# An Empirical Study of Backend Infrastructure in Leading Pakistani Mobile Apps

Sana Habib
Arizona State University/Washington and Lee University
shabib3@asu.edu

Mohammad Taha Khan
Carnegie Mellon University
tahak@cmu.edu

Jedidiah R. Crandall
Arizona State University/ Breakpointng Bad
jedimaestro@asu.edu

## ABSTRACT

Once user data leaves mobile devices, its fate becomes largely opaque within government and telecom ecosystems. In this work, we study the backend infrastructure of seven Pakistani government and telecom apps to examine how server-side systems shape post-device data exposure. We introduce a classification of high-risk domains based on ownership, jurisdictional signals, security posture, and functional role, enabling a systematic characterization of the backend infrastructures associated with our app corpus and the sensitive data they handle beyond the device boundary.

We analyze these apps using static and dynamic analysis, HTTPS interception, multi-resolver DNS resolution, and a geolocation ensemble comprising five independent services — MaxMind, IPinfo, ip-api, DBIP, and BGPView/RIPE — with CDN-aware attribution, alongside WHOIS/BGP-based infrastructure mapping. Across approximately 172 observed domains, we identify four active first-party endpoints handling highly sensitive data, including identity credentials, location information, and communication metadata. Three of these endpoints rely on domestic infrastructure associated with local administrative entities based on ASN and registry-level signals. The remaining endpoint is served through U.S.-based CDN infrastructure despite being organizationally associated with Pakistan. We further observe backend designs that consolidate sensitive data flows into a small number of endpoints, with limited disclosure of data retention and deletion policies in app store listings and privacy documentation. These findings indicate that device-centric security analyses can underestimate exposure, as backend infrastructure placement and jurisdictional context play an important role in shaping data governance and visibility.

## KEYWORDS

IP Geolocation, Jurisdictional Inference, Infrastructure Attribution.

## 1 INTRODUCTION

Every time a user logs into a mobile app, submits personal information, or shares their location, that data traverses a complex backend infrastructure invisible to the user. In Pakistan, such data flows occur within an ecosystem where infrastructure-level exposure risks have been repeatedly documented, with prior incidents involving state-aligned systems affecting millions of users [14, 15, 18, 35, 40, 74, 88].

This risk landscape is shaped by evolving regulatory oversight and state-level monitoring capabilities, including increased filtering, surveillance, and enforcement during politically significant events such as the May 9, 2023 protests and the February 8, 2024 elections [10, 12, 22, 68, 92] — measures reported as deployed or facilitated by government and regulatory authorities [41, 68]. Related legal and technical developments have further expanded lawful access and interception infrastructure [17, 19, 20, 24, 41].

Mobile apps introduce a distinct and underexplored exposure surface. Unlike web services, they routinely transmit structured identifiers — national identity numbers, location data, device identifiers, and communication metadata — to backend systems invisible to end users, making jurisdictional placement and infrastructure configuration key determinants of data exposure. Prior work [64] studied device-level security in seven leading Pakistani apps, identifying insecure credential storage and weak authentication, but device-centric analysis does not capture how exposure evolves after transmission to backend infrastructure.

In this paper, we extend analysis to the network and infrastructure layer. We develop a classification of high-risk domains based on ownership, jurisdictional signals, security posture, and functional role, and apply it to our app corpus to systematically characterize the backend infrastructure processing sensitive user data after it leaves the device. Our analysis combines static and dynamic measurement techniques — HTTPS interception, multi-resolver DNS lookups, CDN[1]-aware attribution, and a five-service geolocation ensemble (MaxMind [78], IPinfo [72], ip-api [71], DBIP [55], BGPView [46], RIPEstat [31]) — along with WHOIS [70] and BGP-based mapping. Across seven apps, we identify approximately 172 unique domains (40 first-party, 132 third-party). Focusing on the first-party subset, we find sensitive data concentrated within a small number of endpoints, amplifying infrastructure-level exposure risk. We identify three structural patterns:

(1) *Direct Administrative Control.* Government-operated endpoints such as `api.pmdu.gov.pk` and `qpapi.punjab.gov.pk` centralize sensitive data under public sector administration. The endpoint `shanakht.nadra.gov.pk` resolves to CDN infrastructure but remains under NADRA[2] administrative control.
(2) *Indirect Control via Telecom Ecosystems.* Telecom-operated endpoints such as `myzongapp-nlbt.zong.com.pk` operate under private entities but include policy-based disclosure provisions enabling access under legal or regulatory conditions.


*Free and Open Communications on the Internet 2026(2), 21–36*


[1] A Content Distribution Network (CDN) is a distributed infrastructure that caches and delivers content from geographically distributed edge servers.
[2] NADRA = Pakistan's National Database and Registration Authority.

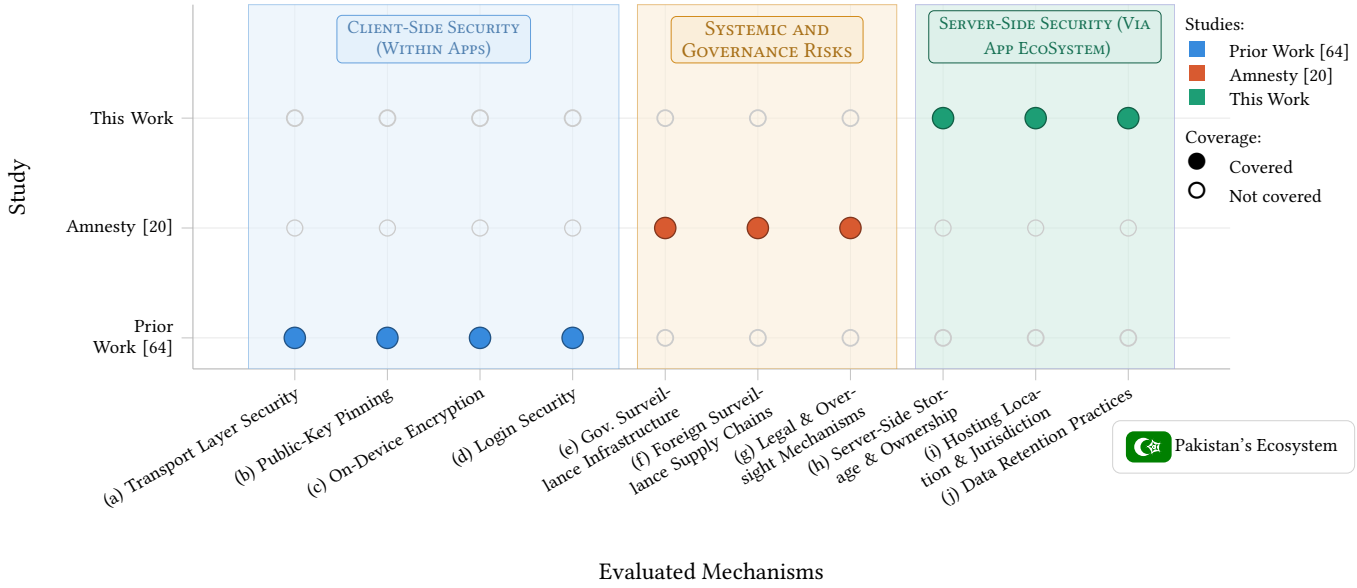



**Figure 1: Coverage of Security Mechanisms Across Recent Studies on Pakistan's Ecosystem.**

(3) *Domestic Infrastructure Exposure.* Most first-party endpoints are hosted within domestic infrastructure, increasing exposure to jurisdictional access and regulatory compulsion under applicable legal frameworks.

## 2 RELATED WORK

This work builds directly on two recent studies of the Pakistani digital environment. Habib et al. [64] analyzed seven leading Pakistani apps, identifying plaintext credential storage, weak authentication, and machine-in-the-middle vulnerabilities — but their analysis stops at the device boundary, leaving backend infrastructure, DNS configurations, and hosting jurisdiction unexamined. Amnesty International's *Shadows of Control* [20] documents lawful interception systems and regulatory gaps that create structural conditions for state access. Together, they establish the technical vulnerability surface and surveillance context of Pakistani mobile apps; what neither provides is the infrastructure measurement layer that connects them. Legal developments — PECA amendments, expanded surveillance mandates, and interception frameworks [17, 19, 24] — sharpen this gap further.

The broader mobile measurement literature has characterized data exposure at the device and traffic layers. TaintDroid [56], Haystack [89], and ReCon [90] establish taint tracking, traffic-level leakage detection, and real-time app-to-server inspection as foundational techniques, while advertising SDK research demonstrates that backend infrastructures operated by third parties can aggregate user data across applications, motivating analyses beyond the mobile device [48, 57, 76]. The backend infrastructure layer — who controls the servers, where they are hosted, and under which legal regimes they operate — remains comparatively underexplored; infrastructure-layer vulnerabilities in SDN configuration [62] and cloud resilience [63] further illustrate this blind spot.

Filling that gap draws on infrastructure measurement techniques from adjacent work. Multi-resolver DNS studies reveal how recursive and anycast setups obscure service ownership [50, 85], and legacy DNS vulnerabilities persist even into next-generation mobile networks [61]. Geolocation databases vary significantly in accuracy [59, 86], motivating ensemble approaches, while CDN studies show edge-based hosting decouples apparent location from administrative jurisdiction [49, 75, 81] — directly relevant to endpoints like `shanakht.nadra.gov.pk`, which resolves to Akamai infrastructure in the United States while remaining under NADRA's control.

Studies of China [58] and Iran [42, 77] establish how domestic hosting mandates and legal compulsion operate together, and cross-border flow analysis confirms that backend jurisdictional placement determines applicable legal regimes [51]. Our work bridges these threads by combining mobile traffic analysis, domain resolution tracing, and infrastructure attribution with a five-source geolocation ensemble and CDN-aware jurisdictional inference — introducing a structured classification of high-risk domains across ownership, security posture, functional role, and jurisdictional signals that prior work addresses in isolation but does not operationalize jointly.

## 3 COORDINATED DISCLOSURE

All seven apps listed in Table 1 are publicly available on the Google Play Store [9] and APKPure [8]. Our study focuses on analyzing server-side exposure risks while adhering to established ethical guidelines for security measurement research. To minimize unintended impact, we followed responsible measurement practices and ensured that all experiments were conducted on researcher-controlled accounts. Network measurements were performed in a non-invasive manner, avoiding configurations that could introduce unnecessary load or disrupt production services.

**Table 1: Ethical Disclosure Timeline for Analyzed Apps.**

| # | App Title | Email / Complaint Date |
|---|---|---|
| 1. | Pak Identity [28] | Apr 07, 2025 |
| 2. | Pakistan Citizen Portal [29] | Apr 07, 2025 |
| 3. | Qeemat Punjab [30] | Apr 08, 2025 |
| 4. | SIMOSA [32] | Apr 13, 2025 |
| 5. | My Zong [27] | Apr 13, 2025 |
| 6. | My Telenor [26] | Apr 13, 2025 |
| 7. | UPTCL [33] | Apr 13, 2025 |

We contacted the developers of each app to disclose potential security and privacy findings. These disclosures were intended to report empirically observed behaviors rather than to elicit or validate developer intent regarding API or service usage. Table 1 reports the date of the first disclosure email sent to each developer; multiple follow-up messages were also issued where applicable, although only the initial contact date is shown for clarity and consistency. The developers of My Zong [27] and My Telenor [26] acknowledged receipt; My Zong additionally requested a detailed report, which we provided. We received an automated acknowledgment from UPTCL [33], with no further follow-up at the time of writing. For Pak Identity [28], Pakistan Citizen Portal [29], Qeemat Punjab [30], and SIMOSA [32], we did not receive substantive responses despite follow-up through official channels.

We also observed changes across app versions. In the updated version of Pak Identity, we observed the inclusion of a root detection mechanism, indicating an evolution in client-side hardening compared to earlier analyzed versions. Moreover, one telecom endpoint (`theomancy.app.telenor.com.pk`) was actively observed during the 15-month measurement period and included in our initial dataset based on the evidence collected at that time. The endpoint was subsequently deprecated before manuscript preparation.

## 4 BACKGROUND AND THREAT CONTEXT

This section provides the context needed to interpret our findings. We first characterize jurisdictional risk within Pakistan by identifying governance environments where legal, administrative, or technical mechanisms may increase the likelihood of sensitive user data being accessed. We then explain why backend infrastructure should be interpreted in terms of organizational control and jurisdiction rather than physical server location. This distinction motivates our infrastructure attribution methodology and the interpretation of jurisdictional exposure throughout the remainder of the paper.

### What Makes a Jurisdiction High-Risk?

We define *high-risk jurisdictions* as governance contexts where monitoring capabilities, uneven oversight, and coercive enforcement may increase the likelihood of sensitive user data being accessed through legal or administrative channels. This is a contextual classification for Pakistan rather than a formal model. Figure 2 and Table 2 summarize this framing.[3] We evaluate each jurisdiction across six dimensions: *Internet Shutdowns*, *Location Surveillance*, *Social Media Monitoring*, *Network-Level Monitoring*, *Backend Data Access*, and *Arrests & Disappearances*. Each is rated *Low*, *Medium*, or *High* based on documented and inferred patterns of digital control. These ratings contextualize inferred exposure and do not imply uniform or deterministic behavior within a jurisdiction.

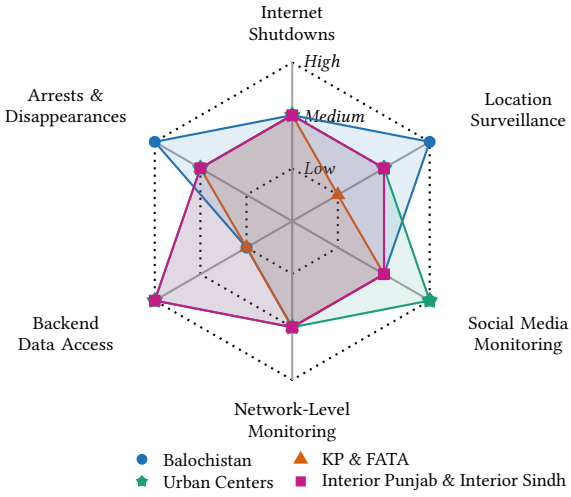



**Figure 2: Radar Chart of Digital Threat Profiles Across High-Risk Jurisdictions in Pakistan.**

*4.0.1 Balochistan.* Balochistan exhibits medium exposure to Internet shutdowns, with high exposure to location surveillance and enforcement-related arrests. Shutdowns during unrest are well documented [38], alongside strong evidence of location-enabled surveillance in enforcement contexts [39, 53, 54, 80, 82, 83]. Arrests and disappearances further reinforce elevated risk [39]. Evidence for backend data access remains insufficient (IE).

*4.0.2 Khyber Pakhtunkhwa (KP) and Former FATA.* This region shows episodic but persistent risk, especially through Internet shutdowns during security operations [1, 43, 73, 79]. Network-level monitoring is present via ISP infrastructure [68]. Evidence for location surveillance and backend data access remains limited (IE).

*4.0.3 Urban Centers: Karachi, Lahore, Islamabad.* Urban centers exhibit structurally persistent but heterogeneous risk. Location surveillance is reported during protests, including geofencing and targeted enforcement [10, 22, 66, 67, 94]. Social media and network-level monitoring are widespread, consistent with reported *China-style* firewall expansion [12, 21, 68], while backend data access is evidenced through reported database leaks, including those involving NADRA [35].

*4.0.4 Interior Punjab and Interior Sindh.* Interior Punjab and interior Sindh show moderate but persistent risk.[4] Expanded filtering has increased social media and network-level monitoring, with documented location surveillance during protest-related arrests [91].

[3] See Figure 6 in Appendix A for a map of the referenced regions.

[4] The terms *interior Punjab* and *interior Sindh* refer to areas of the respective provinces outside the major metropolitan centers (e.g., Lahore and Karachi, respectively). They are informal geographic descriptors rather than official administrative divisions.

**Table 2: Digital Threat Profiles Across High-Risk Jurisdictions in Pakistan**

| # | Dimension | Balochistan | KP & FATA[1] | Urban Centers | Interior Punjab & Interior Sindh |
|---|---|---|---|---|---|
| 1. | Internet Shutdowns | Medium [38] | Medium [34, 73] | Medium [37] | Medium [37] |
| 2. | Location Surveillance | High [54, 80, 82, 83] | Low[2] | Medium [3] | Medium [91] |
| 3. | Social Media Monitoring | Medium [17] | Medium [17, 93] | High [68] | Medium [93] |
| 4. | Network-Level Monitoring | Medium [21] | Medium [1, 21, 43] | Medium [21] | Medium [21] |
| 5. | Backend Data Access | Low[2] | Low[2] | High [2, 6] | High [5] |
| 6. | Arrests & Disappearances | High [39, 69] | Medium [36] | Medium [22] | Medium [45, 91] |

[1] Although FATA merged with KP in 2018, we retain separate labels for consistency with the geolocation sources used in our analysis [87]. [2] IE = Insufficient Evidence.

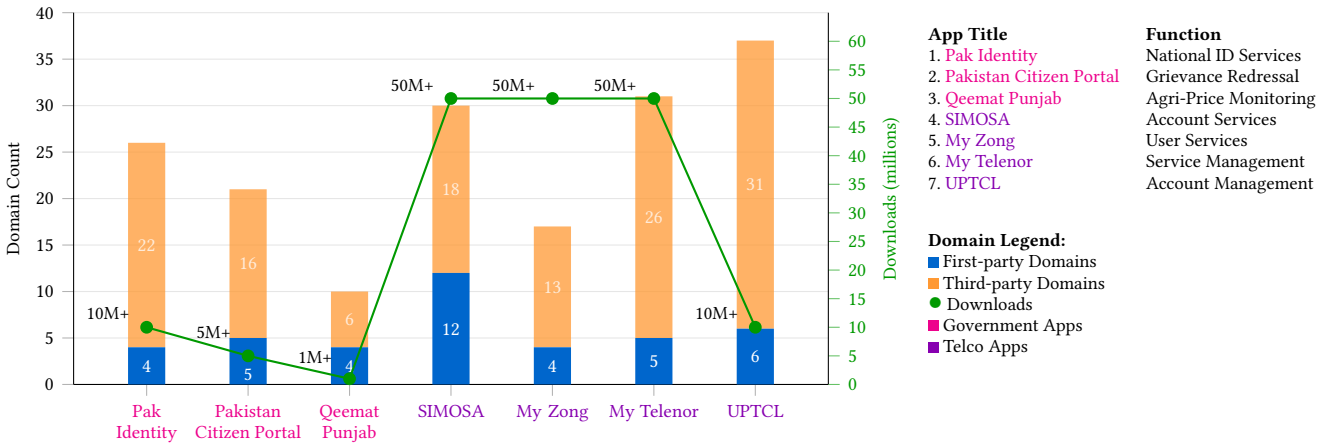



**Figure 3: Domain Inventory from Popular Pakistani Mobile Apps.**

Modern backend services are commonly deployed across cloud platforms and CDNs, where anycast routing and distributed infrastructure can obscure the physical location of origin servers. As a result, precise server geolocation is often difficult to determine with high confidence and is not, by itself, a reliable indicator of data governance.

Instead, governance follows the organizational entity operating the infrastructure. Government agencies, contractors, cloud providers, and hybrid operators determine the legal and administrative mechanisms governing data access, retention, and disclosure. Accordingly, our analysis emphasizes ownership attribution and country-level jurisdictional inference, which can be established with substantially greater confidence than precise physical server location while remaining directly relevant to governance and legal exposure.

# 5 METHODOLOGY

This section describes our methodology for collecting backend infrastructure data and inferring infrastructure ownership, jurisdiction, and server-side exposure characteristics.

## 5.1 App Acquisition and Ethical Setup

We obtained the official apps from the Google Play Store and installed them on a rooted Motorola Moto G7 Plus device. The installed APKs were then extracted from the device using APK Extractor [4] and transferred to an Ubuntu 22.04 analysis workstation via `adb` [7]. All experiments were conducted from a researcher-controlled environment in the United States using dedicated test accounts.

We performed HTTPS-based interaction testing over a 15-month period to identify stable backend endpoints and recurring data flows across app updates, systematically capturing runtime communication patterns over repeated sessions. DNS resolution and jurisdictional inference were then conducted over a dedicated 100-day period to characterize backend infrastructure while reducing the influence of transient routing changes and CDN dynamics.

## 5.2 Threat Model

We consider a threat model in which backend infrastructure may be misconfigured, vulnerable, or subject to administrative access, enabling exposure of sensitive app data after transmission. Client-side compromise and TLS-breaking attacks are out of scope, consistent with prior work [64].

Our analysis focuses on exposure risks arising from backend infrastructure, organizational control, and jurisdiction rather than client-side behavior. We additionally consider state-affiliated and hybrid actors, including entities operating commercial infrastructure under regulatory or legal authority (e.g., telecommunications providers). We do not assume active exploitation; instead, we identify structural and administrative pathways through which transmitted data could plausibly be accessed.

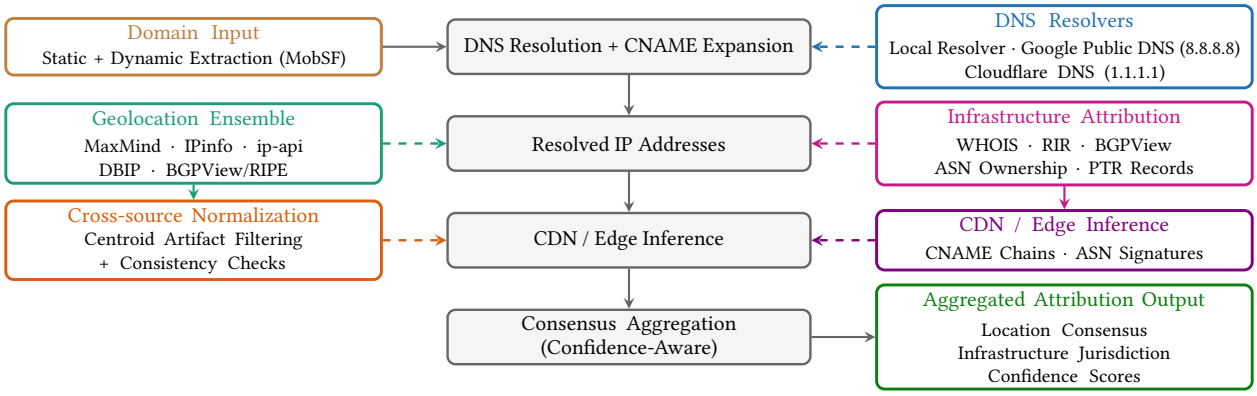



**Figure 4: A Framework for Server Region and Jurisdictional Inference using DNS, Geolocation, and Infrastructure Signals.**

## 5.3 Static and Dynamic App Analysis

We used the Mobile Security Framework (MobSF) [11] to extract embedded domains, API endpoints, and third-party dependencies from app binaries. We then manually classified domains as first- or third-party based on (i) domain ownership consistency with the official app provider, (ii) presence in official documentation or app functionality flows, and (iii) absence of external service indicators such as analytics, advertising, or cloud/CDN providers. Domains flagged by MobSF as suspicious were further reviewed for unexpected or anomalous behavior. Figure 3 summarizes the resulting domain inventory. For example, the Pak Identity app includes 4 first-party and 22 third-party domains.[5]

For dynamic analysis, we deployed a custom root certificate via `mitmproxy` to capture HTTPS traffic. Where apps enforced certificate pinning or root detection, we used Frida [13] to selectively bypass these protections for measurement purposes.

## 5.4 Server-Side Data Exposure Assessment

We identify backend domains handling sensitive data through repeated observations of network traffic, request payloads, and server responses. Each observed data element is mapped to one of eight mutually exclusive categories (see Figure 5). We model exposure as a function of (i) data sensitivity and (ii) infrastructural and administrative properties of the receiving domain, distinguishing between functionally expected transmission (●), structurally risky exposure (★), and non-essential data (■). Classification was performed through independent review by three researchers, with disagreements resolved by consensus; full criteria and examples are provided in Appendix D. We do not treat data collection itself as a vulnerability; instead, we assess whether observed transmission is proportionate to app functionality and whether the receiving infrastructure introduces jurisdictional or administrative risk.

## 5.5 Control and Governance Inference

We infer data control using a combination of technical and documentary signals. *Direct control* is identified through official domains (e.g., `.gov`, `.pk`) and validated ownership records. *Indirect control* is inferred from organizational relationships, hosting arrangements, and privacy policy language indicating disclosure "as required by law" or under licensing agreements. We further analyze privacy policies to assess whether users are provided mechanisms for data deletion and whether retention periods are explicitly specified. We recorded absence of such disclosures as "not specified (NS)", rather than interpreted as absence of policy.

## 5.6 Server Region and Jurisdictional Inference

We infer server region and jurisdiction using a single-vantage, multi-source measurement framework (see Figure 4). Our objective is robust attribution under modern network abstractions, including CDNs and anycast routing, rather than exact physical localization.

*5.6.1 DNS Resolution Procedure.* We resolve domains using `dig` and `nslookup`, extracting A, AAAA, and full CNAME chains. We perform recursive resolution until terminal IP addresses are obtained. To mitigate resolver bias, we query multiple DNS resolvers, including the local resolver, Google Public DNS [60], and Cloudflare DNS [52].

*5.6.2 Geolocation Ensemble.* We queried each resolved IP across $K = 5$ independent geolocation services: MaxMind [78], IPinfo [72], ip-api [71], DBIP [55], and BGPView [47]/RIPE [31]. Each service returns:

$$g_k(\texttt{ip}) = (c_k,\ l_k,\ \mathbf{x}_k),$$

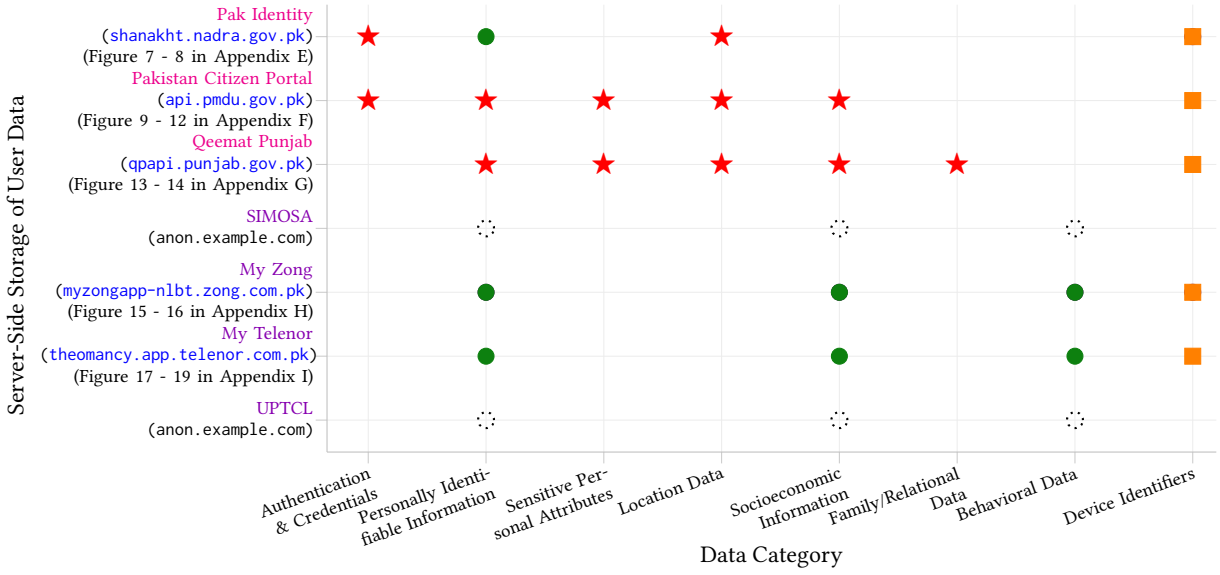
where $c_k$ denotes country, $l_k$ denotes city, and $\mathbf{x}_k$ denotes geographic coordinates. We normalized the coordinates as: $\tilde{\mathbf{x}}_k = \text{round}(\mathbf{x}_k, 3)$.

*Centroid Artifact Handling.* To account for fallback coordinates used by geolocation databases when precise localization is unavailable [59, 86], we define $\mathcal{F}_0$ as the set of known default coordinates commonly returned by major geolocation providers [65][6]:

$$\mathcal{F}_0 = \{(0.0,\ 0.0),\ (38.0,\ -97.0),\ (37.751,\ -97.822),\ (51.507,\ -0.128),\ (39.904,\ 116.407),\ (55.756,\ 37.617),\ (20.0,\ 77.0),\ (30.0,\ 70.0),\ (35.0,\ 105.0)\}$$

[5]The full list of first-party domains across the seven apps is given in Appendix C, and the complete domain inventory is available in Appendix B, due to space constraints.

[6]These coordinates correspond to country- and region-level geographic centroids commonly returned as fallback values by commercial geolocation databases when precise resolution is unavailable.




| # | Category | Observed Data Types |
|---|---|---|
| 1. | Authentication & Credentials | Email ID, Password |
| 2. | Personally Identifiable Information | Full name, Citizen number (CNIC), Mobile number |
| 3. | Sensitive Personal Attributes | Gender, Religion, Blood group, Nationality |
| 4. | Location Data | Precise location coordinates, Physical address, Province |
| 5. | Socioeconomic Information | Profession, Tax certificate |
| 6. | Family / Relational Data | Guardian name, Relationship with guardian |
| 7. | Behavioral Data | Call history, SMS history |
| 8. | Device-Level Identifiers | Device MAC address, IP address, Device OS version |

**Legend**

- Government app
- Telco app
- Non-essential Sensitive Data
- Functionally Expected Data
- Non-essential (non-sensitive) Data
- Inferred Data

**Figure 5: Empirical Data Categories transmitted by Apps to Backend Domains via Network Traces.**

We additionally define $\mathcal{F}_e$ as the set of empirically observed centroids, i.e., coordinates that appear frequently across measurement sources:

$$\mathcal{F}_e = \left\{ \tilde{\mathbf{x}} : \frac{|\{k : \tilde{\mathbf{x}}_k = \tilde{\mathbf{x}}\}|}{K} \geq \tau \right\}.$$

The effective centroid set is defined as $\mathcal{F} = \mathcal{F}_0 \cup \mathcal{F}_e$. We set $\tau = 0.5$, corresponding to majority agreement across independent measurement sources. An IP is classified as centroid-biased and excluded from downstream inference if a dominant fraction of its observations map to centroid-like coordinates:

$$\frac{|\{k : \tilde{\mathbf{x}}_k \in \mathcal{F}\}|}{K} \geq \tau$$

*5.6.3 CDN and Edge Detection.* We identify CDN mediation using ASN metadata, CNAME inspection, and known infrastructure fingerprints (e.g., Akamai, Cloudflare, Fastly, Imperva). When CDN usage is detected, resolved IPs are treated as edge nodes, and jurisdictional attribution is assigned to the controlling ASN rather than the observed edge location.

*5.6.4 Aggregation and Confidence Estimation.* We compute majority-vote estimates for country, city, and coordinates: $\hat{c}, \hat{l}, \hat{\mathbf{x}}$. We define *Confidence*, denoted $C$, as cross-source agreement:

$$C = \frac{|\{k : \text{agreement}\}|}{K}$$

Confidence is reported separately at the country, city, and coordinate levels, with country-level confidence treated as the most stable indicator.

*5.6.5 Infrastructure Attribution.* We augment geolocation with ASN-level analysis using WHOIS [70], RIPEstat [31], ARIN [25], APNIC [44], and BGPView [47]. These signals capture administrative ownership and routing metadata and are treated as higher-confidence indicators of operational control than IP-based geolocation.

*5.6.6 Distinguishing Location and Jurisdiction.* We distinguish between (i) geolocation estimates derived from IP resolution and (ii) infrastructure jurisdiction derived from ASN ownership and routing registries. The latter reflects administrative control over infrastructure, while the former reflects observed network placement, which may be influenced by CDNs and routing policies.

**Table 3: Infrastructure Attribution and Jurisdictional Inference for first-party domains handling sensitive data.**

**(a) Infrastructure Attribution (DNS Resolution, ASN Ownership, and Observed Control Signals).**

| Domain | Infrastructure / ASN | Administrative Control | Jurisdiction (Observed) | Hosting Location | Data Governance (DS[1] / RDD[2] / DRP[3]) |
|---|---|---|---|---|---|
| shanakht.nadra.gov.pk | Akamai Prolexic (AS213120) | NADRA (State Agency) | Pakistan | CDN-mediated (edge abstraction) | Yes[4] / Yes[4] / NS[5] |
| api.pmdu.gov.pk | Direct Hosting (AS24440 / AS9541) | Cybernet / NTC[6] (State Agency) | Pakistan | Pakistan | Yes[4] / Yes[4] / NS[5] |
| qpapi.punjab.gov.pk | Direct Hosting (AS59323) | Punjab IT Board (Provincial Gov.) | Pakistan | Pakistan | Yes[4] / Yes[4] / NS[5] |
| myzongapp-nlbt.zong.com.pk | Telecom backend (AS59257) | CMPak[7] / Zong | Pakistan | Pakistan | Yes[4] / Yes[4] / NS[5] |
| theomancy.app.telenor.com.pk | Inactive / deprecated | Telenor Pakistan | Not observable | Not applicable | Yes[4] / Yes[4] / $\geq$ 1 Year |

[1] DS = Data Sharing. [2] RDD = Request Data Deletion. [3] DRP = Data Retention Period. [4] "Yes" indicates that data sharing/deletion mechanisms are observable or contractually implied under regulatory compliance (e.g., lawful access / government request frameworks). [5] NS = Not Specified. [6] NTC = National Telecommunication Corporation. [7] CMPak = China Mobile Pakistan.

**(b) Geolocation Consensus and Confidence**

| Domain | IP | Country | City | Coordinates (coord) | Confidence ($C_{\text{country}}$ / $C_{\text{city}}$ / $C_{\text{coord}}$) | CDN |
|---|---|---|---|---|---|---|
| shanakht.nadra.gov.pk | 199.46.39.31 | United States | Cambridge | (37.751, −97.822)† | 0.67 / 1.00 / 0.33 | Yes |
| api.pmdu.gov.pk | 203.101.184.112 | Pakistan | Islamabad | (33.723, 73.043) | 0.67 / 0.33 / 0.33 | No |
| qpapi.punjab.gov.pk | 103.226.217.186 | Pakistan | Lahore | (30.0, 70.0)† | 0.67 / 1.00 / 0.33 | No |
| myzongapp-nlbt.zong.com.pk | 209.150.154.153–156 | Pakistan | Rawalpindi | (30.0, 70.0)† | 0.67 / 0.50 / 0.33 | No |
| theomancy.app.telenor.com.pk | – | – | – | – | – | – |

† Centroid artifact detected and excluded from coordinate-level inference. Confidence reflects cross-source agreement across geolocation services. DNS resolution was consistent across local, Google, and Cloudflare resolvers.

## 5.7 Limitations

Our analysis is conducted from a single U.S.-based research environment and may not capture routing, resolution behavior, or application-level behavior (e.g., geolocation-dependent features or localization logic) that may vary across regions or regulatory environments.

Measurements reflect infrastructure state during the study period and should be interpreted as a reproducible snapshot rather than a continuous characterization. Geolocation outputs are influenced by CDN routing, anycast deployment, and database inaccuracies; confidence scores reflect cross-source agreement rather than ground truth, and the centroid-filtering threshold ($\tau = 0.5$) prioritizes precision over recall in jurisdictional inference. ASN-based attribution reflects administrative ownership rather than physical data location, which may differ in CDN-mediated deployments.

First- and third-party classification was performed manually and may misclassify edge cases involving white-label infrastructure or undisclosed affiliations. Overall, we interpret our findings as a conservative, externally observable estimate of jurisdictional exposure rather than a definitive characterization of backend system internals.

# 6 FINDINGS

We identify a primary backend domain per app and perform geolocation and jurisdictional inference using the ensemble framework in Section 5, focusing on high-risk domains. Results from $K = 5$ sources are aggregated via majority vote, with uncertainty captured through cross-source confidence and centroid-based artifact detection. Figure 5 shows hosted personal data types, and Table 3 summarizes infrastructure attribution and geolocation consensus.[7]

## 6.1 Pak Identity — shanakht.nadra.gov.pk

shanakht.nadra.gov.pk is the primary authentication endpoint for Pak Identity app, transmitting national identity numbers, credentials, and location data to NADRA backend infrastructure (Figure 7, Figure 8, Appendix E). DNS resolution reveals CDN-mediated routing via Akamai (AS213120), with the terminal IP (199.46.39.31) corresponding to a Prolexic edge node in the United States. Geolocation results show moderate country-level agreement toward the United States ($C_{\text{country}} = 0.67$), perfect city-level agreement on Cambridge ($C_{\text{city}} = 1.00$), and low coordinate confidence ($C_{\text{coord}} = 0.33$). Centroid artifacts are present in a subset of responses, including (37.751, −97.822), a known fallback coordinate in $\mathcal{F}_0$. The combination of CDN mediation and centroid artifacts yields a *low-confidence geolocation estimate*. Jurisdiction is therefore attributed to NADRA rather than the observed edge location.

[7] We observed incomplete DNSSEC deployment across the five high-risk domains in Table 3; however, as apps rely on TLS for end-to-end encryption, this does not expose user data in transit. No open ports beyond 80 and 443 were identified, indicating a limited externally exposed attack surface.

### 6.2 Pakistan Citizen Portal — `api.pmdu.gov.pk`

`api.pmdu.gov.pk` handles credential transmission and identity verification for the Pakistan Citizen Portal app (Figure 9, 10, 11, and 12 in Appendix F). DNS resolution returns a direct A record (203.101.184.112) with no CDN indirection, attributed to AS24440 / AS9541 (Cybernet / NTC), indicating government-aligned hosting. Geolocation sources consistently attribute the domain to Pakistan ($C_{\text{country}} = 0.67$), with low city-level agreement ($C_{\text{city}} = 0.33$) and low coordinate confidence ($C_{\text{coord}} = 0.33$). No centroid artifacts are detected, indicating that uncertainty arises from cross-provider inconsistency rather than fallback behavior. Combined with direct domestic hosting, this domain represents a *high-confidence jurisdictional attribution under high-uncertainty localization.*

### 6.3 Qeemat Punjab — `qpapi.punjab.gov.pk`

`qpapi.punjab.gov.pk` serves as the backend for the Qeemat Punjab app, receiving location and identity data. DNS resolution returns a direct A record (103.226.217.186) attributed to AS59323 (PITB[8]), confirming provincial government ownership. Geolocation sources consistently attribute the domain to Pakistan ($C_{\text{country}} = 0.67$), with strong city-level agreement on Lahore ($C_{\text{city}} = 1.00$) but low coordinate confidence ($C_{\text{coord}} = 0.33$). The coordinate $(30.0, 70.0)$ is identified as a centroid artifact and excluded from inference. Uncertainty is therefore driven by fallback coordinate behavior rather than disagreement across sources. This domain reflects *stable jurisdictional attribution under centroid-biased localization.*

### 6.4 My Zong — `myzongapp-nlbt.zong.com.pk`

`myzongapp-nlbt.zong.com.pk` is the primary backend for the My Zong app, handling call records, SMS metadata, and account credentials. DNS resolution returns four A records (209.150.154.153–156) under Zong authoritative DNS, attributed to AS59257 (CMPak / Zong). Across all IPs, ensemble inference consistently identifies Pakistan as the country-level jurisdiction ($C_{\text{country}} = 0.67$), with city-level estimates split between Rawalpindi and Islamabad ($C_{\text{city}} = 0.50$) and low coordinate confidence ($C_{\text{coord}} = 0.33$). The coordinate $(30.0, 70.0)$ is consistently flagged as a centroid artifact and excluded from inference. Geolocation outputs are structurally consistent but non-convergent at the city level. Although privately operated, this domain is subject to indirect state access under telecom regulatory and disclosure frameworks (Section 5.5).

### 6.5 Restricted-Observability Cases

Three apps exhibit restricted observability due to deployment or app-level constraints. These cases are not excluded arbitrarily; rather, they reflect real-world conditions under which backend infrastructure may intentionally limit measurement visibility.

**My Telenor**'s backend (`theomancy.app.telenor.com.pk`) was observed to be deprecated during the measurement period, with DNS queries returning no A/AAAA records and no reachable service endpoints. Attribution relies on historical DNS records linking the domain to Telenor Pakistan. We treat this as a *no-observation condition*, reflecting temporal infrastructure changes rather than measurement failure.

[8]PITB = Punjab Information Technology Board.

SIMOSA [32] and UPTCL [33] implement SSL pinning, preventing HTTPS interception and runtime traffic inspection despite our attempts to bypass it. This behavior is consistent with hardened app deployments and directly limits observable network measurements. As a result, geolocation inference cannot be performed using dynamic traffic signals. Instead, our analysis relies on static evidence, including the fact that both apps retrieve data from remote servers.

These cases are excluded from confidence-based aggregation to preserve the integrity of the ensemble methodology, which requires observable geolocation outputs across sources. However, their absence of observable signals is itself informative, reflecting either intentional hardening (SSL pinning) or backend instability (domain deprecation), both of which influence exposure and attribution in practice.

## 7 DISCUSSION AND CONCLUSION

Our analysis shows that sensitive user data is concentrated in a small set of first-party backend domains across the five apps for which backend traffic was successfully analyzed. These domains handle highly sensitive information, including national identity numbers, credentials, location data, and communication metadata, creating significant exposure points where compromise could affect large user populations.

Geolocation analysis reveals a consistent pattern: country-level attribution is stable (primarily Pakistan), while fine-grained localization remains uncertain. For `shanakht.nadra.gov.pk`, Akamai CDN edge nodes in the United States illustrate the separation between delivery infrastructure and administrative control. Jurisdictional attribution is generally more stable than raw IP geolocation, though it remains inference-based.

Telecom-operated domains add further complexity. Zong- and Telenor-associated domains centralize communication metadata under distinct legal and policy frameworks, creating indirect exposure pathways beyond those of state-operated infrastructure. Backend infrastructure is also dynamic: the `theomancy.app.telenor.com.pk` domain was deprecated during the study period, complicating longitudinal measurement.

Geolocation confidence is stronger at the country level than at the city level, underscoring the need to report uncertainty rather than binary labels. None of the analyzed apps provide meaningful data deletion guarantees, suggesting persistent backend retention. A central implication of our results is that privacy risk arises not only from communication with expected service providers, but from the breadth of sensitive data collected, limited transparency regarding its retention and handling, and its concentration within a small number of backend systems. Such concentration amplifies the consequences of security compromise and may expose user data to multiple organizational and legal jurisdictions. These findings support stronger data-minimization and transparency practices for systems that aggregate sensitive user information.

## ACKNOWLEDGMENTS

This work was supported by the Open Technology Fund's Information Controls Fellowship Program, the HIVE Fellowship at the Center for Digital Resilience, and the National Science Foundation under Grant CNS-2452885. We are grateful to the Digital Rights

Foundation in Pakistan for its support and hosting, and to the anonymous reviewers for their constructive feedback, which significantly improved this work.

This research aims to improve the security and privacy of mobile apps used by Pakistani citizens and is intended solely as a constructive contribution to inform better security practices. We do not seek to criticize or assign blame to any organization, agency, or individual. Jurisdictional risk assessments are based on publicly available sources, and references to enforced disappearances are included only to provide context for the regulatory environment, not as independent claims.

## REFERENCES


[1] 2017. People of FATA-origin put under surveillance in Pindi division. (2017). https://www.dawn.com/news/1316244.

[2] 2021. *Body formed to look into NADRA related issues.* https://tribune.com.pk/story/2331293/body-formed-to-look-into-nadra-related-issues

[3] 2021. Senior journalist Absar Alam shot, injured in Islamabad. *DAWN* (20 April 2021). https://www.dawn.com/news/1619325

[4] 2023. *Apk Extractor.* https://play.google.com/store/apps/details?id=braveheart.apps.apkextract&hl=en_US&gl=US

[5] 2023. *The breach of 2.2 million Pakistanis' data and the urgent need for action.* https://www.pakistantoday.com.pk/2023/09/24/not-just-a-wake-up-call/

[6] 2023. *NADRA Data Leaks.* https://www.nation.com.pk/08-Jul-2023/nadra-data-leaks

[7] 2024. *Android Debug Bridge (adb).* https://developer.android.com/tools/adb

[8] 2024. *APKPure.* https://apkpure.net/

[9] 2024. *Google Play Store.* https://play.google.com/store/games?hl=en_US

[10] 2024. *Imran Khan vs Pakistan's government: A timeline of political upheaval.* https://www.aljazeera.com/news/2024/5/9/timeline-a-year-of-ex-pm-imran-khans-arrest-may-9-violence-in-pakistan

[11] 2024. *Mobile Security Framework (MobSF).* https://mobsf.github.io/docs/#/

[12] 2024. *Pakistan's surprising and marred 2024 election, and what comes next.* https://www.brookings.edu/articles/pakistans-surprising-and-marred-2024-election-and-what-comes-next/

[13] 2024. *Unleash the power of Frida.* https://codeshare.frida.re/

[14] 2025. Big Data Leak in Pakistan: Where Is the Government Control? *The Media Line.* (2025). https://themedialine.org/top-stories/big-data-leak-in-pakistan-where-is-the-government-control/.

[15] 2025. Islamabad orders probe into online data leak concerning thousands of Pakistanis. *ARAB NEWS.* (2025). https://www.arabnews.com/node/2614507/pakistan.

[16] 2025. *NAtional Database and Registration Authority (NADRA).* https://www.nadra.gov.pk/

[17] 2025. *Pakistan: Authorities pass bill with sweeping controls on social media.* https://www.amnesty.org/en/latest/news/2025/01/pakistan-authorities-pass-bill-with-sweeping-controls-on-social-media/

[18] 2025. Pakistan Investigates Major Data Breach Exposing Officials' Personal Information Across 1,300+ Websites. *Mobile ID World* (2025). https://mobileidworld.com/pakistan-investigates-major-data-breach-exposing-officials-personal-information-across-1300-websites/.

[19] 2025. *Pakistan: Repeal Amendment to Draconian Cyber Law.* https://www.hrw.org/news/2025/02/03/pakistan-repeal-amendment-draconian-cyber-law

[20] 2025. *Pakistan: Shadows of Control: Censorship and mass surveillance in Pakistan.* https://www.amnesty.org/en/documents/asa33/0206/2025/en/

[21] 2025. *Pakistan tests secret China-like 'firewall' to tighten online surveillance.* https://www.aljazeera.com/news/2024/11/26/pakistan-tests-china-like-digital-firewall-to-tighten-online-surveillance

[22] 2025. Pakistani opposition leader Imran Khan and nearly 200 supporters sentenced over 2023 riots. *PBS News* (2025). https://www.pbs.org/newshour/world/pakistani-opposition-leader-imran-khan-and-nearly-200-supporters-sentenced-over-2023-riots.

[23] 2025. *Prime Minister's Performance Delivery Unit (PMDU) Pakistan.* https://www.pakmissionfrankfurt.de/pmdu

[24] 2025. *To Squash Dissent, Pakistan Adopts China's 'Great Firewall'.* https://inkstickmedia.com/to-squash-dissent-pakistan-adopts-chinas-great-firewall/

[25] 2026. *ARIN: Whois-RWS.* https://whois.arin.net/ui/

[26] 2026. *My Telenor.* https://play.google.com/store/apps/details?id=com.telenor.pakistan.mytelenor&hl=en_US

[27] 2026. *My Zong.* https://play.google.com/store/apps/details?id=com.zong.customercare&hl=en_US

[28] 2026. *Pak Identity.* https://play.google.com/store/apps/details?id=pk.gov.nadra.pakid&hl=en_US&gl=US

[29] 2026. *Pakistan Citizen Portal.* https://play.google.com/store/apps/details?id=com.govpk.citizensportal&hl=en_US&gl=US

[30] 2026. *Qeemat Punjab.* https://play.google.com/store/apps/details?id=com.pitb.qeematpunjab&hl=en_US&gl=US

[31] 2026. *RIPEstat.* https://stat.ripe.net/

[32] 2026. *SIMOSA - Jazz World.* https://play.google.com/store/apps/details?id=com.jazz.jazzworld&hl=en_US

[33] 2026. *UPTCL– App Up Your Life!* https://play.google.com/store/apps/details?id=com.ufoneselfcare&hl=en_US

[34] Irshad Ahmad. 2020. FATA and the Internet. *The News International* (5 April 2020). https://www.thenews.com.pk/print/639470-fata-and-the-internet

[35] Ashfaq Ahmed. 2025. Pakistan: Millions of passwords leaked, your account may be at risk. *GULF NEWS* (2025). https://gulfnews.com/world/asia/pakistan/advisory-pakistanis-told-to-change-social-media-passwords-1.500141524.

[36] Al Jazeera. 2025. Imran Khan's supporters rally in Pakistan on two years of imprisonment. https://www.aljazeera.com/news/2025/8/5/imran-khans-supporters-rally-in-pakistan-on-two-years-of-imprisonment.

[37] Amnesty International. 2024. Pakistan: Election-day Internet Shutdown Is a Reckless Attack on People's Rights. https://www.amnesty.org/en/latest/news/2024/02/pakistan-election-day-internet-shutdown-is-a-reckless-attack-on-peoples-rights/

[38] Amnesty International. 2025. The Pakistani government shut down the internet. I couldn't even tell my family I was safe. https://www.amnesty.org/en/latest/campaigns/2025/09/the-pakistani-government-shut-down-the-internet-i-couldnt-even-tell-my-family-i-was-safe/. Campaigns page.

[39] Amnesty International UK. 2025. Forced Disappearances in Pakistan: The Case of Mahrang Baloch. https://www.amnesty.org.uk/get-involved/join-the-movement/join-a-group-or-network/country-coordinators/country-specialists-blog/forced-disappearances-pakistan-case-mahrang-baloch/. Country Specialists Blog.

[40] Farah Amod. 2025. PKCERT warns of credential breach impacting 180 million users. *PAUBOX* (2025). https://www.paubox.com/blog/pkcert-warns-of-credential-breach-impacting-180-million-users.

[41] Mariyam Suleman Anees. 2024. Pakistan Expands Surveillance Powers Yet Again in the Name of 'National Security'. *The Diplomat* (2024). https://thediplomat.com/2024/07/pakistan-expands-surveillance-powers-yet-again-in-the-name-of-national-security/.

[42] Simurgh Aryan, Homa Aryan, and J Alex Halderman. 2013. Internet censorship in Iran: A first look. In *3rd USENIX Workshop on Free and Open Communications on the Internet (FOCI 13).*

[43] Syed Irfan Ashraf. 2021. Digital apartheid in ex-FATA. *Dawn* (2021). https://www.dawn.com/news/1662964.

[44] Asia Pacific Network Information Centre (APNIC). 2026. Regional Internet Registry for the Asia Pacific. https://www.apnic.net/about-APNIC/

[45] Associated Press. 2025. Arrests at pro-Palestinian protest after violence flares in Pakistan's eastern city of Lahore. https://apnews.com/article/pakistan-protest-lahore-tlp-9286e7e817b29152f8ee6e7783a78f36

[46] BGPView. 2026. BGPView API: ASN and IP Prefix Intelligence Service. https://www.ipaddress.com/website/bgpview.io/.

[47] BGPView. 2026. *BGPView: BGP Data and ASN Lookup Service.*

[48] Reuben Binns, Ulrik Lyngs, Max Van Kleek, Jun Zhao, Timothy Libert, and Nigel Shadbolt. 2018. Third party tracking in the mobile ecosystem. In *Proceedings of the 10th ACM Conference on Web Science.* 23–31.

[49] Matt Calder, Xun Fan, Zi Hu, Ethan Katz-Bassett, John Heidemann, and Ramesh Govindan. 2013. Mapping the expansion of Google's serving infrastructure. In *Proceedings of the 2013 conference on Internet measurement conference.* 313–326.

[50] Patricia Callejo, Rubén Cuevas, Narseo Vallina-Rodriguez, and Angel Cuevas Rumin. 2019. Measuring the Global Recursive DNS Infrastructure: A View From the Edge. *IEEE Access* 7 (2019), 168020–168028.

[51] Anupam Chander and Uyên P. Lê. 2015. Data Nationalism. *Emory Law Journal* 64, 3 (2015), 677–739. https://scholarlycommons.law.emory.edu/elj/vol64/iss3/2

[52] Cloudflare, Inc. 2026. Cloudflare DNS (1.1.1.1). https://developers.cloudflare.com/1.1.1.1/.

[53] Committee to Protect Journalists. 2025. Prominent Pakistani journalist Latif Baloch shot dead in Balochistan province. https://cpj.org/2025/05/prominent-pakistani-journalist-latif-baloch-shot-dead-in-balochistan-province/. CPJ Alert.

[54] Jakub Dalek, Adam Senft, Masashi Crete-Nishihata, and Ron Deibert. 2013. *O Pakistan, We Stand on Guard for Thee: An Analysis of Canada-based Netsweeper's Role in Pakistan's Censorship Regime.* Technical Report. Citizen Lab, University of Toronto. https://citizenlab.ca/2013/06/o-pakistan-we-stand-on-guard-for-thee/

[55] DBIP. 2026. IP Geolocation Database and API Services. https://db-ip.com.

[56] William Enck, Peter Gilbert, Byung-Gon Chun, Landon P. Cox, Jaeyeon Jung, Patrick McDaniel, and Anmol N. Sheth. 2010. TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones. In *9th USENIX Symposium on Operating Systems Design and Implementation (OSDI 10).* USENIX Association, Vancouver, BC. https://www.usenix.org/conference/osdi10/taintdroid-information-flow-tracking-system-realtime-privacy-monitoring

[57] Steven Englehardt and Arvind Narayanan. 2016. Online tracking: A 1-million-site measurement and analysis. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*. 1388–1401.
[58] Roya Ensafi, Philipp Winter, Abdullah Mueen, and Jedidiah R Crandall. 2015. Analyzing the Great Firewall of China over space and time. *Proceedings on privacy enhancing technologies* (2015).
[59] Manaf Gharaibeh, Anant Shah, Bradley Huffaker, Han Zhang, Roya Ensafi, and Christos Papadopoulos. 2017. A look at router geolocation in public and commercial databases. In *Proceedings of the 2017 Internet Measurement Conference*. 463–469.
[60] Google LLC. 2026. Google Public DNS. https://developers.google.com/speed/public-dns.
[61] Sana Habib. 2026. Evaluating the Impact of Legacy DNS Vulnerabilities in FutureG Mobile Networks. In *Workshop on Security and Privacy of Next-Generation Networks (FutureG)*. NDSS Symposium, San Diego, CA, USA. https://doi.org/10.14722/futureg.2026.23093
[62] Sana Habib, Tiffany Bao, Yan Shoshitaishvili, and Adam Doupé. 2022. Mitigating threats emerging from the interaction between sdn apps and sdn (configuration) datastore. In *Proceedings of the 2022 on Cloud Computing Security Workshop*. 23–39.
[63] Sana Habib, Jedidiah R Crandall, and Adam Doupé. 2025. Revisiting SDN Resilience in Cloud and Enterprise Environments. In *Proceedings of the 2025 Cloud Computing Security Workshop*. 28–49.
[64] Sana Habib, Mohammad Taha Khan, and Jedidiah R Crandall. 2025. Examining Leading Pakistani Mobile Apps. *Free and Open Communications on the Internet* (2025), 24–41.
[65] Kashmir Hill. 2016. How an Internet Mapping Glitch Turned a Random Kansas Farm into a Digital Hell. *Fusion* (April 2016). https://theweek.com/articles/624040/how-internet-mapping-glitch-turned-kansas-farm-into-digital-hell
[66] Human Rights Watch. 2023. Pakistan: Mass Arrests Target Political Opposition. https://www.hrw.org/news/2023/05/20/pakistan-mass-arrests-target-political-opposition
[67] Amnesty International. 2020. Pakistan: Amnesty International stands with Aurat March. (2020). https://www.amnesty.org/en/latest/news/2020/03/pakistan-amnesty-international-stands-with-aurat-march/.
[68] Amnesty International. 2025. *Pakistan 2024*. https://www.amnesty.org/en/location/asia-and-the-pacific/south-asia/pakistan/report-pakistan/
[69] Asian News International. 2024. Pakistan: "Worrisome" Statistics On Severe Human Rights Abuse In Balochistan. (2024). https://www.genocidewatch.com/single-post/pakistan-worrisome-statistics-on-severe-human-rights-abuse-in-balochistan.
[70] Internet Corporation for Assigned Names and Numbers (ICANN). 2026. Registration Data Lookup. https://lookup.icann.org/.
[71] ip-api.com. 2026. IP Geolocation API Service. https://ip-api.com.
[72] IPinfo. 2026. IP Address Geolocation API and Data Services. https://ipinfo.io.
[73] Hija Kamran. 2017. A Year Without the Internet. (2017). https://slate.com/technology/2017/08/the-internet-has-been-shut-down-in-pakistans-fata-for-more-than-a-year.html.
[74] Iftikhar A. Khan. 2024. 2.7m citizens' data compromised over five years, probe finds. *Dawn* (2024). https://www.dawn.com/news/1824026.
[75] Rupa Krishnan, Harsha V Madhyastha, Sridhar Srinivasan, Sushant Jain, Arvind Krishnamurthy, Thomas Anderson, and Jie Gao. 2009. Moving beyond end-to-end path information to optimize CDN performance. In *Proceedings of the 9th ACM SIGCOMM conference on Internet measurement*. 190–201.
[76] Douglas J Leith. 2021. Mobile Handset Privacy: Measuring The Data iOS and Android send to Apple and Google. In *International Conference on Security and Privacy in Communication Systems*. Springer, 231–251.
[77] Ashley Lulling. 2023. *Iranian Messaging Apps. Open Technology Fund's Security Lab finds three widely used Iranian messaging apps are not safe*. Open Technology Fund. https://www.opentech.fund/wp-content/uploads/2024/12/Phase_I_Report.pdf.
[78] MaxMind Inc. 2026. GeoIP® IP Geolocation Data and Services. https://www.maxmind.com.
[79] Niala Mohammad. 2024. How the Pashtun Tahafuz Movement Built a Virtual Resistance. (2024). https://www.csohate.org/2024/11/18/pashtun-tahafuz-movement-social-media-use/.
[80] Zubair Nabi. 2013. The anatomy of web censorship in Pakistan. In *3rd USENIX Workshop on Free and Open Communications on the Internet (FOCI 13)*.
[81] Erik Nygren, Ramesh K Sitaraman, and Jennifer Sun. 2010. The akamai network: a platform for high-performance internet applications. *ACM SIGOPS Operating Systems Review* 44, 3 (2010), 2–19.
[82] Open Observatory of Network Interference (OONI). 2026. Pakistan: Internet Measurement Data and Censorship Findings. https://explorer.ooni.org/country/PK. Ongoing longitudinal network measurements.
[83] Pakistan Telecommunication Authority. 2025. *Critical Telecom Data and Infrastructure Security Regulations 2025*. Technical Report. Pakistan Telecommunication Authority. https://www.pta.gov.pk/assets/media/2025-10-29-Critical-Telecom-Data-and-Infrastructure-Security-Regulations-2025.pdf

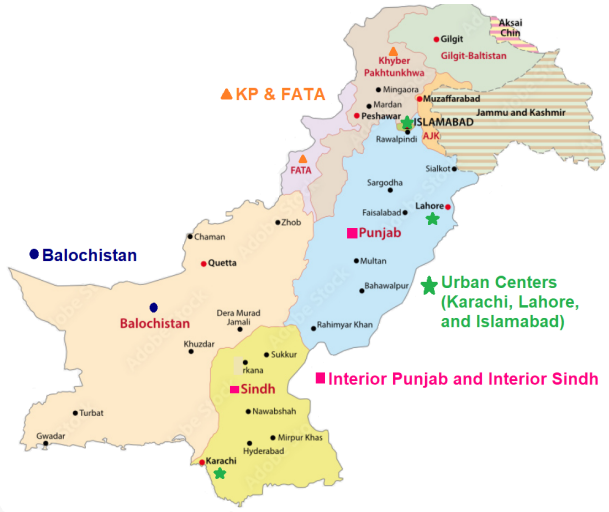



**Figure 6: Pakistan's key regions and urban centers referenced in the threat context [84, 95].**

[84] PakUN. 2026. Political Map of Pakistan. https://pakun.org/pakistan-political-map
[85] Paul Pearce, Ben Jones, Frank Li, Roya Ensafi, Nick Feamster, Nick Weaver, and Vern Paxson. 2017. Global measurement of {DNS} manipulation. In *26th USENIX Security Symposium (USENIX Security 17)*. 307–323.
[86] Ingmar Poese, Steve Uhlig, Mohamed Ali Kaafar, Benoit Donnet, and Bamba Gueye. 2011. IP geolocation databases: Unreliable? *ACM SIGCOMM Computer Communication Review* 41, 2 (2011), 53–56.
[87] Radio Pakistan. 2018. NA passes Constitution (31st Amendment) Bill, 2018 paving way for merger of FATA with KP. https://www.radio.gov.pk/24-05-2018/constitution-amendment-on-fata-aimed-at-bringing-change-in-150-years-old-system-pm
[88] Syed Irfan Raza. 2025. Interior minister forms body to probe SIMs data leak. *DAWN* (2025). https://www.dawn.com/news/1940395.
[89] Abbas Razaghpanah, Rishab Nithyanand, Narseo Vallina-Rodriguez, Srikanth Sundaresan, Mark Allman, Christian Kreibich, and Phillipa Gill. 2018. Apps, Trackers, Privacy, and Regulators: A Global Study of the Mobile Tracking Ecosystem. In *25th Annual Network and Distributed System Security Symposium (NDSS 2018)*. The Internet Society, San Diego, CA, USA. https://doi.org/10.14722/ndss.2018.23353
[90] Jingjing Ren, Ashwin Rao, Martina Lindorfer, Arnaud Legout, and David Choffnes. 2016. ReCon: Revealing and Controlling PII Leaks in Mobile Network Traffic. In *Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services (MobiSys '16)*. ACM, Singapore, 361–374. https://doi.org/10.1145/2906388.2906392
[91] Arshad Sanga. 2026. Punjab Tops List of Threat Cases Against Journalists During March 2026. *Freedom Network Pakistan (FNPK)* (7 April 2026). https://fnpk.org/punjab-tops-list-of-threat-cases-against-journalists-during-march-2026/
[92] Saad Sohail and Kelly Ng. 2024. Imran Khan's arrest left deep wounds still to heal. *BBC News* (2024). https://www.bbc.com/news/articles/cydr0y8yyeeo.
[93] The News International. 2025. Punjab moves sweeping law to monitor habitual offenders, curb anti-social behaviour. https://www.thenews.pk/print/1404294-punjab-moves-sweeping-law-to-monitor-habitual-offenders-curb-anti-social-behaviour.
[94] VOA. 2021. Prominent Pakistan Rights Leader Still In Custody Despite International Criticism. (2021). https://www.voanews.com/a/extremism-watch_prominent-pakistan-rights-leader-still-custody-despite-international-criticism/6184042.html.
[95] World Atlas. 2023. Pakistan Maps & Facts. https://www.worldatlas.com/maps/pakistan

# A GEOGRAPHIC CONTEXT OF PAKISTAN

This appendix provides a geographic reference for the regions discussed in the paper. The map of Pakistan is included to help situate the administrative divisions and major urban centers referenced

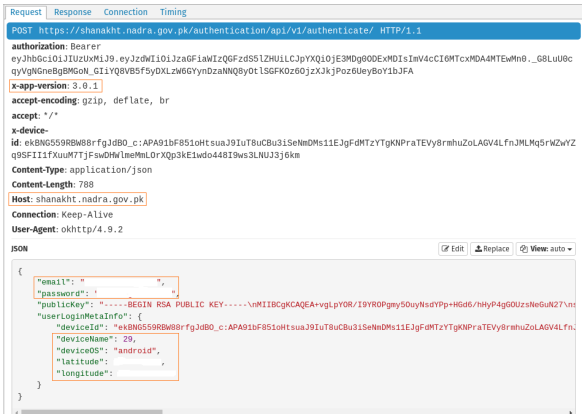



**Figure 7: Pak Identity [28] App: Authentication Request.**

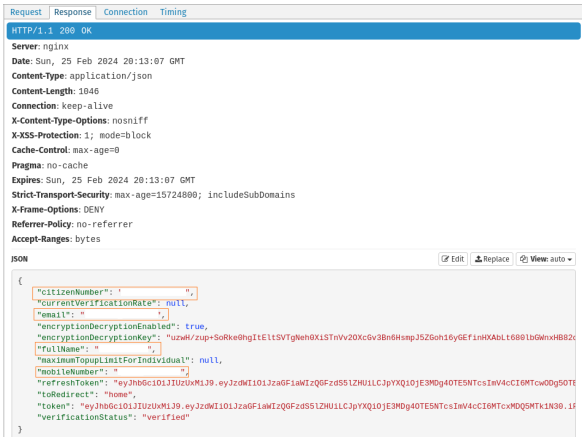



**Figure 8: Pak Identity [28] App: Authentication Response.**

in the analysis. Figure 6 is based on official government boundary data [84, 95].

# B DOMAIN DIRECTORY

Tables 4 and 5 present the domains with which the seven leading Pakistani apps interact. The IP addresses listed alongside each domain correspond to those observed in the MobSF reports; additional IP addresses may be associated with these domains in practice. IP addresses not reported by MobSF are denoted as "Not Listed".

# C FIRST PARTY DOMAINS

Table 6 lists the first-party domains of the seven leading Pakistani apps.

# D DATA CLASSIFICATION CRITERIA

This section defines the criteria we used to classify server-side data exposure. Our framework organizes observed and inferred transmissions by sensitivity and evaluates whether their transmission is functionally required and contextually appropriate.

## D.1 Sensitivity Ordering

We define eight data categories ordered by their potential for identity linkage, re-identification, and downstream harm (see Figure 5).

Authentication credentials and personally identifiable information (PII) constitute the highest-sensitivity tier due to their direct role in identity resolution and account compromise. Sensitive personal attributes (e.g., gender, religion, blood group, nationality) represent legally or socially sensitive information that may enable discriminatory inference or profiling.

Location data is treated as high sensitivity due to its capacity to enable tracking and behavioral inference. Socioeconomic and relational attributes are considered sensitive where they support profiling, targeting, or coercion.

Behavioral data (e.g., call and SMS records) is classified as contextually sensitive, particularly in telecom apps where regulatory obligations may apply. Device identifiers are assigned lower standalone sensitivity but are considered linkage-enabling when combined with higher-sensitivity attributes.

## D.2 Transmission Class Definitions

We define three classes of data transmission based on functional necessity and exposure risk.

*D.2.1 Functionally Expected (●).* This class includes transmissions required for the app's core functionality, where omitting the data would impair or prevent service delivery. Classification is based on functional necessity relative to the app's declared purpose.

For example, My Telenor and My Zong transmit call and SMS records to backend infrastructure as part of telecom service provisioning. Similarly, the transmission of PII for authentication, billing, or account management is considered functionally necessary when directly required for service operation.

*D.2.2 Structurally Risky (★).* This class captures transmissions where the data is either (i) not strictly required for the stated functionality of the app, or (ii) sent to infrastructure whose ownership, jurisdiction, or aggregation context increases exposure risk.

Pak Identity (`shanakht.nadra.gov.pk`) transmits authentication credentials, CNIC information, location data, and additional personal attributes to a centralized government-controlled endpoint. While identity verification may require CNIC transmission, the aggregation of multiple sensitive attributes within a single backend increases exposure and concentration risk.

Pakistan Citizen Portal (`api.pmdu.gov.pk`) transmits attributes such as gender, religion, and blood group, which are not strictly necessary for grievance redressal functionality. Qeemat Punjab (`qpapi.punjab.gov.pk`) transmits precise location data and extended household and socioeconomic attributes (e.g., guardian identity, relationship, and profession), exceeding the minimum functional requirements of a price-information service.

*D.2.3 Non-Essential Non-Sensitive (■).* This class includes low-sensitivity operational signals such as device MAC address, IP address, and operating system version. While not directly identifying in isolation, these attributes may contribute to re-identification or linkage when combined with higher-sensitivity datasets.

**Table 4: Domain Inventory for Major Pakistani Mobile Apps (Part 1).**

| | Domain | IP Address | | Domain | IP Address |
|---|---|---|---|---|---|
| 1. Pak Identity App | | | | | |
| 1. | api.eu.labs.idemia.com | 13.53.153.148 | 2. | www.nadra.gov.pk | 23.62.226.163 |
| 3. | prd.lkms.xantav.com | 18.238.109.25 | 4. | unikrew-faceoff-licensing.azurewebsites.net | 65.52.250.96 |
| 5. | pinterest.com | 151.101.128.84 | 6. | www.shoutcastserver.com | 108.186.91.98 |
| 7. | experience.idemia.com | 18.155.173.86 | 8. | play.google.com | 142.251.116.138 |
| 9. | unikrew-faceoff-telemetry.azurewebsites.net | 65.52.250.96 | 10. | www.google.com | 142.251.186.99 |
| 11. | shanakht.nadra.gov.pk | 199.46.39.31 | 12. | sonarcloud.io | 52.222.169.52 |
| 13. | visa.nadra.gov.pk | 104.22.14.154 | 14. | github.com | 140.82.113.3 |
| 15. | www.facebook.com | 57.144.134.1 | 16. | zoom.net | Not Listed |
| 17. | plus.google.com | 142.251.186.102 | 18. | licensing.prod.veridium-dev.com | 3.64.32.202 |
| 19. | nrclocator.nadra.gov.pk | 23.62.226.171 | 20. | maps.google.com | 142.250.113.101 |
| 21. | www.zetetic.net | 18.238.96.105 | 22. | www.smpte-ra.org | 52.20.185.129 |
| 23. | www.server.com | 172.67.196.208 | 24. | twitter.com | 104.244.42.193 |
| 25. | api.us.labs.idemia.com | 13.49.114.57 | 26. | www.w3.org | 104.18.22.19 |
| 2. Pakistan Citizen Portal App | | | | | |
| 1. | www.googleapis.com | 142.250.114.95 | 2. | api.pmdu.gov.pk | 203.101.184.112 |
| 3. | schemas.android.com | Not Listed | 4. | upload.ffmpeg.org | 213.36.253.119 |
| 5. | pagead2.googlesyndication.com | 142.250.114.156 | 6. | play.google.com | 142.251.116.138 |
| 7. | f-droid.org | 37.218.243.72 | 8. | github.com | 140.82.113.4 |
| 9. | www.facebook.com | 57.144.134.1 | 10. | mobile.events.data.microsoft.com | 52.182.143.213 |
| 11. | cdn.pmdu.gov.pk | 202.83.164.226 | 12. | app-measurement.com | 142.250.115.139 |
| 13. | web.citizenportal.gov.pk | 202.83.164.211 | 14. | plus.google.com | 142.251.186.100 |
| 15. | www.instagram.com | 57.144.134.34 | 16. | pmdu.pmo.gov.pk | Not Listed |
| 17. | www.openssl.org | 34.49.79.89 | 18. | in.appcenter.ms | 4.152.45.255 |
| 19. | citizenportalpk-4e813.firebaseio.com | 34.120.206.254 | 20. | www.amazon.com | 23.194.102.89 |
| 21. | twitter.com | 104.244.42.193 | | | |
| 3. Qeemat Punjab App | | | | | |
| 1. | qpapi.punjab.gov.pk | 103.226.217.186 | 2. | rasta.punjab.gov.pk | 103.111.161.144 |
| 3. | android.bugly.qq.com | 14.22.7.199 | 4. | api.onesignal.com | 104.16.160.145 |
| 5. | pinkribbon.org.pk | 82.180.142.168 | 6. | 103.226.216.242 | 103.226.216.242 |
| 7. | rqd.uu.qq.com | 43.135.106.42 | 8. | schemas.android.com | Not Listed |
| 9. | efenergy.punjab.gov.pk | 103.226.216.162 | 10. | maps.google.com | 142.250.113.100 |
| 11. | plus.google.com | 142.251.186.139 | | | |
| 4. SIMOSA App | | | | | |
| 1. | apps.jazz.com.pk | 119.73.65.137 | 2. | xml.org | 104.239.240.11 |
| 3. | www.youtube.com | 142.251.116.93 | 4. | ktor.io | 13.224.53.110 |
| 5. | myjazz-b2c.firebaseio.com | 35.190.39.113 | 6. | play.google.com | 142.251.116.102 |
| 7. | cdnjs.cloudflare.com | 104.17.24.14 | 8. | jazzapp.page.link | 142.251.186.132 |
| 9. | jazzgames.hub.gamepix.com | 18.238.96.123 | 10. | github.com | 140.82.114.3 |
| 11. | www.facebook.com | 57.144.134.1 | 12. | usrpic.jazz.com.pk | Not Listed |
| 13. | selfcare-msa-prod.jazz.com.pk | 119.73.65.219 | 14. | business-api.tiktok.com | 23.47.52.132 |
| 15. | business-api.tiktok.com | 23.47.52.132 | 16. | api.ipify.org | 104.26.13.205 |
| 17. | www.instagram.com | 57.144.134.34 | 18. | selfcare-cms-prod.jazz.com.pk | 119.73.65.225 |
| 19. | jazzselfcare.page.link | 142.251.116.132 | 20. | socialplus.jazztv.pk | 43.163.57.158 |
| 21. | sync.jazzdsp.com | 119.160.110.35 | 22. | api.mixpanel.com | 130.211.34.183 |
| 23. | fonts.googleapis.com | 142.251.186.95 | 24. | xmlpull.org | 185.199.110.153 |
| 25. | selfcare.jazz.com.pk | 119.73.65.136 | 26. | bajaoapp.page.link | 142.251.116.132 |

**Table 5: Domain Inventory for Major Pakistani Mobile Apps (Part 2).**

| | | | | | |
|---|---|---|---|---|---|
| 27. | www.jazz.com.pk | 54.167.163.183 | 28. | twitter.com | 104.244.42.129 |
| 29. | www.w3.org | 104.18.22.19 | 30. | www.slf4j.org | 195.15.222.169 |
| 5. My Zong App | | | | | |
| 1. | docs.pushwoosh.com | 18.238.96.62 | 2. | www.zong.com.pk | 104.22.70.205 |
| 3. | myzong-bf055.firebaseio.com | 35.201.97.85 | 4. | myzongapp-nlbt.zong.com.pk | 209.150.154.153 |
| 5. | .facebook.com | Not Listed | 6. | graph.s | Not Listed |
| 7. | schemas.android.com | Not Listed | 8. | cp.pushwoosh.com | 46.4.253.88 |
| 9. | goo.gl | 142.250.114.139 | 10. | apimegw.zong.com.pk | 111.119.186.74 |
| 11. | issuetracker.google.com | 142.250.113.102 | 12. | facebook.com | 57.144.134.1 |
| 13. | s.api.pushwoosh.com | 135.181.230.81 | 14. | api.rollbar.com | 35.201.81.77 |
| 15. | ns.adobe.com | Not Listed | 16. | business-api.tiktok.com | 23.47.52.146 |
| 17. | graph-video.s | Not Listed | | | |
| 6. My Telenor App | | | | | |
| 1. | developers.facebook.com | 57.144.134.141 | 2. | youtrack.jetbrains.com | 63.33.88.220 |
| 3. | d1gsed78v7koll.cloudfront.net | 18.238.102.158 | 4. | mobileanalytics.useinsider.com | Not Listed |
| 5. | xenon-66b61.firebaseio.com | 35.190.39.113 | 6. | android.googlesource.com | 142.250.114.82 |
| 7. | theomancy.app.telenor.com.pk | 37.111.152.93 | 8. | www.youtube.com | 142.251.116.93 |
| 9. | facebook.com | 57.144.134.1 | 10. | ns.adobe.com | Not Listed |
| 11. | schemas.android.com | Not Listed | 12. | vidly.tv | 195.201.181.152 |
| 13. | play.google.com | 142.251.116.102 | 14. | gw-asargon.kryptons.com.pk | 104.18.0.55 |
| 15. | telenor.page.link | 142.251.186.132 | 16. | .facebook.com | Not Listed |
| 17. | github.com | 140.82.113.4 | 18. | issuetracker.google.com | 142.251.116.139 |
| 19. | mobile.useinsider.com | 162.159.134.61 | 20. | goo.gle | 67.199.248.12 |
| 21. | business-api.tiktok.com | 23.66.3.70 | 22. | hsargon.kryptons.com.pk | 54.251.71.119 |
| 23. | tpchat.mindbridge.co | 116.71.133.253 | 24. | graph.s | Not Listed |
| 25. | commons.apache.org | 151.101.2.132 | 26. | easypay.easypaisa.com.pk | 103.150.82.5 |
| 27. | xepro-sports.telenor.com.pk | Not Listed | 28. | graph-video.s | Not Listed |
| 29. | api.mixpanel.com | 107.178.240.159 | 30. | www.telenor.com.pk | 104.18.12.112 |
| 31. | goonj.tv | 35.177.22.210 | | | |
| 7. UPTCL App | | | | | |
| 1. | accounts.google.com | 142.251.116.84 | 2. | developers.facebook.com | 57.144.134.141 |
| 3. | console.firebase.google.com | 142.251.116.100 | 4. | mua.cricwick.net | Not Listed |
| 5. | webview.golootlo.pk | 18.238.109.88 | 6. | xml.org | 104.239.240.11 |
| 7. | google.com | 142.251.116.100 | 8. | facebook.com | 57.144.134.1 |
| 9. | ns.adobe.com | Not Listed | 10. | schemas.android.com | Not Listed |
| 11. | media-route-prd-superapp.apps.ocp-isb-prod.ptclgroup.com | 202.125.152.128 | 12. | play.google.com | 142.251.116.102 |
| 13. | myufone-4404b.firebaseio.com | 35.190.39.113 | 14. | pagead2.googlesyndication.com | 142.250.113.154 |
| 15. | webchat01.ufone.com | 203.135.2.43 | 16. | www.google.com | 142.251.186.103 |
| 17. | firebaseremoteconfigrealtime.googleapis.com | 142.250.115.95 | 18. | firebase.google.com | 142.250.115.101 |
| 19. | .facebook.com | Not Listed | 20. | github.com | 140.82.113.3 |
| 21. | www.googleadservices.com | 142.251.116.155 | 22. | issuetracker.google.com | 142.250.113.138 |
| 23. | goo.gle | 67.199.248.13 | 24. | business-api.tiktok.com | 23.66.3.68 |
| 25. | webchat02.ufone.com | 203.135.2.43 | 26. | app-measurement.com | 142.250.115.100 |
| 27. | graph.s | Not Listed | 28. | firebase-settings.crashlytics.com | 142.251.186.94 |
| 29. | chatbot.ptcl.com.pk | 221.120.226.12 | 30. | developer.android.com | 142.251.116.139 |
| 31. | graph-video.s | Not Listed | 32. | xmlpull.org | 185.199.109.153 |
| 33. | firebaseinstallations.googleapis.com | 142.251.186.95 | 34. | goo.gl | 142.250.114.139 |
| 35. | www.w3.org | 104.18.23.19 | 36. | api.whatsapp.com | 57.144.135.32 |
| 37. | www.slf4j.org | 195.15.222.169 | | | |

**Table 6: First-Party (F) Domains, Their Associations, and Intended Purposes.**

| | Intended Purpose | Association | Domains (≈ 40) |
|---|---|---|---|
| 1. Pak Identity App | | | |
| 1. | Identity Control, E-Governance. | National Database & Registration Authority (NADRA) [16] | (i) www.nadra.gov.pk; (ii) shanakht.nadra.gov.pk; (iii) visa.nadra.gov.pk; (iv) nrclocator.nadra.gov.pk; |
| 2. Pakistan Citizen Portal App | | | |
| 2. | Complaint and Grievance Redressal. | Prime Minister's Performance Delivery Unit (PMDU) [23] | (i) api.pmdu.gov.pk; (ii) cdn.pmdu.gov.pk; (iii) web.citizenportal.gov.pk; (iv) pmdu.pmo.gov.pk; (v) citizenportalpk-4e813.firebaseio.com; |
| 3. Qeemat Punjab App | | | |
| 3. | Agricultural Product Price Control. | Government of Punjab, Pakistan | (i) qpapi.punjab.gov.pk; (ii) rasta.punjab.gov.pk; (iii) efenergy.punjab.gov.pk; (iv) pinkribbon.org.pk; |
| 4. SIMOSA App | | | |
| 4. | Mobile Network Services and Customer Engagement | Jazz (Formerly Mobilink) | (i) apps.jazz.com.pk; (ii) myjazz-b2c.firebaseio.com; (iii) jazzapp.page.link; (iv) jazzgames.hub.gamepix.com; (v) usrpic.jazz.com.pk; (vi) selfcare-msa-prod.jazz.com.pk; (vii) selfcare-cms-prod.jazz.com.pk; (viii) jazzselfcare.page.link; (ix) socialplus.jazztv.pk; (x) sync.jazzdsp.com; (xi) selfcare.jazz.com.pk; (xii) www.jazz.com.pk; |
| 5. My Zong App | | | |
| 5. | Telecom Solutions & User Interaction | Zong (CMPak) | (i) www.zong.com.pk; (ii) myzong-bf055.firebaseio.com; (iii) myzongapp-nlbt.zong.com.pk; (iv) apimegw.zong.com.pk; |
| 6. My Telenor App | | | |
| 6. | Telecom Solutions & User Connectivity | Telenor | (i) theomancy.app.telenor.com.pk; (ii) telenor.page.link; (iii) easypay.easypaisa.com.pk; (iv) xepro-sports.telenor.com.pk; (v) www.telenor.com.pk; |
| 7. UPTCL App | | | |
| 7. | Wireless Solutions & User Interaction. | Ufone and Pakistan Telecommunication Company Limited (PTCL) | (i) webview.lootlo.pk; (ii) media-route-prd-superapp.apps.ocp-isb-prod.ptclgroup.com; (iii) myufone-4404b.firebaseio.com; (iv) webchat01.ufone.com; (v) webchat02.ufone.com; (vi) chatbot.ptcl.com.pk; |

### D.3 Inferred Data

Dotted markers indicate data categories inferred as likely transmitted based on app behavior, UI flows, or traffic patterns, but not directly confirmed through decrypted payload inspection. This applies to UPTCL and SIMOSA, where full traffic visibility was not achieved.

### D.4 Adjudication of Ambiguous Cases

Ambiguous classifications were independently reviewed by three researchers. Decisions were based on each app's declared functionality (as stated in Play Store descriptions and privacy policies) and observed network behavior.

Disagreements were resolved through consensus. The guiding criterion was whether the transmission is reasonably expected given the app's stated purpose, and whether the receiving infrastructure introduces additional exposure risk beyond functional necessity.

## E PAK IDENTITY APP

This subsection presents representative snapshots of the test results for the Pak Identity app. User credentials of interest are highlighted with orange rectangles in all figures. Sensitive credentials, including the *citizen number*, *mobile number*, and *password*, have been redacted because they appear in plaintext. Figure 7 shows the client's authentication request to the server, with the plaintext *password* redacted. Figure 8 shows the server's response, with the plaintext *citizen number* and *mobile number* redacted.

## F PAKISTAN CITIZEN PORTAL APP

This subsection presents representative snapshots of the test results for the Pakistan Citizen Portal app. Figure 9 shows the device credentials transmitted to the api.pmdu.gov.pk server during login. Figure 10 and Figure 11 show sensitive user credentials returned in the server's response. User credentials have been redacted because they appear in plaintext. Figures 12a and 12b show the PII, including location coordinates, transmitted when a user submits a suggestion or complaint.

## G QEEMAT PUNJAB APP

This subsection presents representative results for the Qeemat Punjab app [30]. Figure 13 shows that the app transmits PII, including gender, guardian name, physical address, and national identity number, to its backend server at qpapi.punjab.gov.pk. Figure 14

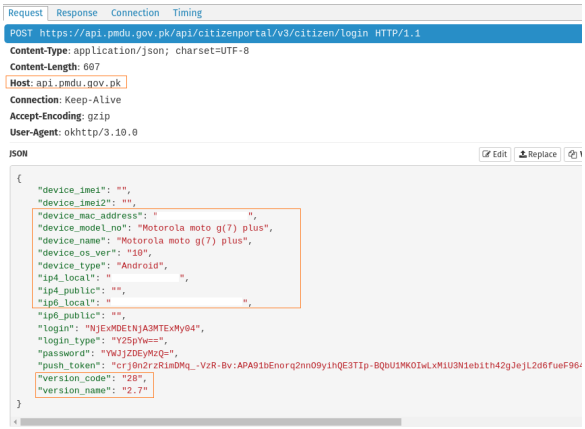



**Figure 9: Pakistan Citizen Portal [29] App: Authentication Request.**

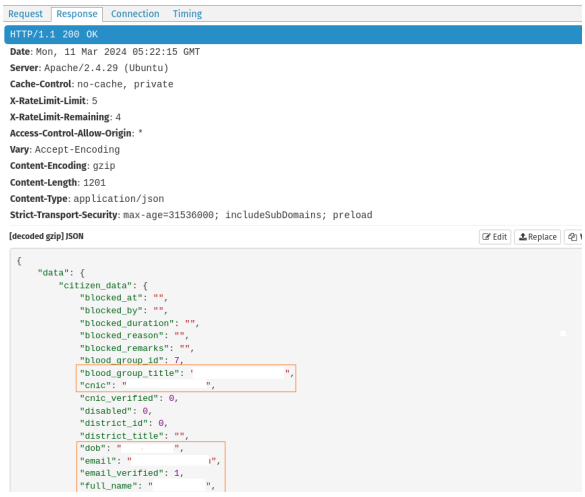



**Figure 10: Pakistan Citizen Portal [29] App: Authentication Reply.**

shows that the app also transmits users' precise location coordinates when they submit a suggestion or complaint.

## H MY ZONG APP

Figure 16 shows that the app transmits an at-risk user's mobile number to its backend server at `myyzongapp-nlbt.zong.com.pk` as part of a request to retrieve the user's call history. Figure 15 shows the server's response, which includes detailed call records containing contacted mobile numbers and the date, time, and duration of each call.

## I MY TELENOR APP

Figure 17 shows that an at-risk user's mobile number is transmitted in the app's network traffic to the backend server at `theomancy.app.telenor.com.pk`. Figures 18 and 19 show the

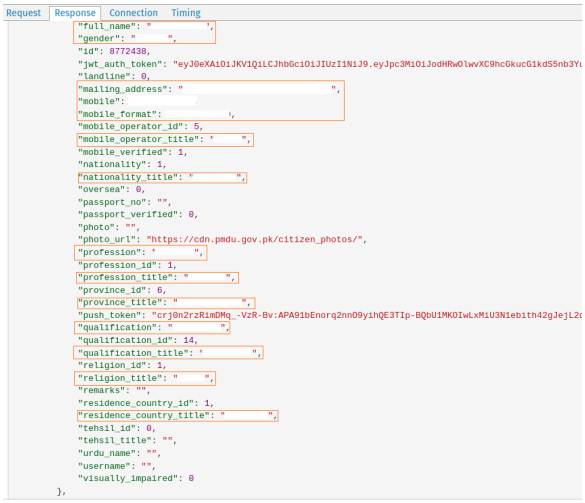
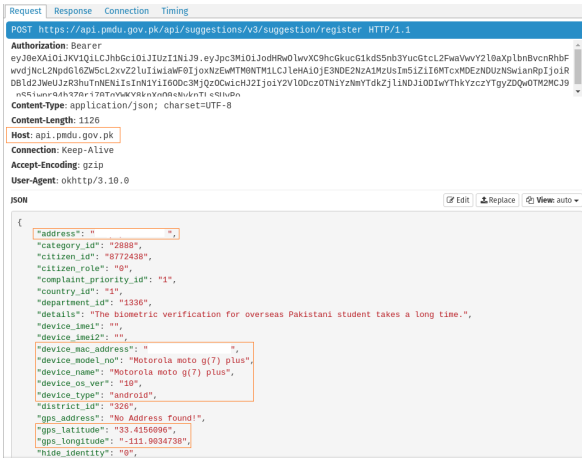



**Figure 11: Pakistan Citizen Portal [29] App: Authentication Reply (Continued).**




**(a) Complaint Submission with PII.**


**(b) Complaint Submission with PII (continued).**

**Figure 12: Pakistan Citizen Portal [29] App: Complaint Submission with PII.**

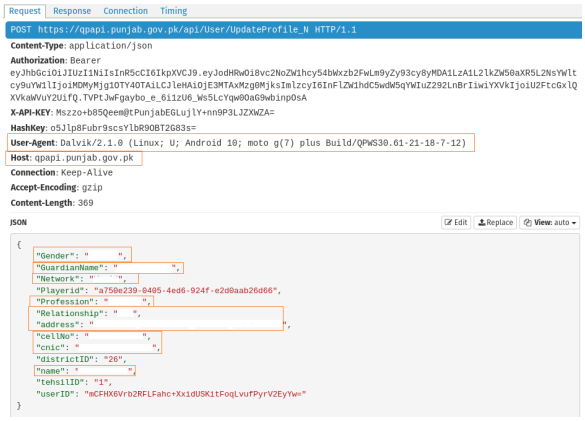



**Figure 13: PII Collection for the Qeemat Punjab App [30].**


**Figure 14: Location Data Collection in Qeemat Punjab App [30].**

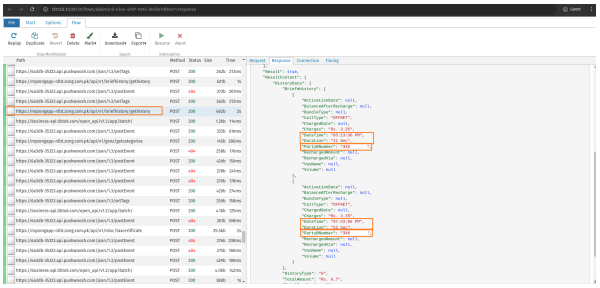


**Figure 15: Call/SMS Records for the My Zong App [27].**

user's call and SMS history, including contacted mobile numbers and timestamps.

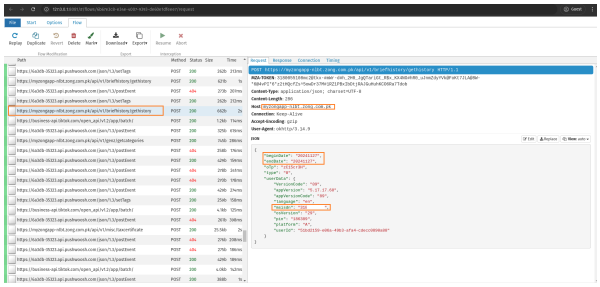


**Figure 16: Mobile Number Visibility in the My Zong App [27].**

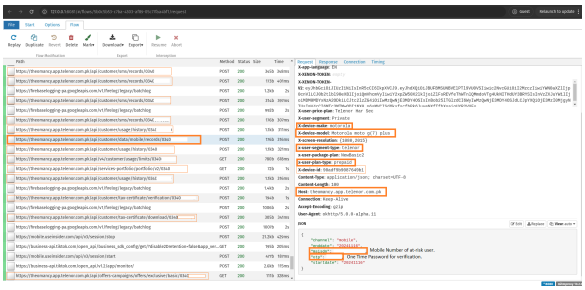


**Figure 17: Mobile Number Visibility in My Telenor App [26].**

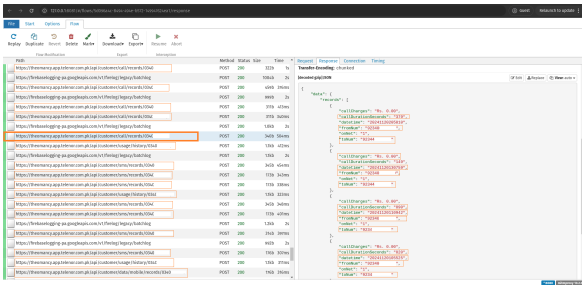


**Figure 18: Call Records for the My Telenor App [26].**

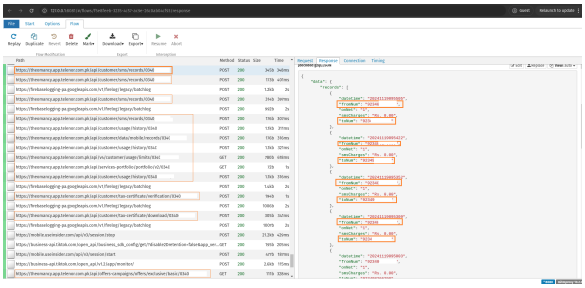


**Figure 19: SMS Records for the My Telenor App [26].**