Figure 2] simultaneously introduces a single point of dependency on an external government system, one SheShield doesn't control. That's a defensible design trade-off, but it's a trade-off nonetheless, and the paper would be less honest if it presented this integration purely as a strength without acknowledging the exposure it creates.

4.4 On Adoption, and Why It May Be the Hardest Problem Here

If the challenges identified during consultation and testing point to one recurring theme, it's this: the technology, on balance, seems more tractable than the adoption problem. Cultural hesitancy, fear of retaliation, unfamiliarity with reporting mechanisms, and — frankly — well-founded skepticism about whether reporting leads to any meaningful response are not problems that better UI design solves. Kumar and Saraswathi (2017) touch on this indirectly in their treatment of the structural barriers surrounding domestic violence intervention, and it applies here with only minor modification: a tool is only as effective as the willingness of its intended users to trust and use it, and that willingness is shaped by forces well outside the app itself — policing culture, family dynamics, social stigma. SheShield's community-support and educational features represent an attempt to address this

indirectly, by building familiarity and trust over time rather than assuming day-one adoption. Whether that's sufficient remains, candidly, an open question.

4.5 Limitations

A few limitations deserve direct acknowledgment rather than a passing mention. First, this paper describes a proposed and partially tested system rather than a system validated through longitudinal, real-world deployment — the testing and consultation findings reported here are formative, not confirmatory, and should be read that way. Second, the AI-based dangerous-area detection and face-recognition components, while grounded in established technique, haven't been evaluated here against demographic or environmental variation (lighting conditions, camera quality across device tiers) in the kind of depth that a deployment-ready system would require. Third, reliance on external infrastructure — the National ID service in particular — introduces a dependency this paper hasn't fully stress-tested against outage or policy change. And finally, the consultation process, while multi-stakeholder, involved a relatively small and geographically concentrated sample; generalizing findings beyond that context, especially to the "global scale" ambition mentioned earlier in this paper, would be premature without further validation.

4.6 Implications and What This Might Mean Going Forward

None of this is meant to undercut the case for SheShield so much as to place it more accurately. Taken together with prior systems reviewed here, the results suggest that the technical groundwork for effective mobile-based safety reporting is fairly mature at this point — the harder, less-solved problem is the social and institutional layer surrounding it: trust, sustained engagement, and meaningful law enforcement follow-through. SheShield's contribution, read this way, is less a technological leap than a careful synthesis — one that takes seriously both the lessons of precedent systems like Protibadi (Ahmed et al., 2014) and SafeTipin (Viswanath & Basu, 2015) and the specific prevalence patterns documented for this context [Table 1; Table 2]. Whether that synthesis translates into real reductions in harm is, ultimately, a question only sustained field deployment and independent evaluation can answer — and one this paper leaves appropriately open rather than prematurely resolved.

5. Conclusion

SheShield offers, at its core, a fairly modest proposition dressed in fairly sophisticated engineering: that the distance between harm and help can be shortened, meaningfully, through thoughtful design. Its combination of real-time reporting, location-based alerts, identity verification, and localized accessibility reflects lessons drawn from prior safety systems as much as original insight — and that, arguably, is a strength rather than a weakness. What the development process made clear, though, is that technology alone resolves only part of the problem; adoption, trust, and institutional follow-through remain the harder, slower work. SheShield doesn't claim to end eve-teasing or domestic violence — no app reasonably could — but it does offer a workable, testable framework for reducing the friction that so often keeps women from reporting at all. Its ultimate significance will depend less on the elegance of its architecture and more on whether it earns sustained trust in the communities it's meant to serve.

Author Contribution

S.S. conceived and designed the study, led problem analysis and requirement gathering, developed the system architecture and application features, conducted functional and usability testing, analyzed the results, and wrote, reviewed, and approved the final manuscript.

Acknowledgement

The author S.S. would like to thank the stakeholders, including law enforcement representatives and community organizations, who participated in consultations during the development of SheShield. The author also acknowledges the institutional support that facilitated this research.

Competing Financial Interests

The author S.S. declares no competing financial interests.

References

- Ahmed, N., Ferdous, H. S., Rifat, M. R., Rizvi, A. S. M., Ahmed, S., Ahmed, S. I., Jackson, S. J., & Mansur, R. S. (2014). Protibadi: A platform for fighting sexual harassment in urban Bangladesh. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 2695–2704). ACM. <https://doi.org/10.1145/2556288.2557140>
- Akash, S. A., Al-Zihad, M., Adhikary, T., Razzaque, M. A., & Sharmin, A. (2016). HearMe: A smart mobile application for mitigating women harassment. In 2016 IEEE International WIE Conference on Electrical and Computer Engineering (WIECON-ECE) (pp. 87–90). IEEE. <https://doi.org/10.1109/WIECON-ECE.2016.8009068>

- Aspire News. (2017). Aspire News. Retrieved September 28, 2017, from <https://play.google.com/store/apps/details?id=com.collectiveray.aspire>
- Das, S., & Sharma, S. (2019). A survey on privacy and security issues in Internet of Things (IoT). *International Journal of Computer Sciences and Engineering*, 7(3), 30–36.
- Gupta, J., Sinha, D., Tasca, M., & Saggurti, N. (2018). Associations between harassment and psychosocial health among Indian women. *Journal of Interpersonal Violence*, 35(13–14), 2943–2967.
- Johnson, M. R., & Dasgupta, S. D. (2018). Understanding the challenges of eve-teasing in urban India: A qualitative study. *Indian Journal of Psychological Medicine*, 40(5), 416–422.
- Kaur, J., & Bhardwaj, M. (2020). Mobile application for women safety: A survey. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 6(3), 249–253.
- Komosion. (2017). Aurora. Retrieved September 28, 2017, from <https://play.google.com/store/apps/details?id=com.komosion.aurora&hl=en>
- Kumar, R. S., & Saraswathi, I. (2017). Domestic violence: Prevalence, causes, and intervention strategies. *Journal of Family Medicine and Primary Care*, 6(3), 517–520.
- Mane, M. I. A., Babar, M. J. R., Patil, M. S. S., Pol, M. S. D., & Shetty, M. N. R. (2016). Stay Safe application.
- Mukherjee, A., & Deshmukh, P. R. (2018). Prevalence and determinants of domestic violence among women in a slum area of Mumbai. *International Journal of Community Medicine and Public Health*, 5(7), 2755–2760.
- Muteeb, M., Muhammad, J., Sarosh, Y., Yousaf, M. A., & Shahid, S. (2016). MehfoozAurat: Transforming smartphones into women safety devices against harassment. In *Proceedings of the Eighth International Conference on Information and Communication Technologies and Development*. ACM.
- Rahman, M. A., Yasmin, F., & Alam, A. K. M. M. (2018). Data security and privacy in mobile health: A survey. *Journal of Medical Systems*, 42(7), 126.
- Roy, S., Sharma, A., & Bhattacharya, U. (2015). MoveFree: A ubiquitous system to provide women safety. In *Proceedings of the Third International Symposium on Women in Computing and Informatics* (pp. 545–552). ACM. <https://doi.org/10.1145/2791405.2791543>
- Sen, D., & Sengupta, S. (2018). An IoT-based framework for preventing crimes against women in India. In *Proceedings of the 2018 3rd International Conference on Internet of Things: Smart Innovation and Usages* (pp. 1–5). IEEE.
- Singh, S., Singh, A., Praveen, V. K., & Jain, A. (2019). Prevalence, determinants and health effects of domestic violence among women in reproductive age group in a slum area in Delhi: A cross-sectional study. *Indian Journal of Community Medicine*, 44(1), 29–33.
- Smith, S. G., Zhang, X., Basile, K. C., Merrick, M. T., Wang, J., Kresnow, M. J., & Chen, J. (2018). The National Intimate Partner and Sexual Violence Survey (NISVS): 2015 data brief – Updated release. National Center for Injury Prevention and Control, Centers for Disease Control and Prevention.
- Techila Solutions. (2017). With U (Women Safety). Retrieved September 28, 2017, from <https://play.google.com/store/apps/details?id=com.techila.withu>
- Thakur, U., Rahangdale, P., Mendhe, D., Umate, D., & Bhagat, T. (2017). Girls safety. *International Journal of Engineering Science*.
- Uma, D., Vishakha, V., Ravina, R., & Rinku, B. (2015). An Android application for women safety based on voice recognition. Department of Computer Science, BSIOTR, Savitribai Phule Pune University.
- Viswanath, K., & Basu, A. (2015). SafeTipin: An innovative mobile app to collect data on women's safety in Indian cities. *Gender & Development*, 23(1), 45–60. <https://doi.org/10.1080/13552074.2015.1013669>
- Zayan Infotech. (2017). Women's Security. Retrieved September 28, 2017, from <https://play.google.com/store/apps/details?id=com.zayaninfotech.security>